TECHPLUS MEDIA Publication

ITPV

Connecting with Solution Provider in
EMERGING MARKET

■ Northern ■ Eastern ■ Maharashtra ■ Gujarat ■ MP & Chattisgarh ■ North East ■ Southern ■ UP & Uttarakhand ■ Bihar & Jharkhand

Covid Revolution in Cyber Security

Indranil Chatterjee
General Manager, Security & Compliance,
Jio Platforms

Sudeep Das
Technical Leader, IBM Security Systems,
IBM India/South Asia

Sonit Jain
CEO, GajShield Infotech

Ripu Bajwa
Director and General Manager,
Data Protection Solutions, Dell Technologies

Mathivanan Venkatachalam
Vice President, ManageEngine

Sunil Sharma
Managing Director, Sales,
Sophos India & Saarc

Ujwal Ratra
Chief Operating Officer,
Astra Security

IN CONVERSATION

AMJ 2020 was the Biggest Quarter for Palo Alto Globally

Harpreet Bhatia
Director, Channels & Strategic Alliances,
India & Saarc, Palo Alto

IBM to Expand Ecosystem to Engage Non-Traditional Partners

Lata Singh
Director, Partner Ecosystem,
IBM India and South Asia

SOLUTION SHOWCASE

HR Processes get Intelligent, Artificially

Dr. Gaurav Hirey
Founder & CEO, GoEvals

Focusing on Surveillance, Robotics and Autonomous Computing

Krishna Rangasayee
CEO & Founder, Sima.ai

Amit Kumar Mitra
Sr. Director, SiMa.ai

Sudershan Vuruputoor
Site Lead, SiMa.ai

TECHPLUS MEDIA

Tech Data | DELL Technologies AUTHORIZED DISTRIBUTOR

F1 INFOTECH PVT. LTD.

POWEREDGE R840 SERVER

Turbocharge customer data analytics and drive faster insights.

Say hello to the latest generation of Dell EMC PowerEdge, designed and built specifically to drive faster insights from data-intensive and data analytical workloads. Providing the ideal platform for organisation using HPC and in telecommunications, finance, industry, security and public services, the R840 delivers consistent high performance across business-critical applications.

The R840 is part of a complete portfolio of Dell EMC PowerEdge servers and is powered by 2nd Generation Intel® Xeon® Scalable processors with Intel® Optane™ DC persistent memory. Take back control of the IT lifecycle with intelligent automation and stay protected with integrated security.

The PowerEdge R840 enables your customers to:

- Take advantage of four-socket performance in a dense 2U design
- Minimize latency with up to 24 direct-attached NVMe drives
- Scale capacity and performance with up to 26 2.5” HDDs and SSDs, 62%* more than the previous generation
- Accelerate applications with up to 2 double width GPUs or up to 2 FPGAs
- Drive workload consolidation, dense virtualization and in-memory databases
- Automate maintenance and routine tasks

PowerEdge R840

Boost performance and minimize latency:

- Choose an all-flash configuration with up to 24 direct-attached NVMe drives
- Add up to 12 NVDIMMs of memory

To find out more, please contact us.

Sunil Gupta | sunil@f1infotech.com | +91 98112 68548
Ankur Mehta | Ankur.Mehta@techdata.com | +91 93129 78007

Scan QR Code

SEAGATE

Keep your business's data. Keep your cool.

Skyhawk drives, now with in-house data recovery services.

Rescue
DATA RECOVERY SERVICES
3 YEARS INCLUDED*

*2TB & above

Service available on below mentioned Model Numbers

ST2000VX008,ST2000VX015,ST3000VX009,ST4000VX007,ST4000VX013,ST6000VX001,ST8000VX004,ST10000VE0008, ST8000VE000,ST10000VE0008,ST12000VE0008,ST12000VE0008,ST16000VE000,ST8000VE001,ST12000VE001,ST16000VE002

NOW AVAIL Instant drive replacement at SeaCare+ centres in Chennai, Kolkata, Mumbai and New Delhi.

For sales enquiries, contact: North & East: **Siddharth Singh**– 9891003558. West: **Tanmay Shah** – 9978099666. South: **Kiran Bobby** – 9880948355. **For product related queries, contact: Rahul Seth (Surveillance Lead) - rahul.seth@seagate.com.**

For marketing support, contact: rishi.prasad@seagate.com

Seagate Authorised Distributors: Fortune Marketing Pvt. Ltd. – 011-30890014 • **Prama Hikvision (I) P. Ltd** – 9890218148

LOG YOUR CASES › support2.seagate.com

FREE DRIVE DROP BACK › Call to know more or email to: pickupservice@inspirisys.com

LOCATE SEACARE AT › www.seacare.co.in

TOLL FREE › NO ISD REQUIRED
000.800.440.1392
9AM – 5PM (MON – FRI) INDIA TIME

Download Skyhawk App, share a picture of this advert on Skyhawk App Chat & you can win an exciting gift! | 17

SKYHAWK SURVEILLANCE

SKYHAWK PARTNER APP
CONNECTED ON THE GO.

20,000+ DOWNLOADS
Thank you for your support !!

Download Now
ANDROID APP ON Google play
Download on the App Store

CONTENT

SOLUTION SHOWCASE

HP DNJ T130

24" Printer

HP Thermal Inkjet, HP Color Layering Technology, PhotoREt IV, Up to 2400 x 1200 dpi, Automatic Color Calibration, Automatic Pantone Calibration, Offset simulation and CMYK plus

HP DNJ T530

36" Printer

HP Thermal Inkjet, HP-GL/2, HP-RTL, JPEG, CALS G4, 27 sec/page on A1, 79 A1 prints per hour, Up to 2400 x 1200 optimised dpi,Direct print from mobile apps on Android and Chrome OS

HP DNJ T830

36" Printer

Print, copy, scan HP Thermal Inkjet, Memory 1 GB, Up to 2400 x 1200 optimized dpi, Scan resolution, optical Up to 600 dpi, Windows, HP DesignJet Utility for macOS and Windows

---

For more details Contact: Mr. Chandan Sinha @ 09831781941

TRISITA MARKETING P LTD.

8 Ho Chi Minh Sarani, Harrington Mansion, Ground Floor, Flat 22, Kolkata -700071
Email: chandan.sinha@trisita.com, Web.: www.trisita.com


TECHPLUS Media Publication
itVARnews®
Insights for Next Gen Solution Provider
Presents
6th Future of Work
ISV Summit & Awards 2021
Recognising Tech Disruptors
COMING SOON
REGISTER NOW
SUMMIT HIGHLIGHTS
03+
Knowledge Sessions
100+
Leading ISV
1000+
Attendees
03+
Hours of Networking
TECHPLUS MEDIA

COVID REVOLUTION IN CYBER SECURITY

In 2020 and in 2021 as well, breaches are the digital pandemic proving to be just as insidious and difficult to stop as Covid-19. The pandemic is in fact revolutionizing the cyber security landscape in India as businesses and their customers are forced to take a holistic approach, which has delivered multiple years' worth of transformation in a matter of months. Let's analyse few of the trends that are helping organizations be prepared for all present and future uncertainties

Amit Singh

The year 2020 was the one that everyone would like to forget. From a cyber security perspective too, 2020 was buzzing for all the wrong reasons. While the world was focused on the health and economic threats, cyber criminals were capitalizing on the crisis.

2021 is not much different either. The Union transport ministry recently received an alert from the Indian Computer Emergency Response Team (Cert-IN) regarding targeted intrusion activities directed towards the country's transport sector. This comes after a slew of cyber security attacks on Indian government's domains over the past few months. In February 2021, there were reports of new phishing emails using compromised government accounts to target groups of officials, attempting to lure them into sharing their passwords on a page that mirrored the government's official mail server sign-on website. Earlier in March, American cyber intelligence company Recorded Future said that it uncovered a cyber operation that was focused on India's electricity grid and other critical infrastructure. While the company did not link the power outage in Mumbai to the operation, it did not rule out a link.

These are mere glimpses of the cyber security threat landscape which has become a major scare for businesses and governments, alike. Today's cyber criminals are often well-funded, some even sponsored by rogue government organizations. In addition, stealthy and persistent

attackers now have the skills and tools to do everything from taking down power grids to targeting hospitals and financial institutions with ransomware.

Remote work makes security complex

The threat scenario has got further complex with the higher dependence on cloud and distributed workspaces. "There is a rise in the need to secure endpoints, as multiple access points from multiple locations are connected to a corporate network. However, the lack of security in remote work environments exposes vulnerable devices to potential cyber attacks," elaborates Indranil Chatterjee, General Manager, Security & Compliance, Jio Platforms. "The massive work-from-home directive has upended security professional's responsibilities. In fact, a recent survey of executive decision-makers conducted by Deloitte found: 69 percent executives expect the number and size of cyber events to increase over the next 12 months," he adds.

The increase in remote working calls for a greater focus on cyber security, because of the greater exposure to cyber risk. This is apparent from a recent study which highlights that almost 47 percent of individuals fall for a phishing scam while working at home. In addition, as per NTT's 2020 Intelligent Workplace Report, 76.9 percent of organizations find it more difficult to spot IT security or business risk brought about by distributed working.

Yet, most businesses still struggle with effectively preparing themselves with

NUMBERS SAY IT ALL

- **1** cyber attack in every 11 seconds is predicted in 2021
- **69%** executives expect the number and size of cyber events to increase over the next 12 months
- **47%** of individuals fall for a phishing scam while working at home
- **34%** of data breaches involve internal actors, increasing the risk of data leak by these remote users up to 60%
- **$1000** is the price of patient records, compared to credit card data, which goes for just $12-20 and email addresses at around $100 in bulk
- **76.9%** of organizations find it difficult to spot business risk brought about by distributed working
- **41%** of respondents from India review and test their cyber security incident response plan (CSIRP) only once each year
- **₹ 140** million is the average total cost of a data breach in India in 2020, an increase of 9.4 percent from 2019
- **55%** of executives are planning to ramp up their cyber security spending in 2021
- **51%** of the executives are adding full-time cyber security staff in 2021

cyber security response system. A recent IBM and Ponemon Institute study highlighted that 41 percent of the respondents from India review and test their cyber security incident response plan (CSIRP) only once each year. This is an alarming fact, specifically in the light of the current pandemic since many organizations had to overnight shift to a hybrid work environment leading to many unforeseen risks.

Further, as per IBM's 2020 Cost of Data Breach report, Indian companies witnessed an average of Rs 140 million total cost of a data breach in 2020, an increase of 9.4 percent from 2019. In contrast, companies with fully deployed security automation were able to detect and contain a breach 27 percent faster than those with none. This showcases the importance of technology preparedness, highlights Sudeep Das, Technical Leader, IBM Security Systems, IBM India/South Asia.

In fact, intellectual property will be hackers' next golden ticket. In 2020, we saw a rise in healthcare breaches, likely because patient records often fetch up to $1,000 each. Compared to credit card data, which goes for just $12-20 and email addresses, which average around $100 in bulk, it makes complete financial sense.

> "A recent survey by Deloitte found that 69 percent of executives expect the number and size of cyber events to increase over the next 12 months."
>
> **INDRANIL CHATTERJEE,**
> General Manager, Security & Compliance, Jio Platforms

Enterprises get proactive

The ongoing Covid-19 pandemic has forced the enterprises to adopt a proactive rather than a reactive approach to address the potential security threats. This is bolstered by a recent PwC study which found that 55 percent of executives are planning to ramp up their cyber security spending in 2021 despite the majority of them, 64 percent, expecting business revenues to decline. PwC found that cyber security is more business-critical than ever before. Almost 51 percent of the executives are adding full-time cyber security staff in 2021.

The growing seriousness towards cyber security is pushing the cyber security spending in India. According to a joint study conducted by PwC India and the Data Security Council of India (DSCI) the cyber security market in India is set to grow from USD 1.97 billion in 2019 to USD 3.05 billion by 2022, at a compound annual growth rate (CAGR) of 15.6 percent. The growth rate is nearly 1.5 times the global growth rate of cyber security expenditure.

As per market experts, escalating threats make it clear that regardless of what you do, you cannot protect against everything. All organizations need to plan for allowable levels of vulnerability based on their risk tolerances. Instead of solving a specific problem, enterprises must establish built-in resilience that allows them to adapt, evolve and change their security posture.

The confluence of mobility, cloud, and social networking has multiplied risks across the distributed workforce. These factors call for a new approach to security that's driven by knowledge of threats, assets, and adversaries. One in which security incidents are seen as a critical business risk that may not always be preventable but can be managed to acceptable levels. "We call this model 'Awareness to Action.' This approach comprises of four key precepts: security is now a business imperative; security threats are business risks; the most valuable information must be protected; and all activities and investments should be driven by comprehensive, current information about assets, ecosystem threats, and vulnerabilities," informs Chatterjee.

Customers are now looking for security technologies which can help protect their data, provide end-to-end security across multiple environments, new authentication methods, monitoring services and most importantly re-imagine their

> “Companies with fully-deployed security automation are able to detect and contain a breach 27 percent faster than those with none. This showcases the importance of technology preparedness.”
>
> **SUDEEP DAS,** Technical Leader, IBM Security Systems, IBM India/South Asia

risk assessment. Indeed, few of the trends are helping organizations innovate and be prepared for all present and future uncertainties.

Zero Trust gains currency

With the explosion of cloud computing, adopting Zero Trust approach makes more sense as it assumes no barriers: don't trust anything by default, starting with the network. 'Zero Trust' ensures that critical assets can only be reached by those offering proof positive that they have the credentials, identity, and need to access them.

Developed by Palo Alto Networks' John Kindervag, unlike traditional systems that believe data needs protection from only the players outside of the organisation, Zero Trust model treats all users as potential threats and sets authentication and access restrictions accordingly.

Though the concept of Zero Trust has been around for some time, it gained currency in 2020 due to the perimeter-less approach useful for employees working from different locations.

Organizations are displaying renewed vigour around combining identity, data, network, and device security into a common analysis platform to better deliver security context and build on an organization's Zero-Trust journey. "Companies are realizing that the siloed security programs are not delivering the right level of risk view to them and it is necessary to drive horizontal data analysis across all the security telemetry data that is available for the most critical resources in the organization – people, data and infrastructure," explains Das.

Data, endpoint to stay critical

The regulatory landscape for privacy and data protection is expected to reach a tipping point in 2021, forcing Indian organisations to comply with not only global regulations (like General Data Protection Regulation) but also with the proposed Indian legislation – the Personal Data Protection

> “Over 34 percent of data breaches involve internal actors with financial and non-financial motives, increasing the risk of data leak by these remote users up to 60 percent.”
>
> **SONIT JAIN,** CEO, GajShield Infotech

Bill, 2019 (which was sent to a joint standing committee of the Parliament and is expected to be tabled in the Parliament soon), the Aadhaar Act, 2016, and other such regulations.

Gaining complete visibility and control on each and every piece of information leaving enterprise boundaries will be an important step in their war against cyber-attacks. "We see a newer data security approach being adopted, that keeps data at the centre of all security measures to prevent data exploitation. Security solutions will need to transform their product architectures so that they help enterprises to step up from traditional allow/block binary security approach to a more modern 'Allow But Monitor' approach, considering the increase in work from home setup using collaborative business, cloud and SaaS applications. This is possible only if they have deeper data context visibility to ensure smoother and controlled operations, preventing data breaches and attacks," shares, Sonit Jain, CEO, GajShield Infotech.

> "Endpoint security has become a necessity to manage multiple open points and help regulate data traffic and monitor the incoming and outgoing connection of sensitive and mission-critical data."
>
> **RIPU BAJWA,** Director and General Manager, Data Protection Solutions, Dell Technologies

Security architectures have to move closer to data and need to have an integrated context-based data security approach that helps organisations to secure data and prevent unauthorised access to critical data, through Zero Trust framework, thus ensuring protection of data even with the remote and roaming users. Data security edges will become the new normal, he adds.

The recent PwC-DSCI report reveals that data security products will grow at a CAGR of 22.2 percent in India; the fastest in the world. The demand for privacy-related solutions is expected to pick up as organisations will compete to gain business advantage in this technological environment and avoid hefty fines or penalties for non-compliance. Organisations actively serving in other markets will spend to comply with critical regulations like the UK's Privacy Protection Act, 2018, and the California Consumer Protection Act.

Further, in the current scenario when businesses are operating from remote locations, centralized security systems prove ineffective. "Hence, endpoint security has become a necessity to manage multiple open points and help regulate data traffic and monitor the incoming and outgoing connection of sensitive and mission-critical data. Soon, more organizations will find the answers to their security problems in endpoint security. It reduces the risk of harmful data breaches, ensures advanced threat prevention and can also avoid remediation costs in the long run," shares Ripu Bajwa, Director and General Manager, Data Protection Solutions, Dell Technologies.

In fact, organizations are looking at extended detect and response (XDR) and endpoint protection which is more based on behavioural analysis than just your signatures. So, XDR has now become the new model for end point security, adds Harpreet Bhatia, Director, Channels & Strategic Alliances, India & Saarc, Palo Alto Networks.

Defined as SaaS-based threat detection and incident response tool, XDR integrates multiple security products into a single security operation system. It provides a holistic view of the threats across the technology landscape and helps organisations go beyond the typical detective controls.

Cloud security moves towards SASE

To keep their operations smooth and running, businesses are adopting a multi-cloud setup and it is predicted that almost 83

percent of enterprise workload will move to the cloud, further complicating their security. A recent study suggested that over 34 percent of data breaches involve internal actors with financial and non-financial motives, increasing the risk of data leak by these remote users up to 60 percent, discloses Jain.

Hence, organizations are opting for cloud security to protect data and applications running on multiple cloud infrastructures. Gartner estimates a growth of 31.2 percent on cloud management and security services, thereby emphasizing the need for sure-fire cloud-based security.

However, as the cloud management and security get complex with multi-cloud environment, it is driving a need for converged services to reduce complexity, improve speed and agility, enable multicloud networking and secure the new SD-WAN-enabled architecture. "There will be more cloud-first security mechanisms such as the Security Access Service Edge (SASE), which is the consolidation of several existing security mechanisms such as SD-WAN, NGFW, Zero-Trust and more. SASE is a security framework for enabling secure and fast cloud adoption. It ensures users and devices have secure cloud access to data and services, from anywhere and anytime," states, Mathivanan Venkatachalam, Vice President, ManageEngine.

From a customer's perspective SASE is a platform that solves complexity in securing the remote employees. With reduced hardware footprint in SASE architecture, it lowers the operations cost and operational management workload. SASE is going to be a big trend going forward," suggests Bhatia.

> "With the incorporation of deep learning into security setup, next-gen security products are expected to be self-governing, self-learning, and self-aware, thus, requiring minimal manual intervention."
>
> **MATHIVANAN VENKATACHALAM,**
> Vice President, ManageEngine

Talent crunch puts focus on SOC

With a lack of skilled personnel being a major inhibitor to maximize the efficacy of security investments, we are seeing more organizations evaluating Cyber Security-as-a-Service (CSaaS) or Security Operations Center (SOC) option. "SOC empowers the organization to work with a security firm specializing in various security services. Security as a Service can help with the maintenance and operationalization of the security controls thereby driving security through an SLA-driven program rather than a traditional path of consuming an on-prem security solution," specifies Das.

Businesses are increasingly focused on adopting SOCs to strengthen breach response capabilities. The adoption of SOCs which are modern and boast of integrated incident response, threat intelligence and threat hunting capabilities will increase. This will be driven primarily by the need to protect the crown jewels, such as intellectual property, brand equity, business systems and data.

CSaaS offers benefits such as cost-effectiveness, scalability, and digital transformation. "Though CSaaS has significant advantages, but its adoption had been slow in India. However, Covid-19 has accelerated its adoption and made enterprises realise its importance in securing an organisation with no boundaries," highlights Jain.

AI to deliver on security

To keep up with the rate and speed of cyber-attacks is extremely difficult for humans. Thus, using technologies such as AI to beef up cyber security and improve the rate of responding to attack is more

> "AI algorithms can learn to spot suspicious patterns in network traffic, authentication, and user behaviour. As an early warning system, AI allows the security team to react to events as they are happening and well before any long-lasting damage can occur."

SUNIL SHARMA, Managing Director, Sales, Sophos India & Saarc

of a necessity than a matter of choice. Many of the experts expect that advances in AI and ML will allow devices to self-secure, and heal by as much as 80 percent by 2022. In fact, AI can help the understaffed and under-resourced security teams to stay on top of cyber threats and attacks.

According to a recent research report, the market cap of AI-in cyber security is expected to hit USD 14.18 billion by 2025. But, what makes AI a big deal in cyber security? There are three significant reasons:

- AI provides proactive threat mitigation capabilities required for constant supervision and adaption to security vulnerabilities.
- With AI, users receive security alerts in real-time to activate quick threat mitigation.
- Along with machine learning, AI can be hands-on in preventing threats rather than detection.

An AI algorithm can, not only be used to scan emails for simple spam and phishing campaigns, but also for more dangerous threats like thread-jacking and business email compromise attacks. "But more than that, these algorithms can learn to spot suspicious patterns in network traffic, authentication, and user behaviour. AI solutions act as an early warning system for organisations. It allows the security team to react to events as they are happening and well before any long-lasting damage can occur," shares Sunil Sharma, Managing Director, Sales, Sophos India & Saarc.

Further, AI and ML applications are being embedded into the cyber suite of offerings – especially in security intelligence, detection and response (IDR), endpoint security and security testing. In addition, companies are evaluating their AI journey for security to ensure that it is moving from just a promise phase to actual delivery of AI-based security insights.

"While we have witnessed the use of AI/ML within the realm of security, moving forward, organizations will embrace the power of machine learning to help them monitor their risks across all security controls. There are mountains of security telemetry data available with all IT landscapes and not all of this data is being analyzed and used for security monitoring and threat hunting. ML-based tools could provide the necessary insights from each of these controls - be it the security information and event management (SIEM) system or the user behavior analysis system or the identity risk monitoring system and more importantly the data security systems," elaborates Das.

However, many say that it's early days for AI in cyber security with some unique challenges. "False positives are a big challenge as no one likes to hamper the UX for security. Then there's challenge about security of the training data. What if the malicious actors target the training data? These are some real challenges and we need to take care of these before we see more AI

in security. At the same time, there are few great innovations happening in this space with IBM Watson introducing intelligent threat analytics. Google has been doing spam filtering for years now using sophisticated machine learning algorithms. Considering the growth in volume and complexity of attacks, there will be an increased AI adoption in security," states Ujwal Ratra, Chief Operating Officer, Astra Security.

Automation to drive security strategy

Cyber risks are here to stay and they are going to rise (as it only takes one bad click to breach your system). In 2020, we saw the rise of threat attackers cherry pick protocols that were used for meaningful exploitation. Even with the increased awareness on the importance of cyber security, globally, it is predicted that in 2021, there could be one attack every 11 seconds. Hence, the need of the hour moving forward, is to focus on the entire threat lifecycle in a proactive manner.

Moreover, organizations have traditionally struggled to take quick and auditable action on security insights that are provided by various protection systems in the organizations due to either lack of man-power or lack of process. Like the application of automation in other fields, in security too, it frees the workforce to concentrate on more skill-based tasks. As per a research, due to the sheer volume of tasks associated with cyber security, IT teams miss out on 74% of events/alerts that sometimes blow out of proportion. With automation in place, such detection and lower-level problem resolution can be taken care of by the machines. In fact, investments in orchestration and automation technologies can help ensure that the detected incidents are addressed in a systematic and compliant manner.

> "There are few great innovations happening in AI space with IBM Watson introducing intelligent threat analytics. Google has been doing spam filtering for years now using sophisticated machine learning algorithms."
>
> **UJWAL RATRA,**
> Chief Operating Officer, Astra Security

Road ahead

Security has always been fundamental to digital transformation, while earlier it was just an enabler, now it has become a business accelerator. This is the reason why cyber security leaders have now become a part of business decision-making processes and as the years' progress, we can expect their role to become crucial for the success of a business.

"As the dependency on technology increases, the reliability of new-age technologies like AI will also increase to nurture a relationship between humans and machines. Not only this, but security automation will become a buzzword for organizations looking to secure their critical data in the future," states Bajwa.

Further, the usage of IoT devices and 5G networks will open up a whole lot of security gaps with hardware-based authentication seen as a solution. "Similarly, emerging/new security models such as password-less authentication, User Behavior Analytics (UBA) and more will continue to evolve at a far quicker rate than usual in order to keep pace with the growing cyber security needs. With the incorporation of deep learning into security setup, next-gen security products are expected to be self-governing, self-learning, and self-aware, thus, requiring minimal manual intervention," concludes Venkatachalam.

AMJ 2020 WAS THE BIGGEST QUARTER FOR PALO ALTO GLOBALLY

Harpreet Bhatia, Director, Channels & Strategic Alliances, India & Saarc, Palo Alto Networks, highlighted that the company saw robust growth as well as 20 percent increase in its channel footprint in 2020 not only due to its strong product portfolio but also over its channel-friendly strategies during the pandemic. He underlined the brand's initiatives including easing payment terms, partner program changes and partner enablement training to support channel partners during the tough phase

Amit Singh

HARPREET BHATIA, Director, Channels & Strategic Alliances, India & Saarc, Palo Alto

As businesses turned to work-from-home environment, how the demand for security solutions was impacted during 2020?

From our business perspective, we saw the biggest quarter globally during May, June and July 2020. Security has become a board room conversation over the last four to five years and directly impacts the CEOs and not just CIOs or CISOs.

Covid-19 and the resulting restrictions tested the readiness of the enterprise infrastructure and the resources to handle business continuity and cyber attacks. Many of the CXOs spent sleepless nights to get the infrastructure ready for remote working. However, major concern for them was to secure their infrastructure from cyber attacks. While cloud adoption was picking pace pre-Covid, however, during the Covid-times demand for cloud spiralled manifold. Hence, cloud security became a point of conversation. Moreover, businesses moved on from traditional endpoint security to embrace extended detect and response (XDR), which is more based on behavioural analysis than just signatures.

The third piece, which grew was the adoption of SASE (Secure Access Service Edge) with an embedded SD-Wan and a DLP offering. The SASE adoption was supported by the strong trend towards cloud, as you need not backup your entire remote branches and employee traffic onto the data centre and then redistribute it. Our Prisma Access is a cloud-based fire wall as a service model, which eliminates the need of an additional layer of hardware on the branches or at remote locations. While a VPN or legacy infrastructure deployment may take 2-3 months, Prima Access solution can be deployed within 4 days for over 7000-8000 employees. Hence, SASE is definitely the trend which is changing the landscape of end point security.

Please talk about the challenges faced by the channel partners during the year 2020? How did you support channels for smooth functioning?

As Covid restrictions were imposed, channel partners faced challenges as the shipments in transit and orders placed with the distributors got stuck. This resulted in delay in payments and the entire cycle got disrupted. In order to support our partners, we offered relaxed payment terms to our distributors, who in-turn passed on the benefits to the partners/ resellers.

In addition, we suspended the minimum booking requirement for the channel partners to stay and continue with our Next Wave Partner Program. We also waived the condition for new partners to mandatorily invest in NFR.

Further, as our partners and their resources were mostly idle during the Covid restrictions, we utilized that time by offering online sales and pre-sales enablement programs. The whole idea was to move our partners more into the next generation technology including SASE and cloud security, so that they could not just sell more but also sell what is relevant in today's market.

How has Covid-19 pandemic affected your channel footprint?

During 2020, we witnessed our partner footprint to increase rapidly. There was 20 percent increase in the number of partners in India. Besides India-based global partners, we observed lot of partners offering niche solutions like IoT for healthcare, SOC management, and cloud services, joined us during the last year.

What is the kind of partners you are looking at?

It is our stated strategic vision to look at quality and never quantity. The customer conversation has changed completely as they look for the outcome of the solution and not the components of the solution. Our solutions are also designed to address customer pain-points through documented deliverables. Hence, we look for partners who fit in our portfolio and are willing to learn, invest and get into new technology areas. The key is to increase profitability for our partners, as the more they invest on the services around the technology areas the more profitable they will become.

Recommend Model for Photo Segment

HP DNJ Z6 44" PostScript Printer

A1 Black and White HP DesignJet Large Format Printer, Perfect for Enterprise, Print speed up to 556 ft²/hr Ethernet, USB interface for direct printing from USB flash drive

HP DNJ Z6 24" PostScript Printer

A1 Black and White HP DesignJet Large Format Printer, Perfect for Enterprise, Print speed up to 450 ft²/hr Ethernet, USB interface for direct printing from USB flash drive

For more details Contact: Mr. Chandan Sinha @ 09831781941

TRISITA MARKETING P LTD.

8 Ho Chi Minh Sarani, Harrington Mansion, Ground Floor, Flat 22, Kolkata -700071
Email: chandan.sinha@trisita.com, Web.: www.trisita.com

IBM TO EXPAND ECOSYSTEM TO ENGAGE NON-TRADITIONAL PARTNERS

While elaborating on IBM's channel strategy and plans for 2021, Lata Singh, Director, Partner Ecosystem, IBM India and South Asia, reiterates the company's efforts to re-strategize channels and partner programs during the pandemic, and its committed USD 1 billion investment globally

Amit Singh

As businesses turned to work-from-home environment, how was the demand for security solutions impacted during 2020?

As remote working became the new norm, businesses continued to battle new security challenges while supporting the requirements of a large remote workforce. This trend resulted in a robust demand for IT security as highlighted in the global market study conducted by IDC last year. The report estimated the worldwide spending on security-related hardware, software, and services to be USD 125.2 billion, which is an increase of 6 percent over 2019. It also estimated the worldwide security spending to reach USD 174.7 billion in 2024 with a CAGR of 8.1 percent over the 2020-2024 forecast period.

Given the enterprise security scenario, businesses require a 'Zero Trust' security strategy which evolves with the changing landscape by:

- **Increasing the efficacy of existing security controls by:**
  - Diligently prioritizing and monitoring all security alerts including fine-tuning the rules to address new requirements, like employees logging in at odd hours from different locations.
  - Continued risk assessment and monitoring of both new and existing assets, which are exposed to the Internet to enable remote working.
  - Creating awareness around 'social engineering' attacks through regular trainings and real-life examples.
- **Investing in additional security controls** especially around data and identity security since they are the most critical assets for any organisation.
- **Breaking the siloed approach towards data security and threat management** to quickly identify data breaches and contain them especially in a remote working model.

Looking at the challenges posed by Covid-19, how did you re-strategize channels and partner programs during the pandemic?

Like most businesses, our channel partners faced the twin dilemma of – providing seamless business continuity to minimize impact on their clients and ensuring continued skilling to respond to the dynamic client requirements.

LATA SINGH,
Director, Partner Ecosystem, IBM India and South Asia

In 2020, IBM committed USD 1 billion investment globally to help partners provide their clients with a seamless and secure journey to the cloud. In addition, to accelerate growth and innovation and to provide greater value to our partners globally, we introduced program enhancements and simplification including the launch of Hybrid Cloud Ecosystem, Partner World 2.0, Red Hat Marketplace and Industry Cloud Ecosystem.

In India, we witnessed an increased demand for cloud solutions, cyber security, remote workforce

and business continuity planning. To enable our partners navigate through the changing business landscape, we introduced a range of new initiatives including:

- **Digital resources** like digital workshop, which provides access to key virtual selling, training and learning tools; and IBM Virtual Client Center, which provides 24/7 access to solutions, demos, webinars etc.
- **Skills enablement programs** like IBM Skills Gateway, which provides access to digital badges and professional certifications and Seismic portal, which offers a range of enablement materials on demand.
- **Engagement solutions** like My Digital Marketing, which is a no-cost digital collaboration platform offering 'ready-to execute' digital campaigns and Business Partner Connect, which offers both IBM and Red Hat partners the ability to discover new collaboration opportunities, by leveraging Watson's matching technology to help them find the right tools for shifting business needs.

What is your future channel roadmap and plans?

We believe that an ecosystem of partners is essential to drive value for clients and to accelerate co-creation and co-innovation to bring the best platforms, products and services to the market. This platform-economy approach aligns with our ecosystem commitment and is well reflected through the dedicated 'Build and Services' track in our Partnerworld 2.0 program.

In 2021, we plan to unite with our ecosystem partners to deliver consistent client experiences and 'get to market' and 'go to market' their way through:

- **Personalized partner experience** through a single focal
- **Alignment with IBM sellers** to exclusively work with partners who will help them drive growth, identify opportunities and deals across Build, Service and Sell tracks
- **Deep technical expertise** to help architect solutions using IBM technology
- **Access to hybrid cloud build resources** to design, build and/or migrate solutions with IBM systems and software technology
- **Creating opportunities to drive demand and success** through additional demand generation and cloud engagement funds, and digital campaigns to identify new opportunities based on client buying behaviours.

Keeping pace with the evolving market requirements and the convergence of AI, Cloud, IOT, Blockchain and 5G, we will expand our ecosystem to bring in the next generation of 'non-traditional' partners that are disrupting the industry while deepening our relationships and supporting our partners including Individual Software Vendors (ISVs) and Managed Service Providers (MSPs) to transform their client experiences.

ALL'S WELL THAT ENDS WELL

For many businesses, Covid-19 came as a blow, however, for security channels and solution providers Covid-19 opened up doors of opportunities despite some initial troubles. As the businesses moved towards WFH environment and cyber attacks spiraled, the fortunes of security channels changed drastically

Amit Singh

The rapid and unexpectedly broad disruption to businesses around the world due to Covid-19 pandemic left channel partners struggling to maintain security and business continuity for themselves as well as for their customers.

Due to Covid-19 restrictions, most of the channel partners found themselves unable to service their customers for quite some time. "With Covid restrictions in place, channel partners got their shipments stuck in transit and orders placed with the distributors got stalled. This resulted in delay in payments and the entire payment cycle got disrupted," highlights Harpreet Bhatia, Director, Channels & Strategic Alliances, India & Saarc, Palo Alto Networks.

In addition, many of the partners were in shock for almost two months. "Most of the customers froze funds and were only spending on renewals during March, April and most of the May. Customers' reluctance to spend resulted in negative growth in revenues during this period," discloses Ronny Ferrao, COO, Essen Vision Software.

However, things improved for channels during June, when restrictions started to lift and businesses started opening up. Subsequently, majority of the businesses revived spending on technology and cyber security as they moved on to cloud platforms and realized the acute need to keep cyber attacks at bay.

Brands re-visit channel strategies

Security brands re-strategized their channel strategies and partner programs to address partner

> In order to support our partners, we offered relaxed payment terms to our distributors, who in-turn passed on the benefits to the partners/resellers.

HARPREET BHATIA, Director, Channels & Strategic Alliances, India & Saarc, Palo Alto Networks

challenges and heightening demand for next-gen security solutions.

Many of the brands modified their partner programs to address channel partner challenges. "In order to support our partners, we offered relaxed payment terms to our distributors, who in-turn passed on the benefits to the partners/ resellers," shares Bhatia.

He further states that the company suspended the minimum booking requirement for the channel partners to stay and continue with its Next Wave Partner Program. It also waived the condition for new partners to mandatorily invest in NFR.

In addition, IBM committed USD 1 billion investment globally to help partners provide their clients with a seamless and secure journey to the cloud in 2020. "To accelerate growth and innovation and to provide greater value to our partners, we introduced program enhancements and simplification including the launch of Hybrid Cloud Ecosystem, Partner World 2.0, Red Hat Marketplace and Industry Cloud Ecosystem," underlines Lata Singh, Director, Partner Ecosystem, IBM India and South Asia.

> To accelerate growth for our partners, we introduced program enhancements and simplification including the launch of Hybrid Cloud Ecosystem, Partner World 2.0, Red Hat Marketplace and Industry Cloud Ecosystem.

LATA SINGH,
Director, Partner Ecosystem, IBM India and South Asia

However, few of the partners refuted the claims around relaxed payment terms and changes in partner programs. "We didn't come across a single security vendor, which offered relaxed terms or eased partner programs and targets in favour of the ailing partners. In fact, many of the partners suffered a lot as payments were stuck with customers," reveals Ferrao.

On the other hand, partners like Vishal Bindra of ACPL Systems, mentions that they received extensive support and relaxed payment terms from distributors. "Distributors have been extremely helpful for us during the tough time with their extended credit beyond the standard credit line of 30-45 days," informs Bindra, CEO, ACPL Systems and cyber security startup Klassify.

Increased focus on training

As the vendors foresaw an increased demand for cloud solutions, cyber security, remote workforce and business continuity solutions, they focused on enabling partners to build solutions on new-age technologies. "As our partners and their resources were mostly idle during the Covid restrictions, we utilized that time by offering online sales and pre-sales enablement training. The whole idea was to move our partners more into the

next generation technologies including SASE and cloud security, so that they could not just sell more but also sell what is relevant in today's market," shares Bhatia.

"We introduced a range of new initiatives including digital resources like Digital Workshop and IBM Virtual Client Center, which provides 24/7 access to solutions, demos, webinars etc. In addition, we offered skills enablement programs like IBM Skills Gateway for access to digital badges and professional certifications, and Seismic portal for enablement materials on demand," adds Singh.

She further adds that partners showed great interest for engagement solutions like My Digital Marketing, which offers 'ready-to execute' digital campaigns, and Business Partner Connect, which offers both IBM and Red Hat partners the ability to discover new collaboration opportunities, by leveraging Watson's matching technology to help them find the right tools for shifting business needs.

Sunil Sharma, Managing Director, Sales, Sophos India & Saarc, highlights that over the last 12 months, Sophos has conducted more than fifty certification trainings and ten local trainings for partners to enable them in all areas of cyber security including cloud security.

Channel revenues took a boost

While the Covid-19 restrictions were lifted during June 2020, security channels and vendors saw a stage wise demand of cyber security solutions. During the strict lockdown phase, businesses were focused on business continuity solutions including cloud computing.

"At this stage, cyber security was not the top priority. However as cloud adoption increased and people started working from home, cyber attacks spiralled rapidly. This led to an acute demand for cyber security measures and skilled professionals in the second stage," explains Sharma.

He adds that in the third stage, as businesses continue to transition in the new normal, we see organizations becoming serious about cloud security and adopting a zero-trust security posture. This third stage will continue in the future as organizations want to be prepared for any kind of pandemic and subsequent rise in cyber attacks.

The increased demand for cyber security solutions enabled the security partners to make up for the losses made during the AMJ quarter. "We were forced to work really hard to meet our customer demands for cyber security solutions including endpoint security, cloud security, DLP, data classification and rights management. In fact, H2 of 2020 contributed heavily to our revenues," discloses Bindra.

"We witnessed high surge in demand from verticals like pharma, BFSI, ITeS and manufacturing. In fact, we were able to cover the losses made during the previous half of the year and exceeded revenues of 2019," adds Ferrao of Essen Vision. The company executed a major data classification and DLP project worth USD 1 million entailing 12,000 endpoints for a large pesticide company in India. It is looking at over 35 percent growth in 2021 over its revenues in 2020.

Hence, 2020 overall was quite resourceful for the security channel partners and solution providers.

"Distributors have been extremely helpful for us during the tough time with their extended credit beyond the standard credit line of 30-45 days."

VISHAL BINDRA, CEO, ACPL Systems

"With surge in demand from verticals like pharma, BFSI, ITeS and manufacturing, we were able to cover the losses and exceeded revenues of 2019."

RONNY FERRAO, COO, Essen Vision Software

HR PROCESSES GET INTELLIGENT, ARTIFICIALLY

Dr Gaurav Hirey, Founder & CEO, GoEvals, outlines how their HR platform uses scientifically validated tools across employee lifecycle to simplify HR processes

DR. GAURAV HIREY
Founder & CEO, GoEvals

Please talk about your HR solutions portfolio?

GoEvals is a tech start-up established in December 2019. We focus on creating innovative digital solutions for people management with focus mainly on three areas:

- Candidate selection for recruitment
- Employee satisfaction and sensing
- Organizational performance and success

We have nine tools across the whole employee life cycle and currently we are live with three of the GoEvals selection tools:

- The GoEvals video interview platform
- Compatibility index platform: It is a competency testing platform which allows recruiters set an assessment test by which they can evaluate the candidate's skills and capabilities.
- Candidate on-boarding and reference check: This tool eliminates all the ground work that is required in the on-boarding process.

Beyond the recruitment process, how do your solutions help in other HR functionalities like evaluation and

assessments?

We are focusing on performance management, 360 degree feedback, and succession planning. We have covered the employee performance, employee satisfaction and sensing aspect which is helping managers assess the mood of the employee and also intelligently provide nudges to the manager to take action, if the platform senses that some employees are not meeting the standard parameters.

Can the GoEvals tools integrate with the ERP solutions in organizations?

We are already in talks with one of the big HR ERP companies and they want to offer GoEvals as an add-on to their clients. We are hoping that those conversations will be done by the end of the year. If all goes right then we will be working alongside one of the big giants in the area.

Are the GoEvals tools applicable both for entry level and lateral recruitments?

The platform is built to cater to all levels. When we build the competence testing platform we ensured that we have the leadership competency included in the library of competency. At this moment, this can be used across levels and the initial feedback from our clients is that they are using it across levels, 65-70 percent of the usage is for entry level and mid-level hiring but we have had clients who are using it for senior level hiring too.

How many clients are already on-board and what are their use cases?

We went live in October 2020 and so far we have 23 clients including start-ups, MSMEs, and large conglomerates who are currently using the platform. We have many clients who are using our platform to do their campus recruitment. They are setting up the assessment test using the GoEvals competency platform and then fix a video interview.

Over the last four months our data base have become double; there has been 11,000 candidates on the platform who have taken the test.

> "We are focusing on performance management, 360 degree feedback, and succession planning. We have covered the employee performance, employee satisfaction and sensing aspect which is helping managers assess the mood of the employee and also intelligently provide nudges to the manager to take action."

Since the recruitment actions are not happening real time, how does the synchronization happen between the recruiter and the potential employee?

Once we finalize the questions for the interview, we can create a video assessment test through our tool within 15 minutes. Candidates can take the test through a link shared by us. We can decide the time-frame of the test, and the candidate will need to answer all the questions within the time limit. As they submit the test, the platform notifies us with an evaluation link against the list of all the students that took the test.

Best thing is that multiple evaluators can evaluate the same candidate. The top 10 candidates come up organically on the basis of the scores provided by the evaluators. This process also eliminates the chances of any bias.

What is the average cost incurred for deploying the GoEvals HR solution?

On an average our subscription costs Rs 10,000 a month. This is user-based, so in Rs 10,000 you can have 8-10 users using the platform and there is no cap on the number of video interviews or competency tests. Being a SaaS based solution; it can be deployed across the organization at multiple locations.

Do you have provisions to take care of recruitments for overseas markets?

We do work with international clients, we have couple of clients who are using GoEvals in the middle-east and are also in conversation with a bank in US. For large scale hiring in foreign companies, we have a separate platform for mobility and Visa management.

What are your key focus areas in 2021?

In 2021 we want to roll out all the nine tools by September. In addition, as part of our international expansion, we are in active conversation with partners in Malaysia, Thailand and Singapore as well as in the middle-east. Further, we are targeting to acquire over 100 customers by 2021-end.

HP DesignJet T2600 36-in MFP

Print, copy, scan, HP Thermal Inkjet, Memory 128 GB, Print quality color (best) Up to 2400 x 1200 optimised dpi, Scan Resolution, Optical Up to 600 dpi, Direct print from mobile apps on iOS, Android, and Chrome OS; email printing with HP ePrint and HP Smart app for iOS and Android

HP DesignJet T2600 36-in PostScript MFP

Print, copy, scan, HP Thermal Inkjet, Print quality color (best) Up to 2400 x 1200 optimised dpi, Direct print from mobile apps on iOS, Android, and Chrome OS; email printing with HP ePrint and HP Smart app for iOS and Android

HP DesignJet T2600dr 36-in MFP

Print, copy, scan, HP Thermal Inkjet, Print quality color (best) Up to 2400 x 1200 optimised dpi, Direct print from mobile apps on iOS, Android, and Chrome OS; email printing with HP ePrint and HP Smart app for iOS and Android

HP DesignJet T2600dr 36-in PostScript MFP

Print, copy, scan, HP Thermal Inkjet, Print quality color (best) Up to 2400 x 1200 optimised dpi, Direct print from mobile apps on iOS, Android, and Chrome OS; email printing with HP ePrint and HP Smart app for iOS and Android

For more details Contact: Mr. Chandan Sinha @ 09831781941

TRISITA MARKETING P LTD.

8 Ho Chi Minh Sarani, Harrington Mansion, Ground Floor, Flat 22, Kolkata -700071
Email: chandan.sinha@trisita.com, Web.: www.trisita.com

FOCUSING ON SURVEILLANCE, ROBOTICS AND AUTONOMOUS COMPUTING

KRISHNA RANGASAYEE
CEO & Founder, Sima.ai

AMIT KUMAR MITRA
Sr. Director, SiMa.ai

SUDERSHAN VURUPUTOOR
Site Lead, SiMa.ai

Krishna Rangasayee, CEO & Founder, Sima.ai; Amit Kumar Mitra, Sr. Director, SiMa.ai; and Sudershan Vuruputoor, Site Lead, SiMa.ai, take us through different use cases and applications where the solutions are being deployed.

Please talk about your journey?

SiMa was started in November 2018 with 60+ people and was working mostly in the Bay area and we recently started our site in Bangalore. Our lead investors are Dell Technologies, Amplified partners and link. In the past 10-15 years machine learning has played a very big part in reshaping the cloud. We use Google Maps or Apple Maps to go even the smallest distances, so you can understand how cloud has changed and effected our lives.

In the next 10-15 years, the larger market will be Edge and machine learning will play a very big part in re-shaping everything in the Edge. Our primary focus is to build a purpose build machine learning platform for the Edge. We believe that is the missing link that is preventing the scaling of Edge. That is the intent and vision behind what we have started and it has been 2 years and we are very close to production.

What are the use cases and applications for AI/ML that can be leveraged for scaling up?

¬We have 3 market priorities –a large category is on smart vision these are security surveillance, health metring, security applications, retail safety. The second one is robotics and drones and the third one is autonomous computing. People have deployed an application for lot of infrastructure and due to the pandemic people have added a new capability added to the existing infrastructure. They want to add thermal monitors, social distance monitors in the security cameras. These require a lot of high performance machine learning and they want to leverage the existing infrastructure by creating new applications with new capabilities. The third category of use cases we see is around public safety and we make sure in high security areas people are identified only from facial recognition.

What is the update on the design and development centre and how are you looking at India as a market?

India has a great talent pool in almost everything we do be it hardware design, software design etc. In the last 10 years India has a lot of experience in systems not just in technology but in individual aspects and solving applications. At the end of the day the company is defined by its people the strength of the people we have. We are starting small in India, Amit is heading our software efforts and Sudarshan is heading our hardware efforts. The site in India is going to be for more than development we will be doing systems application and lot of other key things for both the Indian market and other markets there.

It's a very logical choice to have a site in India, because you name any technology company OEM, technical service providers you have all the ecosystems in Bangalore.

Does the India centre also provide support and services to the global customers?

That's the plan once the production starts there will be a business and application support team who will work from here and support the customers in the different time zones. Then understand our technology and help it adapt in other way understand the legacy application and help them out.

The complete AI-ML solution that we are trying to do requires expertise in multiple domain not just the ML & AI that's just the front end it includes the computer architecture, computer vision etc. they all have to come together to provide a solution. In a survey I found that 10% of all the major international companies like Intel and all are Indians. This is because there is a large talent pool here and this replenished very quickly as there are almost every year nearly 250,000 engineers coming from the different institutions. So this is what every company is looking for we are also utilising that here at SiMa also.

What are the key focus areas and initiatives planned by SiMa for the next 12-18 months?

I have joked that I have only four problems. One needs to build an amazing product, we need to have amazing customers, need to have amazing talents and have amazing investors. We feel very good and worked very hard to get into this position in the last two years and now it's about being paranoid putting our head down every day and continue to do these four things very well. We are also well funded so the need for funding is for later.

Nothing Raises $15 Million in Series A Funding Round Led by GV (formerly Google Ventures)

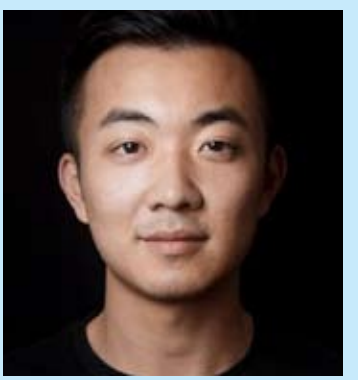
- **Announcement comes following Nothing's $7 million seed financing from high-profile entrepreneurs and tech leaders and undisclosed funds from Kunal Shah, CRED, Founder**
- **With the new funding, the company plans to expand its operations in Europe with headquarters in London and release its first smart devices in the coming months.**

Nothing, a new forward-thinking London based consumer technology company, announced today that it has raised $15 million in a Series A round led by GV (formerly Google Ventures).

With the new funding, the company plans to expand its team and operations, further invest in R&D, as well as launch its community and first products in the coming months.

"We are grateful to have a venture capital firm of this caliber help in building Nothing together with us," said Carl Pei, CEO and Co-founder of Nothing. "We plan to aggressively grow the company, in particular our R&D and design capabilities, to realize our mission of removing barriers between people and technology."

"Carl Pei is a seasoned entrepreneur with marketing, hardware, and distribution experience that is key to bringing new devices to market," said Tom Hulme, General Partner at GV. "His vision for smart devices is compelling, and we have high confidence that with Carl's global mindset, the Nothing team will have a meaningful impact on the market for consumer technology."



CARL PEI
CEO and Co-founder, Nothing

TOM HULME
General Partner, GV

The new round takes the total amount of financing Nothing has raised to over $22 million. Previous investors include notable tech leaders and investors such as Casey Neistat, Kevin Lin, Steve Huffman, Kunal Shah.

Nothing also plans to open up for its community and the general public to invest as part of its Series A round. More details will be announced in the coming weeks

ASIRT Completes 9 Years of Service for IT Channels

The association which currently operates in Mumbai, Thane and Navi Mambai, has aggressive plans to expand presence by building chapters across the country

Association of Systems Integrators and Retailers in Technology (ASIRT), an association of system integrators and retailers has recently completed nine years of service to the IT ecosystem. Founded in 2012, ASIRT currently has 200+ members.

The association's nine year-long service is filled with achievements like TechDay. ASIRT has successfully completed 90 editions of TechDay, which is its monthly flagship event. It helps members to connect with vendors as well as business coaches, legal and tax advisors.

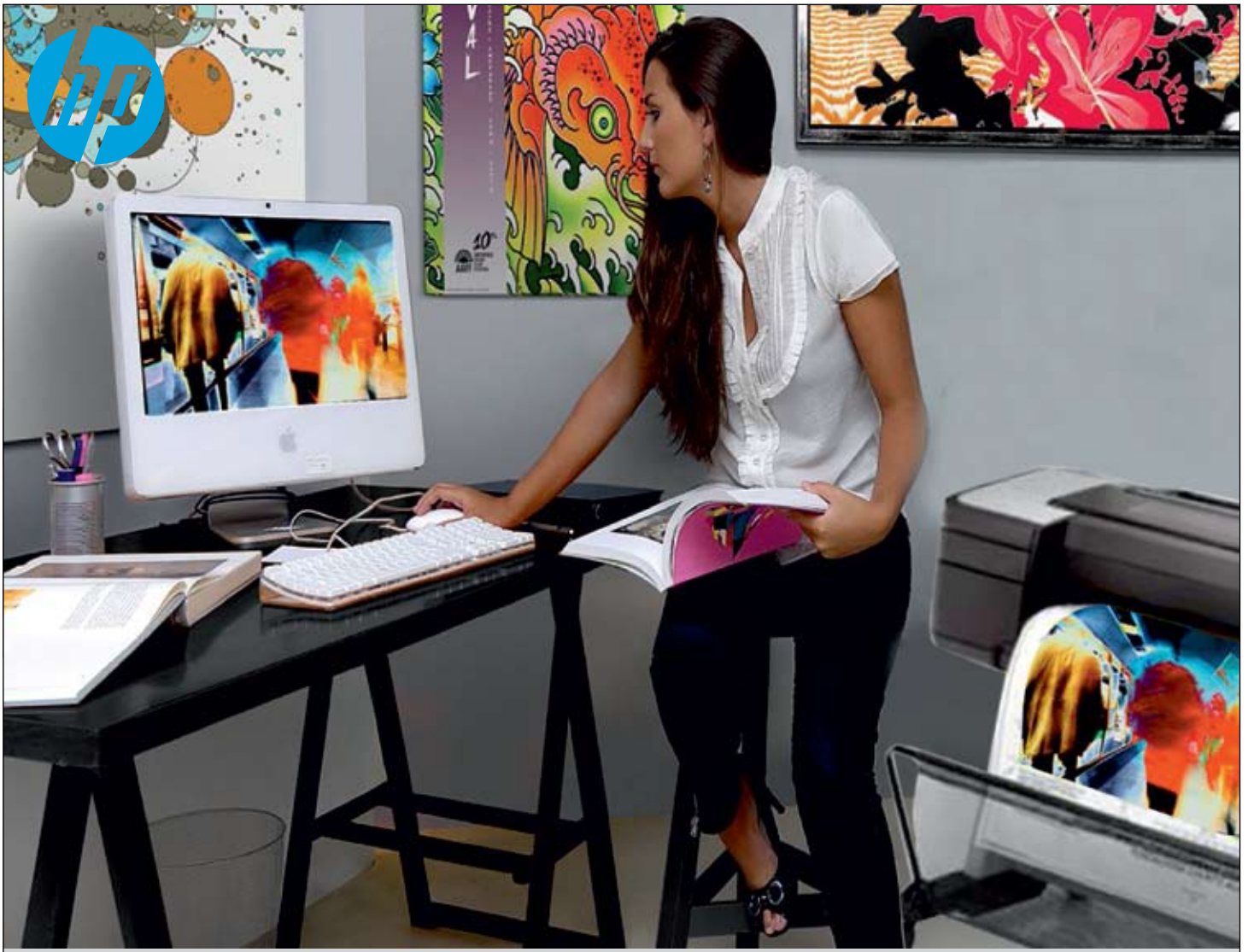
In addition, ASIRT's initiatives like TechEdge, ASIRT Gold Membership Program, and ASIRT Consortium have been quite popular among the member partners. TechEdge offers an opportunity for members' staff to get technical and soft skill training. ASIRT Gold Membership Program helps members to leverage their premier status to earn higher revenues.

Further, ASIRT Consortium enables members to collaborate with the consortium members to cover the spectrum of IT services. It enables partners build and win unparalleled and unexplored business opportunities through collaboration with other members.

Besides organizing cricket every Sunday and ASIRT Cricket Premier League annual tournament to increase bonding among the members, the association has been aggressive with its Inner Wheel initiative meant for spouses of the members to socialize and interact.

While the board of the association meets every month to discuss and act on various matters of the association, it has a strong grievance cell to address and resolve technical, commercial and support issues related to vendors, OEMs, distributors and between members.

The association which currently operates in Mumbai, Thane and Navi Mambai, has aggressive plans to expand presence by building chapters across the country.



HP DesignJet T1700 DR PS 44" Printer

HP Thermal Inkjet, Print quality color (best) Up to 2400 x 1200 optimized dpi, Direct print from mobile apps on iOS, Android and Chrome OS; email printing with HP ePrint and HP Smart app for iOS and Android Memory 128 GB (virtual), 1 Year Limited Warranty

---

For more details Contact: Mr. Chandan Sinha @ 09831781941

TRISITA MARKETING P LTD.

8 Ho Chi Minh Sarani, Harrington Mansion, Ground Floor, Flat 22, Kolkata -700071
Email: chandan.sinha@trisita.com, Web.: www.trisita.com

Channel Point

Building Security Resilience

The year 2020 was the one that everyone would like to forget. From a cyber security perspective too, 2020 was buzzing for all the wrong reasons. While the world was focused on the health and economic threats, cyber criminals were capitalizing on the crisis.

Today's cyber criminals are often well-funded, some even sponsored by rogue government organizations. In addition, stealthy and persistent attackers now have the skills and tools to do everything from taking down power grids to targeting hospitals and financial institutions with ransomware.The new breed of cyber attack can employ advanced persistent threats (APTs) and might include techniques such as remote-controlled malware to disrupt systems. The consequences can range from enormous financial losses to severe reputational damage for organizations.

The growing seriousness towards cyber security is pushing the cyber security spending in India. According to a joint study conducted by PwC India and the Data Security Council of India (DSCI) the cyber security market in India is set to grow from USD 1.97 billion in 2019 to USD 3.05 billion by 2022, at a compound annual growth rate (CAGR) of 15.6%. The growth rate is nearly 1.5 times the global growth rate of cyber security expenditure.

Few of the trends are helping organizations innovate and be prepared for all present and future uncertainties. Organizations are displaying renewed vigour around combining Identity, Data, Network, and Device security into a common analysis platform to better deliver security context and build on an organization's Zero-Trust journey. Companies are realizing that the siloed security programs are not delivering the right level of risk view to them and it is necessary to drive horizontal data analysis across all the security telemetry data that is available for the most critical resources in the organization - people, data and infrastructure.

KALPANA SINGHAL, Editor
(E-mail: kalpana@techplusmedia.co.in)

TECHPLUS MEDIA

EDITOR: KALPANA SINGHAL
CONTENT HEAD: Amit Singh
ASSISTANT EDITOR: Rajneesh De
CORRESPONDENT: Aaratrika Talukdar
CORRESPONDENT: Atreyee Chakraborty

INTEGRATED MARKETING COMMUNICATION:
Aakash Vahal
Saugata Mukherjee, Mamta Dhiman,
Nishit Saxena

ASSOCIATE ANALYST
Shaithra S

SALES:
Pratap Jana

PRODUCTION HEAD:
Aji Kumar

WEBSITE:
Sheetal Varshney/Ramesh Kr

PROMOTION:
Vikas Yadav /Amit Pandey

CIRCULATION:
Pratap

FINANCE:
Inder Pal

HEAD OFFICE:
370A, Sant Nagar, East of Kailash, New Delhi
Tel: 41625763, 26237405, 41620042
Email - kalpana@techplusmedia.co.in

MARKETING OFFICE:
10 UF, West Wing, Raheja Tower,
MG Road, Shanthala Nagar, Ashok Nagar,
Bengaluru, Karnataka-560001

Delhi: 9711841991 | **Mumbai:** 9711841992
Kolkata / Guwahati: 9331072026
Bangalore: 9354347953

OWNED, PRINTED & PUBLISHED BY ANUJ SINGHAL Printed at Modest Graphics Pvt. Ltd., C 52-53, DDA Shed, Okhla Industrial Area, Phase - I, New Delhi-20, Place of Publication: 370A, 2nd Floor, Sant Nagar, East of Kailash, New Delhi-110065, Editor- Anuj Singhal

#1 Backup for Service Providers

Exceed Customers Service level agreements (SLAs) while increasing margins & revenue

VEEAM | CSPPARTNER PROGRAM

Postal Registration No. - **DL(S) 01/3377/2019-21 Posting Date - 13-14, 27-28**
Registered with Registrar of Newspapers of India under RNI No. **DELENG/2010/32787**

OWNED, PRINTED & PUBLISHED BY ANUJ SINGHAL, Place of Publication: 370A, 2nd Floor, Sant Nagar, East of Kailash, New Delhi-110065, EDITOR: Anuj Singhal