THE EXPRESS GROUP

COMPUTER RESELLER NEWS crn.in

CRN India

NEWS, ANALYSIS AND PERSPECTIVE FOR TECHNOLOGY INTEGRATORS

MAY 2018, VOL.1 NO.2 PAGES 48 , ₹75

CHANNEL DIRECTIONS 2018
16 - 17 MARCH | NOVOTEL, HYDERABAD

+

Special Focus

Fortinet expects significant growth from MSSP Partners

Launchpad

Kaspersky Threat Management & Defense

WHY ENTERPRISE SECURITY IS A GOLDMINE FOR CHANNEL PARTNERS

As the pace of digitization accelerates, Indian enterprises are now increasingly being exposed to global threat vectors. This has increased the opportunity for specialized solution partners

7 REASONS WHY CRN OFFERS YOU THE BEST ROI ON YOUR MARKETING SPENDS IN 2018

1

CRN has been the voice of the channel for over two decades. Reintroduced this March in a fresh information-rich 14 Section Editorial format, the magazine offers detailed research, management strategies, channel analysis and the latest technology news. Making it the go-to 'must-read and must-advertised' in monthly print resource and reference tool for guiding successful partnerships. The magazine is also supported by several Print-Plus initiatives which would be of interested all our advertisers.

2

As part of the magazine relaunch, we are offering an early bird offer to advertisers who book space before March 31, 2018

Size of Ad	No of Insertions	Free Insertions	Duration
Full Page (A4)	3	1	Quarter
Full Page (A4)	6	2	6 Issues
Full Page (A4)	9	3	1 year
*cost per insertion: Rs. 75,000			

3 EVENT TIE-INS

Given our extensive experience in events and a dedicated in-house team, we offer our Partners a choice of events:

- **CRN Channel Leadership Summit**
- **CRN Channel Directions**
- **Customised Events**

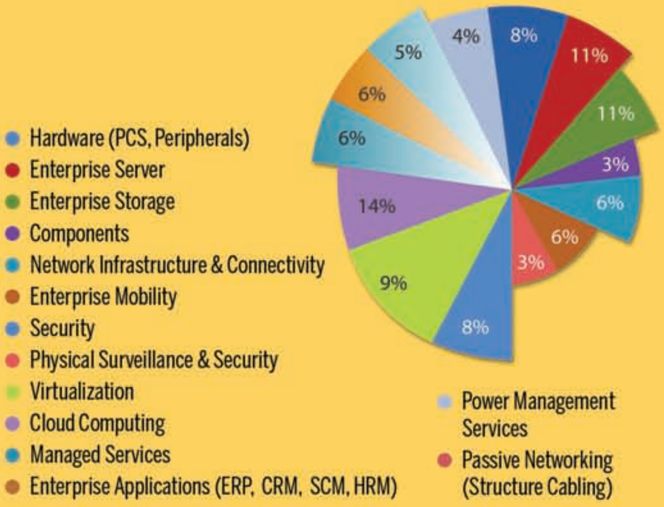
4 AUDIENCE DEMOGRAPHICS

INDUSTRY VERTICALS - 80% System Integrators target industry like Government, BFSI, Healthcare, Telecom, Infrastructure, Manufacturing & Hospitality

BFSI
IT/ITES
TELECOMMUNICATION
PHARMA/HEALTHCARE
MANUFACTURING
SOHO
HOSPITALITY
LOGISTICS
INFRASTRUCTURE
RETAIL
GOVERNMENT
FMCG EDUCATION
AUTO & AUTO ANCILLARY

KEY PRODUCTS AND SERVICES

Nearly 70% specialize in emerging technologies like Cloud Computing, Virtualization, Managed Services etc.



5 DIGITAL

We offer you a comprehensive four-point digital offering that covers:

- **Branding (Banner Ads, Video Ads)**
- **Information (blogs, digital books, case study/white paper)**
- **Engagement (partner microsites, dedicated emailers)**
- **Conversations (social media engagement, podcasts, online surveys)**

6 KNOWLEDGE INITIATIVES

Given both our global insights and an in-depth knowledge of the Indian market, we offer our Partners Customised publications that include:

- **ebooks**
- **Coffee table books**
- **Article series,**
- **Interviews,**
- **Panel discussions,**
- **Videos,**
- **Research Papers**

7 COMPLETE PEACE OF MIND

Knowing that this offer is brought to you by **CRN**, which is now part of **The Indian Express Pvt. Ltd.** one of India's largest and most respected media conglomerates which also publishes Express Computer and organises Marquee Events in the B2B space including Technology Sabha, Technology Senate, and BFSI Technology Conclave.

For more information and marketing initiatives, please contact Ravi Nair at 98209 55602 and ravindranath.nair@expressindia.com

Vol 1. No. 2. May, 2018

Chairman of the Board
Viveck Goenka

Sr Vice President - BPD
Neil Viegas

Editor
Srikanth RP*

Delhi
Mohd Ujaley,
Sandhya Michu

Mumbai
Nivedan Prakash,
Abhishek Raval,
Mohit Rathod

Bengaluru
Rachana Jha

DESIGN
National Design Editor
Bivash Barua

Asst. Art Director
Pravin Temble

Chief Designer
Prasad Tate

Senior Graphic Designer
Rekha Bisht

DIGITALTEAM
Head of Internet
Viraj Mehta

Web Developer
Dhaval Das

Layout
Vinayak Mestry

Photo Editor
Sandeep Patil

MARKETING
National Head
Harit Mohanty

Regional Heads
Ravi Nair - West
Prabhas Jha - North
Durga Prasad - South
Debnarayan Dutta - East

Marketing Team
Shankar Adaviyar,
Ajanta Sengupta
Navneet Negi
Aparna Tawde

Circulation
Mohan Varadkar

Scheduling
Santosh Lokare

PRODUCTION
General Manager
B R Tipnis

Manager
Bhadresh Valia

ENTERPRISE SECURITY: A BIG PROFITABLE OPPORTUNITY

Nivedan Prakash
nivedan.prakash@expressindia.com

The significance of enterprise security has increased multi-fold in the recent times due to proliferation of cybercrime, information being more distributed, and legislations becoming more stringent. The business impact of security incidents and an evolving regulatory landscape have taken Board level cognizance and this is where we are seeing continued end user spending for security products and services.

However, increasing cost, complexity of IT, and the changing threat landscape has made it difficult for organisations to manage security considerations on their own. This is where managed security services have gained momentum, which co-incidentally, has also become a key thrust area for traditional partners as well. Convergence of factors such as skills shortages, evolving and increasing threat landscape, and compliance challenges is leading organizations to seek help from MSSPs.

The evolution of advanced threats continues to cause greater operational pressure on organisations, driving them to look at MSSPs to reduce the pressure and better security threat management. Looking at this trend and also to ensure the partners deliver the best value, security, and service to the end customers, most of the IT security vendors have designed a robust, customer-focused MSSP program from the ground up.

The industry is also witnessing growth in cloud-based security services, which is being driven by both large and SMB segments. The primary reason is that enterprises realize the operational benefits derived from a cloud-based security delivery model. The enterprises with an installed security infrastructure have come to a realization that they do want to explore the Opex model. And even those customers, who are yet to take a decision on their security spend, are exploring this model.

From the security vendors' perspective, they are making increased investments in their partners such as providing them with additional tools and resources to succeed in the competitive market. This allows the channel partners to be updated with the latest technical knowledge, enabling them to differentiate themselves, and leading to new business opportunities.

IMPORTANT

Whilst care is taken prior to acceptance of advertising copy, it is not possible to verify its contents. The Indian Express (P) Ltd. cannot be held responsible for such contents, nor for any loss or damages incurred as a result of transactions with companies, associations or individuals advertising in its newspapers or publications. We therefore recommend that readers make necessary inquiries before sending any monies or entering into any agreements with advertisers or otherwise acting on an advertisement in any manner whatsoever.

Computer Reseller News®
RNI Title code NO. MAHENG/14221 .

Printed and Published by Vaidehi Thakar on behalf of The Indian Express (P) Limited and Printed at Indigo Press (India) Pvt.Ltd., Plot No.1C/716, Off. Dadoji Konddeo Cross Road, Byculla (East), Mumbai 400027 and Published at 1st floor, Express Towers, Nariman Point, Mumbai 400021. Editor: Srikanth RP *
* Responsible for selection of news under the PRB Act. (Editorial & Administrative Offices: Express Towers, 1st floor, Nariman Point, Mumbai 400021)

CONTENT

CHANNEL DIRECTIONS 2018
16 - 17 MARCH | NOVOTEL, HYDERABAD

Special Focus

Channel Chief

Channel Chief

CXO Speak

CISO Corner

Partner Corner

Launchpad

Wall Colors and Flooring
Building Costs

Polycom

WHY ENTERPRISE SECURITY IS A GOLDMINE FOR CHANNEL PARTNERS

As the pace of digitization accelerates, Indian enterprises are now increasingly being exposed to global threat vectors. This has increased the opportunity for specialized solution partners.

■ Sandhya Michu

With a fast rising digital economy, India today is witnessing sophisticated attacks from organized players. Attacks are becoming more targeted and are increasingly resulting in high-value data breaches. Not surprisingly, India today ranks among the top five countries at risk for cyber attacks. India also is among the top five countries in the world for countries that are affected by ransomware. With a growing number of devices connected to the Internet, a number of organizations in India are facing challenges of ensuring security for connected devices.

Increasing pace of cyber attacks and the inability to keep systems updated and patched, coupled with lack of internal talent, has opened up huge number of opportunities for specialised solution partners. Additionally, smartphone penetration and an exponential rise in IoT devices are leading to newer attack surfaces. As the sophistication of cyber attacks increase, solution partners are finding increasing business opportunities for relatively new services such as managed security services and patch management.

Moving from selling antivirus to security solutions

With plain vanilla security products such as antivirus and firewalls becoming a commodity, solution partners are shifting gears, and are looking at niche solutions that command higher margins. A case in point is Pyramid Cyber Security and Forensic, which offers security as a service, compliance related services and forensics. Sharing his view on the immense potential of this business, Alok Gupta, CEO of Pyramid Cyber Security and Forensic, says, "Compliance in security-as-a-service is turning to be a high profitability business for partners. Being a niche player in forensics, we command a premium as high as 30% in most of the cases. I think there's a lot of money to be made in adding security services to the offerings of MSPs which can translate into margins of 20% or much more. In addition to the margin on reselling services, MSPs should look to take over their clients' needs for compliance services, implementation of security policies and procedures, and documenting of those policies and procedures for maintaining this profitability."

With cyber attacks hitting even small and medium businesses, the need for cyber security specialists who have the requisite skill sets have accelerated. Agrees Biswajeet Saha, CEO, SEA Infonet, a value-added security products distributor, "We see immense growth in the cybersecurity landscape arising from the increase in threat patterns and also the increase in mobile devices and cloud computing. Additionally, technologies like anti-APT and EDR has opened up the perception of cybersecurity needs among SMBs and enterprises."

"If there's one lesson to learn from cybercriminals, it is the collaboration and practice sharing. Knowledge is power, as we know, and so keeping a breach secret only helps the attackers – if an exploit isn't made public, it can be used on the next company and the next. In order to stop it, free sharing of information among business and enterprise, cybersecurity professionals, and security software vendors is essential," states Raunaq Singh, SVP, Targus Technologies, a Gurgaon-based solution provider.

> "IT IS CLEAR THAT MONITORING CLOUD ASSETS AND INFRASTRUCTURE WILL CONTINUE TO BE A CHALLENGE AND THAT'S WHERE THE OPPORTUNITIES ARE. EVEN SMALLER COMPANIES ARE LOOKING TOWARDS HAVING A SHARED CISO."
>
> **Atul Ahuja**
> Vice President, Softline Asia

Cloud security is a big bet

Cloud-based security is making a huge impression on the channel. As more security solutions move to the cloud, partners are facing a changing market that often requires them to link up with cloud providers and IT security vendors to broaden the suite of products they offer to customers.

"Organisations continue to adopt cloud technologies at a rapid rate, but information security is not picking up that pace. It is clear that monitoring cloud assets and infrastructure will continue to be a challenge and that's where the opportunities are. Even smaller companies are looking towards having a shared CISO. It is all about getting the best and also cutting CAPEX at the same time," says Atul Ahuja, Vice President, Softline Asia.

SERVICES GIVEN BY CHANNEL PARTNERS

- Monitoring deployment of security policies, periodic system health checks, sharing do's and dont's on a regular basis and during targeted malware attacks, etc
- Updating inputs given by the respective Security OEM on a constant basis and making the customer to do the patch updation immediately
- Identifying the breach/threat (What is going to has gone out, what kind of attack is happening)
- Containment (Work on how to stop the further damage)
- Eradicate the Threat (Stop the outflow of traffic from particular port or application etc, remove malware)
- Recovery (Steps to bring the system to a healthy state as before)
- Evaluate and Lessons (this is done for the future readiness)
- Developing cybersecurity framework that is a blend of known industry regulations and collective experience over the years

Increasing complexity of security solutions, lack of in-house expertise and budget constraints is pushing the demand for Managed Security Services, which has now become the most attractive segment both by size and growth. It is expected to be close to 55% of the overall cybersecurity services market by 2025 and is expected to grow at a healthy CAGR of approximately 12%.

Giving a fresh perspective, Krishnaraj Sharma, director, and CEO, iValue Infosolution, says, "Security is not just about technology but a collaborative approach of threat intelligence, prevention technologies, detection technologies, associated services in a collaborative model sharing knowledge and expertise across all players. Hence,

ACPL UNLOCKS CYBERSECURITY OPPORTUNITIES FOR THE DIGITAL ECONOMY

A two-decade-old technology firm, ACPL, has been an established specialist in Information Security partner from Delhi. The company has been strengthening its foothold in the information security space and strongly believes that network security will play a major role in Internet-driven connectivity world more than ever before.

Banking high on the early days of building cybersecurity Infrastructure, IT companies have made a robust transition to digital. This needs the cybersecurity at all level - infra, application and end consumer levels. Privacy and compliance is another one which is driving need of cyber security.

“A lot of focus on enhancing the data breach prevention, ransomware is pushing enterprises to boost their protection capabilities. Despite these opportunities, finding the talent is a big challenge, “There are very few people being chased by lot many. Even procurement of specialized tools is being bought on L1 cost, there is a need for a specialist who can address the pain areas of CIOs and CISOs,” Bindra opines.

ACPL has been a front-runner in offering its services to leading electrical and electronics manufacturer, insurance and mobile and payment wallet firms.

In last three years, ACPL has built on new capabilities to meet the security needs. Security Audit capability has been with ACPL for a long time. Now, the company is looking at Machine learning and artificial intelligence in a big way. "We have adopted both of these in our own developed technologies like Klassify and ACRS. But this is a very vast area, we will continue to invest more and more in this. Along with this area, we are investing heavily in automation and orchestration," says Bindra.

Moving forward, the company is investing in the cloud, IoT, and critical infrastructure. The company has invested heavily in manpower in these areas and have invested in the full-fledged lab and are working hands-on and developing use cases for the security. Moreover, it is developing own IP to unlock new opportunities.

> “SECURITY-AS-A-SERVICE IS MORE LUCRATIVE THAN TRADITIONAL HARDWARE SUPPORT SERVICES. THIS IS BECAUSE A CUSTOMER IS NOT OUTSOURCING TO REDUCE COST BUT TO IMPROVE EFFICIENCY”
>
> **Vishal Bindra,**
> CEO, ACPL Systems

security needs to be viewed from a holistic and business risk perspective and not from a product/service or technology view.”

Asserting his views, Vishal Bindra, CEO, ACPL System says, “Security-as-a-Service is more lucrative than traditional hardware support services. This is because a customer is not outsourcing to reduce cost but to improve efficiency. In this scenario, any solution partner who can showcase the effectiveness, competence, better TCO and maturity in processes bundled with certified manpower will get the mandate.”

Meeting the customer's need

Customer networks are rapidly evolving to keep pace with new innovations and consumer demands. So is the role of security providers. Digital transformation enables digitisation of all customer-centric services which effectively asks for most of the application to come towards the edge of the network. It’s a huge opportunity for all security partners to work on building products and services around application performance, application availability, and application protection. More and more consumer-centric approach in the business gives larger opportunity in areas of end-point protection and mobility management.

Therefore, network security players can forecast huge business growth and prospects in the enterprise security space in India in the coming years. But are they equipped to embark on this journey? Opines Vishal Bindra, “Large enterprise customers are investing heavily in securing digital assets. Customers are investing in secured user experiences. We are working with them to provide strong and robust security architecture and secured application view so that they have an integrated security overview and not an overlay.”

This trend is now extending to SME customers too. States NKR Venkat, Director-Sales, Digital Track, “Today, every enterprise — from the SOHO to the large enterprise are giving importance to cybersecurity. SOHO and SME organisations have traditionally restricted their security investment to A/V and UTM solutions, whereas midsize and large enterprises are trying to have a whole gamut of security solutions, like UTM, A/V, Anti-malware protection, dedicated IPS, DLP, IRM solutions, encryption, SSL-VPN, etc. to ensure that they are highly protected.”

Preparing for next decade opportunities

For security solution providers, it is important to stay ahead of the threat. Many solution partners are conducting comprehensive security audits to assess the current threat scenarios and take IT initiatives for the next 3 to 5 years along with compliance needs to arrive at a road map of hardware, software and service needs in a phased manner. Security providers are also investing in skilled resources to use the SDKs provided by OEMs and build their own layer of security on top so that they can use their own IP and create their own unique niche in the market.

A case in point is Targus Technologies. "With Artificial Intelligence, IoT, Business Analytics, and Robotics taking centre stage in the next decade, it is imperative that we give security the attention that is required to make businesses safe. Targus plans to work closely with its OEMs (such as Juniper, Fortinet, etc.) to provide high levels of hardware and advanced threat protection. We intend to secure all seven layers of our customers' network and business," informs Singh.

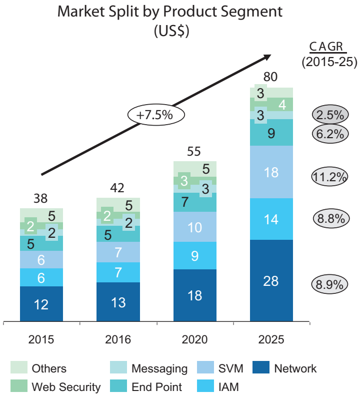
Similarly, Softline is looking at an integrated security solutions approach for on-premise and cloud infrastructure deployments. Softline India has a dedicated CoE for security offerings and has an on-going program with Barracuda to skill its consultants and solution architects.

Audit and Compliance are basic needs of customers around security which is driven by governance, risk, and compliance (GRC framework). Using their expertise, channel partners are looking at compliance as an opportunity.

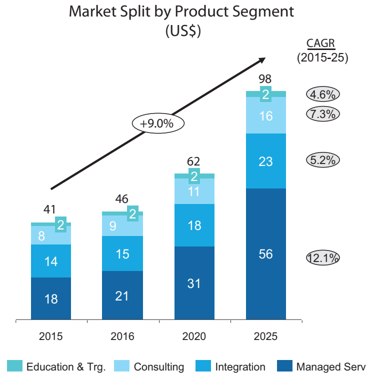
"We have vertical practices around Government and banking which are highly compliance driven and we have service offerings for most compliance needs of all leading industry verticals," adds Sharma of iValue. Another security partner is trying to build the NOC and SOC setup so that it is able to monitor the customer security infrastructure with 24/7 facility.

Essen Vision is looking at the collaborative approach to deliver best of breed services. "We are putting a practice in place for every unique service offering we are talking about. This includes internal R&D centres which contribute better in bringing out self-sustained skills from team with

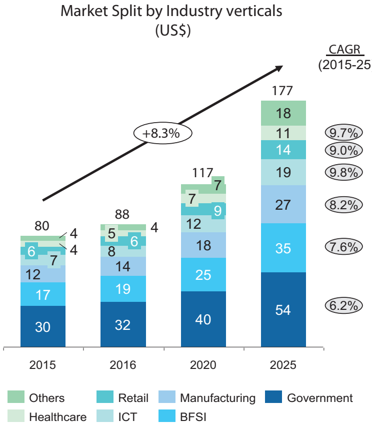
Global Cyber Security market projections by product segments



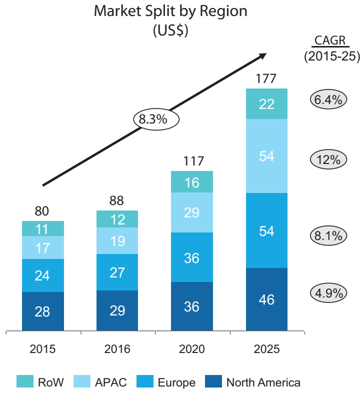
Global Cyber Security market projections by service segments



Cyber Security market projections by verticals



Cyber Security market projections by region



Nasscom-DSCI: Growing Cyber Security Industry, Roadmap for India

> "TODAY EVERY ENTERPRISE IS GIVING IMPORTANCE TO CYBERSECURITY. SOHO & SME ORGANISATIONS HAVE TRADITIONALLY RESTRICTED THEIR SECURITY INVESTMENT TO A/V AND UTM SOLUTIONS, WHEREAS MIDSIZE AND LARGE ENTERPRISES ARE TRYING TO HAVE A WHOLE GAMUT OF SECURITY SOLUTIONS TO ENSURE THAT THEY ARE HIGHLY PROTECTED."
>
> **NKR Venkat,**
> Director-Sales, Digital Track

HOW PYRAMID IS MAKING ITS OWN SPACE IN CYBERSECURITY

Delhi based Pyramid focuses on three interrelated domains viz. Cyber Security, Digital Forensics and Fraud Management with clients in government, enterprises and SME sector in India, Middle East, Africa and the United States. The firm has helped almost all law enforcement agencies in building their cybercrime and cyber forensic capabilities by setting up cyber security and digital forensic Labs and training over 3000 plus investigation officers on technical investigation skills. The company has also helped several enterprises in detecting and analysing cyber threats and attacks under 'pay as you go' managed security and fraud management service offerings.

The company has established cybersecurity and forensic labs for police, investigation and intelligence agencies in the last couple of years. Some of the significant ones are Hyderabad Police, Delhi Police, Maharashtra Police, Intelligence Bureau, Central Bureau of Investigation, Directorate of Forensic Science etc.

“We have taken this journey by training more than 3000 policemen over the country, known as 'chain of custody'. In India, there are 50 labs, of which we have done 35 labs. Now such labs are getting set up in district levels,” informs Alok Gupta, Founder and CEO of the company.

> “COMPLIANCE IN SECURITY-AS-A-SERVICE IS TURNING TO BE A HIGH PROFITABILITY BUSINESS. BEING A NICHE PLAYER IN FORENSICS, WE COMMAND A PREMIUM AS HIGH AS 30 PERCENT”
>
> **Alok Gupta,**
> CEO, Pyramid Cyber Security & Forensic

innovative cyber use cases. We are also focusing on cloud security this year bringing in solutions that integrate tightly with their on-premise security to simplify management and administration. We are firstly looking forward to exploring machine learning/ AI capabilities available with current technologies like DLP, APT, SIEM and analytics,” says Shetty. Essen Vision has also invested heavily in manpower for setting up a full-fledged lab and is working hands-on to develop use cases for security. The firm is also developing its own IP to get more success. “Security audits capability has been with us for a long time. Now on ML and AI, we have adopted both of these in our own developed technologies like Klassify and ACRS. Moreover, we are investing heavily in automation and orchestration as well,” clarifies Shetty.

Dealing with security breaches

While partners are upping the ante against cyber threats and becoming the first point of contact for the customers in case of any security breach, they have a serious challenge in terms of educating clients on allocating appropriate budgets for security. Highlights Saha, “Being a security provider, we educate organisations to think differently today. They need to transform from the “security as per budget” mindset to “budget as per security needs” approach. This is important as organisations typically spend huge sums on IT infrastructure but do not have proper financial planning when it comes to securing the same.”

> “ORGANISATIONS NEED TO TRANSFORM FROM 'SECURITY AS PER BUDGET' MINDSET TO 'BUDGET AS PER SECURITY NEEDS' APPROACH”
>
> **Biswajeet Saha**
> CEO, SEA Infonet

Ahuja of Softline says, “At Softline, we start investigating the incident. Gathering information of the incident is important in validating that an incident has occurred, identifying the suspect cause of incident, isolating the infected system and eradicating the cause of the breach. This is followed by implementing policy, procedures and technology that is necessary to prevent the recurrence. Additionally, a security audit or risk assessment combined with network penetration testing to identify weakness in the network can also be done.”

Partners have helped customers recover from Ransomware attacks, helped prevent prevalent malware in their networks. With the help of vendors, partners have also helped with intelligence on breaches in security, helped in incident forensics and have also collaborated with law enforcement agencies to nail cybercriminals.

“We have various methods available under “operate” pillar which starts from basic incident reporting mechanism and prioritisation as it's difficult for the on-ground team to

> “TARGUS PLANS TO WORK CLOSELY WITH ITS OEMS TO PROVIDE HIGH LEVELS OF HARDWARE AND ADVANCED THREAT PROTECTION. WE INTEND TO SECURE ALL SEVEN LAYERS OF OUR CUSTOMERS’ NETWORK AND BUSINESS”
>
> **Raunaq Singh**
> SVP, Targus Technologies

identify what needs to be acknowledged first. Later, we tend to follow a mix of NIST and SANS methods to respond, recover and investigate the incident for future references reducing response time,” shares Shetty.

Cybersecurity needs to be approached with a holistic perspective. In most cases, people and processes are the weakest link in the chain and not technology. Hence it’s critical to look at multiple perspectives such as technology, compliance, threat vectors, key assets, processes, and people with continuous review system to identify new vulnerabilities and fix them proactively.

“The extensive learning over time helps us to prepare customers at every stage to be ahead of the threat. Since threat vector is active all the time, the key is to assess risk and be ready to manage the threat to be ahead of the curve with continuous assessment. In case of the breach, we have forensic tools and solutions for analysing and preventing further loss of critical info and clean up the entire ecosystem from malware,” says Sharma.

With new threats evolving every second, this space will continue to see many new niche technologies coming into the market. To stay relevant, solution partners will have to constantly upgrade their skill sets, and take advantage of new and emerging technologies.

(With inputs from Rachana Jha)

ESSEN VISION SIMPLIFYING SECURITY BUSINESS WITH A COLLABORATIVE APPROACH

Mumbai based Essen Vision Software has been offering consultations and products in the area of network security and network management. In the dynamic world of IT, Essen Vision is equipped to provide the most advance demand to its customers. The company has built its service capabilities around four pillars Design, Consult, Implement and Operate. Having any number of these pillars in customers environment, there is always a scope of doing rest of them or enhance existing one with assessment programs.

Fundamentally, the company looks at security in a layered approach, sits one layer after the business, that is infrastructure which is dynamic in nature hence there is always a scope of tweaking security to adapt to digital transformation. Today, the company has been winning customers in the field of BFSI and telco segments.

"Though customers adopting the best of technologies, we see a huge lag in skills and processes. This eventually leads to failure in Collaboration and Automation. Here we see an opportunity for the partners to offer the right process and skills to fructify customers current investments," says Nityanand Shetty.

This year, the company is looking at the collaborative and automotive approach to deliver best of breed services. “We are putting a practice in place for every unique service offering we are talking about that includes internal R&D centers which contribute better in bringing out self-sustained skills from a team with innovative cyber use cases. We are also focusing on cloud security this year bringing in solutions that integrate tightly with their On-premise security to simplify management and administration,” he informs.

The company is exploring machine learning/ AI capabilities available with current technologies like DLP, APT, SIEM, Analytics, etc. at customer environment. The security provider has acquired some of the key skill sets to keep up with these technical skills who understand customer business domains very well to bring direction to this model driven by use cases.

In the future, all business domains will be impacted by digital transformation with the new concepts coming in like IOT, Artificial Intelligence, Cloud Hosting Data Centres etc. “We are ready to be a part of this transformations and be with our customers to help them adapt seamlessly. But Digital Transformations will have its own set of worries for Security. At, EssenVision we are ready with a cyber framework to keep up with these security challenges,” he concludes.

> “WE ARE EXPLORING MACHINE LEARNING / AI CAPABILITIES AVAILABLE WITH TECHNOLOGIES LIKE DLP, APT, SIEM & ANALYTICS”
>
> **Nityanand Shetty,**
> MD, Essen Vision

F-SECURE TRANSFORMS INTO AN END-TO-END CYBERSECURITY PLAYER

Looking at the changing cybersecurity landscape, the security major is not only strengthening its technological foundation but also leaveraging the strong network of its channel partners

By **Sandhya Michu**

International cybersecurity solutions provider, F-Secure, has been going through a transformational phase for last two years globally as well as in India. The company has been putting efforts to change its positioning from being an antivirus company to an end-to-end cybersecurity solution provider. "The transformation is in rapid motion in all spheres of the company," says F-Secure's Head of Asia Pacific Corporate Business, Amit Nath, who recently moved to the global sales director - sales enablement role at F-Secure.

The company is strengthening its technological foundation and leveraging technologies to build a robust and agile cyber defence framework in India. F-Secure's growth can be attributed to diversification, both in terms of product portfolio and market strategy. Channel has been instrumental in driving the company's growth in India. In the past two years, the company has acquired close to 2,000 new customers and 400 channels partners.

"We are a very customer and partner-centric company and are constantly looking to build on this differentiation by gathering first-hand inputs from our channel partners across markets. This proactive approach allows us to add to our existing product portfolio and build new technologies and features and solutions in keeping pace with the rapidly-evolving global cybersecurity landscape," puts in Nath.

Nath explained the strategy behind migrating towards an end-to-end cyber security player, "We are working very closely with our select partners while leveraging their strength in reaching out to new customers. We believe in value business and that's why we work cohesively with our top 50 business partners, as these partners contribute 80% of the business to F-secure. Our joint efforts to understand the customer's pain areas in security has paid off well and we have successfully pivoted from being an antivirus company to an end-to-end cybersecurity solution provider."

The company has been doing large series of global acquisitions and building new products. As the cybersecurity market is changing drastically, F-Secure feels the market needs automated detection and response solution rather than just reactive antivirus. The company is building security solutions around predict, prevent, respond and detect. With the renewed focus on business and channel, 2017-18 had been a great year for F-Secure. The company claims to double the business and its partners base.

"In the recent times, we have seen global ransomware attacks hitting the businesses globally. But none of our customers were impacted as we offer a high degree of protection. Besides, we are also educating customers on their infrastructure and appraising them with vulnerabilities within the systems and do regular security audits. Some customers are fairly matured and come to us with the problem to fix the gap," he informs.

F-Secure believes to carry out more value business in spite of the volume business. "I don't see the value of channel business getting diminished, as more and more companies are doing direct business with the customers. In my view, its growing constantly. None of the company can grow if their channel is not happy. However, we still feel there is a need to do more work for partners," asserts Nath.

As the company is becoming more dynamic for partners and customers, it is also preparing its partners to start pitching for newer technology and take early mover advantage. "Currently we are having a dialogue with a new set of partners who are offering solutions beyond antivirus like vulnerability assessment, detection and response solutions. We also have a strong channel ecosystem in India, with over 200 channel partners and we are constantly adding new partners. We look for the partners who have this service-oriented business model," concludes Nath.

“WE DON'T WANT TO OVERSUBSCRIBE THE CHANNEL”

Palo Alto Networks believes in taking prevention-oriented approach for managing the enterprise security solutions. The company is betting big on cloud services and realigning its key partners for these opportunities

By **Sandhya Michu**

In terms of technology alliance to provide integrated security solutions and services to customers, Palo Alto Networks works with key cloud providers including VMware, Citrix, Amazon Web Services, Microsoft Azure and more. It provides both on-premise and cloud based security, which addresses the hybrid model needs largely followed by most organizations and enterprises in recent times.

Although, Palo Alto Networks was a late entrant in the Indian security market and compete with large vendors like Cisco, Juniper, Check Point, Fortinet and others, but with renewed focus on channel and global security alliances. The company looks optimistic in penetrating this market. Compared to competitors, company largely focuses on prevention strategy using automation and integration approach to strengthen security offering.

Harpreet Bhatia, Director-Channel and Strategic Alliances, India and SAARC, Palo Alto Networks talks about how the security landscape has moved the company from a network security to enterprise security provider, “I think threats are seamless be it on the network, end point and cloud. The one big demarcating factor is our Threat Intelligence Cloud which basically observes threats across all our 45000 plus customers across the globe and has threat analytic data. When you have such a big engine that will allow us to innovate, and automate and can deploy protective and preventive mechanism across all the three areas.”

The another big move taken by Palo Alto was the formation of Cyber Threat Alliance. This alliance shares threat intelligence in central a pool which is also shared with the govt of the USA and with top corporation. The company leverage this data in deploying automated framework. Recently, the company has announced applications framework whereby it is opening this threat intelligence cloud for startups and established security companies to develop their products and solutions.

Channel is a big focus

Besides its dominance in the large enterprise,the company has started extending its footprint more across mid-market. The company is scaling channel ecosystem in India and helping them to be more profitable. Its channel program offers more rebates, renewal protection and incentives especially for partners who are technically sound to support and service our customers well. The company is offloading many services to the channels as they conduct health check of customers’ security posture through the proof of concepts and work as a security adviser for their customers.

Palo Alto in 2018 will be primarily focused on giving proactive protection to customers in any vertical be it network, end point security and cloud security.

“We don’t want to oversubscribe the channel. On channel front, we have yet to see the Indian managed security service provider getting matured wherein globally most of the service providers and large IT service company are consuming security as a service. We see there is slow interest. However, with our cloud providers we are building a new pool of born on cloud set of partners.Channels are critical to us both in terms of market coverage. Hence we align with large loyal partners with local presence through a two tier model. The optimized channel strategy then spans across the ecosystem of distributors, systems integrators, service providers and small resellers,” he added.

“Partners should start embracing cloud security and understand the framework, as the network side of the business will not be seeing much of growth. But both endpoint and cloud will be the main run rate business for the channel,” concluded Bhatia.

20% OF THE TOP BFSI COMPANIES CHOOSE SYSTECH TO PROTECT DATA

Having an unrivalled expertise, combined with unparalleled customer support, SYSTECH Technocraft Services prefers to offer its customers a range of the most reliable and effective solutions from which, together, it can cherry-pick the best solution for each situation

By **Jitesh T Dave**

In the time where we experience change and security threat on daily basis, you may not have heard of SYSTECH Technocraft Services, but it's likely that we've already been keeping your data safe somewhere in the world. We are currently suppliers to five of the 10 top banks, six of the top 10 insurance companies and two of India's three leading credit information organisations. We are independent specialists and distributors in Managed File Data Protection. In a world where data travels between people, organisations, countries and continents all of the time, we protect it at every step of our 'Protect, Detect, Respond' cycle, advising, installing and maintaining software and systems that protect data throughout its life, wherever it travels.

We have unrivalled expertise, combined with unparalleled customer support – this has been the primary reason why 20 per cent of the top companies in BFSI sector have chosen to trust SYSTECH to advise them on how to protect their data.

We are independent and offer an open, honest and timely service providing completely unbiased advice to our customers. We prefer to offer our customers a range of the most reliable and effective solutions from which, together, we can cherry-pick the best solution for each situation.

Our independence means our customers come to us as trusted advisors, whether they want us to review and shortlist solutions, implement new software or just advise on extending their existing protection. When it comes to helping our customers grow, we are always on-hand to provide support for bids and proposals, identifying and resolving potential threats to success when landing new clients and nurturing existing ones.

> WE ARE CURRENTLY SUPPLIERS TO FIVE OF THE 10 TOP BANKS, SIX OF THE TOP 10 INSURANCE COMPANIES AND TWO OF INDIA'S THREE LEADING CREDIT INFORMATION ORGANISATIONS
>
> JITESH T DAVE,
> DIRECTOR – SALES, SYSTECH TECHNOCRAFT SERVICES

From migrations to complex data flows, our skilled team of experts have integrated, developed and generated the most complex workflows imaginable. In the process of migrating thousands of scripts, we sometimes create applications for customers that other companies would find useful.

Rather than reinventing the wheel for each customer, we pool our knowledge and make these solutions available to our customers as a free trial once they have been thoroughly quality assessed. In sharing our progress this way, we are able to keep offering the best solutions and keep costs down for our customers.

We also nurture relationships with our suppliers rather than just selling products. We find this benefits our clients in more ways than one. When we spot a gap in the market, or a challenge our customers face, we liaise with our suppliers to help them to continue developing new solutions to keep your data safe.

(The author is the Director – Sales, SYSTECH Technocraft Services)

"WE NEED TO TAP SPECIALIZED SKILL SETS AMONG THE CHANNEL PARTNERS"

In an interaction with CRN's Nivedan Prakash, **Stanimira Koleva**, Senior Vice President and MD, Asia Pacific and Japan, Citrix, talks about the significance of the India market and the various initiatives being taken to tap the burgeoning market opportunities

How significant is India as a market for Citrix?

In India, our own teams, partners, as well as customers are always thinking of something new. It is one of the most technology savvy markets and fastest growing regions for Citrix. The country has been delivering very positive indications, especially around the government's policies. Recently, I met the CIO of one of the largest manufacturing companies here in India and came to know that they've been looking at Blockchain to enable new ways of providing leasing and finance to their dealer channel as well as customers. It's very impressive to see how fast they figured out the usage of Blockchain. What brings me here is the opportunity, as India is a critical market in the context of Citrix. We have major R&D setup here and it is one of the largest locations worldwide.

When you interact with the customers here in India vis-à-vis other markets, do you see any similarities in the way they approach a problem? Do you come across any common challenges being faced by them or it varies from market to market?

There are a few similarities that I can share along with flavours of how they pan out or manifest themselves. All the customers, for example, know that they need to adopt cloud and migrate to certain services and workloads. However, it happens very differently in various markets and that too at different speeds. Like in APJ, Australia and New Zealand, we see the most aggressive adoption of cloud – nine out of 10 customers that I speak with follow 'cloud first' strategy in whatever new service they adopt.

In the APJ region, India is second after Australia in terms of cloud adoption. The environment of the players in the market is evolving rapidly because you not only have all the big public cloud players like Microsoft, AWS and Google, but also a good and healthy local ecosystem of players. Besides, the country is leading the way in mobility solutions' adoption.

On the other hand, the conservative markets like Japan or some markets in South East Asia, which are dominated by highly regulated industries, we see slower adoption of cloud. But, everyone is thinking in terms of how they are going to get there. However, across the regions, large enterprise will continue to live in a hybrid environment for years to come.

The other thing is everyone's attention towards cyber security, which has become a prominent trend across the region. Even in India, enterprises are aware about vulnerabilities and how critical it is for them to protect their business environment. We want to play a role here by taking the multi-layered approach.

Another trend has been in the area of workspace transformation. In India, people see it as a key pivot for maintaining competitiveness in the business and growing productivity. In some countries like Japan, it is all regulatory driven. The government in Japan actually published rules of what workstyle innovation looks like. We see very different ways of them driving workspace transformation and they are now more aggressively looking at mobility, which India had been embarking on for years.

Is there any particular initiative that has been taken to tap the opportunities, which have come up as part of India's digitisation drive?

We are looking at a couple of initiatives to beef up our capabilities to deliver extended services around mobility. We can work with large organisations for the deployment of mobility solutions or may be moving to cloud. Secondly, we are making an investment for geographical expansion in the country. We want to go beyond the metro areas, which is so far fairly well covered, and expand our footprint in Tier 2 and Tier 3 cities. These cities will be covered by our distribution network.

Since cyber security is one of the key focus areas for Citrix, are you going to engage with specialised partners in this domain?

Keeping cyber security in mind, we need to tap the specialised skill sets among the channel partners. We have started working with a few consulting organisations and service providers around security. We have to also look beyond how our actual channels are changing in terms of cloud versus on-premise capabilities. We may actually need to work with some new players around cloud and hyper convergence. Hyper convergence is very relevant to our business because it removes some of the complexity and upfront investment in spending on new services.

Going forward, what will be the key priorities for the company?

Apart from the technology priorities that have been mentioned above, we want to have more CIO conversations. Since more than 70 per cent of our business comes from large enterprises, it is imperative for us to increase our relevance among key decision makers. Besides, we are also looking to scale up our services portfolio. There is a lot of R&D effort being made towards integrating virtualisation with our networking portfolio; and we want to make sure that we offer more parts of our portfolio into the existing base.

As far as cloud is concerned, we don't just see it as a new way of delivering IT. We need to make changes in the way we support customers in cloud. Cloud adoption services are becoming much more critical. From the investment point of view, it's not all about convincing a customer to buy or testing it and figuring out if it works, but also being with them on the entire journey In the cloud domain, we are ready to change our model of interacting with partners and customers.

Lastly, we will continue to look at geo expansion and take initiatives to acquire new customers or maybe breaking into new mid-market and SME segments. We are also looking to revisit expansion of use cases in our large enterprise customers.

"WE HAVE BEEN ABLE TO OPEN NEW DOORS FOR OUR PARTNERS"

Barracuda Networks has over the years become a strong player in the cloud space. **Murali Urs**, Country Manager – India, Barracuda Networks, in an interaction with CRN, sheds light on Barracuda's market presence, offerings and growth plans

By **Rachana Jha**

What sort of direction is the company moving to, in terms of the market, technology, environment and innovations?

We are Cloud Connected Storage and Security Solution providers, and have become very strong in the cloud space in the past couple of years. We offer around eight to nine products cutting across technologies, which include security availability (application delivery, availability and storage). In the security space, we cut across four different threat vectors – email, network, web and applications. Of the eight or nine technologies we sell, we are now focused more on four which are the key pillars of the company globally, which is basically email security, coming through the O365 offering. Then we have the Next Generation Network Firewalls; basically the network security part. We are also focused on backup, because we have a great presence on the backup front, especially purposeful backup solutions followed by cloud, because we are probably way ahead of our competitors when it comes to cloud solutions. We have been doing business only with channel.

We have registered authorized, preferred and premier categories of channel partners – each one has to be a registered partner. Following registration, they decide on what kind of commitments both of us need to give each other, then we decide where the partner fits in. The premier is highest category of partners with a larger target and larger commitment from their side as well as from our side; whereas, the preferred have lesser target. The qualification criterion from a technical standpoint is lower than premier – the number of people need to be certified, sales officials and technical officers. We have close to around 70 partners, but focus-wise there are around 20 to 25 partners we engage with consistently. They bring in opportunities, they open their account list, then we plan call out days with them. We also do EDM blasts with them. We put significant efforts to generate joint opportunities and leads for all these partners. We do customer events, market development fund contribution for their marketing activities, which helps them have an event together and position our technologies for their customer base. The partners find a huge attached rate with Barracuda primarily because we have that sort of products. It's not that we give one technology and just walk away; Barracuda always gives an opportunity for them to sell more to the same customer.

What will be the focus areas for the company this year?

All the four pillars definitely have potential. Backup, network security and firewalls are never-ending markets. I think from interest, engagement and talking standpoints cloud is important – it's an upcoming market. Everybody wants to see what new we can bring on to that particular platform. We are able to engage with a lot of Microsoft Cloud partners – the MSPs. We're also able to attract numerous AWS partners.

The large opportunity we actually see is O365, because we are the only vendor who can actually give cloud based immune security. We can give cloud based backup and we can do cloud based archive, which no other vendor can talk about. From a single console, you can manage all of them. The opportunity is phenomenally large, because native customers of O365 do have these challenges which we address. There are other vendors also in the market. But, they do it in bits and pieces. One vendor will do only backup, one vendor will only look at immune security. We are able to give a complete bundle which addresses all the three key challenges of customers.

What efforts bein put to equip partners to address the changing market requirement?

We have a Barracuda University or the Barracuda Campus, where authorized partners are given a complete permission to access the entire content of what our internal people learn – almost everything; right from sale certification to pre-sales to post-sales handling of customers. Partners can do this online. To bring the attention of partners to this particular portal, we conduct sessions in every city and we try to conduct on-premise certification training, wherein the parrners get certified on the spot – this is particularly for the pre-sales teams.

Post-sales, they need to go through a larger curriculum to get the certification. This financial year we completed a six-city round of events including 'Learn and Earn Session' where we had a very unique way of making partners learn what Barracuda has to offer.

Currently which are the primary focus verticals for the company?

Each technology comes with a specific focus. In web application, firewall has typically been in the BFSI sector in India. We have many customers in the BFSI vertical using our vast solutions. When it comes to email security, our customers include education institutes, manufacturing companies, PSUs, IT, ITES companies or anyone of them, because email security is a core infrastructure any customer would like to have. Now we're seeing the same kind of traction happening with backup – we are able to sell across multiple verticals from the backup standpoint. Archiving typically has been only for IT-ITES and for the BFSI. We haven't seen manufacturing organizations wanting to do email archiving, because we don't know what their compliance or requirement is. For BFSI, compliance is a big factor; they need to store emails for long time. Whereas in IT-ITES deals with customers outside India, they have their own challenges, because the employer's attrition is very high. Hence, they'd like to retain emails; they are buying a lot of archives.

> THE LARGE OPPORTUNITY WE ACTUALLY SEE IS O365, BECAUSE WE ARE THE ONLY VENDOR WHO CAN ACTUALLY GIVE CLOUD BASED IMMUNE SECURITY
>
> MURALI URS,
> COUNTRY MANAGER – INDIA,
> BARRACUDA NETWORKS

What's your opinion on the prevention and detection debate which has been a talk point in the industry?

Barracuda plays in all the three – prevention, detection and remedial. You need to have technology that enables you detect things even before they happen. Barracuda has two technologies which are very crucial to customers' environment. One is email, wherein we have a service called Email Threat Scanner (ETS), which is absolutely free of cost service to scan, exchange online as well as exchange on premise. Secondly, we have a product called Barracuda Vulnerability Manager, specifically designed for web applications. We can scan customers' web application, which will be running on an Apache Server or a Web logic Server. We also provide a dashboard to the customer, featuring what are the kinds of threats those web applications have. That is from a detection standpoint; and both of these are free, which is the greatest USP of Barracuda and a great advantage for us. Next is the prevention part, wherein we have four different vectors – event security, web security, network security and application. All four are backed up by a fantastic ATP. Barracuda is probably the only vendor in this space. We have ATPs for email, NG, application and web filter. We have close to 150,000 customers in this area, and have crossed 300,000 subscriptions of our product. We get a huge amount of feedback from those customers into our GIN (Global Intelligence Network). Additionally, we have thousands of honeypots that we have deployed worldwide. We are able to give a fantastic ATP solution, where our hold percentage is only five to seven per cent. The balance 90 to 95 per cent can be passed through, because the intelligence we gather is coming not from one specific vector.

What's your message to the partners?

With Barracuda Solutions or with Barracuda Networks, you basically are partnering with an OEM which gives you a platform to sell more products with existing customers. With the products, we have been able to open up new doors for our partners. Secondly, we are definitely a partner whom you need to work with to get into the cloud, because Barracuda is one of the best vendors today providing cloud technology. It could be public cloud or SAS model, addressing the largest market with O365 customer base, the largest AWS market and largest Azure market.

CYBER SECURITY WILL MOVE TO BECOME SOFTWARE DRIVEN

Amidst the evolution of sophisticated cyber threat landscape, Checkpoint has been advocating software driven security for more than two and a half decades.

By **Abhishek Raval**

There are broadly six trends prevalent in the IT space combined with cyber security: Ransomware, artificial intelligence (AI), cryptocurrencies, espionage (state sponsored wars), demand for cloud security and Internet of Things (IoT). "Our solutions revolve around each of these trends. Any device that has an IP, software and connected to the internet is hackable. Recently an incident occurred where a vacuum cleaner was hacked. Checkpoint reported a hack in the SmartThinQ app of the LG's HomeBot Hoover (a vacuum cleaner) by using the owner's email ID. The cars can also be breached. They have a software connected to an IP, which can be upgraded. Anything run on a software can be hacked into. Right from the air condition, to music system and even the steering of the car," informs Bhaskar Bakthavatsalu – Managing Director, India and SAARC, Check Point.

The critical Infrastructure is also vulnerable. A firesale attack can take down the critical infrastructure like the electricity grid, water supply, aviation, transportation, trains etc. Even the Aadhaar data of the citizens can be erased in one stroke.

These threats are making the boards of companies raise issues on the cyber security readiness of the company, its customers etc. While the physical borders of the company can be defined and monitored, it doesn't apply to the cyber world. There are no boundaries. "Countries are collaborating with each other on improving the cyber security posture, is a good development. We also see many companies who are ready from a futuristic perspective too," says Bakthavatsalu.

Checkpoint also provides solutions for the mobility space. In the future, everything will be custom fitted onto the mobile - it's already happening in payments, ticket booking, shopping and many more activities. "The PM is is aggressively pushing the JAM trinity. Chandrababu Naidu wants to provide a 250 mbps line for last mile connectivity, but what if the farmer's phone is compromised and all the money is siphoned off? The mobile will become a critical asset of the individual and thus it, by default, becomes the target of threats. A mobile device can be controlled and hacked by sending a simple SMS, or a WhatsApp message. The attacker can remotely handle the mobile device using his laptop and also keep a watch on the activities of the victim. It's very easy to perpetrate these attacks - Google search certain information, pay $10 and the attack gear is available," he points out.

The online ticketing platform can be blocked by bombarding the traffic on the platform. Thus, the cinema goers will not be able to book the tickets. This can sabotage the movie. This can be easily done by outsourcing the job to a hacker, who doesn't even reside in the country. Ransomware as a service and hacker as a service is provided and easily available online. No longer is there a need to learn coding.

"In such a dreadful scenario, cyber security will move to become software driven. Checkpoint has been advocating software driven security for more than two and a half decades. We are already in the age of SDN and Software Driven Security. The entire credit for this should go to cloud technology. Considering the advanced threats floating around, cheaper solutions are not the answer. For example, which pacemaker should the patient go for - a $10 or a $10,000? He should always go for the best quality solution. It's a matter of life and death. Likewise in the cyber security space. Unfortunately, the marketing gimmicks makes the enterprises go for the cheaper solutions. What we have noticed from our surveys is that customers aren't protecting their mobile devices. They have not bought a solution for their mobiles," comments Bakthavatsalu.

"

IT IS IMPORTANT FOR THE PARTNERS TO BE UP TO THE SPEED WITH THE MARKET DEVELOPMENT AND DESIGN AND WORK ON NEW OFFERINGS

BHASKAR BAKTHAVATSALU,
MANAGING DIRECTOR, INDIA &
SAARC, CHECK POINT

Privacy and confidentiality is a major right of every citizen and he would not like his information to be leaked. At Checkpoint, a security demo is given which involves a simple exercise of an app download. If the app is malicious, it immediately takes control of the device after the user accepts the terms and conditions, usually in a hurry. The mobile device that requested the app download can remotely handle all the photos, messages on the user's mobiles, which downloaded the app. Thereby, the mobile device is compromised.

Checkpoint takes a comprehensive view of all the threats and identifies them. The approach is not siloed to specific threats. We provide an end-to-end cyber security framework, which has the next generation firewall, followed by threat prevention, advanced threat prevention, then connect with cloud, mobile and networks. A panel with an unified architecture shows in a single window view the activities happening in the network," explains Bakthavatsalu.

This provides various recommendations and the action to be taken. The threats are evolving by the day and are getting stealthier and companies should only partner with vendors who are also evolving and matching up to the pace. The product viz, 'Check Point Infinity' is the first consolidated security across networks, cloud, and mobile, providing unparalleled threat prevention to keep customers protected against the growing number of cyber-attacks. The platform also has a single management platform. It allows to take fast action to remediate the threat.

"In this backdrop, it is important for the partner community to be up to the speed with the market development and design and work on new offerings. They should come out of the comfort zone of their traditional offerings. It's also important to say 'no' to unviable prices being demanded by the customers. To empower, skill and keep the employees motivated is important than anything else. I have seen many small companies challenging bigger ones just because the way they have focused on the employees and their thought process. Even though attrition happens, vendors should continue to invest in their employees. It's a must. If that happens, no vendor can fulfill the gap of partners. Unless the vendors want to do direct selling. Checkpoint's philosophy has always been to work through the channel partner community," adds Bakthavatsalu.

AI CAN BE USED IN FRAUD DETECTION AND PATTERN RECOGNITION

Hero MotoCorp is betting big on Machine Learning (ML) and Artificial Intelligence (AI). CRN's Sandhya Michu speaks to **Vijay Sethi**, CIO and Head CSR, Hero MotoCorp about how digital transformation is posing new security threats and making the job of CIO and CISO all the more challenging and complex.

How is Hero MotoCorp is leveraging technology to remain competitive?

Technology is core to our business. Currently, we are in the process of experimenting in new areas, competency upgrade, and innovation. With the use of technology, the scale at which the IT initiatives at Hero MotoCorp were being implemented are amplified. We encourage people to work on innovative ideas beyond regular projects. We have set up a Centre of Excellence (CoE) centered around activities related to Blockchain, Machine Learning and IoT to work on emerging technologies.

In your view, how AI and ML will disrupt the security landscape?

Information security is paramount to all the companies -- be it large or mid-sized companies. Protecting customers and internal data and information in complex security threats is making the role of CIO and CISO more challenging and complex. Earlier, we used to protect the information security from limited end points such as datacenters, laptops and mobiles. Today, it is going beyond mobile, IoT and sensors. Hence, the possible exit points for getting the information out are increasing day by day.

At Hero MotoCorp, we secure our information around three factors: Process, People and Technology. There is a huge amount of evolution in these three areas. As we progress, lots of global practices are coming in process and existing processes are getting matured. In technology side, some of the new technologies which are coming is leading to an increased threat, but some of the technological developments will lead to security advancement, for example Artificial intelligence. AI can play a huge role in today's time to mitigate the risk which is growing on a daily basis. It is humanly impossible to track all sorts of threats and risk which are there. The second piece is machine learning. From a Hero MotoCorp perspective, we have a multilayer security architecture. We have invested in technology, which not only does prevention and detection but also predictions.

Where do you see the scope of AI in security?

Evolving technologies and the growing numbers of "always on", "always connected" devices, tools and commodities have increased cyber-threats opportunities for access and interference. Security personnel are finding themselves overwhelmed by the multiplicity of attack vectors and tools available to the cyber-criminals, and are increasingly looking to a new ally, in the quest for cyber security. AI can be used in fraud detection, behavior and pattern recognition, behavior predictions. At this stage, we are exploring the tools available in the market. In a year or so, we see AI will become mainstream.

What were the key IT initiatives taken up by Hero MotoCorp?

We are already big users of 3D Printing, simulation, and it's beyond new technologies like social, mobile, cloud and analytics. Moving forward, we are investing to make AI and ML the next growth engine for our business. At Hero, we are willing to explore new technologies and working with many startups in the areas of AI and ML. We will be replicating this experience in our new and existing manufacturing facilities to constantly drive innovation and efficiency. As we move forward, we will integrate the current solutions with other solutions as part of our focus on digitization, which in turn is aligned with the strategic business objective of achieving Industry 4.0 standards.

What are some of the key concern areas for Hero Motocorp?

Security is a critical concern and we want this to be a key element of our culture. To this end, all our developers are trained in secure coding practices. We are working to improve the group's information security position through training and awareness campaigns.

Parallels®

The fastest, easiest, and most powerful application for running Windows® on Mac®—without rebooting. Includes 30+ utilities to simplify everyday tasks on Mac and Windows.

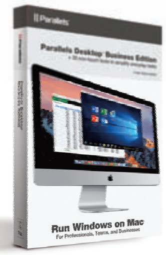
Parallels® Mac Management for Microsoft SCCM
Seamlessly integrate Mac into existing Microsoft SCCM infrastructure. Extend your Microsoft SCCM to manage Mac computers like you manage Windows PCs.

RAS
RDSH
VDI
ERP
CRM

Parallels® Remote Application Server
Access and use applications and data from any device and OS, from anywhere.

Easy to Use, Flexible, and Secure
Brilliant Mobile Experience
Extended Flexibility
On-demand Scalability

Parallels Desktop® for Mac Business Edition
Run Windows on Mac with the best performance: for professionals, teams, and IT managers.


Parallels
Parallels Desktop Business Edition
Run Windows on Mac
For Professionals, Teams, and Businesses

Contact our sales team at **sales@systech.co.in** about a **Special Promotion!**

Valid until
15 June 2018

All India Distributor:
Systech Technocraft Services Pvt. Ltd.
Mob. : +91-98 927 08950
Email : sales@systech.co.in I www.systech.co.in
Tel.: +91-22-2812 1113 / 39 / 6510 3242
Mumbai • Bengaluru • New Delhi • Pune • Chennai • Hyderabad

SYSTECH
solutions at work
TECHNOCRAFT SERVICES PVT. LTD.
ISO 9001:2015 & 27001:2013

FORTINET EXPECTS SIGNIFICANT GROWTH FROM MSSP PARTNERS

Fortinet, last year, has revamped its MSSP partner programme, alongside introducing new offerings for its MSSP partners. **Jitendra Ghughal**, Director, Channels – India and SAARC, Fortinet shares the company's position and plans ahead

By **Mohit Rathod**

How has been Fortinet's performance last year?

In the first three quarters of 2017, we saw significant growth; and we are happy with the growth that we delivered in India and the SAARC region. The highlight is that we have not just grown our business of the flagship Fortigate products, but also other products that are part of Fortinet Security Fabric range. Fortinet Security Fabric is not just one concept or solution; it is about combining and integrating multiple solutions and ensuring that they work well. It's also a broad portfolio of solutions which work in an automated manner and provide intelligence that customers require - for them to understand what's their threat landscape. Last year we have been successful in growing or business across our entire range of products.

As far as the channel structure is concerned, we have been doing pretty well in terms of number of partners, partner certifications, sales certifications and technical certifications. We have observed that there's a lot of interest about network security institute; we have a security enablement learning centre, wherein we have exciting programmes for our partners.

What's your roadmap and focus areas for 2018 and ahead?

In 2018, we will be focusing heavily on three market segments: telecom, government and BFSI. We have already started investing in these segments and we are going to see good results, particularly in the BFSI space. We have already seen a lot of success in the government segments over the last couple of years. Even in the telco space, we have been able to grow our business significantly. In the telco segment, particularly for our partners, we have revamped our Managed Security Services Providers (MSSP) partner programme last year; alongside, we have also come up with some new offerings for our MSSP partners. We expect that this year, there will be a major growth from our MSSP partners.

What are your efforts for partner enablement and skilling?

We have different approaches in terms of enabling our partners. Primarily, we have an online tool for partners – this is available through a common partner portal, through which partners get access to the sales training resources. We have also made technical training free for partners; whereas, previously partners were required to pay for technical training. Moreover, we have our resouces and we deliver classroom tranings; we also have third-party training centres for customised training or certain end-user training. We also invite select partners to our offices and provide trainings, depending upon our business plans with these partners.

We have a partners programme which primarily has four levels – authorised, silver, gold and platinum; alongside by MSSP gold and MSSP platinum for MSSP partners. For each of these levels, we have a clearly defined certification requirement for both, sales and technical. For the last four quarters, we have been running a promotion – which will also continue this year – wherein we are rewarding partners for completing their certification. For example, when an authorised partner completes the required sales and technical certifications, we provide rewards for that organisation by upgrading them to a higher level of partnership. We also provide them incentives of about $400. This is a mutually beneficial programme which ensures that partners get their resources trained.

We have this programme for all levels of the partner's organisation. We also have technical and sales training programmes for different profiles of partners. For example, certain partners are only keen on selling our core techologies. Whereas, many other partners are interested in selling security fabric solutions. Thereby we follow and module based approach and we have designed different modules; partners can decide the products and solutions that they want to sell, and which segment they want to focus on. Based on this, partners can choose their modules. The best part for partners is that this is absolutely free; they just need to register themselves as partners.

How many partners are actively working with Fortinet?

We have around active 650 partners working with us throughout India, across all the categories. This includes partners having presence in India, but also working with us globally; such as Netmagic, Dimension Data, Accenture etc.

A typical reseller normaly buys the product and sell it to the customer. In terms of MSSP, there are different solutions, such as Customer Premise Equipment (CPE) based solution. When a typical telco partner sells services to customers, the partner would provide our product and manage the product from their data centre or security operations centre (SOC). They charge customers on a monthly basis.

There are other models as well, wherein they provide solutions on a multi-tenancy basis. Partners take our products, virtualise the solutions and assign a customer for each virtual domain and manage it from their premise. They deliver these security services from the cloud for customers, but it is managed completely by the partner.

Do you think the role of MSSP will be predominantly critical than traditionl channel partners?

At this point of time, it is difficult to predict the direction of business, but we have solutions for both. Typically, large enterprise customers require security to be managed from their own premises. However, in the future, more and more SMB customers will move towards MSSP based solutions. Large customers such as banks or government organisations would like to keep security under their control. Smaller customers don't possess enough resources, and they ideally want networking security requirements managed by a third party. It's not just about management, SMB customers don't even have to invest. We also have solutions such as Bring Your Own License (BYOL).

> "AS PART OF CHANNEL ENABLEMENT, WE HAVE MADE TECHNICAL TRAINING FREE FOR PARTNERS
>
> JITENDRA GHUGHAL
> DIRECTOR, CHANNELS - INDIA & SAARC, FORTINET

What's the differentiating factor Fortinet has created in terms of channel programme?

The most important factor is the combination of resources, and tools – this is something that sets us apart. Apart from our NSE programme, we also have tools like renewal tracking portal for our partners, deal registration tool etc. Another offering, Cyber Threat Assessment Programme (CTAP), allows partners to implemeny box at a customer's premise and register it with our CTAP domain, and run the box to generate a report. On top of that, we are also providing them incentives. For example, we are now providing incentives to partners for generating reports and closing deals.

What are the similarities or differences between your partners in India and other markets?

Partners' approach in all markets are quite similar to each other, because the issue they are addressing is global in nature. Network security is not different in other countries. In some markets like Nepal, we don't have many resellers who close deals on the role. A slight difference between India and Nepal is that in India, partners either depend on Fortinet or internal resources for sales; whereas in countries like Nepal – where we don't have a direct presence – resellers depend more on our distributors.

Each market has its own requirements and we work accordingly, so we wouldn't like to replicate best practices in other markets. We are happy with our performance across markets and we have been growing well in all markets. For instance, last year we marked huge growth in Bangladesh; we invested in resources a few years ago, and it provided us with the dividend.

What are the company's expectations from the partner ecosystem?

Partners should have enough resources in terms of sales, pre-sales and post-sales – this will support our customers. Partners should also possess enough number of certifications that we require. We require partners to approach us proactively for the deals that they identify in the market. We do business only through partners, and partners are the ones who interact with the end-customers, so it is crucial for us to have interactions with our partners. We have a three tier distribution model. Our authorised distributor is not allowed to sell our products to an unregistered reseller. Even our partners are required to buy only from our authorised distributors.

'AS-A-SERVICE' MODEL: THE FUTURE FOR PARTNERS OPERATING IN CYBER SECURITY DOMAIN

It will be difficult for partners, who are offering traditional cyber security solutions, to continue with their current model. Cloud has upended the business models. The ease with which products can be provided 'as a service' over the cloud is making the businesses of many partners redundant. **K K Mookhey**, Founder & CEO, Network Intelligence, and **Altaf Halde**, Global Business Head, Network Intelligence speak to CRN

By **Abhishek Raval**

With the emergence of cloud, how do you see the evolution of cybersecurity players in the channel partner business?

K K Mookhey: The quickly emerging and faster growing cloud-first and mobility-first startups are changing the way enterprises use IT. They are providing a huge value addition to enterprise end users. The same applies to the channel partner ecosystem. Cloud is disrupting our business. The conventional trading business of the channel partners is already disappearing unless the channel partner makes a value addition in the offering.

Technology Goliaths like Microsoft and AWS are gobbling up technology companies and serving their solutions over their cloud offerings like Azure or AWS. Web application firewall is provided as a service. Even Privilege Identity Management (PIM), which was provided as a product is now available as a service. The same goes for Identity and Access Management (IAM) too. In such a scenario, the role of the players like Network Intelligence becomes 'cloudy'.

Precisely why, the conversation with the system integrators usually involves how can we take bundled solutions to the end customer? This is where we tie the offerings from Network Intelligence with that of OEMs and deliver it as a bundled solution. Ways are also being explored to deliver services on an Opex model. Channel partners will invest in the Capex and then deliver using an Opex arrangement. The channel partners will have to identify the pockets of value addition.

MANAGED SECURITY SERVICES WILL BE A KEY THRUST AREA FOR US. THIS WILL BE POWERED BY THE TECHNOLOGY BEING DEVELOPED IN-HOUSE

What's the level of maturity among the customers in terms of how they see the Opex model?

Altaf Halde: There are two levels of maturity. One class of customers is in an advanced phase and understands the requirements and the potential of cloud. The second level has identified the importance but needs partners like us to help them understand the potential and then implement. Moreover, the customers trust and see us as a partner in real terms when we go as a consultant whereas they perceive us as a seller when we represent a product company.

K K Mookhey: The consumers with installed cybersecurity infrastructure worth millions of dollars have come to the realization that they do want to explore the Opex or as-a-service model. The other type of customers who are yet to take a decision on their cybersecurity spend are also exploring the same model. They are becoming averse to the Capex model with mandates even coming from as higher an authority like the board of the company to freeze the Capex expenditure.

You have also launched new products and are in the process of entering into new LoBs. What's the latest update?

K K Mookhey: I have a mantra in business- if a company does more than three times of the same thing, then either it doesn't know its business or it doesn't know enough about the space of cybersecurity. Companies should automate routine activities.

This thought is the genesis for our product 'Firesec'. I was working on a firewall review project from a telecom company. There were 100 firewalls with the largest firewall having close to 15,000 rules. To review it manually wasn't possible. We automated it by writing code for doing the review. This is the birth story of Firesec. The challenge with most of the end users is they are not able to optimally use the mammoth cybersecurity infrastructure bought over the years. Firesec helps them do just that. It passes through the network and recommends changes and suggests how certain security products can be better configured. Firesec not only helps in automation but also orchestration, wherein IP blocking and rule development can be automated after a ticket has been generated in response to an incident identified by the SIEM solution in the Security Operations Center (SOC). This is currently done manually by the L1 and L2 staff at the SOC. Firesec will be able to integrate with all the security technologies and examine if they are optimally configured.

Our other offering, 'Insight', is a Big Data analytics product for the security analysts. It's provided as a service by doing a 'Compromise Assessment'. We plug the product at the end user location and tell them whether they have been hacked already. But they are unaware about it. Insight has been built on the 'elastic' stack platform. It was realized that Elastic can be used to deliver threat hunting, CISO dashboards etc. Hitherto the traditional solutions weren't able to do the analysis because they couldn't take the massive amount of log volume. Elastic is able to intake gigabytes of logs and do the analysis before designing user friendly dashboards to bring the analysis to the fore.

What efforts have you invested in skilling your teams?

Altaf Halde: There are two more differentiators we have. Network Intelligence runs an independent business of cybersecurity training. It has been nine years since the training business is operational. Our internal hiring happens from these training interventions. The clients, in fact, ask us when the next batch is getting over for them to hire the required cyber security staff. Our competitors also look forward to hire from the same pool. The students passing out of our institute are immediately employable. There is no need for 'shadowing' or 'on the job training'. The consultants working internally at Network Intelligence are the trainers. They are hands on with the operational and practical aspect of working with the clients. They inculcate the same in the students too. Thus, the training intervention is designed for the students to become problem solvers and trouble shooters from day one.

Secondly, skill upgrade and knowledge transfer are followed religiously at the company. In the skill upgrade space, employees have been certified with the various cloud security certifications. The demand for cloud security professionals is high. We are a cloud-first company. Network Intelligence's SOC and vulnerability management infrastructure runs on Azure. The cloud security certification program began two years ago. We are a Microsoft cybersecurity partner, which leans more towards Azure and Office 365. This is because a majority of the users are moving these applications on the cloud. The employees have acquired AWS security certification too. The efforts to get the employees IoT security certified has just started. Training programmes are also being run on 'Critical Infrastructure' security.

What's the direction and key thrust areas that channel partners will take in 2018, in the cybersecurity space?

K K Mookhey: Managed security services will be a key thrust area for us. This will be powered by the technology being developed in-house and also that will be procured. International business will also be a focus area. We have set up shop in the USA and Singapore last year. The attention will be on four markets: India (60 per cent business), the Middle East (40 per cent), the USA and SE Asia.

Altaf Halde: Thrust will also be on skill development and training. The demand for cyber security jobs is only going to move northwards and we will play a significant part in providing skilled professionals to the industry in 2018.

GROWTH AND SUSTAINABILITY IS A PROMISE FROM CISCO TO ITS PARTNER ECOSYSTEM

Cisco is transitioning quickly from a hardware focused company to a software services entity, as networks and data centers become more software defined. **Daisy Chittilapilly**, Managing Director, Partner Organisation, Cisco India & SAARC, explains how the networking giant is looking at the partner ecosystem as it tries to grow faster than the market

By **Nivedan Prakash**

At a broader level, what are your plans and strategies?

Cisco is clearly in a transition. We were largely a hardware focused company but we are now in the transition to become more software and services oriented. In fact, we have a public stated goal of moving around a significant percent of our business to software services by 2020. This is a big transformation that is happening at a company level, which is true for the channel partner ecosystem.

In the last two years, we have bought 16 companies. All of them are software. We always had an innovation engine focused on three strategies: the build, buy and the partner strategy. We have added two new ways in which we stay ahead in innovation. We commit investments to corporate development. We also invest in niche companies. These companies either complement our technology portfolio or give us the differentiation or advantages in terms of speed to market.

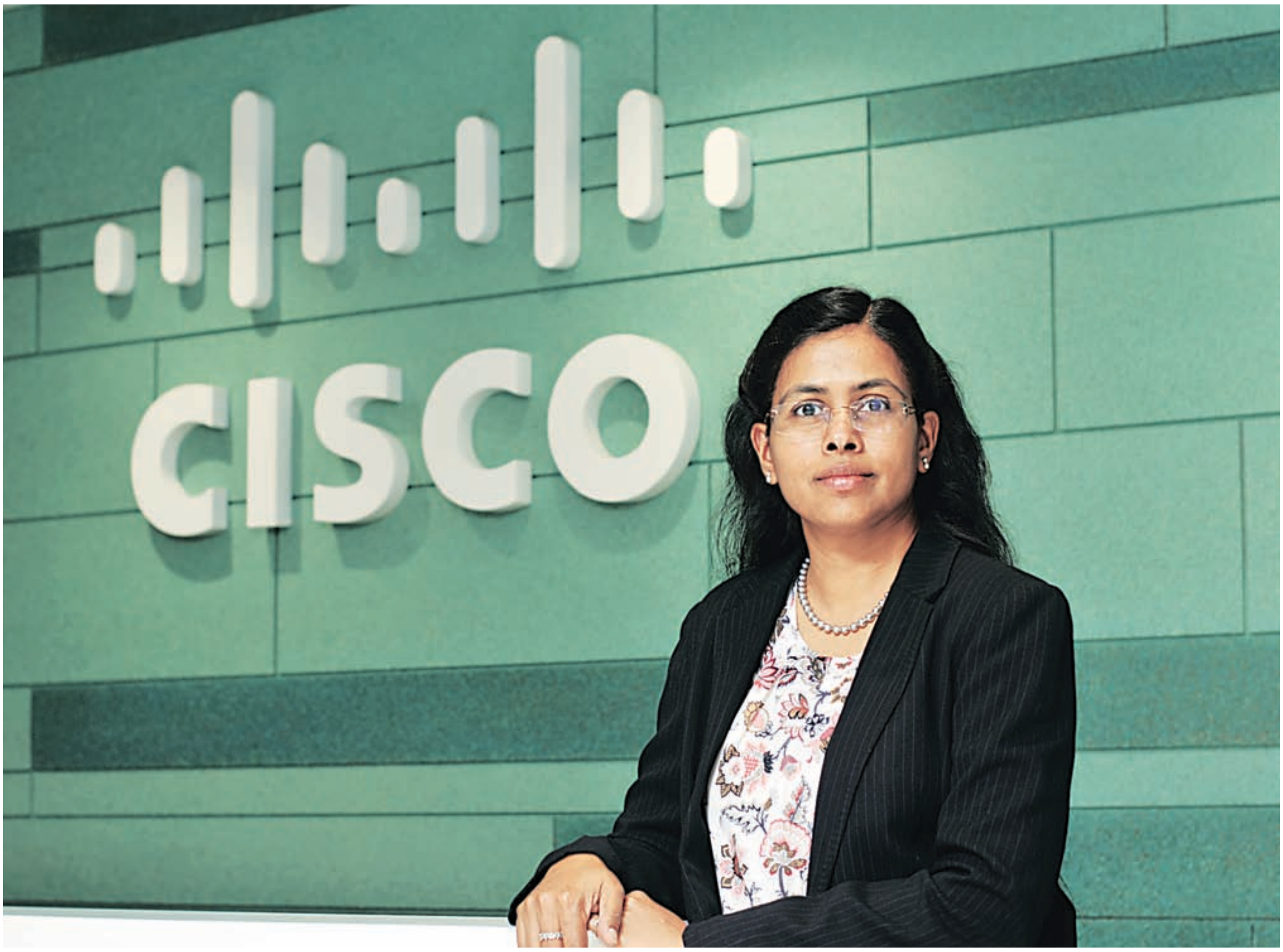
All the strategies around innovations are to focus on primarily five things. The first is the Internet of Things. The second pillar is on the security side. The third piece which we have focusing on now is multi-cloud. The fourth pillar of our technology focus in term of how do we make sure that all the technology we build is giving data insights to the customer which will help them take better decisions. And, the fifth is making life easier for employees, which means you can work here or you can work from home and you can be equally efficient whether you are in the boundary of the office or you are outside.

How do you deal with a partner ecosystem especially when the company is undergoing this transition phase?

We always had a very transparent communication channel with our partners through all the transition we have made. We have bought many companies to successfully build our business through acquisitions, so our channel and our partners always had to learn some new thing. We bought over 200 companies and every company has brought a new technology to Cisco. Cisco partners know that Cisco does not stay quiet for too long and they have this relearning capability in their genes, and that I think is the reason for the longevity that we enjoy with many partners.

Is there any specific program that has been designed for this transition phase?

Yes. We're building a lot of toolkits internally which are given to partners. This is to ensure that they have the necessary tool kits to make sure that they go armed to the customer with the right level of data about our installed base. We are also doing a lot of enablement. We have an internal team called 'Customer Success', which is focused on conversation with our customers about taking the shift towards more adoption. Our sales team focuses only on the partners to



advise them on how to make this shift with Cisco.

At our global partner summit, we announced two programs .The first is; Migrate to Digital as a program. We are also advising partners on what service lines can be built on top of technology that Cisco is providing that actually allows for creation of more value added services. We have also now made a new announcement for digital system integrators which essentially allow partners to participate in projects which are outcome based for customers and need not necessarily be resale partners.

Are you also looking to engage with more specialized partners beyond your traditional ones?

Absolutely, we have already done that. We had to do that because when we re-entered security about 4 years ago in a meaningful way was that the partner eco-system that did the security business was not the part of our ecosystem that was doing traditional networking portfolio business for Cisco. We have specialised partners who are very focused in one particular technology. We have IoT partners and also partners focused on the OT side. We will continue to augment and broaden our partner base.

> “OUR ‘CUSTOMER SUCCESS’ TEAM IS FOCUSED ON CONVERSATION WITH THE CUSTOMERS ABOUT TAKING THE SHIFT TOWARDS MORE ADOPTION

Any message for your existing or prospective partners

Cisco has always has been and always will be partner focused. We are very focused on our partners; we are very focused on the go to market push through the channel. We will be at the cutting edge of technology and will give our partners plenty to play with in terms of technology. We will create markets which we can jointly monetize. We will provide relevance in the digital world for partners. Growth and sustainability is something that is a promise from Cisco to its partner ecosystem.

"ONE OF THE MAJOR DIFFERENTIATORS WHICH WE BRING TO THE CUSTOMER IS INTEGRATION"

Symantec is looking to transition into a much more bigger enterprise security player with huge investments in R&D and a series of acquisitions. **Ganesan Arumugam**, Director - Partner Sales Symantec India, shares with CRN's Rachana Jha, on how his firm is looking at channel partners to help the company achieve its key objectives

Where do you see Symantec moving into, in terms of the market, technology, environment and, innovations?

We have transitioned in a bigger way into the security portfolio in the past three years. We spin off information protection as separate company and sold it. So Symantec became a completely 100% security focused company. Since then, we have increased our investments in R&D and added new products and did new acquisitions. In the last two years we have done a lot of things. We acquired Blue Coat Systems which is on the enterprise software side. We brought in the network security portfolio and DLP which is information protection.

On the consumer side we bought LifeLock. This firm is into identity protection for the consumer, so that's a big business in terms of devices and other stuff. We also added SkyCube which is into mobile security, and Fireglass, which is an agentless isolation solution that eliminates ransomware, malware and phishing threats in real-time. We're the first or the only company which has brought in and integrated these solutions into our stack already. This is why a lot of interesting thing are happening on the product side. Today, we are the largest cyber security software company in the market with a $5 billion turnover. In the one year, we have launched more than ten new products. This is all the result of the R&D and investments which we've done. With the acquisition of Blue Coat and the new products that we've got, we are the only company that can address 80% of an organisation's security needs.

We also have a CASB solution which is a CloudSOC solution which we offer to the customer and this integrates all security applications. This has great significance for DLP as all policies can be applied uniformly.

WE ARE THE LARGEST CYBER SECURITY SOFTWARE COMPANY WITH A $5 BILLION TURNOVER

What sort of initiatives have you taken for your partners?

We have launched our new partner program Secure One a year back. Today, for all the Blue Coat partners or the Symantec partners, it is a single program. The Secure One program offers three things. Firstly, it gives all the information about the partner program and how they can interact with the organisation in terms of opportunity or connecting to the people. Secondly, we have another module called Partner University. This is where all this training is available. Besides the technical data sheets and other information, we have streamlined content in terms of product and given special emphasis on role based training. So today if there is a partner who is going in for DLP, he can go through a 30 minutes training programme and he will understand what the DLP solution is about, how to qualify an opportunity, how to talk about this technology and also what is our product future. This is followed by a quiz and partners can get a certification once they successfully answer all the questions.

Since cloud is going to have an increased focus, are there any special efforts being put to engage with your partners?

It is more of in a transition stage right now. We have brought in some products in to the cloud already. E-mail security as a cloud solution is available. There are partners who have access to our portal. They can directly login the orders and provision cloud services for the customer. In the SEP cloud, we have created a marketplace with our distributor. In India, we have signed up with Ingram and in their Ingram marketplace you will see there is the SEP cloud and partners and customers can go and directly place the order and provision and make use of it. We have tied up with AWS, Azure and recently with Oracle Cloud. All these cloud solutions will be available on their cloud. It is already available on AWS. Gradually, for all the cloud products, we are trying to bring it into the common cloud platform, so that it is available for our customers. There is a great focus and strategy in place to address the cloud market. We have the technology and the products.

What were the key initiatives that have been taken by the company that has created a difference for Symantec especially in India?

India is a very tough market and very price sensitive. Competitive pressures are there, and it is part of our job. One of the major differentiators which we bring in to the customer is integration. At the end of the day, the best technology wins and it is the customer who has the final say on which technology they want to go with and which technology they don't want to go with. I have competition in each and every area which I work in. Each one will have around 10 competitors, but we're present in all the solutions stack and my competition in each stack is different.

From the partner perspective, we come across as a vendor whose partner program is mature, more transparent, and simpler to work with. and if you talk to few partners, then you will notice that they will vouch for it. I am quite sure that none of our competitors have such an extensive partner program.There are only a handful of mature players in the industry that have a clear partner program in place.

> “
> WITH THE ACQUISITION OF BLUE COAT AND THE NEW PRODUCTS THAT WE HAVE GOT, WE ARE THE ONLY COMPANY THAT CAN ADDRESS 80 PERCENT OF AN ORGANISATION'S SECURITY NEEDS
>
> GANESAN ARUMUGAM, DIRECTOR - PARTNER SALES, SYMANTEC INDIA

Any particular message that you want to give it to your existing partners and for those who can be the prospective ones in the future?

I would like partners to stay focused, as it brings in a lot of difference to the business. They should not get distracted by the deals. Besides, they have to be loyal to their customers so they are aware what's all happening at their end.

There is enough market for all of us to play. There are enough dollars that can be earned together. All we need to stay focused.

TREND MICRO BANKS UPON ROOT-CAUSE SOLUTIONS TO ADDRESS MULTIPLE SECURITY PROBLEMS

In an interaction with CRN, **Nilesh Jain**, Vice President – South East Asia and India, Trend Micro, shares about the company's unique market positioning, current security trends environment and focus areas for 2018 and 2019

By **Nivedan Prakash**

How was the year 2017 for Trend Micro?

The year 2017 has been fantastic and we have been growing significantly. Our revenues have been doubling every year. There are multiple factors contributing to this growth. The first factor is that the overall security market is growing, due to rising threats and consumer awareness. There are not many vendors who understand the threat scenario from a holistic point of view. Customers are looking for vendors who can provide solutions today, but also can be long-term partners. Trend Micro fits the bill. The second factor is that we have added a lot of new solutions and products; we are a truly large enterprise security company. In network security, we have strengthened our positioning by acquiring tipping point IVS from HPE, which has made us a dominant player in the anti-APT business – customers today are looking for vendors who can give them anti-APT solutions covering all the entry and exit points. We have also been a leader in hybrid cloud security. A lot of customers are now adopting cloud, and we are well positioned to cater to their needs.

Many customers, particularly in the BFSI, government and pharma sectors, are concerned about their compliances, vulnerability – that's where we have been providing our solutions such as Virtual Patching; we have more than 30 per cent market share in this space. End-point market has also been growing. Earlier there were not many attacks on end-points, but in the last few years, we have seen a lot of sophisticated attacks on end-points, and we have been a leader in providing solutions in this space. We have been able to attract a lot of customers from our competitors as well. Apart from BFSI, government and pharma sectors, IT and ITES is also a major sector.

How much boost has digital migration given to Trend Micro's business in India?

This can be categorized in two parts – government driven initiatives and technology driven initiatives. Government is trying to automate all the processes, digitize all the records. We are participating in numerous such requirements of governments and have been able to see good success. However, more success is yet to come; I am hoping to see sizeable revenue from government-led digital initiatives in the next two years. In the technology-driven digitization, private sector customers are forced to adopt new technologies such as cloud, big data, robotics etc. Any organization not adopting these technologies is left behind. This has given boost to security needs among organizations, and that's where we have seen a good momentum; most of our revenue has come from the technology-led changes in private enterprises.

As an organization, we ourselves have to adopt these new technologies, which we did a long time ago. We have been using cloud since 2004-2005, so we were able to envisage the advantages of cloud. We have also been using big data for many years now. We are also working closely with OEMs to provide solutions. Even in

Machine Learning (ML), we have incorporated our solutions.

How significant has been the role of channel partners in Trend Micro's growth story?

Channel partners are very important. We have a full-fledge channel team. Organisation like ours can't grow 100 per cent year-on-year without the support of channel partners. We have been leveraging channel partners not just for reaching out to customers, but also to make sure that most of our deployments are done by channel partners. We completely understand that channel partners are critical for our growth story. Hundred per cent of revenue is from distributors.

We categorize channel partners based on their specializations. We have multiple products, and over time many specialized channel partners have evolved. For instance, channel partners in the cloud space deal with our hybrid cloud security offerings. Similarly there are partners specializing in network security and end-point security. There's another category of partners – System Integrators (SI) – who specialize in everything such as TCS, Infosys, Wipro. Besides, there are also Tier II partners.

We have over 2500 SMB channel partners. Every quarter we do more than 500 unique transactions with partners. In the enterprise space, we have 40-45 partners in India.

Our expansion plan, in terms of partners, will be based on our product strategy. We are growing rapidly in hybrid cloud security services, network security. We certainly have plans to acquire more partners in the network security space, beyond Tier I cities. We have reached a stage wherein we see hundreds of new customers coming in every year, and we need sufficient partner strength which can cater to this. Apart from Delhi, Mumbai and Bengaluru, we have offices in Chennai, Kolkata, Hyderabad. We are also having plans to have representatives in Chandigarh and Kochi.

“ WE HAVE REACHED A STAGE WHEREIN WE SEE HUNDREDS OF NEW CUSTOMERS COMING IN EVERY YEAR, AND WE NEED SUFFICIENT PARTNER STRENGTH WHICH CAN CATER TO THIS

Do have any channel program in place at your company?

We do have channel programs, but channel program is an evolving thing. We always had deal registration, incentives for sellers. At the end of the day, channel partners and we walk for customers. Wherever there's a change in customer trends and requirements, our channel programs also change. For the last two year, we have been heavily focusing on hybrid cloud security, wherein we have been giving incentives to our channel partners to not just ensure they have a good margin, also earn a good services revenue. We have also been giving incentives to channel partners' sales and technical teams.

In the services part, do you think the role of Managed Security Service Providers (MSSPs) will be crucial?

MSSP partners have different connotations to them. There are partners who manage security and services on behalf of customers, so they might own the assets too. MSSPs are important, but these days most of the customers realize that they can't completely outsource security. Most of the customers who hold critical infrastructure, who are driven by compliances and regulatory boards, would like to have ownership and control over security. We have a good model of hybrid security services wherein customers hold products with them, while still outsourcing a lot to channel partners. We see the world moving more towards hybrid security services.

There is a shortage of skilled professionals in this space. What efforts are put by Trend Micro to build this gap?

Apart from the regular trainings, we have a certification training program wherein many channel partners enrol. We have realized that solving the problem of today doesn't solve the problem of tomorrow. Globally we have created the concept called 'Trend University'. I am working with our global team to set it up in India too. We understand that skill is one of the biggest success factors to customers to protect their security operations.

What is the roadmap for 2018 and ahead?

As long as you keep sensing the change in the customer environment and keep on addressing those requirements, the growth will come. My first priority for the next couple of years is to remain very close to customers from multiple perspectives. For this, we have to recruit the right set of channel partners, train them well and make sure that there's a matrix among channel partners wherein we can evaluate how well our customers are being served. Channel partners who serve the customers well will get incentivised separately.

SONICWALL AIMS TO TAP LARGE ENTERPRISE SEGMENT

With major presence in the SMB space, SonicWall will continue to leverage its stronghold in the mid market, alongside tapping the large enterprise segment. **Wias Issa**, VP and GM - APJ, SonicWall, shares the company's strategy to take the channel partners on this journey

By **Nivedan Prakash**

What's your mandate for the company in this region and how do you see the India market growing vis-a-vis other countries in this region?

India has been the most successful country in terms of business. India continues to be one of the largest investment areas in terms of resources including research and development, engineering, support, sales, sales engineering, marketing. We have resources across the country including major cities such as Mumbai, Bengaluru and Delhi.

Do you see any similarities between Indian and foreign customers in terms of the way they approach security challenges?

In terms of similarities, there are too many products and the security landscape has changed tremendously. Unfortunately, the complexity of the security vendor market has made solving those problems even more difficult. I have observed that members are copying each other in terms of their capabilities. This year in APJ and India specifically, one of my key messages to the market is that SonicWall is not a one dimensional company – this is a misperception we have been facing for the last several years. SonicWall is about tools; we are here to solve real problems, whether it be phishing email, nauseous files, or encrypted communication. Sonicwall is well positioned to be able to provide these solutions.

What are your efforts to reposition the company in the market?

Trust has been gained over time and there are multiple ways to gain that trust. One of the factors behind this is the support that we provide to customer after we sell the solutions and the ongoing innovations. There are already several thousand customers in India alone on SonicWall. My priority to build the brand is making sure that those existing thousands of customers here in India are aware of our other security solutions. Customers are buying security, so they can make sure that their core business can easily operate. We will be focused on ensuring that the market – both customers and channel partners – is aware of Sonicwall's true new identity.

Do your efforts also require realignment of your go-to-market strategy?

We have looked at what segments of the market – such as education, finance or government – are important for us. We have prioritised a number of market segments. The other area is around tha right solutions to present to those specific segments. We had a fairly successful business in the smaller market segments, and now we are focusing aggressively on the higher end of the market. We have around 4,000 global customers. What we don't have is significant presence within these accounts. Thereby, our focus is also on going up market and enterprise, and going horizontally into some of the some of the key verticals. SonicWall primarily has been focusing more on the mid market of SMB customers and now, there will be an enhanced focus on the large accounts. The SMB business is a foundation upon which we will build the enterprise and large enterprise business. The SMB market for us is still critically important, so we will be focusing on both. For a company like SonicWall which started off in the SMB market space, to move up is significantly easier than a company which has been operating a large enterprise – this is an advantage for us.

How are you geared up to address new market requirements emerging from the new threat landscape?

We arguably have the most effective deep packet inspection technology in the market, because we build our technology around that and our ability to decrypt traffic. Today, roughly 68 per cent of all internet traffic is encrypted. For example, a bank looking at almost 70 per cent encrypted traffic, will need to then decrypt to see what's good and what's bad. A lot of companies are operating blindly and the attackers have become savvy. One of our core competencies is around email security solutions; and we recently made a tremendous innovation wherein we are able to integrate our sandboxing technology with our email security solution – this allows us to find unknown threats. We're able to identify unknown threats using that same marketing technology integrated with our email security, which means that when a malicious URL is sent to a specific user via email, we're able to catch that. We also have a strong secure mobile access technology that allows us to protect users outside the corporate network.

In terms of what makes us different, about a year ago, we launched a sandbox technology. Sandboxing itself is not an innovation; sandbox has been around for almost a decade, and we introduced our sandbox in technology about one year ago. It allows us to do real time inspection, sandboxing at the memory level. The problem today is that hackers and designers and purveyors of our have become very sophisticated; they encrypt malicious behaviours. All these expose that for a very short time period anywhere from 10 to 30 seconds at the memory level. We're able to do the inspection at the memory level and in advance of a weaponised exploit.

In terms of large enterprises in India, do you already have some use cases which can become a reference point as you approach more customers?

For the last few years we have been selling solutions and now published our case studies. We have got ourselves across all verticals with good stories. For example, with one of the smart cities, we have closed one of the east side projects. Recently we have closed one deal in the insurance sector.

How critical would be the role of your partner ecosystem to take your success story forward?

We've been around for 25 years we've been a channel-first company for the majority that time period. We're working very closely with some of the largest systems integrators and resellers. Many of our partners are leveraging our deal registration programme. We should do a partnership where SonicWall solutions experts approach the end customers directly, whether it be on the heels of a customer event or some sort of marketing campaign or lead generation event. Then we will have discussions with the customers, identify the systems integrators or partners.

"WE ARE GOING TO TAKE ONE OF THE MAJOR STRATEGIC INITIATIVES TO BUILD OUR BRAND, AS IT IS IMPORTANT FOR PEOPLE TO UNDERSTAND THAT WE ARE A TOTAL SECURITY SOLUTIONS PROVIDER

In your bid to tap large enterprises, will you also look at engaging with more specialised security partners?

Yes, definitely. For example, there are partners who are more security focused. Whereas there are also large partners or systems integrators to do multiple things – security, cloud, data centre services. Also distributors role are crucial because various distributors have inroads or closer alliances with different types of partners.

What would be your key priorities and game-plan for 2018 and ahead?

Today we're having in-depth business discussions with all of our distributors. We're going to take one of the major strategic initiatives to build our brand, as it is important for people to understand that we are a total security solution provider. We are focused on solving real customer problems, in a manner that's not complex to understand. Another area of focus for us around solutions – helping more customers solve the email security challenge. One of the other benefits of our email security solution is that we have three form factor even applying for those customers who continue to maintain their own Microsoft machines environments. We have a virtualised version of that for customers' virtualised environments. We also have a cloud solution for customers who are migrating to Office 365. Moreover we will focus on motivating partners. Our promotions and incentive programmes are not just for distributors, but also our resellers. We want to make sure that the relationship is mutually beneficial and everyone in the sales cycle is being rewarded for their hard work and activity.

AI TAKES CYBER SECURITY TO A NEW LEVEL FOR HDFC BANK

The capabilities of current security technologies coupled with the power of Artificial Intelligence (AI) will take the cyber security preparedness to the next level, says **Sameer Ratolikar**, CISO, HDFC Bank highlighting his bank's AI based Cyber Security Operations Center (CSOC)

Artificial Intelligence is explored for information security because there are questions raised about the effectiveness of the currently available solutions to thwart the attacks which are becoming more sophisticated, innovative and targeted.

AI can complement with the current security solutions and decipher the anomalies, which are non-signature, behaviour and heuristics based. For example, the security logs in the Security Incidents and Events Management (SIEM) can only serve a limited purpose however this data coupled with AI solutions has the potential to detect the anomalies, threats which are sitting latent in the system, waiting for the right time to hit. Another use case can be finding trends on the amount of file uploads on PCs and search for aberrations. AI can also team up with other solutions to bring to the fore any divergence in terms of the times during which the applications are accessed by the employees and how can it be detrimental to the company. AI and ML will achieve objectives, not yet achieved by the current solutions, which are reactive in nature.

AI CAN COMPLEMENT WITH THE CURRENT SECURITY TECHNOLOGIES AND DECIPHER THE ANOMALIES, WHICH ARE NON-SIGNATURE, BEHAVIOUR AND HEURISTICS BASED

HDFC Bank has completed a pilot for AI based Cyber Security Operations Centre (CSOC) and soon, the bank will go live. The log data from CSOC is put for processing on the AI solution having big data capabilities and it was done for about eight months on a cloud platform. The bank has close to 100,000 employees. The AI solution will help in monitoring insider threats. The aforementioned anomalies were successfully found using the AI platform during the pilot.

AI has deep learning (DL), self learning and machine learning (ML) as major components. There are well established algorithms in each of these areas. One team will manage the CSOC and the second team will focus efforts for threat hunting by writing rules for machine learning. The bank will have 70-80 per cent contribution from the vendors and close to 20 percent from the internal teams. CSOC is a combination of SOC, threat hunting, breach readiness teams, threat aggregation platforms, red teaming, etc.

"Dark web monitoring is a part of the overall security. We are working on dark web solutions, like real-time defacement and vulnerability monitoring. The solution should have features like early detection of malware presence; in case any data is available for sale in the dark web, how soon are we able to know about it," states Ratolikar.

The economics of security

CISOs will have to balance the budgets to focus only on their crown jewels. The company's residual risk and cyber risk tolerance level will have to be identified. However, that said, banks are a regulated entity. The relationship with the customer is heavily based on trust. Thus there is consensus among the bank CISO community that the reputation risk is also equally important. As a result, even the risk tolerance levels have to be continuously tightened.

The investment in cyber security is determined by the risk management principles. Proper controls are put in place after doing regular threat and risk assessment exercises. Adequate investments should be made based on the kind of threats and risks faced by the organisations. If required, heavy budget allocations must be made. Cyber security is a business risk and it has found its place in boardroom discussions too. The importance given to cyber security in banks is way ahead than in any other Industry. "We have also found companies paying ransom when their crown jewels are locked by a ransomware. But there is no certainty that the data will be released after the ransom is paid. Neither is there any assurance that the systems will not be attacked again," mentions Ratolikar.

QUESTIONS ASKED ON CYBER SECURITY IN BOARDROOM DISCUSSIONS

- What is the cyber security preparedness to counter ransomware and from other emerging threat vectors?
- What if we would have been attacked with a threat similar to the one faced by a MNC this year ?
- What would have been our preparedness ?
- The impact on us, the extent of damage faced ?
- What would have been our strategy to mitigate and come back strongly after the attack?
- Questions pertaining to IT security budgets are also asked. If at all, what is the scope to enhance the IT security budget to safeguard the crown jewels ?
- Which are the vulnerable areas which can potentially be attacked and is there enough visibility on those areas ?

Importance of cyber security framework

The concept of perimeter security has collapsed with the onset of API banking. For payment enablement, banks have to talk to government agencies, payment aggregators, corporates etc. When banks are interfacing with hundreds of third parties, the idea of perimeter has vanished. Banks should have an ideal cyber security framework.

The HDFC bank's approach is to have a four point- Prevent, Detect, Respond and Recover framework. To have multiple preventive controls that covers the entire ground in terms of the channels through which the customer is served or the bank operates internally or with the third parties. Deception technology is an upcoming space in the detection piece. It's a honeypot created for the hacker. The technology serves the purpose of knowing well in advance about who is trying to target the information infrastructure of a particular organisation, and how it's done. For example, create a honeypot for credit card and debit card numbers. This way, the potential hacker is lured to hack the duplicate card registry. The system triggers an alarm after the hacker attempts to get the information, which actually is not a genuine database but a honeypot. After the detection comes the response. There are enough systems in place to quarantine the attack and invoke the DR, in order to mitigate the damage.

Too much focus on prevention is unfruitful because there will always be functions that will have residual risk for e.g. USBs used for cheque truncation is a risk. There are chances of malware getting infiltrated through them, given that there are thousands of employees. Even if a single employee clicks on the infected mail, the network can get affected, through open shares, privilege escalations, with the threat vector, which can be an APT attack, ransomware, etc. This can affect the crown jewels too.

The last part is recover, which majorly deals with DR and BC, where the Recovery Time Objective (RTO), Recovery Part Objective (RPO) comes into play. For the crown jewels, there has to be a file, storage based and database backups. This is a part of the recovery strategy, where BCP and DR is an integrated component.Managing security at an ecosystem levelIDRBT, every quarter organises CISO forums, which is well attended by the CISOs from major BFSI institutions. It is developing to be a good platform to share thoughts on the challenges faced, and the developing threat vector scenario. This apart, there are various informal forums, where selected CISOs meet to exchange thoughts on the impending issues. The CISOs also get multiple advisories and presentations from IDRBT. A consortium of banks can come together and leverage machine learning for information security. The decision whether to join such a consortium depends upon the priorities of each bank.

KTMD – AN ENTERPRISE STRATEGY FOR SECURE DIGITAL TRANSFORMATION AND BUSINESS CONTINUITY

Kaspersky Lab has launched a new solution targeting the enterprise customers – Kaspersky Threat Management & Defense – that protects against advanced threats by bringing together and reinforcing the capabilities of Kaspersky Anti Targeted Attack, Kaspersky Cybersecurity Services and the new Kaspersky Endpoint Detection and Response. This solution is Kaspersky Lab's response to the rise of advanced attacks & complex threats.

On the sidelines of this launch, Shrenik Bhayani, General Manager, South Asia, Kaspersky Lab, says, "Any enterprise organization concerned with advanced threat protection can benefit from Kaspersky Threat Management and Defense. It is especially relevant for financial and government industries with strict regulatory and data protection requirements."

The uniqueness of this solution is that it combines the multiple threat protection capabilities companies are looking for: advanced threat discovery & protection (with Kaspersky Anti Targeted Attack), incident response (with Kaspersky EDR) and outsourced management of targeted attack detection and incident recovery (Kaspersky Managed Protection, Incident Response services).

The innovative protection technologies that are available as part of Kaspersky Threat Management and Defense includes the following:

- Industry-leading and proven malware pre-filtering technologies, which block malicious payloads even before execution;

- Centralized event aggregation from endpoints for instant access and initial analysis;
- Process activity visualization and detailed analysis of suspicious object actions in the operating system;
- Use of a comprehensive set of technologies for the detection of previously unknown threats and targeted attacks, such as a sandbox and data correlation engine;
- Ability to react to threats, including the prevention of attack propagation in the network by denying execution of harmful objects;
- Vendor-provided services, including security awareness training, incident response, an expert-level threat data feed and indicators of compromise related to specific customer needs.

"It's hard to find the same scale of comprehensive, full-circle protection against advanced threats. All of this makes the offering unique in the current market," adds Bhayani.

He further states, "We see the growing trend and need for further integration of threat intelligence solutions aimed at stopping advanced attacks on businesses. Our long-term goal is to develop an umbrella solution that will allow cybersecurity officers to benefit from an integrated interface with access to Kaspersky Lab solutions and external advanced threat protection."

Meanwhile, the customers interested in extending Kaspersky Anti Targeted Attack capabilities should reach out to local Kaspersky Lab partners. Beginning with the launch of Kaspersky Anti Targeted Attack, the company has been offering complex solutions against advanced threats. The Kaspersky Endpoint Detection and Response solution is another pillar complementing this approach. Hence, the Kaspersky Threat Management and Defense solution performs best as a single platform, allowing for unified administration and automation of the whole threat management cycle, but is also available as three standalone solutions (Kaspersky Anti Targeted Attack, Kaspersky EDR and Kaspersky Cybersecurity Services).

Giving an overview of the pricing that would be offered to the customers, Bhayani comments, "The price of our solution depends on many factors, including the specifics of a client's infrastructure, network topology, the amount of information to be processed and packaging of the solution together with Kaspersky Cybersecurity Services. We are confident that our solution, despite being a premium one, provides significant value and is priced competitively."

CHANNEL DIRECTIONS 2018:

A PLATFORM WHERE BUSINESS HONCHOS SEE OPPORTUNITIES

CRN Channel Directions 2018, a two-day mega event organised by CRN India, was held on March 16 and 17, 2018 at Airport Novotel, Hyderabad. The event was planned to stage the different vendors who announced their channel plans and strategies that would, in turn, set directions for the channel community for this year. The conference also witnessed active participation from the country's most influential solution providers as well as new age partners from tier II and III cities. The first print edition of CRN India, a monthly magazine, was also unveiled on the occasion.

PUBLIC CLOUD IS A KEY ENABLER OF DIGITAL TRANSFORMATION

Shalin Patel, Partner Sales Head, VMware India

In his session, Shalin Patel spoke about ‘accelerating digital business transformation’. He stated how digital transformation is all about creating new possibilities for businesses. He said, “We need to innovate constantly, give better customer experience to ensure that they stay connected with you – give them the experience which does not allow then to move. That is how you constantly create new customer base, and reach out to them with innovative ways. Customers are looking at three business outcomes whenever they look at any digital transformation journey – business agility and innovation, exceptional mobile experiences and protection of brand and customer trust. We all face cyber threats today. The infrastructure is not safe. It’s all about ensuring that the infrastructure is protected. Application and data is protected so that the brand is not compromised.”

Patel informed that VMware focuses on four IT strategies which help customers in terms of solution delivered. The company helps its customers in modernising their data centres, integrating public clouds, empowering digital workspaces and transforming security.

“Public cloud is a key enabler of digital transformation. Sixty-seven per cent of VMware’s enterprise customers rely on multiple clouds. In India, VMware does 95 per cent of its business through partners. We are a completely partner driven organisation Besides, we have more than 20,000 transacting partners who do business per quarter, over 1,100 technology partners, and more than 4,000 service providers connected with us,” added Patel.

CHANNEL DIRECTIONS 2018
16 - 17 MARCH | NOVOTEL, HYDERABAD

8.5 BILLION IT SPEND EXPECTED IN 2018

Srikanth RP, Editor, Express Computer and CRN

Srikanth RP provided an overview of the Indian IT industry. He discussed some of the research based facts and figures which indicated that India's IT industry is projected to grow from 9.2 per cent to 87.1 billion in 2018, up from 79.7 billion. The public cloud service in India is spread to grow about 2.6 billion.

He mentioned that government is a huge IT spender and also spoke about IT expenditure in 2018. US$ 8.5 billion IT expend is expected in 2018 with increase of 8.9 per cent. IT services happen to be one of the biggest chunk where channel partners can play big role. Srikanth said, "BFSI, manufacturing, telecom, and retail are the expected major verticals from spending perspective."

From spending perspective cyber security tops the list. Apart from that cloud computing is also one of the top priorities. Srikanth also spoke about the huge opportunities in the market and how technology is making them better and easier to use. He added, "Hybrid cloud deployment is a big opportunity because a lot of SMBs want to transition to the cloud.Partners can step in and educate them more on the benefits."

BUSINESSES DEMAND A BETTER OUTCOME

Devendra Taneja, Director, PC Solutions

Devendra Taneja explained the need why the channel industry has to re-invent itself in the digital age. Businesses today demand a better outcome; businesses are changing rapidly and getting a digital makeover. Taneja said, "Channel ecosystem is left with no choice and had to re-invent itself. Technologies like AI, IoT, and Blockchain have been part of the business today. If you want to do well in terms of customers, you need to go digital. All the parameters of business have changed. Connectivity and cloud are transforming the way IT has been consumed or being consumed and places where IT is being deployed. The needs of conventional business and new business are absolutely 180-degree. The power and cost of consumption of cloud is reducing.

He added, "Today any idea idea which works well can give it a fly. Today canvas is absolutely clear – your imagination, engagement with customers, and your ability will give you plenty of opportunities to create your own jackpot. Unlike conventional IT in the new there are no established player and no boundary set. Your imagination can be your new idea. You have to have different mindsets who know how to engage with the customer for solution selling; and, you have to be sensitive to the customers need."

CUSTOMER EXPERIENCE IS THE TOP PRIORITY

Ranjan Chopra, Managing Director, Team Computers

Ranjan Chopra shedded light on building business models around next-gen technologies. He said, "Providing a great customer experience is our top priority. We build and maintain IT infrastructure, applications, and analytics. We understand your needs – identify, integrate and support high quality and cost optimised IT Solutions. We must know the customer's need and address them. We make your business intelligent and future-proof."

Speaking about uberisation, Chopra said, "If we don't do our business, someone else is going to do it. How do we uberise our own business is important. Innovation, thinking, imagining and re-imaging are important factors for building business models. We must know how to imagine and re-imagine things. We must be able to spot the trends and market opportunities early. This can be an important reason for our growth. We must focus on sales and delivery teams which can enable us to grow our business. This strategy can help us to understand our customer needs better and quickly and grow much faster against the competition."

HOW CAN PARTNERS CAPITALISE ON DIGITAL TECHNOLOGIES

An insightful panel discussion witnessed participation from industry experts such as Jayantha Prabhu, Group CIO, Essar Group & Business Head-Inda, AGC Networks; Hiren Shah, Head – Technology, Reliance General Insuranc; Ishaq Quadri, Consultant Hospital CIO and Secretary, HIMSS India; RS Shanbhag, CMD, Valuepoint Group; Nitin Shah, CMD, Allied Digital; Nityanand Shetty, MD, Essen Vision; and Shrenik Bhayani, GM, Kaspersky Lab (South Asia).

According to Nitin Shah, internal information is important before you start with your customer. "

Quadri added, "Choosing the right digital strategy can lead change through the organisation. I would look at whether a particular company or SI has the passion and understanding.

Prabhu further stated, "In today's world, innovation and digital are major traits for large scale businesses. The way we evaluate technology has also changed in today's world – every CIO is now connected on social media, where they discuss about channels. For technology finalisation, there's no requirement of meeting with OEMs, because everybody can access content on the internet. Additionally, support and OEM backing is equally crucial. Today, we don't buy technologies in pieces, we have a detailed roadmap planned for digital transformation. "

Shanbhag informed, "In terms of the digital world, we have been diversifying in many ways. In one of my recent meeting, the entire conversation was changed when I brought in the AI piece for L1 and L2 support."

Shetty stated, "The moment you use the word 'partner', the trust factor also comes along. We should be made part of their yearly planning. Most the time at organisations, the discussions happen with the vendors and partners remain in the background. We need to guide an organisation on IT that will lead to business benefits as well."

Shah added, "We deal with multiple technology partners, and we do have a checklist, but checklists don't result in a full-proof solution. When we look for partners, irrespective of the size, we look for the teams – this is important for day-to-day projects and long term as well.

DIGITAL FORENSIC IS GROWING RAPIDLY

Alok Gupta, Founder & CEO, Pyramid Cyber Security & Forensic

Alok Gupta showcased 'Forensic- a new tech opportunity for solution providers'. He said, "This is the area where we see a lot of opportunities. Crime – whether it is conventional or internet driven – has some sort of digital element in it. Fraud is invented every day and people are using digital medium to do it and hence, Digital Forensic is growing rapidly. Another big emerging area is the Cloud Forensics.."

Mentioning the importance of forensic in today's world, Gupta stated. "Forensic can add great value to your businesses. Digital Forensic is a space where you can make a lot of money. This is more like an emergency situation or on-demand situation. One can establish cyber crime investigation centres, digital forensic labs and cyber intelligence centre, government and law enforcement agencies by providing solution and services involving design, consulting tools, software integration, implementation and capacity building. Apart from this, they can assist in solving insider frauds, intellectual property thefts, and financial and white collar crimes and more using digital forensic and incident response services. Moreover, one can develop products and tools and sell globally and provide forensic as a service."

HOW ENTERPRISES CAN BENEFIT FROM KTMD SOLUTION

Shrenik Bhayani, General Manager, Kaspersky Lab (South Asia)

CRN also introduced a platform called 'LaunchPad', where vendors as well as partners get an opportunity to showcase their new offerings such as products and solutions to the market. At the conference, Kaspersky Lab chose to leverage this platform and unveiled its new offering 'KTMD' (Kaspersky Threat Management and Defense Solution). Shrenik Bhayani took this opportunity and explained how KTMD can be beneficial to the enterprises. He said, "KTMD is our answer to cyber security risk mitigation in an era of digital transformation. We have launched the ATP and we have EDR and have packages of cyber security service around it. From 1986 to 2006, the number of malwares in the market is close to one million; three lakh ten thousand malwares are getting detected per day. As we move further into the digital journey, everything is prone to attacks. Cyber security costs around $ 450 billion per year. Systems need to be safe, secured and immune by design. You need to protect your platform. You need to protect your architecture and the application."

In addition to Kaspersky's offerings, Bhayani said, "Anything to do around security, we can bring on our values in terms of our products and in terms of services. We offer cyber security trainings. We have an online and offline module. The offline module is about engaging the employees by playing the games – they get a lot of awareness through this. It's a unique way of bringing the awareness. There is security training which we do for the customers in terms of how you respond to an incident and how do you manage this incident. Crimes will happen; what is important is how fast you detect it and how fast you can respond to it. We can do active hunting, and we can do penetration testing and forensic. If you are interested in building your skill sets, we can help you build the skill set."

SPEND 80 PERCENT OF THE VALUABLE TIME ON PLANNING

KV Jagannath, Managing Director, Choice Solutions

KV Jagannath spoke about 'Negotiating to success-the right way!' He said, "Negotiation power comes from alternatives. Most of the people come to the negotiation table without alternatives. Confidence comes from planning for negotiation. Spend 80 per cent time on planning and the rest for smooth execution. Without preparation, you will fail in any negotiation. Planning and preparation are the crucial steps to success. Identify your key goals, brainstorm your options and plan your open move. Negotiators must move past positions and focus on interests to achieve their goals. People's demand may be incompatible or at least complementary."

Jangannath also discussed the importance of relationship with clients. He explained that we do get little overboard with our client relationships at times. "Make sure you keep a little distance in client relationship, especially in places where you may have to negotiate on periodic basis. Relationships should be in such a way that even if we do not take position, we still get to know their interests well. Power, perception of trust, perception of fairness are the elements of negotiation. Value creation happens with collaboration. The primary focus should be on increasing the overall pie and similarities between two people also helps. Personality affects nine per cent of negotiations. Gender negotiations is another important factor. One must know the need to capitalise. It is the ability to influence, it is about the command over language, and it is about the knowledge – gained and shared."

HOW CAN CHANNEL PARTNERS COMPETE IN A DIGITAL WORLD

Sanchit Vir Gogia, Chief Analyst, Founder and CEO, Greyhound Research

The session was loaded with cases studies which provided interesting insights on the day-to-day business challenges of CIOs and CMOs, and how channel partners can leverage these data-points by building new capabilities for emerging technologies such as Blockchain, IoT, AI, and Machine Learning. Gogia said, "With more and more customer services going digital for organisations – be it banks, retail, automobile companies – the role of channel partners gets more crucial as these companies' major focus is on enhancing the customer experience, not the technology. Today majority of the channel partners are so focused on technology and they leave aside customer experience."

The key highlight of the session was the insights about how the 1:1:1 model and startups are disrupting the business of the traditional set of large companies and their changing IT needs.Today, CIOs are looking for solutions where they can monetise the data points; every single year, they generate so the marketing teams can compete with the startups." He also sensitised channel partners on how, within the channel, new age IT startups are emerging and trying to penetrate into traditional channel partners' existing business, customers base and opportunities.

Quoting a recent study conducted by Greyhound, Gogia highlighted, "There are 300 channel partners in India, having a one-man-show, one product and making one million dollars every year; $300 million is being made by these new-age partners and it is a missed opportunity for the channel partners." Gogia urged partners to move away from a traditional mindset to consultation-led sales approach, learning lean management practices and actively getting leads from social media. In his statement, he said, "Marketing is the weakest link in the channel partner's journey. You can't transform for tomorrow on today's date using yesterday's mindset."

INSUR-TECH: A GOLDMINE FOR PARTNERS

Hiren Shah, Head – Technology, Reliance General Insurance

The year 2018 will be that of digital insurance, as customers are increasingly adopting new technologies in their daily lives and with that, expect new business opportunities, highlighted Hiren Shah, Head – Technology, Reliance General Insurance. Presenting a customer's perspective of the macro view from a CIO's standpoint, he strongly urged the audience to start tapping insur-tech as an emerging business opportunity.

Insur-tech and digital insurance products not only increase customers and business satisfaction, but are also more flexible, adaptable and provide a vastly faster time-to-market. Modular product development provides the ability to focus on those parts of the insurance value chain where one can generate most business and let the infrastructure and core backend systems be outsourced as Insurance as a Platform (IaaP) by those who see their core offering in that space.

Talking about the areas where partners can play a role of digital advisor and consultant, he said, "There is an obvious opportunity for online portals and e-commerce players. Digital brokers and traditional insurers are also looking to collaborate with insur-tech in order to stay ahead of the rapidly evolving ecosystem."

Talking about the current trends in the insurance sector, Shah explained, "Traditionally insurance covers the risk, but at Reliance, we are focused on risk mitigation. Technology integration plays an important role in driving this change and make a faster delivery. All these trends open up new business growth for a technology partner. Interestingly, Google is keen on the insurance business. There are many e-commerce players who have shifted to the insurance business. For example, e-commerce giant Alibaba sells eight million pocket insurance policies in a day and each policy has one-day and one-hour validity."

MAKING VDI MORE ATTRACTIVE TO PARTNERS

Mohan Bhat, Co-founder and MD, Accops Systems

Virtual Desktop Infrastructure (VDI) is an emerging concept across industries, Bhat pointed out. Talking about the concept and solutions offering of Accops on VDI, he said, "Workspace virtualisation and having remote access to business data anytime, anywhere and on any device, is the need of the hour. In addition, keeping data secure at an affordable cost is the biggest challenge faced by most of the companies, especially in the mid-market segment. Accops, a one-stop shop for workspace virtualization, understands this growing sentiment and brings together the performance, management, and functionality essential for enterprise remote access together."

Virtual desktop infrastructure assures a strong business opportunity for Accops' channel partner in the ecosystem. The company has enabled organisations to get faster RoI from VDI projects by integrating all required functions into a single product suite.

He further stated, "Accops' customer sees 50 per cent reduced TCO compared to other leading products. VDI sees a bigger scope for companies who are looking at digital transformation and cyber security at the most."

BUILDING TECHNICAL COMPETENCIES

Prabhat Kumar Sinha, Director, Astric Group

In order to drive a winning digital roadmap, the need of the hour is to figure out a successful digital strategy and building technical competencies to meet this change. Astric Group is among the first IT companies from Bihar which has been building capabilities and driving technological advancement in the state. Sinha believes in building the right competency approach to management and leadership. Sinha said, "If you are ready to help a customer, get it right; technology will automatically happen, so don't think about technology, think transformation," while emphasising on the need for people to realise that deep learning and AI can create many new jobs for people in the IT space.

He added that the GST is also going to provide a huge amount of business intelligence, analytics, and dashboards. This gives an idea about the sheer volumes of data that the GSTN will be creating, and subsequently, the IT support and partners enablement will be the core of this change.

DIGITAL TRANSFORMATION WITH MODERN WORKPLACE SOLUTIONS

Suresh Ramani, CEO, Tech Gyan

Suresh Ramani, CEO, Tech Gyan, in his session, stated, "We have transformed from typical system integrator four years ago, and become a focused solution provider for Microsoft. We strive to improve the productivity of each individual and team. The thumb rule for digital transformation success is a cultural change and cloud technology is the heart of this," said Ramani.

He encouraged partners to start embracing this digital change without creating a new team of app developers. "In the next few years, reduction will happen in the way traditional IT works. Device, identity, and data management are the big areas in which traditional partners can enter. You have got an established customer and now the time has come to co-work with the born-on-the-cloud partners. In the west region, we are focusing on the collaborations and leveraging each other's skilled capabilities. Digital transformation can't be done alone; partnering and building new capabilities can make a lot of difference for a large section of old and new partners."

LESSONS FROM MY ENTREPRENEURIAL JOURNEY

Alok Gupta, MD, Unistal Systems

When an entrepreneur embarks on a journey, it is natural to have larger-than-life ambitions. With new age companies like Flipkart and Ola Cab lapping up hundreds of millions of dollars, one imagines his 24-year-long entrepreneurial journey to be nothing less spectacular. Sharing the same experience, Delhi based Alok Gupta narrated his lessons from his entrepreneurial journey – before the established or budding IT companies.

Unistal was among the pioneers when data recovery business was taking off in India. "We were among the few players in this domain, our first billing number 0001 was to the PMO. Till today the PMO has been our customer for our data recovery and data wiping services and softwares. We receive year-on-year appreciation from NIC," commented Gupta.

Gupta got a major breakthrough when the company developed a crash-proof product for two leading Indian PC makers Wipro and HCL. The excitement of winning our first big project worth ` 5 lakh from the erstwhile PC maker makes me feel good still, informed Gupta.

The first thing that I learned about entrepreneurship was that it is actually the first step that is the hardest – taking that leap of faith, to quit whatever else that you are doing, and to dive into this world of uncertainty. I learned that a successful venture requires 100 per cent attention, focus, and effort. Secondly, ventures need a full-time manager or else they'll just distract you and derail your existing efforts if you aren't careful.

For Unistal, the another milestone for the company was when it entered into the oil and gas business. Gupta recalled that before becoming a product company from a channel partner to distributor of data recovery solution, Unistal capitalised on each and every opportunities which came its way. From these experiences, I learned that doing something you are passionate about outside the bounds of a traditional job can lead to more stability. You will be the one to ensure your own success and your team," he concluded.

TECH CAN HELP WOMEN 'LEAPFROG' MEN IN THE WORKPLACE

Nazmeen Ansari, CEO, Matrix3D Infocom

Amidst difficult economic circumstances and a job market where the participation of male workers is considerably higher than their female counterparts, Indian women are taking new steps in the technology sector, an area dominated by men, informs Nazmeen Ansari, CEO, Matrix3D Infocom. Breaking the glass ceiling hasn't been easy for women leaders in IT. There has been an increase in the hiring of women leader in the middle order. However, the top jobs are still secured mostly by men, she expressed during her session.

While quoting the International Labour Association report, she highlighted, "Still 51 per cent of the women are doing entry-level jobs. We have to help give women skills they will need to be successful at work, and to work with men in companies to help them advocate for women and be good allies.

Ansari said, "If we combine the best of the global technology industry with the ingenuity and resourcefulness of women on the ground to solve the digital divide challenge, we can unlock a colossal wave of human potential and freedom for future generations. Women need empowerment over protection. We need to understand and make others understand that 'digital' is not just a tool, but a means to bring about social, attitudinal, behavioural and cognitive changes. Nothing impacts a company more than the role of its women."

MAXIMISING THE VALUE OF TECH INVESTMENTS

KrishnaRaj Sharma, Director& CEO, iValue solutions

KrishnaRaj Sharma presented how technology start-ups are disrupting markets. Brands like Ola, Uber and many more have used technology as the heart of their business and seen success. Their success makes for a strong case to evaluate the use of technology intrinsic to one's business model to reach important business milestones. Companies, therefore, have to be ready to completely reinvent themselves before the technology changes end up overwhelming them. The core message of his session was to compel partner to keep moving beyond conventional tactics to reshape, rethink and re-imagine business models and use technology as a market disruptive force if you want to stay ahead of the game or rather stay relevant in the game at all.

ACCELERATING DIGITAL TRANSFORMATION THROUGH DMS

Prachi Bhatnagar, GM, NetSpider Infotech India

The session focused on the document management systems (DMS) and how NetSpider is winning large government projects like Bombay Municipal Corporation and Banaras Hindu University and playing a catalyst role in scanning and documents digitisation. Bhatnagar further explained that the NetSpider team is looking for partners and her team is designed to help customers exploit the power of document management to enhance their customer experiences, develop new digital products, deliver seamless services, and improve core operations.

NetSpider aims to partner with customers to transform their traditional infrastructure with the flexibility of the DMS, and maximise the value of connected devices. The company has made investments in simplifying DMS and enhancing intelligence at the edge to enhance the IT experience for customers.

In conclusion, Bhatnagar said, "As digital transformation is exploding, businesses must evaluate what it means for them. Businesses will either become proficient in digital transformation or will fail and struggle to survive."

DEMYSTIFYING THE SECURITY LANDSCAPE

NK Mehta, CEO& MD, Secure Network Solutions India

The session was centred around the changing cyber security landscape and newer opportunities for channel partners. Mehta talked about the significance of building new capabilities so to that partners can act as a security advisor. Sharing his thoughts on this significant topic, Mehta presented a comprehensive view on how the learning curve in IT security is getting shorter. "We don't expect customers to build a security team. As a channel partner, we build our skills, leave the security to us and we need to build this trust," said Mehta.

Citing this, Mehta urged partners to focus on building the skillsets. He also asked partners to understand what is forcing companies to invest in cyber security.

"Earlier selling cyber security solutions to the customers was a tough task and used to see security as a dead investment but now there are awareness, as they know the cost associated recreating the data in case of any data breach. We see cybersecurity as one of the technologies to stay in demand for a next decade," added Mehta.

RNI Title code NO. MAHENG/14221