



# Dealing With Hypervulnerability in a **Hyperconnected World**

Building Cyber-resiliency that Leverages Improved Threat  
Visibility Using Extended Detection and Response

A LUNCH THINK TANK

Moderated by Parminder Kaur, Director & Head of Security Practice, ICT

F R O S T  S U L L I V A N



IT thought leaders from a variety of industries participated in a Think Tank luncheon hosted by Frost & Sullivan, the global growth advisory company for over 60 years.™ The group assessed the evolving hypervulnerabilities in enterprise infrastructures entrenched with digital technologies. This article will present key insights, providing a framework for enterprises ready to begin their journey of secure hyperconnectivity.

### Key Takeaways from the Discussion



A digital-first strategy is the top priority for enterprises and is leading to a hyperconnected environment.



Traditional approaches have become less effective, so enterprises must deploy lateral security across networks, endpoints, applications, and cloud workloads.



A holistic view of network, devices, cloud, and applications through unified management is imperative for extended threat detection.



Enterprises must adhere to the regulatory compliances in their IT/OT framework to minimize security risks.



Enterprises must adopt best practices for securing identity and access to minimize the threat landscape.

We live in a time of exciting, albeit risky, options for how to work and play online. As the world becomes more and more digitized, hyperconnectivity, which allows everything and everyone to connect from almost anywhere and at any time, will continue to evolve. These connections will be person-to-person, person-to-machine, and machine-to-machine; interactions will be one-to-one, one-to-many, or many-to-one. From a business perspective, hyperconnectivity will enable greater collaboration between employees, customers, partners, and vendors across the supply chain. As a result, swifter decisions will be made, more data will be accessed more quickly, and strategies and plans may even be adjusted in real time. Revenue, customer service, and operational efficiencies will improve.



## Corporate Agility at a Price

Corporate agility and hyperconnectivity come at a price. As corporate data is shared in both secure and unsecure environments, protecting it becomes a big concern. Borderless organizations, which many see as the future, will change business dynamics. Cloud applications remain pivotal in building borderless enterprises and help address business disruption and supply chain challenges. However, most next-generation technologies, such as the cloud, have opened cyberthreat avenues for criminals to exploit.

Cybersecurity, which previously centered on traditional network firewalls and endpoint security, has expanded, and now includes next-generation firewalls, application security, cloud security, workload protection, extended detection and response (XDR), identity and access protection, and much more. Security approaches such as secure access service edge (SASE) platforms that include zero trust also aim to overcome the biggest cybersecurity hurdles through cloud-delivered services.







## An Industry Perspective

Speaking with Frost & Sullivan, a Tata Communications thought leader offered this industry perspective: “CISOs are often challenged with scattered and limited threat intel of their infrastructure. Disparate systems and solution silos often leave the blind spots in their cyberdefense.” Yet the likelihood of attack has increased by about 60 to 70% in the hyperconnected ecosystem. It takes roughly 227 days to detect and contain a breach, greatly exacerbating the repercussions and damage done to enterprises large and small. A granular and unified view of the infrastructure is therefore needed to monitor and remediate threats.

India’s cybersecurity spending reached about 3.3 billion in 2022 and is on track to grow at a CAGR of 18.3% by 2025.

Hyperconnectivity is a key business enabler that requires great enterprise agility but cannot be served by a single endpoint solution. To achieve hyperconnectivity, today’s enterprises must update legacy systems, leverage secure cloud solutions, and maintain IT/OT security. **Parminder Kaur**, Frost & Sullivan, expressed, “Building cyber-resiliency is important. But it requires a comprehensive approach that includes strategy, visibility, compliance, and risk evaluation to identify security gaps and achieve the desired security posture.”





# Security for a Hybrid Workforce

The shift to hybrid work has exacerbated many of today's technology challenges. When the COVID-19 pandemic and transition to remote work accelerated, faster migration to the cloud became necessary, and many on-premises network and security protocols have been lost.

**Kaur** noted:

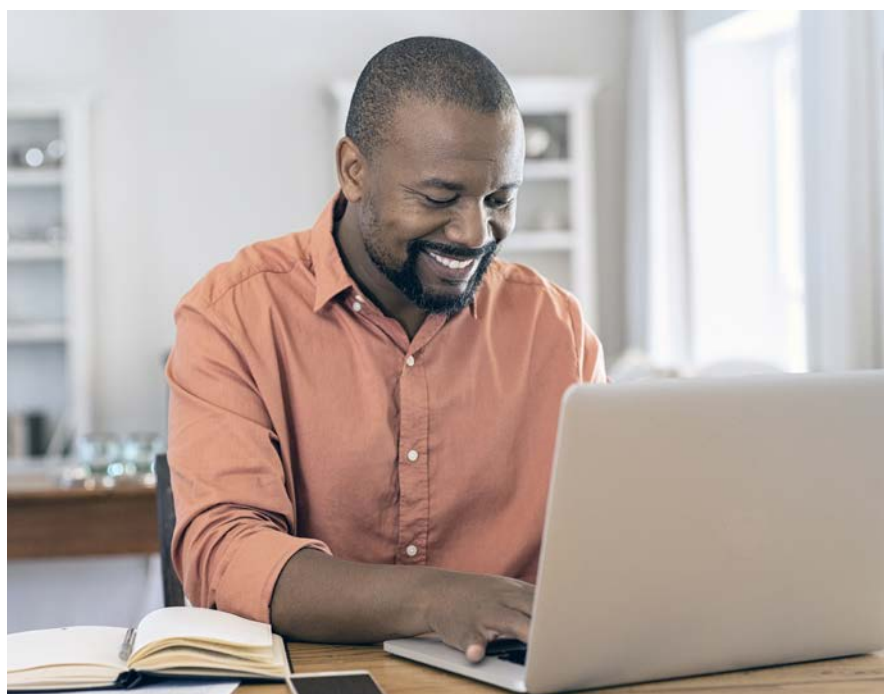
“

**IT administrators and chief security officers are faced with the mammoth task of protecting far-flung workspaces and mobile devices from greater exposure and ongoing security threats. Remote arrangements mean less direct oversight of employee activities, making educating employees about security risks and protocols critical.”**

Bad actors continue to exploit the distributed work landscape, and security breaches are rampant. **Praveen Mishra**, Yes Bank, stated, “Moving outside the perimeter and investing in the cloud, working on your organization's governance, risk, and compliance (GRC) and zero trust implementation will help in securing the new perimeter.”

Industries must comply with regulations or guidelines to build strong cyberdefense.

The CERT-In mandate to report cyberincidents within 6 hours comes at a time when enterprises have limited threat visibility. This step from CERT-In intends to improve organizations' security posture and will lead them to invest in best-of-breed security solutions for improved threat detection and analysis. Security management challenges, however, could push enterprises to consider partnering with a service provider that can offer enhanced threat detection solutions.





# Managed Threat Detection, Response, and Remediation

Advanced threats demand next-generation solutions that extend beyond security information and event management (SIEM) to offer a complete threat analysis of networks, devices, applications, and cloud without generating false positives. The move from reactive to proactive threat monitoring strategies and a predictive security architecture extends the traditional perimeters to ensure comprehensive threat identification, detection, response, recovery, and prediction. As a Tata Communications spokesperson stated, “Enhanced threat detection and response services delivered from cloud reduce mean time to detect and respond to cyberthreats. The cloud delivered approach proactively manages threats across the enterprise landscape.”







## Designing Security Permission Levels

“Managing user access privileges and using secure authentication techniques are important to secure data, applications and corporate assets,” said **Sanjivan Shirke**, UTI Asset Management. Access layers must be appropriately designed and monitored with least privilege to users. A zero trust model treats every user, whether internal and external, as a potential threat and requires proper authentication.

## Securing and Governing APIs

Cyberthreats can emerge in application programming interfaces (APIs), which are customized software interfaces many companies use. “The API interfaces are subject to breaches, making API governance and security a major issue. Enterprises must keep APIs behind a web application firewall or API gateway that can be accessed through a secure protocol, such as HTTPS,” noted **Rohit Rane**, HDFC Pension. Securing APIs by allowing access from a virtual private cloud and using authenticated API requests provide the desired security to sensitive data.








# Securing the Enterprise and Third-party Networks

Unfortunately, opportunities to breach complex, multilayered digital ecosystems, including mobile devices and connections to less-secure third-party networks, make it likely that even the most secure enterprises will be compromised at some point. While enterprises are on the road to implementing an SASE platform, a structured approach is essential.

While enterprises are on the road to implementing an SASE platform, a structured approach is essential.

To reap the benefits of hyperconnectivity over the long term, enterprises must leverage a strong, ever-evolving cybersecurity strategy. Key components should include:

-  Threat visibility using XDR solutions
-  Advanced endpoint and mobile workforce security
-  Zero trust framework and protocols
-  Security permission and privilege access control
-  Stricter API governance and controls
-  Comprehensive and managed security services

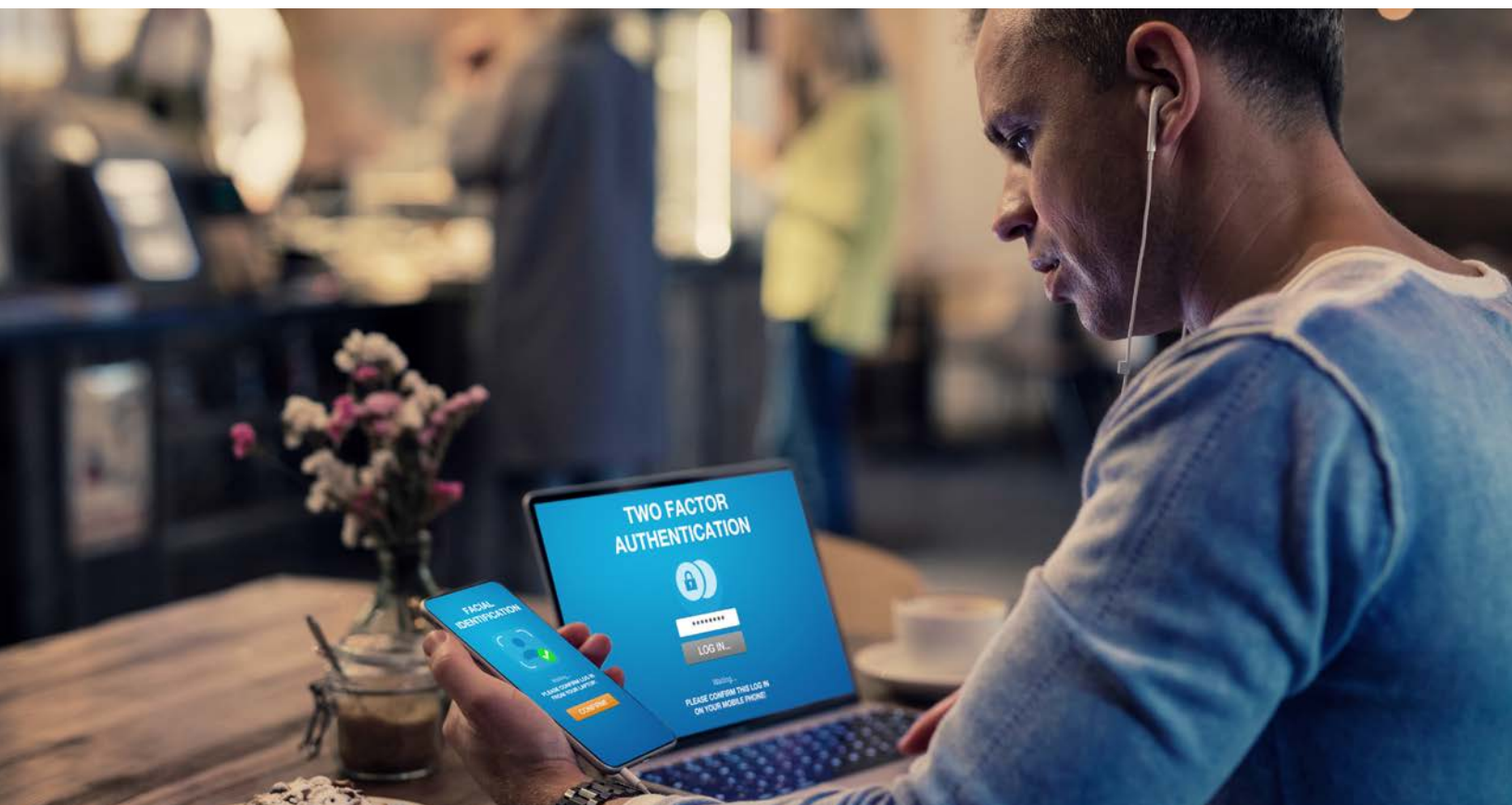




# An Ongoing Journey to Achieve Cyber-resilience

“Cybersecurity will always be an ongoing journey. The state of digital transformation will keep maturing, and cybersecurity strategies must also transform,” stated **Praveen Mishra** of Yes Bank. Ultimately, the hyperconnected world, with all its possibilities, will continue to expand—and with it the need for greater security. In recent times, the role of managed security service providers has increased multifold to ensure secured networks and security management. A unified and intelligent platform approach through local security operations centers (SOCs) and skilled cybersecurity teams will ease the most cumbersome security operations and accelerate the enterprise’s journey to achieve security transformation. Predictive, proactive, and automated security solutions built on unified security platforms will help enterprises to build a secure digital environment. Greater use of security automation and, most importantly, a security culture will lead the way to security transformation in the hyperconnected world.

Discover more Connected Security strategies here: [Tata Communications](#)





## Think Tank Luncheon Participants



**Anurag Sonpali**

Vice President Information Technology  
Future Generali India Life Insurance



**Ghansham Mhatre**

Head - IT Operations  
L&T Infotech



**Jayesh Thaker**

Head Of Information Technology  
GRP Ltd



**Praveen Mishra**

Senior Vice President -  
Information Security  
Yes Bank



**Rohit Rane**

Chief Information Security Officer  
HDFC Pension Management  
Company Limited



**Sanjivan S Shirke**

Head - Information Security and SVP  
(Information Technology)  
UTI Asset Management Company  
Limited





# About Tata Communications

A part of the Tata Group, Tata Communications (NSE: TATACOMM; BSE: 500483) is a global digital ecosystem enabler powering today's fast-growing digital economy in more than 190 countries and territories. Leading with trust, it enables digital transformation of enterprises globally with collaboration and connected solutions, core and next gen connectivity, cloud hosting and security solutions and media services. 300 of the Fortune 500 companies are its customers and the company connects businesses to 80% of the world's cloud giants.

*TATA COMMUNICATIONS and TATA are trademarks or registered trademarks of Tata Sons Private Limited in India and certain countries..*

## GROWTH IS A JOURNEY. WE ARE YOUR GUIDE.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: [Start the discussion](#) →