

## Strength in Unity: Decoding the Path to Cyber Resilience



**Harish Kumar GS**  
Check Point Software  
Technologies



**Amit Kulkarni**  
Allied Digital  
Services



**Ripu Bajwa**  
Dell Technologies  
India



**Nityanand Shetty**  
Essen Vision



**Debasish Mukherjee**  
SonicWall



**Cherian Thomas**  
Wysetek Systems



**Vivek Srivastava**  
Fortinet



**Sudip Banerjee**  
Zscaler



**Dhananjay Ganjoo**  
FS

# Looking for a compact, efficient and robust UPS? Look no further!



Presenting

## Liebert ITA2 30kVA

*A fully digital, highly reliable, double-conversion UPS solution.*

Its cutting-edge design enables seamless integration into your current system, or various other ecosystems. And it's tailored for global deployment in a low carbon, compact footprint. The ITA2 is the ultimate level of engineering and dynamics from Vertiv. So, you can deploy this innovative, next-gen and extract great performance at low costs. Adding up to peace of mind. If you're looking to power your infrastructure, or upgrade your already protected systems, the ITA2 is a great addition to your support backup.

Talk to us today!

Explore solutions at [Vertiv.com/en-in](http://Vertiv.com/en-in)  
Call Tollfree : 1-800-2096070  
E-mail : [marketing.india@vertiv.com](mailto:marketing.india@vertiv.com)

Corporate Office : Plot C-20, Rd No.19, Wagle Ind Estate, Thane (W), 400604. India



SCAN CODE  
TO KNOW MORE



# Industry-leading innovation



Crucial® T500 PCIe® Gen4 NVMe™ SSD with heatsink



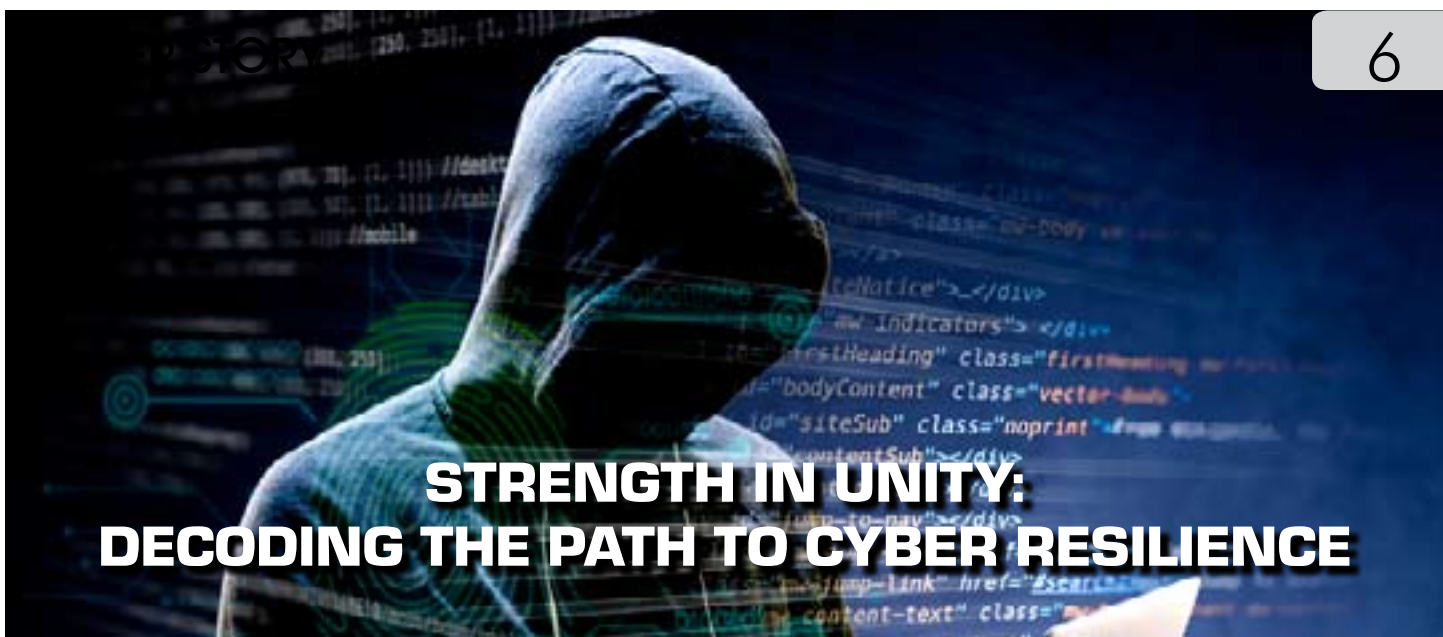
## National Authorised Distributors

Rashi Peripherals Limited  
Ms. Manisha@ +91 8879690065

Supertron Electronics Pvt. Ltd.  
Mr. Sanjay@ +91 9811059025

[www.crucial.in](http://www.crucial.in) | [1800-425-3234](tel:1800-425-3234)





## STRENGTH IN UNITY: DECODING THE PATH TO CYBER RESILIENCE

### IN CONVERSATION

The Highest Risk for a Breach in Organization is Insider Threat

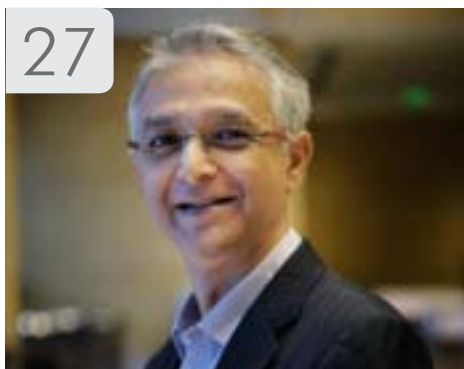
17



CHERIAN THOMAS, Director, Wysetek Systems

Automation and Orchestration Work Best When There is a Unified, Integrated Security Stack to Share Information in Real-Time

27



DHANANJAY GANJOO,  
Managing Director, India & SAARC, F5

Enterprises are going for Vendor Consolidation despite the Risk of getting Monopolized

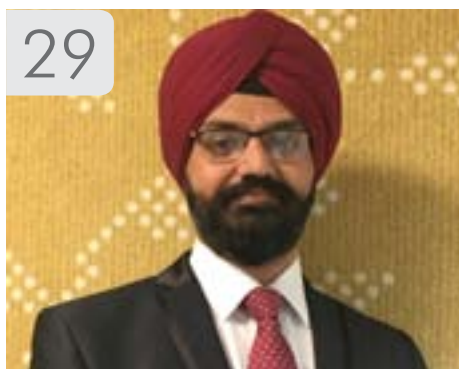
21



AMIT KULKARNI, Executive VP and Head  
Cybersecurity Business, Allied Digital Services

Integrating Recovery as the Capstone of Cybersecurity Framework Offers True Cyber Resiliency: Dell Technologies

29



RIPU BAJWA, Director & General Manager,  
Data Protection Solutions, Dell Technologies India

Enterprises Demand Integrated, Holistic Solutions to Maximize Security, Visibility, and Agility

24



DEBASISH MUKHERJEE,  
VP, Asia Pacific and Japan, SonicWall

Unified Security Improves up to 80% Visibility and Control, 50% Security Performance: Zscaler

32



SUDIP BANERJEE, CTO, APJ, Zscaler

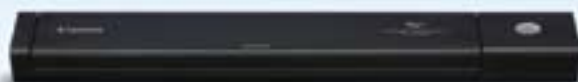
# COMPACT AND POWERFUL DOCUMENT SCANNERS FOR EVERY DIGITIZATION NEED



DR-C225II



DR-C240



P208-II



DR-F120

**CHECK OUT OUR HIGH SPEED DOCUMENT SCANNER RANGE:**

Personal  
Scanners



P-208II

Workgroup  
Scanner



DR-C240

Network  
Scanner



Scan Front 400

Departmental  
Scanners



DR-M1060

Production  
Scanners



DR-G2140

**Business Can Be Simple**

FOR SALES ENQUIRIES : West Bengal - Suvrendu Mitra : 98316 62162, Inderjit Yadav : 99030 25352,  
Saptarshi Bhandari - 98308 56977; Bihar - Virvijay Singh : 95235 96990;  
Jharkhand - Lokesh Nath : 70860 14183; Odisha - Bharat Kumar Singh : 91675 32045



# Strength in Unity: Decoding the Path to Cyber Resilience

*In an era where cyber threats evolve at an unprecedented pace, organizations find themselves entangled in a paradox of vulnerability. This in-depth analysis unfolds the intricacies of cyber resilience, uncovering the key culprit – the complexity of security capabilities in modern organizations, while spotlighting the need for a unified approach that transcends the fragmented landscape of disparate security tools*

Amit Singh





“Modern and mature organizations often have a more complex infrastructure with numerous connected systems, applications, and devices with a large number of employees who are susceptible to cyber-attacks through phishing or social engineering,” observes Amit Kulkarni, Executive Vice President and Head Cybersecurity Business, Allied Digital Services.

Even with sufficient funds and maturity, organizations often struggle to defend against sophisticated cyber threats due to their reliance on outdated security models. Traditional firewalls and VPNs, for instance, can create blind spots in encrypted traffic, leaving networks vulnerable to attacks. Attackers exploit weaknesses like weak passwords, unpatched systems, and phishing emails to gain unauthorized access and launch ransomware, malware, or data theft, adds Sudip Banerjee, CTO, APJ, Zscaler.

According to PwC, Cyber risks are cited as the biggest threat faced by Indian organizations, with 38% of respondents feeling highly or extremely exposed to it. Dhananjay Ganjoo, Managing Director, India &

SAARC, F5, attributes this vulnerability to IT system complexity, human-related risks, supply chain security issues, delayed upgrades, advanced persistent threats, low security awareness, financial constraints, and the rapid growth of cyber threats.

Additionally, the emergence of large language models (LLMs) like ChatGPT in 2023 signals a continuing trend into 2024, with AI-driven attacks becoming more sophisticated, bypassing security controls such as multi-factor authentication (MFA) and zero-trust frameworks.

“Moreover, there has been a shift towards exploiting zero-day vulnerabilities and credential theft tactics, with cybercriminals employing more sophisticated bypass methods like stealing cookies and session cookies as organizations adopt multifactor authentication. Deepfake videos and vishing attacks will remain prevalent,” says Harish Kumar GS, Head of Sales, India and SAARC, Check Point Software Technologies.

“On the other side, an increased number of security vendors and specialized point solutions have made it difficult to create a



“There has been a shift towards exploiting zero-day vulnerabilities and credential theft tactics, with cybercriminals employing more sophisticated bypass methods like stealing cookies and session cookies as organizations adopt multifactor authentication. Deepfake videos and vishing attacks will remain prevalent.”

**HARISH KUMAR GS,**  
Head of Sales, India and SAARC,  
Check Point Software Technologies



unified secure environment with the best possible product implementation with interconnection and management, highlights Kulkarni of Allied Digital.

"The higher number of security tools organizations use today slows down the response as the ability to detect and respond gets more complicated as a lot of these tools do not have integration capabilities amongst each other. The lack of effective playbooks and automated orchestration of response also hinders effective response to cyber threats in these environments," seconds Nityanand Shetty, CEO, Essen Vision.

Further, the commercial rollout of 5G, industry 4.0, and the proliferation of IoT devices have heightened the need for robust cybersecurity, particularly in India, where organizations face an average of 2146 weekly attacks compared to 1239 globally, as per Check Point's Threat Intelligence Report for India.

### **A multitude of security tools**

The first layer of the cybersecurity challenge lies in the complexity introduced by the sheer number of security

tools organizations employ. Averaging 31.58 tools, these measures are intended to fortify organizations against a diverse range of cyber threats. However, the unintended consequence is the creation of a complex quagmire where the lack of correlation among these tools generates visibility gaps. This maze not only complicates the security landscape but also diminishes the ability to detect and respond to cyber threats effectively.

"Organizations conventionally prefer to select multiple vendors/products to avoid dependency on one vendor and have different layers of protection from different sets of product owners with best-of-the-class products for certain segments of the requirement," says Kulkarni of Allied Digital.

Industry experts emphasize that the extensive use of disparate security tools introduces challenges in terms of integration and coordination. The noise generated by these tools further complicates matters, making it difficult for security teams to differentiate between routine security operations and potential threats.



**“Each security tool typically generates its own set of logs, alerts, and data. With a plethora of tools in place, security teams are inundated with a vast amount of information from disparate sources, making it challenging to gain a comprehensive view of the organization’s security posture and effective detection and response to cyber threats.”**

**AMIT KULKARNI**, Executive Vice President and Head Cybersecurity Business, Allied Digital Services





In fact, implementing the security tools as per best practices and integrating disparate security tools to share data and orchestrate response actions can be complex and time-consuming. Compatibility issues, lack of standardized protocols, and vendor-specific APIs can hinder seamless integration, limiting the effectiveness of automated response workflows and threat intelligence. "Each security tool typically generates its own set of logs, alerts, and data. With a plethora of tools in place, security teams are inundated with a vast amount of information from disparate sources, making it challenging to gain a comprehensive view of the organization's security posture and effective detection and response to cyber threats," highlights Kulkarni of Allied Digital.

The complexity of modern cybersecurity environments often results in fragmented data and alerts that are difficult to correlate and analyze, impeding effective detection and response capabilities. "This fragmentation causes delays in investigation and remediation processes, increases the risk of

human error, and limits the agility and scalability of security operations. To overcome these challenges, organizations should adopt a cloud-native platform integrated with AI, providing comprehensive visibility across users, devices, applications, and workloads," adds Banerjee of Zscaler.

### Critical delays in threat response

A recent Cloud Threat Report has brought to the forefront a critical issue plaguing organizations—the prolonged time it takes security teams to resolve alerts. Averaging six days, with a significant portion exceeding the four-day mark, this delay is untenable in a threat landscape where attackers are swift and opportunistic.

"As per many surveys, the average dwell time, the amount of time an attacker is present in the network before either acting or being discovered, is in the range of 6 months. This is a huge threat to organizations," says Vivek Srivastava, Country Manager, India & SAARC, Fortinet.

Kulkarni of Allied Digital points out the



“Attackers often escalate their tactics if they perceive that their initial attempts are not being addressed promptly. An extended response time may embolden attackers to launch more sophisticated attacks or expand their scope, exacerbating the impact on the targeted organization.”

**RIPU BAJWA**, Director & General Manager,  
Data Protection Solutions, Dell Technologies India



consequences of delayed threat response. “In case of the extended response time, there is a risk of the attacker gaining unlimited lateral access within the infrastructure. This may lead to extended downtime or exfiltrate valuable data, such as customer records, intellectual property, or financial information, leading to regulatory fines, legal liabilities, and damage to brand reputation.”

“Attackers often escalate their tactics if they perceive that their initial attempts are not being addressed promptly. An extended response time may embolden attackers to launch more sophisticated attacks or expand their scope, exacerbating the impact on the targeted organization,” adds Ripu Bajwa, Director & General Manager, Data Protection Solutions, Dell Technologies India.

Experts say that CISOs need to move past the previous focus on preventing access by attackers and start assuming they have already been breached and put emphasis on detection tools. “According to the ESG analysis, organizations that implemented Fortinet Security Operations solutions

realized significant savings and benefits. The time to identify threats was reduced from 168 hours (21 business days), if detected at all, to less than an hour and often only seconds using Fortinet EDP technologies,” details Srivastava of Fortinet. The time to triage these threats was reduced from eight hours to 10 minutes, and the time to contain them dropped from 4.2 hours to one minute based on Fortinet’s integrated approach, he adds.

The extended response time is not merely a symptom but a systemic issue that can be traced back to the difficulties organizations face in deploying automation and orchestration. In environments saturated with poorly integrated security tools, the automation of responses becomes a formidable challenge. The consequence is a setback in reducing the mean time to detect and respond to cyber threats—a critical metric in the realm of cybersecurity.

### **Lack of automation and orchestration**

Organizations relying on a multitude of poorly integrated security tools



“ The synergy required for effective automation and orchestration is severely compromised in environments where security tools operate in silos. The lack of integration hinders the swift deployment of responses, prolonging the overall threat response time. ”

**NITYANAND SHETTY,**  
CEO, Essen Vision





find themselves grappling with the complexity of orchestrating responses.

"The synergy required for effective automation and orchestration is severely compromised in environments where security tools operate in silos. The lack of integration hinders the swift deployment of responses, prolonging the overall threat response time," explains Shetty of Essen Vision.

In a landscape where time is of the essence, the setback in deploying automation and orchestration becomes a critical factor. The inability to automate routine responses and orchestrate a coordinated defense significantly hampers an organization's ability to thwart cyber threats effectively.

"Poorly integrated security tools can create a significant set of challenges like limited data exchange between the tools, incomplete visibility, slower response time, and increased human interventions," adds Kulkarni of Allied Digital.

"Integrating various tools with their different features and capabilities can become a nightmare for any security leader. In

our opinion, no matter what security philosophy an organization adopts, it's critical that all individual solutions work together to deliver layered protection and comprehensive visibility with control," says Debasish Mukherjee, Vice President, Asia Pacific and Japan, SonicWall. Furthermore, organizations need to from time to time take stock of their cybersecurity tools to ensure that there is end-to-end visibility and the ability to share intelligence across the unified security framework. These tools need to provide real-time and consolidated threat information that can then form the basis of informed security policy decisions.

"Lack of thorough visibility and tight integration of various security solutions results in solutions around automation/orchestration being rendered nearly ineffective. This has given rise to the precedence of new-age solutions built around breach attack simulations, threat intelligence, XDR, and SOAR which are tightly integrated, thereby considerably reducing the time to detect/respond to attacks," shares Cherian Thomas, Director, Wysetek Systems.



“Integrating various tools with their different features and capabilities can become a nightmare for any security leader. All individual solutions must work together to deliver layered protection and comprehensive visibility with control.”

**DEBASISH MUKHERJEE,**  
Vice President, Asia Pacific and Japan, SonicWall





“The Security Orchestration Automation and Response (SOAR) platform essentially acts as an open platform that helps an organization automate its response to a cyber-attack or a threat to an attack by orchestrating the chain of actions. SOAR reduces the time taken to address a cyberattack and remedy a gap in cybersecurity,” says Bajwa of Dell Technologies.

When compared to traditional methods, SOAR does not require an IT analyst or have a prerequisite of data science skills in an individual while initiating a response to a cyberattack. In SOAR, the response to an attack is automatically initiated when it detects an anomaly. Thus, it can reduce response time and control the damage caused by a cyberattack.

### The unified approach

As organizations embark on rapid digital transformation initiatives, the need for a streamlined and effective cybersecurity strategy becomes paramount. Siloed security solutions, often implemented in a piecemeal fashion, prove to be inadequate in providing comprehensive protection.

“The rapid pace of digital transformation demands a cybersecurity strategy that can keep up. Siloed solutions not only introduce complexities but also hinder the scalability required to adapt to the evolving threat landscape,” notes Shetty of Essen Vision.

Enter the unified security offering—a consolidated cybersecurity stack that serves as a singular point of contact during crises. The core principle is to streamline operations, enhance visibility, and provide seamless integration. This unified approach emerges as a beacon of hope in the convoluted landscape of cybersecurity.

A unified security offering addresses the challenges posed by disparate security tools and siloed solutions. By consolidating security measures, organizations gain a holistic view of their cybersecurity posture. The increased visibility allows for more effective threat detection, while seamless integration facilitates a coordinated and swift response to cyber threats.

“We are increasingly seeing enterprises embarking on a journey of consolidation and enhanced integration as far as security is



“We are increasingly seeing enterprises embarking on a journey of consolidation and enhanced integration as far as security is concerned. A consolidated security architecture uses a multi-layered approach that protects various IT attack surfaces such as applications, databases, Cloud, networks, endpoints, and identity.”

**CHERIAN THOMAS**, Director, Wysetek Systems



concerned. A consolidated security architecture uses a multi-layered approach that protects various IT attack surfaces such as applications, databases, Cloud, networks, endpoints, and identity,” shares Thomas of Wysetek Systems.

As per Gartner, adopting a cybersecurity mesh architecture will reduce the financial impact of security incidents by an average of 90%. “This level of interconnectivity between the tools can be achieved only if they are from one vendor,” highlights Kulkarni of Allied Digital. “Despite the risk of getting monopolized by one vendor, enterprises are going for vendor consolidation. This provides them benefits such as seamless integration and interoperability, improved security effectiveness, better automation capabilities, simplification in operations and management, better team management due to consolidation is skills, and finally cost optimization,” he adds.

“According to a recent Gartner survey, the trend of organizations pursuing a vendor consolidation strategy has surged from 80% in 2022 to an impressive 97% in 2023. This sharp increase

underscores a widespread industry realization that a consolidated cybersecurity approach not only simplifies security operations but also enhances the effectiveness of an organization’s overall security posture,” states Srivastava of Fortinet.

“We are also witnessing a notable trend towards cybersecurity vendor consolidation within enterprises, as working with numerous vendors and solutions is impractical and ineffective. Consolidation streamlines security operations, enhances efficiency, and saves budget, akin to purchasing a comprehensive vehicle rather than individual components,” seconds Kumar of Check Point.

### Realizing the benefits

The unified approach is a paradigm shift in cybersecurity. It’s not just about consolidating tools; it’s about creating a cohesive and integrated defense strategy that adapts to the dynamic nature of cyber threats.

A unified security provides broad visibility throughout the whole IT infrastructure, breaking down barriers and allowing for a holistic view of the



“The trend of organizations pursuing a vendor consolidation strategy has surged from 80% in 2022 to an impressive 97% in 2023. This sharp increase underscores that a consolidated cybersecurity approach not only simplifies security operations but also enhances the effectiveness of overall security posture.”

**VIVEK SRIVASTAVA,**  
Country Manager, India & SAARC, Fortinet



# Pros and Cons of Multi-Vendor Security Strategies

Ripu Bajwa, Director & General Manager, Data Protection Solutions, Dell Technologies India



**W**hile a multi-vendor approach in security can offer certain benefits such as diversity of solutions and reduced dependency on a single vendor, it can also present several challenges and negative impacts for businesses:

**Complexity and Integration Issues:** Managing security solutions from multiple vendors can introduce complexity into the IT environment. Integration between different security products may not always be seamless, leading to interoperability issues, gaps in coverage, and increased administrative overhead.

**Increased Cost:** Procuring and maintaining security solutions from multiple vendors can be more expensive than opting for a single-vendor approach. Licensing fees, support contracts, training costs, and integration expenses can add up, potentially straining the organization's budget.

**Difficulty in Management and Monitoring:** With multiple security tools in place, it can be

challenging for security teams to effectively manage and monitor the entire environment. Each solution may have its own management interface and reporting mechanisms, making it harder to gain a holistic view of the organization's security posture.

**Vendor Management Overhead:** Dealing with multiple vendors requires significant effort in terms of vendor management. This includes vendor selection, contract negotiations, vendor

relationship management, and coordination of support activities. This overhead can divert resources and attention away from core security objectives.

**Increased Vulnerability Surface:** Each security solution introduces its own set of potential vulnerabilities. Managing multiple vendors means having to track and address vulnerabilities across various products, increasing the organization's overall attack surface and potentially exposing it to more security risks.

**Fragmented Support and Accountability:** When issues arise, the presence of multiple vendors can lead to finger-pointing and a lack of accountability. It may be unclear which vendor is responsible for resolving a particular issue, leading to delays in incident response and resolution.

**Training and Skill Requirements:** Security personnel need to be trained on the use and administration of each security product, which can be time-consuming and resource-intensive. Maintaining proficiency across multiple platforms may also require additional investment in ongoing training and certifications.

Overall, while a multi-vendor approach can offer flexibility and diversity in security solutions, businesses need to carefully weigh the potential drawbacks. It is essential to strike a balance between leveraging best-of-breed solutions and minimizing the negative impacts of a fragmented security landscape for more efficient results.



**RIPU BAJWA**, Director & General Manager,  
Data Protection Solutions, Dell Technologies India





organization's security posture. "This improved visibility enables faster threat detection and more effective incident response. Secondly, a single security system simplifies integration by ensuring smooth communication among various security components," shares Ganjoo of F5.

"Interoperability, better visibility, reduction in false alarms, improved functionality, data centralization, effective sharing of threat intelligence among tools, smooth orchestration, and an improved MTTR in case of any breach, are some of the key advantages of a unified security platform," adds Shetty of Essen Vision.

The benefits of a unified security offering extend beyond streamlined operations and enhanced resilience. Organizations that have successfully transitioned to consolidated security stacks report substantial cost reduction and improved results in their cybersecurity efforts.

Not only does it reduce the total cost of ownership by minimizing the expenses associated with managing and maintaining disparate security tools, but it also

yields better results in terms of threat detection and response.

"The cost-effectiveness of a unified security offering is evident in both the short and long term. A global manufacturing company that switched to a unified security offering from Zscaler, resulting in significant benefits: The company was able to streamline its security infrastructure by reducing the number of security tools from 40 to 4 and consolidating security vendors from 15 to just 1," discloses Banerjee of Zscaler.

This consolidation allowed the company to save over \$2 million per year in security costs and achieve an impressive 300% return on investment within three years. "They experienced an 80% improvement in visibility and control, gaining better insights into their network, cloud, and endpoints, and a 50% improvement in overall security performance. The company's mean time to detect and respond to threats decreased by 90%, enabling it to swiftly address security incidents, which reduced by 70%," highlights Banerjee.



“A global manufacturing company saved over \$2 million per year in security costs and achieved 300% RoI within three years of implementing a unified security solution. The company's mean time to detect and respond to threats decreased by 90%, enabling it to swiftly address security incidents, which reduced by 70%.”

**SUDIP BANERJEE,**  
CTO, APJ, Zscaler



“Improved visibility through unified security enables faster threat detection and more effective incident response. Secondly, a single security system simplifies integration by ensuring smooth communication among various security components.”

**DHANANJAY GANJOO,**  
Managing Director, India & SAARC, F5

## Decoding the future of cyber resilience

The year 2024 stands as a pivotal moment—a moment where organizations are not just combating cyber threats but evolving their entire approach to cybersecurity. The path to cyber resilience is not a static one; it is a dynamic journey that requires adaptability, integration, and a unified mindset. As we decode this future, the message is clear: the era of consolidated security stacks is upon us, heralding a new age of cyber resilience.

As we peer into the future of cyber resilience, it becomes evident that technologies like AI/ML, Blockchain, automated threat response, and zero trust architecture will play a pivotal role in fortifying organizations against the ever-growing sophistication of cyber threats.

“We expect zero trust to be mandated in a wide range of industry use cases which will start a robust effort to develop real zero trust architectures for various industries. And with it, certifications will emerge to check solutions that only embrace parts of zero trust and do so in

fragmented point solutions. Zero trust only works as a comprehensive architecture for IT systems. In 2024 we will see new zero trust certifications begin to separate real zero trust from marketing gimmick,” shares Bajwa of Dell Technologies.

As organizations step into the future of cyber resilience, the emphasis on reducing complexities and embracing consolidated security stacks becomes more pronounced. This isn’t just a technological evolution; it’s a strategic shift that positions organizations to not only withstand the challenges of today but thrive in the face of the unknown threats that tomorrow may bring.

In conclusion, the unified defense strategy, facilitated by consolidated security stacks, is the cornerstone of the evolving cybersecurity landscape. As we chart the course for the future, the fusion of adaptive technologies, strategic methodologies, and a commitment to continuous improvement will be the guiding forces in building a cyber-resilient world. The era of unified defenses is not just a response to the challenges of today; it is a proactive stance against the uncertainties of tomorrow.



**CHERIAN THOMAS,**  
Director, Wysetek Systems

# The Highest Risk for a Breach in Organization is Insider Threat

Cherian Thomas, Director, Wysetek Systems, shares invaluable insights into the latest trends and challenges in a brief interaction with Amit Singh. He discusses the growing sophistication of cyber threats, the impact of security tool complexity, and the emerging trend of cybersecurity stack consolidation

■ **Amit Singh:**  
**What are the latest trends you see in cybersecurity? Why do even well-funded, mature organizations find themselves vulnerable in the face of increasingly**

**sophisticated cyber threats?**

Cherian Thomas: One of the most critical trends in the digital landscape is the ever-increasing sophistication and persistence of cyber threats. Attackers are constantly in pursuit of developing new strategies

and techniques to breach enterprises, compromise sensitive data, and disrupt services.

This has led to an increased focus by enterprises to improve the security of their IT landscape and implement controls that take a holistic view of protecting the fragmented

attack surface and somewhat vulnerable infrastructure. Identity management, hybrid workloads, insider threats, and compliance are driving huge innovations in the security landscape of enterprises.

In the current scenario, even well-funded mature organizations find

Cont'd on Page 20





KONICA MINOLTA

# EXPERIENCE THE COLOURFUL TRANSFORMATION RETHINK COLOURS

## RETHINK INTELLIGENT INNOVATIONS FOR WORKPLACE







PRINT | COPY | SCAN

### A3 Colour & Mono Multifunctional Printers **bizhub i-Series**

For more information: SMS "KM MFP" send to 52424 or Call: 1-800-266-2525.

**Konica Minolta Business Solutions India Pvt. Ltd.**

[www.konicaminolta.in](http://www.konicaminolta.in) | [marcom@bin.konicaminolta.in](mailto:marcom@bin.konicaminolta.in)

Connect with us:      

Giving Shape to Ideas



## TRANSCON ELECTRONICS PVT. LTD.

205, 2nd Floor, Center Point Building, Hemanta Basu Sarani,  
Opp. Lalit Great Eastern Hotel, Kolkata - 700001  
Ph.: 22488118, 22488210, 22481620,  
Mobile: +91-8337071326, Fax: 03322486604  
Email: [abhishek@transconelectronics.com](mailto:abhishek@transconelectronics.com),  
Website: [www.transconelectronics.com](http://www.transconelectronics.com)

themselves at risk due to the increase in attack surface vectors, sophistication and volume of threats, and lack of visibility across the IT landscape and interoperability between the numerous point security solutions.

The highest risk for a breach in any organization is insider threat – its employees – be it the result of intentional or accidental events; most data breaches can be traced back to Identity compromise.

■ **Amit: Studies indicate that organizations use an average of 31.58 disparate security tools. How does this complexity impact visibility and hinder effective detection and response to cyber threats?**

Cherian: The complexity of the IT Landscape is the cause of vulnerabilities in an enterprise. With the sprawl in “n” number of point security solutions and tools, management and integration of the same has become a huge challenge.

The more components, dependencies, and integration, the more time and effort is spent by the IT team in managing, maintaining, and securing the enterprise. This invariably leads to a back-door entry or a vulnerability not sufficiently secured.

■ **Amit: Are you seeing enterprises consolidating their cybersecurity vendor landscape and**

**reducing complexities in cybersecurity stacks? How does this consolidation contribute to better crisis management and overall resilience during cyber threats?**

Cherian: We are increasingly seeing enterprises embarking on a journey of consolidation and enhanced integration as far as security is concerned. A consolidated security architecture uses a multi-layered approach that protects various IT attack surfaces such as applications, databases, Cloud, networks, endpoints, and identity. They essentially feed on the same threat

**does it address the visibility gaps and integration challenges seen in organizations using disparate security tools?**

Cherian: The foremost benefits of deploying a unified security architecture are visibility, interoperability, and integration. This enables better correlation of security alerts and logs across applications, databases, Cloud, networks, and endpoints thereby enabling coordinated threat detection, quicker incident response, and immediate identification of indicators of compromise in the environment. So in a nutshell it helps build a

“ A consolidated security architecture uses a multi-layered approach that protects various IT attack surfaces, enhancing management, security, and defense. It helps build a resilient security platform with better controls to prevent a breach and reduces the time to respond, difficult to achieve in a siloed approach. ”

prevention technologies and strategies thereby enhancing management, security, and defense.

■ **Amit: What, in your opinion, are the key advantages of a unified security offering, and how**

resilient security platform with better controls to prevent a breach and also reduces the time to respond which is very difficult to achieve in a siloed approach.

However, it may not be feasible to just rip and replace but I would suggest that enterprises embark on the journey towards

a Zero Trust Architecture thereby making the security landscape absolutely impregnable and highly resilient.

■ **Amit: Looking ahead to 2024, what are the major cybersecurity trends you see as organizations move towards digital transformation and cyber resilience? Do you see cybersecurity stack consolidation as a trend?**

Cherian: Modernization and automation are becoming increasingly important in security. Automated processes can help reduce the time it takes to detect and respond to breaches. In this fast-paced world, applications define the success of businesses. APIs are at the heart of every such use case. Organizations use APIs to connect to services and to share potentially sensitive data hence solutions around API protection, application monitoring, database activity monitoring, and bot protection are going to become more and more relevant.

Further, customers are increasingly having meaningful conversations with us around Zero Trust Architecture. The latest trends are to try and cover security from a holistic 360-degree angle. Solutions around cloud security, dark web monitoring, breach attack simulation, SASE, risk quantification, EUBA, and SOAR are the latest trends in the market today.



# Enterprises are going for Vendor Consolidation despite the Risk of getting Monopolized

Amit Kulkarni, Executive Vice President and Head Cybersecurity Business, Allied Digital Services, sheds light on the strategic shift towards vendor consolidation in cybersecurity, in a compelling discussion with Amit Singh. Despite the looming risk of potential monopolization by a single vendor, enterprises are actively embracing this approach. From the latest trends shaping the threat landscape to the challenges posed by disparate security tools, he sheds light on critical aspects such as response times, automation struggles, and the growing importance of consolidated security solutions. Gain valuable insights into crisis management and building resilience in the face of evolving cyber threats. Read on to gain valuable insights into crisis management and building resilience in the face of evolving cyber threats



**AMIT KULKARNI,**  
Executive VP and Head  
Cybersecurity Business,  
Allied Digital Services

### ■ Amit Singh: With cybersecurity risks topping enterprise concerns, how do you foresee the impact of emerging threats like generative AI-driven attacks, electrical vehicle attacks, and increased IoT and industrial technology threats in 2024?

Amit Kulkarni: Cybersecurity risk continues to appear at the top of the risk register for most enterprises. Attack vectors are multiplying, and attackers become more sophisticated every day. Cyberspace is now a contested military domain occupied by a mix of state actors, intelligence agencies, hacker groups, and private companies.

Based on some of the top research firms, the following important areas are going to be of major focus in 2024:

- Generative AI-driven attacks
- Electrical vehicle attacks
- Increased attacks on IoT and industrial/operational technologies
- Rise in ransomware attacks
- Supply chain attacks
- Zero-trust architecture

Cybercriminals are continuously evolving their tactics to bypass security defenses and exploit vulnerabilities. Mature organizations have a more complex infrastructure with numerous connected systems, applications, and devices with a large number

of employees who are susceptible to cyber-attacks through phishing or social engineering. The attack surface to enforce security measures has increased which makes it difficult to protect the organization from cyber threats. On the other side, an increased number of security vendors and specialized point solutions have made it difficult to create a unified secure environment with the best possible product implementation with interconnection and management.

### ■ Amit Singh: While the use of multiple security tools offers

“Despite the risk of getting monopolized by one vendor, enterprises are going for vendor consolidation. This provides them benefits such as seamless integration and interoperability, improved security effectiveness, better automation capabilities, simplification in operations and management, better team management due to consolidation in skills, and finally, cost optimization.”

### diversified protection, how do you address the challenges of implementing and integrating these tools seamlessly for effective threat intelligence sharing and automated response workflows?

Amit Kulkarni:

Organizations conventionally prefer to select multiple vendors/ products to avoid dependency on one vendor and have different layers of protection from different sets of product owners with best-of-the-class products for certain segments of the requirement. Though the reasons for selecting multiple products are right, there are several disadvantages to having a large number of security tools to protect your environment.

Implementing the security tool as per best practices and integrating disparate security tools to share data and orchestrate response actions can be complex and time-consuming. Compatibility issues, lack

making it challenging to gain a comprehensive view of the organization's security posture and effective detection and response to cyber threats.

### ■ Amit Singh: How crucial is an effective and swift security incident response in preventing extensive damage during a cyber threat or attack, especially concerning the risk of attackers gaining extended access and potentially exfiltrating sensitive data, leading to regulatory consequences, legal issues, and reputational harm?

Amit Kulkarni: We are moving towards building a more cyber resilience infrastructure which refers to an organization's ability to anticipate, withstand, recover from, and adapt to cyber threats and incidents while continuing to operate effectively.

Security incident response is the structured process that organizations follow to effectively detect, investigate, mitigate, and recover from cybersecurity incidents. These incidents can range from malicious attacks, such as malware infections and data breaches, to inadvertent events, such as accidental data loss or system outages. The primary goals of security incident response are to minimize the impact of the incident, restore normal operations, and prevent

similar incidents from occurring in the future.

Identifying and containing a security incident or an active attack is extremely critical. In case of the extended response time, there is a risk of the attacker gaining unlimited lateral access within the infrastructure. This may lead to extended downtime or exfiltrate valuable data, such as customer records, intellectual property, or financial information, leading to regulatory fines, legal liabilities, and damage to brand reputation.

■ **Amit Singh: How does the deployment of automation and orchestration get affected when organizations rely on poorly integrated security tools? What role does this play in the meantime to detect and respond to cyber threats?**

Amit Kulkarni: As the interoperability between the tools is restricted, automation and orchestration are limited based on each tool's ability to interact with the other tool. Poorly integrated security tools can create a significant set of challenges like limited data exchange between the tools, incomplete visibility, slower response time, and increased human interventions.

In the absence of automated data aggregation and correlation, security teams may struggle to gain comprehensive visibility into the organization's

IT environment security. Without automation, security teams may rely on manual processes to detect and analyze security incidents. This can lead to delays in identifying suspicious activities or anomalies. It may also overwhelm analysts, leading to alert fatigue and delays in prioritizing and investigating critical alerts.

■ **Amit Singh: Are you seeing enterprises consolidating their cybersecurity vendor landscape and reducing complexities in cybersecurity stacks? How does this consolidation contribute to better crisis management and resilience during cyber threats?**

Amit Kulkarni: Gartner in 2022 came up with the concept of Mesh Architecture. It means every security system integrates with every other security system in the cybersecurity architecture. According to Gartner, adopting a cybersecurity mesh architecture will reduce the financial impact of security incidents by an average of 90%. This level of interconnectivity between the tools can be achieved only if they are from one vendor. But having all the tools from one vendor poses a risk of putting all the eggs in one basket.

Despite the risk of getting monopolized by one vendor, enterprises are going for vendor consolidation. This provides them benefits such

as seamless integration and interoperability, improved security effectiveness, better automation capabilities, simplification in operations and management, better team management due to consolidation is skills, and finally cost optimization.

Consolidation provides a centralized platform and visibility for better control and incident management. A consolidated security infrastructure can enhance overall resilience to cyber threats by providing a more cohesive and coordinated defense posture. With integrated security solutions, organizations can adapt more quickly to evolving threats, deploy countermeasures rapidly, and adjust their security strategies in response to changing threat landscapes, ultimately improving their ability to withstand and recover from cyber crises.

■ **Amit Singh: What are the best practices you would suggest to improve cyber resilience through reduced complexities, increased visibility, and effective detection and response?**

Amit Kulkarni: Cyber resilience is crucial for organizations to withstand and recover from cyber threats effectively. It helps minimize the impact of security incidents, maintain business continuity, protect sensitive data, and preserve trust and reputation with customers and stakeholders. Best practices improve cyber resilience by reducing

complexities, increasing visibility, and enhancing detection and response capabilities:

- Conduct regular risk assessments by using certain global frameworks like NIST, ISO 27001, CIS controls to identify and prioritize cybersecurity risks across the organization. Assessments should consider factors such as threat likelihood, potential impact, existing vulnerabilities, and critical assets.
- Centralized 24x7x365 SOC for security monitoring, and threat detection to proactively identify and respond to emerging threats in real-time by using automation and orchestration tools to reduce manual effort, improve response times, and scale security capabilities.
- The most important aspect of cyber resilience is the recovery in case of an attack. Build comprehensive incident response plans and conduct regular tabletop exercises and simulations to test the effectiveness of response procedures. Practice scenarios ranging from common threats to advanced persistent threats (APTs) to ensure readiness and improve coordination between stakeholders during cyber.
- Provide regular cybersecurity training and awareness programs to educate employees about common threats, best practices, and security policies.





## **Enterprises Demand Integrated, Holistic Solutions to Maximize Security, Visibility, and Agility**

**DEBASISH MUKHERJEE,**  
Vice President, Asia Pacific and Japan,  
SonicWall

Debasish Mukherjee, Vice President, Asia Pacific and Japan, SonicWall, in a detailed interaction with Amit Singh, shares profound insights into the vulnerabilities that even well-funded organizations face in the relentless battle against cyber threats. From the nuanced challenges of cyber hygiene to the exploitation of legacy defenses, he delves into the complex dynamics shaping the cybersecurity landscape. Read on to deep dive into the intricate world of cybersecurity as Mukherjee unveils the critical role of unified security solutions in fortifying organizations against evolving threats, providing strategic guidance for navigating the ever-changing cybersecurity terrain.

■ **Amit Singh: In the face of increasingly sophisticated cyber threats, why do even well-funded, mature organizations find themselves vulnerable, and how do attackers exploit cyber hygiene issues or compromise legacy defenses?**

Debasish Mukherjee:

While organizations today are much more aware and consciously investing in cybersecurity solutions, the challenges are still ever so dynamic. Sometimes just the simple lack of proactive cybersecurity practices means ransomware, malware, and other threats easily go unnoticed.

Large organizations mean hundreds or thousands of employees, which in turn means hundreds or thousands of endpoints to be secured, an extensive roster of IoT devices, multiple physical locations to protect, plus expansive network and cloud environments affording incalculable access points to cybercriminals.

Once cybercriminals have exploited a target, attackers will attempt to download and install malware onto the compromised system. In many instances, the malware used is a newly evolved variant that traditional anti-virus solutions don't yet know about.

■ **Amit: How does the deployment of automation and orchestration get affected when organizations rely on poorly integrated**

**security tools? What role does this play in the meantime to detect and respond to cyber threats?**

Debasish: To combat today's dynamic and vulnerable cyber threat environment, organizations are deploying a variety of the latest and newer security tools and services from maybe different partners or vendors. One major issue in such a scenario is how to integrate these various offerings into the organization's existing infrastructure to create and support a cohesive security solution.

Integrating various tools with their different features and capabilities can become a nightmare for any security leader. In our opinion, no matter what security philosophy an organization adopts, it's critical that all individual solutions work together to deliver layered protection and comprehensive visibility with control.

Furthermore, organizations need to from time to time take stock of their cybersecurity tools to ensure that there is end-to-end visibility and the ability to share intelligence across the unified security framework. These tools need to provide real-time and consolidated threat information that can then form the basis of informed security policy decisions.

■ **Amit: As organizations grapple with rapid digital transformation initiatives, how do siloed security**

**solutions exacerbate the challenges they face? Are you seeing enterprises consolidating their cybersecurity vendor landscape and reducing complexities in cybersecurity stacks?**

Debasish: It is very evident in today's time that siloed solutions can't keep up with modern cybersecurity needs. The dynamic nature of cyber threats is making solutions redundant very quickly.

Today's demands

■ **Amit: What are the key advantages of a unified security offering, and how does it address the visibility gaps and integration challenges seen in organizations using disparate security tools?**

Debasish: Moving to a unified security solution can make all the difference in helping organizations achieve enhanced long-term value. It provides tremendous flexibility to develop and constantly

“Today's demands are more on the lines of integrated, holistic solutions that can maximize security, visibility, and agility. With cybersecurity becoming a major part of any organization's core business strategy, there is a need to understand attackers' tactics, techniques, and procedures (TTPs), and commit to threat-informed cybersecurity strategies.”

are more on the lines of integrated, holistic solutions that can maximize security, visibility, and agility. With cybersecurity becoming a major part of any organization's core business strategy, there is a need to understand attackers' tactics, techniques, and procedures (TTPs), and commit to threat-informed cybersecurity strategies to defend and recover successfully from business-disrupting events. This surely calls for integrated solutions and consolidated cybersecurity partners and vendors.

update and upgrade the company's physical and virtual security operations. All systems can be managed from a common platform, making system functionality consistent across all tasks. This equates to simpler, less expensive system additions, and hardware, and software upgrades.

SonicWall's approach to Unified Threat Management (UTM) creates a security environment that delivers firewalling, content protection, anti-virus, anti-spam, and intrusion prevention on a single hardware platform.

Protection starts at the gateway, and blocks both internal and external threats, at multiple access points and all network layers.

### ■ Amit: What are the best practices you would suggest for improving cyber resilience through reduced complexities, increased visibility, and effective detection and response?

Debasish: Today security teams and organizations live in difficult times with increased incidences of sophisticated threats and attacks that are being developed by highly skilled cybercriminals. Also, these cybercriminals clearly understand that security teams often lack the human and financial resources necessary to keep pace and may not be well-equipped to defend against the latest threat.

In such a scenario, it's very important to have a more holistic and intrinsic approach to securing your organization.

First and foremost, understanding the risks is very critical. Decision makers must understand the risks that their organizations face from the vast number of threat scenarios - phishing, spearphishing, CEO Fraud/BEC, ransomware, traditional malware, crypto-mining malware, other threats, and just dumb mistakes and address them as a high priority.

Conducting a security audit thus then becomes necessary once a risk assessment is done. Taking stock of an organization's current security infrastructure,

including its security awareness training programs, the security solutions they have in place, and the processes it has implemented to remediate is a crucial step towards protection.

Security solutions deployment should be a holistic exercise, from the cloud services that are employed to detect and remediate threats down to every endpoint solution. This doesn't mean single sourcing of security infrastructure, but it does require that appropriate reporting and monitoring mechanisms be in place so that security teams can have a full understanding of their organization's security posture in as close to real-time as possible.

Employees form the most important asset of an organisation therefore it's necessary to have proper training and awareness programs put in place that will equip them to make better judgments about the emails they receive, how they surf the web, how they use social media, and so forth. The goal of any security awareness training program is to help users to be more aware and more skeptical about what they receive in email, what they view on social media, and what they consider to be safe to access.

### ■ Amit: Can you share insights from successful cases where organizations have transitioned to consolidated security stacks? What benefits have they experienced in terms of cost reduction, improved results, and

### overall cybersecurity resilience?

Debasish: As companies expand and grow, with multiple offices and a huge number of connected devices, combined with the complexity of business networks bring to light the need for stronger defense and a more secure remote access solution.

Our clients across industry segments cater to a wide range of business needs and operations. With the advent of Work from Anywhere (especially post-pandemic) becoming more of a business necessity, the need for advanced email and web security solutions and endpoint protection becomes necessary.

Our experience with our customers has shown that deploying holistic and integrated security solutions creates better end-to-end visibility and the ability to share intelligence across the unified security framework is more accurate. Also, the detection and remedy of risks can be done at a much greater speed and an advanced level. In the long run, collection, and consolidation of all the threat information and data helps organizations to form robust security policies and practices in place.

### ■ Amit: Moving forward, do you believe more organizations will focus on reducing complexities and turning to consolidated cybersecurity stacks? What industry trends and developments are driving this shift toward a unified

### defense strategy?

Debasish: Enterprise security has become a very common and concerning topic of discussion for today's SMEs and large corporates. Today, thousands of organizations are out shopping for new or upgraded cybersecurity solutions. While they may differ in size, industry, use case, and more, at the end of the day, they're all looking for basically the same thing: A reliable solution that performs as advertised, at a price that fits within their budget, that can be up and running as soon as possible thus providing real-time effective solutions to combat and manage complex networks from a single pane of glass. This trend is something that's here to stay for as long as dynamic cyber threats are lurking around.

Also if organizations are going to have any hope of keeping up with their expanding attack surfaces and growing number of at-risk systems and devices, they're going to have to maintain an automated, comprehensive, and adaptable vulnerability management program that can proactively mitigate risks throughout all attack surfaces.

We have witnessed that many SMB organizations (specifically) who can't manage and monitor their complex cybersecurity environment eventually engage with Managed Security Service providers to combat attacks and challenges so they can then stay focussed on their core business. This is a trend that would continue to make sense in today ever evolving environment.



# Automation and Orchestration Work Best When There is a Unified, Integrated Security Stack to Share Information in Real-Time



**DHANANJAY GANJOO,**  
Managing Director, India & SAARC, F5

Dhananjay Ganjoo, Managing Director, India & SAARC at F5, in an interesting conversation with Amit Singh, sheds light on vulnerabilities faced by well-funded organizations. Addressing the pressing issues of delayed upgrades, advanced persistent threats, and low-security awareness, he proposes a strategic embrace of upcoming technologies. From AI telemetry for proactive cybersecurity to data masking for compliance, Ganjoo navigates the complexities and highlights the importance of a unified security approach. Read on for an insightful conversation on fortifying cybersecurity resilience in the face of ever-evolving threats

■ **Amit Singh: In light of the persistent vulnerability of well-funded organizations to sophisticated cyber threats, could you elaborate on the specific challenges contributing to this vulnerability?**

Dhananjay Ganjoo: Despite the proliferation of cybersecurity recommendations and significant increases in worldwide cybersecurity investments, we still see that well-funded organizations are vulnerable to sophisticated cyber threats. According to PwC, Cyber risks are cited as the biggest threat faced by Indian organizations, with 38% of respondents feeling highly or extremely exposed to it. This is majorly due to the complexity of their IT systems, human-related risks such as social engineering, and

supply chain security issues. Delayed upgrades, advanced persistent threats, low-security awareness, restricted finances, and the rapid growth of cyber threats all contribute to this vulnerability.

Therefore, to strengthen their security infrastructure, organizations can leverage the upcoming technologies:

- **AI Telemetry for Cybersecurity:** By continuously collecting and analyzing vast amounts of data from diverse sources, AI algorithms can swiftly identify anomalies, potential breaches, and emerging threats. This proactive system will help organizations with real-time response and adaptation and enhance overall cybersecurity effectiveness.
- **AI in API Testing:** Incorporating Artificial Intelligence (AI) into API testing is a strategic move poised to enhance business

operations. AI-driven tools create test scripts, predict issues, and identify patterns, streamlining testing processes.

- **Data Masking for Security:** As cyber threats surge and data protection regulations tighten, the need for data masking software is set to soar. Recently, the Indian Government implemented Aadhaar Card Masking due to privacy concerns. Businesses, across sectors like healthcare and finance, are leveraging data masking to ensure compliance, bolster security, and safeguard sensitive information.

■ **Amit: How does prolonged reaction time affect cybersecurity resilience in managing hybrid and multi-cloud infrastructures amid expanding cloud**

**workloads, given the rapid evolution of cyber threats?**

Dhananjay: The intricacies of managing hybrid and multi-cloud infrastructures, combined with the rapid expansion of cloud workloads, present substantial opportunities for attackers to obtain a foothold in the cloud. The attack surface expands quickly, often in unexpected or inadequate ways, as businesses store and handle more data in the cloud. The extended reaction time of about 6 days, with 60% of organizations taking more than 4 days to handle security warnings, is extremely troubling in a threat landscape where attackers move quickly, frequently within hours. These delays give plenty of opportunity to the threat attacker to exploit vulnerabilities. Prolonged reaction times cause additional damage, and data breaches

allow attacks to build persistence within hacked systems. In an environment where rapid and targeted cyber assaults are common, lowering response times is critical for minimizing possible damage thus strengthening cybersecurity resilience.

### ■ Amit: How do poorly integrated security products impact the adoption of automation and orchestration in organizations striving to enhance their cybersecurity programs?

Dhananjay: As cyberattacks increase with each passing day, organizations are driven to allocate a significant portion of their budgets to enhancing their security programs, safeguarding corporate assets, brand reputation, and infrastructure from hackers. As per the PwC report, 55% of Indian organizations are making bold investments in cybersecurity. They are shifting their focus on implementing complete incident response plans, processes, and workflows to respond to anticipated occurrences. However, some organizations face challenges as they rely on poorly integrated security products which have a substantial impact on automation and orchestration adoption. Automation and orchestration work best when there is a unified and integrated security stack to share information in real-time. With poorly linked solutions, the automated process becomes fragmented, resulting in delays, inefficiencies, and potential gaps in threat detection and response.

Security orchestration and automation solutions enable a more focused and streamlined approach and

methodology for detecting and responding to cyber threats by integrating the company's security capacity and resources with existing experts and processes, automating manual tasks, orchestrating processes, and workflows, and resulting in faster and more effective incident response.

### ■ Amit: How are enterprises benefiting from the trend of consolidating their cybersecurity vendor landscape, and in what ways does a unified security offering address visibility gaps, integration issues, and enhance overall cybersecurity resilience?

Dhananjay: There is a noticeable trend among enterprises towards

“ AI algorithms swiftly identify anomalies, potential breaches, and emerging threats, offering real-time response and adaptation to enhance overall cybersecurity effectiveness. ”

consolidating their cybersecurity vendor landscape and reducing complexities in cybersecurity stacks. According to a recent survey by PwC, 71% of Indian organizations are gathering and analyzing cybersecurity and IT data for risk management and opportunity identification. Indian businesses are seeing technology disruptors as opportunities, with 69% of Indian executives seeing Generative AI as an opportunity. Organizations are progressively consolidating their cybersecurity vendor landscape to streamline operations and improve resistance to cyber

threats. This move intends to improve visibility, increase incident response efficiency, and minimize complexity. The cost savings, increased coordination among security departments, and ease of compliance all indicate a dedication to establishing a robust cybersecurity posture in an ever-changing threat landscape.

In my perspective, a unified security offering provides significant benefits by resolving visibility gaps and integration issues seen in organizations that use separate security tools. For starters, it provides broad visibility throughout the whole IT infrastructure, breaking down barriers and allowing for a holistic view of the organization's security posture. This improved visibility enables faster threat detection and more effective incident response. Secondly, a single security

system simplifies integration by ensuring smooth communication among various security components. This minimizes the difficulties of administering many tools, resulting in more efficient and integrated security operations. Furthermore, unified offerings frequently provide centralized management, which reduces the need for different interfaces and simplifies the entire security architecture. Finally, this method improves the organization's ability to respond to evolving threats, increases operational efficiency, and promotes overall cybersecurity resilience.

### ■ Amit: What are the best practices you would suggest for improving cyber resilience through reduced complexities, increased visibility, and effective detection and response?

Dhananjay: Given the fast development of networks and the evolving threat landscape, attaining cyber-resilience is difficult as businesses lack real-time information on the security posture of their IT assets and infrastructure.

Because no organization is too small, obscure, or off-the-radar to be targeted by a cyber-attack, cyber-resilience is essential for modern organizations. Companies must keep up with the threat landscape and strengthen their defenses as more sophisticated assault activities reach common hacker groups.

Here are some of the steps that organizations can take to increase its cyber-resilience:

- Adopting a cybersecurity framework
- Maintaining security during web application development
- Automating and integrating security tools
- Performing consistent, threat assessment and security testing
- Encrypting web application data
- Constantly updating security patches
- Applying authentication, role management, and access control
- Avoiding Security Misconfigurations
- Train stakeholders with application security training
- Regular scanning for security threats
- Onboarding security solutions such as WAF & WAAP



**RIPU BAJWA,**  
Director & General Manager,  
Data Protection Solutions, Dell Technologies India

## Integrating Recovery as the Capstone of Cybersecurity Framework Offers True Cyber Resiliency: Dell Technologies

In an era dominated by rapid technological advancements and the omnipresent threat of cyberattacks, enterprises face an uphill battle in fortifying their cybersecurity posture. Ripu Bajwa, Director & General Manager, Data Protection Solutions, Dell Technologies India, delves into the complexities of cybersecurity, recovery challenges, and the evolving threat landscape, in this exclusive interview with Amit Singh. Bajwa sheds light on the factors contributing to organizations' susceptibility, the impact of recovery processes, and the paradigm shift towards unified security offerings. Join us in unraveling the nuances of cybersecurity and the path forward in the digital realm.

■ **Amit Singh: In light of the escalating cyber threats and the significant impact on enterprises, could you elaborate on the factors contributing to their susceptibility and the challenges**

**associated with recovery processes?**

Ripu Bajwa: Cybersecurity is more critical than ever, given the rapid technological advancements and the increasingly sophisticated cyber threats. According to the Dell Technologies 2023 Innovation Index report, just

33% of Indian businesses have evaluated a larger, distributed attack surface for potential risks. With an attack occurring every 11 seconds, cybersecurity can no longer be an afterthought. Some of the major reasons why even bigger enterprises are falling prey to

cyberattacks include:

**Unchecked digitization:**

The unprecedented growth of blockchain and cryptocurrency has given threat actors unprecedented access to the sector. This, coupled with newer and evolving phishing mechanisms, has given



access to targeting the banking industry with new and improved TTPs.

**Limited institutional sharing of threat intelligence:** While collecting data/ information from diverse sources may be easy, deploying threat intelligence to improve mechanisms to detect and respond is more difficult. Currently, there is a lack of agility in the security teams to prioritize and execute the detection and response mechanisms.

**Limited knowledge of security protocols:** Employees are the first layer of defense in most cases and the lack of detection infrastructure retards the time to respond to threats. Executives will likely have to embrace new digitization cybersecurity norms to meet business requirements, irrespective of the cybersecurity maturity levels of their organization.

**Arduous recovery processes:** Recovery cyberattacks can be unpleasant and time-consuming. It also gives leeway to attackers to launch another campaign while the system recovers from previous incidents.

This has prompted businesses in India to re-look their cybersecurity strategies and upgrade their security infrastructure for the future of work. The changing tech landscape has shifted the overall business approach to cybersecurity. Continuous monitoring, threat intelligence, and advanced security technologies are now standard practice. However, we continue to underline that the same new-age technologies being used by businesses for growth and risk-detection, like Artificial

Intelligence, open multi-cloud ecosystem, 5G, and Internet of Things, expand the attack surface for cyber threats. This has brought critical sectors like health, energy, and finance, to the limelight due to their vulnerability to cyber threats.

## ■ Amit: How does an extended response time in cybersecurity impact an organization?

Ripu: An extended response time in the context of cybersecurity can have significant consequences in a threat landscape where attackers act within hours. Here's why:

**Increased Attack Window:** With attackers operating swiftly, every minute counts. An extended response time

legal repercussions.

**Escalation of Attack:** Attackers often escalate their tactics if they perceive that their initial attempts are not being addressed promptly. An extended response time may embolden attackers to launch more sophisticated attacks or expand their scope, exacerbating the impact on the targeted organization.

**Compromised Infrastructure:** Delayed response allows attackers to establish a foothold within the network, making it harder for defenders to detect and eradicate the threat. This could lead to persistent access, allowing attackers to carry out further malicious activities undetected.

**Regulatory Compliance Violations:** In many industries, organizations

prolong the recovery process, leading to long-term damage to the brand.

This is one of the reasons why we recommend the IPDRR formula. Integrating recovery as the capstone of the cybersecurity framework offers any business true cyber resiliency.

Identification: Itemize and justify the specific elements to be protected and why

**Protection:** Determine the specific protection elements needed and how to implement them

**Detection:** Put in place strategies and actions that detect potential cybersecurity breaches quickly and accurately

**Response:** Plan the communication, analysis, mitigation, and improvements to apply in the event of a breach

**Recovery:** Construct recovery plans that include improvement contingencies and thorough communication.

## ■ Amit: How does a Security Orchestration Automation and Response (SOAR) platform streamline cyberattack response, particularly in reducing response time and aiding data recovery?

Ripu: The Dell Technologies 2024 Global Data Protection Index Cyber Resiliency Multi-Cloud Edition helped us evaluate that in today's digital landscape, robust data protection measures and AI security are indispensable for any business, safeguarding sensitive information from potential breaches

“ A consolidated cybersecurity approach often results in cost savings and operational efficiencies, as organizations can rationalize their security investments and optimize resource allocation ”

means a longer window of opportunity for attackers to carry out their malicious activities, potentially causing more damage or achieving their objectives before defensive measures can be put in place.

**Data Breach:** A delayed response increases the likelihood of a successful breach. Attackers can exploit vulnerabilities, steal sensitive data, or disrupt critical systems during this time, leading to financial losses, reputational damage, and

are subject to regulatory requirements mandating timely response to security incidents. Failing to meet these requirements can result in penalties, fines, and legal actions, further adding to the consequences of delayed response.

**Reputational Damage:** News of a security breach or data leak can severely damage an organization's reputation and erode customer trust. A delayed response may exacerbate the negative publicity and

and ensuring the trust of customers and stakeholders. Additionally, a well-defined solution for data recovery is equally crucial, serving as a contingency plan to swiftly address and rectify any instances of data corruption or loss, thereby minimizing disruptions and preserving the integrity of business operations.

A Security Orchestration Automation and Response (SOAR) platform essentially acts as an open platform that helps an organization automate its response to a cyber-attack or a threat to an attack by orchestrating the chain of actions. SOAR reduces the time taken to address a cyberattack and remedy a gap in cybersecurity. There are three key components of SOAR, which include threat and vulnerability management, response to threats, and automation of security operations.

SOAR includes pre-set guides that will lead individuals in the organization facing an issue to take insights from the platform while resolving or dealing with an attack. This allows flexibility for an organization to invest in SOAR platforms while not having the appropriate data science skills in the employees. Recovery of data can be done in less time with aid from a SOAR platform while ensuring that the impact of the attack is controlled.

When compared to traditional methods, SOAR does not require an IT analyst or have a prerequisite of data science skills in an individual while initiating a response to a cyberattack. In SOAR,

the response to an attack is automatically initiated when it detects an anomaly. Thus, it can reduce response time and control the damage caused by a cyberattack. This platform also has the added advantage of broader aggregates of security data from third-party sources and endpoints, thus a more diverse familiarity with vulnerabilities against which the platform can warn an organization. An organization will also be able to protect large volumes of data at different locations through a common protocol while using SOAR platforms.

### ■ Amit: How does the growing trend among enterprises to consolidate their cybersecurity vendor landscape contribute to streamlined operations, improved crisis management, and enhanced overall resilience during cyber threats?

Ripu: In recent years, we have observed a growing trend among enterprises towards consolidating their cybersecurity vendor landscape, aiming to streamline operations and reduce complexities within their cybersecurity stacks. This consolidation involves adopting integrated security platforms or suites that offer comprehensive protection across various threat vectors.

This shift towards consolidation brings several benefits, particularly in terms of crisis management and overall resilience during cyber threats. By reducing the number of vendors and solutions in their

cybersecurity infrastructure, enterprises can achieve greater visibility and control over their security posture. This centralized approach enables faster detection and response to security incidents, as security teams can more efficiently correlate and analyze data from disparate sources.

Moreover, consolidation facilitates better coordination and collaboration between different security functions, such as network security, endpoint protection, and threat intelligence. This alignment improves the organization's ability to mount a unified defense against cyber threats and enhances its overall resilience to evolving attack techniques.

Furthermore, a consolidated cybersecurity approach often results in cost savings and operational efficiencies, as organizations can rationalize their security investments and optimize resource allocation. This allows them to allocate more resources towards proactive security measures, such as threat hunting and security awareness training, thereby further strengthening their cybersecurity posture. As enterprises continue to prioritize cybersecurity amidst evolving threat landscapes, this trend towards consolidation is expected to persist, driving further improvements in security posture and risk mitigation strategies.

### ■ Amit: What are the major cybersecurity trends you see over 2024 as organizations move towards digital transformation and

### cyber resilience?

Ripu: Dell Technologies aims to catalyze customers to achieve Zero Trust outcomes by making the design and integration of this architecture easier. Zero Trust is the way that we will end up securing AI, and ultimately quantum will be the thing that powers it over the long term for the performance and efficiency needed to scale it into a global system.

We expect zero trust to be mandated in a wide range of industry use cases which will start a robust effort to develop real zero trust architectures for industries ranging from core defense to universities performing government-funded research, to critical infrastructure industries and parts of our digital infrastructure. And with it, certifications will emerge that correct one of the major issues with zero trust – anyone can call anything zero trust even if they only embrace parts of zero trust and do so in fragmented point solutions. Zero trust only works as a comprehensive architecture for IT systems. In 2024 we will see new zero trust certifications begin to separate real zero trust from marketing.

Cybersecurity consolidation and automation go a long way in ensuring better results. Shared intelligence across the cybersecurity stack means teams can maximize the use of automation and AI/ML while being a more cost-effective solution. Vendor sprawl during times of crisis is not even a consideration for organizations with consolidated security stacks.

# Unified Security Improves up to 80% Visibility and Control, 50% Security Performance: Zscaler



SUDIP BANERJEE, CTO, APJ, Zscaler

As the digital landscape evolves, organizations face escalating cyber threats that challenge traditional security models. Even well-funded enterprises grapple with vulnerabilities stemming from outdated approaches. Sudip Banerjee, CTO, APJ, Zscaler, underscores the urgency for organizations, irrespective of financial prowess, to transition to a zero-trust security model and embrace cloud-native platforms, in a brief interaction with Amit Singh. In this insightful interview, he delves into the limitations of outdated security models, the role of automation and orchestration, and the best practices to enhance cyber resilience. Banerjee also shares success stories of organizations streamlining security stacks and provides a forward-looking perspective on the cybersecurity landscape.

■ **How can organizations address the challenges of fragmented data and alerts in modern cybersecurity environments, and what role does a cloud-native platform integrated with AI play in enhancing detection, response, and overall security posture?**

The complexity of modern cybersecurity environments often results in fragmented data and alerts that are difficult

to correlate and analyze, impeding effective detection and response capabilities. This fragmentation causes delays in investigation and remediation processes, increases the risk of human error, and limits the agility and scalability of security operations. To overcome these challenges, organizations should adopt a cloud-native platform integrated with AI, providing comprehensive visibility across users, devices, applications, and workloads. This platform enables fast and automated detection and response to cyber threats, ensuring a proactive

and efficient security posture.

Zscaler's data security platform offers a unified approach to data protection, threat prevention, and posture management, streamlining security operations and effectively defending against evolving threats. By leveraging a cloud-native platform integrated with AI, organizations can enhance visibility, accelerate detection and response, and effectively safeguard their data and infrastructure.

■ **How does the deployment of**

**automation and orchestration get affected when organizations rely on poorly integrated security tools?**

Automation and orchestration are crucial for improving the speed and accuracy of detection and response mechanisms. However, their effectiveness can be hindered by poorly integrated security tools, facing challenges such as lack of interoperability, inconsistent data formats, manual workflows, and human errors. These obstacles compromise the



quality and timeliness of detection and response efforts, increasing the risk of security breaches. To address these challenges, organizations require a cloud-native, integrated data security platform equipped with APIs and seamless integration with leading automation and orchestration tools. This integration eliminates data and alert silos, simplifies management processes, and reduces overall complexity.

By adopting such a platform, organizations can streamline their security operations, automate repetitive tasks, share information between security tools, and reduce reliance on manual workflows. This leads to a more efficient and effective detection and response mechanism, strengthening the organization's ability to defend against cyber threats. Successful implementation of automation and orchestration relies on a well-integrated data security platform that is cloud-native, API-enabled, and compatible with leading automation and orchestration tools. Leveraging such a platform allows organizations to overcome challenges, simplify management processes, and achieve timely and consistent threat detection and response capabilities.

**■ What are the best practices you would suggest to improve cyber resilience through reduced complexities, increased visibility, and effective detection and response?**

To enhance cyber resilience, I recommend implementing several best practices:

- Adopting a Zero Trust approach, which follows a 'never trust, always verify' mindset to grant permissions and access based on user identity and context.
- Implementing a continuous security validation process to regularly test and measure the effectiveness of security controls and tools against real-world scenarios and benchmarks.

a collective effort to combat cyber threats and vulnerabilities.

**■ Can you share insights from successful cases where organizations have transitioned to consolidated security stacks?**

Let me provide you with an example of a global manufacturing company that switched to a unified security offering from Zscaler, resulting in significant benefits: The company was able to streamline its

90%, enabling it to swiftly address security incidents, which reduced by 70%. By adopting a unified security approach, they enhanced their overall cybersecurity resilience and readiness, embracing the principles of the Zero Trust model and leveraging the benefits of a cloud-native architecture.

**■ Moving forward, do you believe more organizations will focus on reducing complexities and turning to consolidated cybersecurity stacks?**

Indeed, many organizations are prioritizing the reduction of complexities and the adoption of a unified security stack due to several factors: Firstly, the increasing number of cyber threats and regulatory risks has heightened the focus on security measures, prompting organizations to seek comprehensive security solutions. Secondly, the widespread adoption of cloud, mobile, and IoT technologies necessitates the protection of dynamic environments and a diverse range of devices. Thirdly, the demand for agility, scalability, and efficiency has driven the need for secure digital transformation objectives, leading organizations to seek unified security solutions that align with their evolving requirements. Lastly, organizations recognize the importance of meeting customer expectations for seamless and secure user experiences, prompting them to prioritize a unified security approach to safeguard sensitive data and maintain trust.

**“ To enhance cyber resilience, organizations must adopt a 'never trust, always verify' mindset, implement continuous security validation, leverage AI and ML technologies, foster a strong security culture, and collaborate with industry peers for threat intelligence. ”**

- Leveraging artificial intelligence and machine learning technologies to automate tasks and augment human capabilities, enabling faster and more accurate threat detection and response.
- Building a strong security culture and awareness within the organization by providing regular training to employees and stakeholders on the latest threats and best practices.
- Collaborating with industry peers and partners to share threat intelligence and exchange best practices, fostering

security infrastructure by reducing the number of security tools from 40 to 4 and consolidating security vendors from 15 to just 1.

This consolidation allowed them to save over \$2 million per year in security costs and achieve an impressive 300% return on investment within three years. They experienced an 80% improvement in visibility and control, gaining better insights into their network, cloud, and endpoints, and a 50% improvement in overall security performance. The company's mean time to detect and respond to threats decreased by



## Tech for a Sustainable Future

**S**ustainability has moved swiftly up the executive agenda in recent years. Even at the height of the Covid-19 pandemic, becoming a truly sustainable and responsible business was a top priority for most CEOs.

Beyond the great promise of protecting people and the planet, companies with a higher sustainability performance—across environmental, social, and governance (ESG) indicators—perform better financially than their peers.

Just as digital transformation required every company to become a technology company, with technology at its heart, now every business needs to become sustainable—and technology is again taking center stage.

Technology is—and will continue to be—the fundamental driver of sustainability for organizations, and their supply chains, customers, and broader business ecosystems. As per a recent Accenture survey, 92% of companies aim to achieve net-zero targets by 2030, which will require the deployment of advanced technologies to measure, reduce, and remove an organization's carbon footprint. Technology is essential to improving transparency and traceability in global supply chains. It helps companies uncover insights to spur action, whether that means transforming customer experiences or building a more sustainable organization.

While technology is a fundamental driver of sustainability, the solution itself needs to be monitored so that it doesn't become a problem. Technology can and does create sustainability issues. For example, training a single AI model can emit as much CO<sub>2</sub> as five relatively ordinary cars do in their lifetimes. And using a mobile phone for just one hour a day for one year produces some 1.4 tons of CO<sub>2</sub>—that's more carbon emissions than two round-trip flights between London and Glasgow. This brings technology within the ambit of the sustainability efforts of organizations. Hence, the priority must be to design and deploy sustainable, green technology to harness the benefits of meeting the sustainability agenda.

There are clear benefits to harnessing technology to drive sustainability. In fact, companies that adopt sustainable technology to a significant extent achieve 4% higher ESG scores on the Arabesque S-Ray dataset—a global specialist in measuring ESG metrics—than those that do not. This can translate into an 11% jump in their ESG ranking. And between 2013 and 2020, companies with consistently high ESG performance tended to generate 2.6-times higher total shareholder returns, compared to those with mid-range ESG scores.

So, what's holding back organizations? For many, the transformation is daunting. Nearly one-fifth of the organizations say their biggest challenge is that they are not aware of the unintended consequences of technology. Lack of ready solutions is a big concern, as is the complexity associated with adopting these solutions. And then, there's what we call the intent-action gap—only 7% of companies have fully integrated their business, technology, and sustainability strategies.

As sustainability strategies take shape, the IT Leader of the business will be the common denominator as different members of the C-suite take "ownership" of specific aspects and become reliant on technology to achieve their objectives.

Moving ahead, CXOs must take a fresh look at their technology through the lens of sustainability. In this issue of ITPV Magazine, we have highlighted comprehensive sustainable technology strategy—one that makes technology more sustainable and uses that technology to drive sustainability at scale. It is time to push the reset button and reimagine a healthier, wiser, and sustainable world!

Enjoy reading and please don't forget to share your feedback at [kalpana@techplusmedia.co.in](mailto:kalpana@techplusmedia.co.in)

*Kalpana Singhal*

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

**EDITOR:** KALPANA SINGHAL  
**CONTENT HEAD:** Amit Singh  
**CONSULTING EDITOR:** Rajneesh De  
**NEWS ANALYST:** Ishita Gupta  
**CORRESPONDENT:** Bhawna Thapliyal  
**NEWS REPORTER:** Anindita Majumder, Urmi Saha

**INTEGRATED MARKETING COMMUNICATION:**  
Arunim Agrawal, Mamta Kapoor

**ASSOCIATE ANALYST**  
Shaithra S

**SALES:**  
Anushikha Singh | Pratap Jana

**PRODUCTION HEAD:**  
Aji Kumar

**WEBSITE:**  
Gaurav Rana

**PROMOTION:**  
Amit Pandey, Nikita Gurung

**CIRCULATION:**  
Pratap Ram

**FINANCE:**  
Inder Pal

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

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

**Delhi:** 91-8178321837 | **Mumbai:** 91-98997 01316  
**Kolkata & Guwahati:** 91-9331072026  
**Bangalore:** 91-8851119532

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

ITPV does not claim any responsibility to return adequate postage. All rights reserved. No part of this publication may be reproduced in any form without prior written permission from the editor. Back Page AD will carry RNI Number & Imprint Line

Note: While every possible care is taken prior to accepting advertising material, it is not possible to verify its contents. ITPV will not be held responsible for such contents, or for any loss or damages incurred as a result of transactions advertising/advertorial in this publication. We recommend that the readers make necessary inquiries and verification before remitting money or entering into any agreement with advertisers, or otherwise acting on advertisement in any manner whatsoever.

## Pantum India Product Line

Business is Complicated, Printing Should be Simple

Vibrant 18 Series



Elite Series



PT-L280 Series



PT-L380 Series



PT-B680 Series



Simple&Smart Series



Simple&Smart Series



Mighty Series



4S Efficiency Series



Max Series

**PANTUM SERVICE TOLL FREE NO.: 18003098240**

**WWW.PANTUM.IN**

SALES REGION	PHONE NOS.	SALES REGION	PHONE NOS.
West Bengal & North East	98302 28532	Bihar & Jharkhand	9334317035

Know more on @PantumIndia



**SAMSUNG**

# Interactive display for future-ready education.

## WAC Series



Experience an intuitive digital board that fulfils  
the demands of modern education.

### Key features



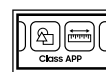
Android  
OS-based



Easy  
multitasking



Multi-screen  
sharing



Intelligent app  
for classes

Scan to know more



Image simulated for representational purposes only.  
Please dispose off e-waste and plastic waste responsibly. For more information of for e-waste pick up, please call 180057267864.

Cheit-17001/23