Futurum

Lenovo

Enhancing Cyber-Resilience: A Multi-Layered Approach to Data Infrastructure, Protection, and Security

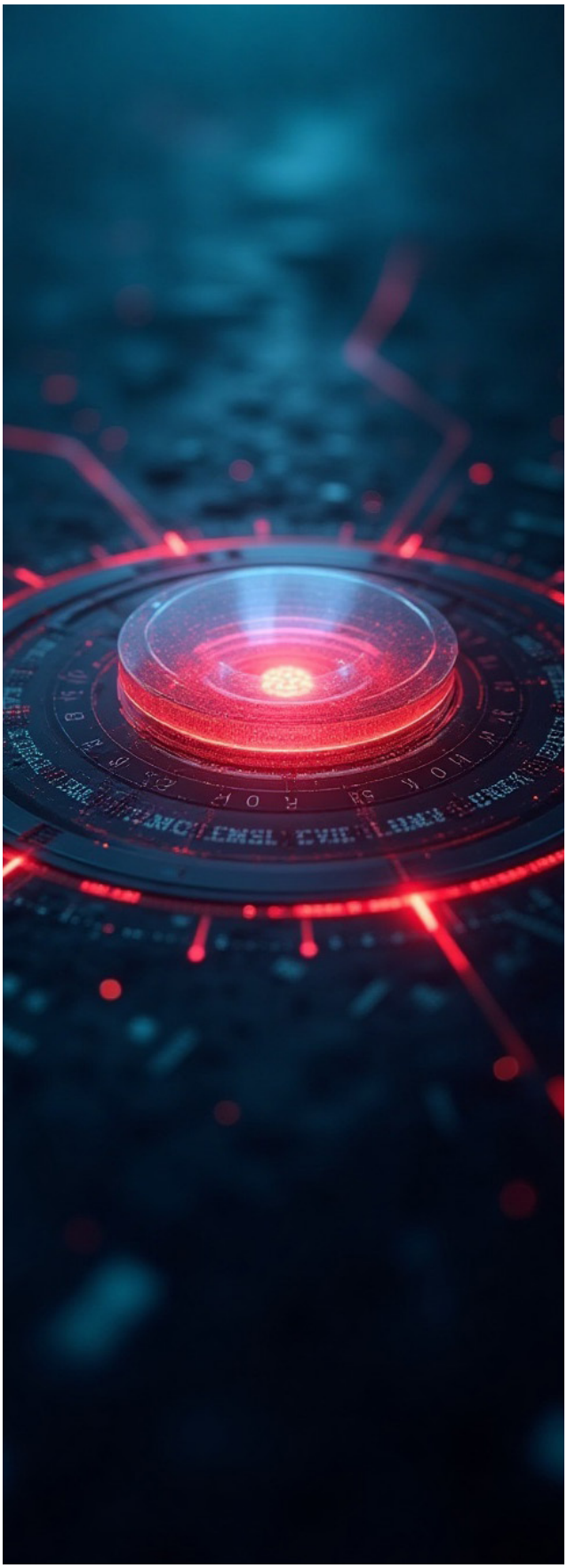
APRIL 2025

Introduction

When it comes to cyber-resilience, much emphasis is placed on reacting to data breaches such as ransomware attacks. However, the modern cyber threat landscape encompasses a broader range of increasingly innovative attack techniques. **In fact, more than 40% of respondents in The Futurum Group's 1H25 Cybersecurity Decision Maker study indicated that their organization has experienced three or more significant security incidents over the past 12 months**. These incidents ranged widely and included ransomware, cloud security incidents, and business email compromise.

The broad range of attacks creates the need for a more comprehensive and "layered" approach to cyber-resilience that encompasses not only reacting to the inevitability of successful attacks, but also taking more proactive and preventative measures. Data infrastructure is a particularly important component of the cyber-resilience conversation, as attackers are ultimately seeking data. It thus becomes necessary to manage risk at the primary storage layer, while facilitating comprehensive data protection.

Furthermore, a layered approach to cyber-resilience is particularly critical for small-to-midsized businesses (SMBs) and smaller enterprises. Compared to larger peers, such businesses are typically more limited in terms of the cybersecurity technologies already in place and their overall IT and security headcount.



The Role of Data Infrastructure, Protection, And Security

When it comes to data infrastructure, optimizing cyber-resilience encompasses inhibiting and detecting malicious access to data, while enabling fast recoverability of data in the event that a breach occurs. Preventing unauthorized access to data requires a multi-faceted defense strategy encompassing encryption, access controls, and network security measures. Despite strong preventative measures, breaches may still occur. Ensuring rapid recoverability of data is crucial for business continuity and minimizing operational disruption.

What To Look for from a Data Infrastructure Provider

Data infrastructure provides the foundation for cyber-resilience. It is critical in preventing and uncovering the breadth of evolving cyberattacks, and allowing the organization to recover their most critical data and business services following a breach. As such, Futurum Research recommends the following actions.

Inhibiting and Uncovering Malicious Access to Data

The first step in cyber-resilience is taking all measures possible to prevent malicious access to the data, to begin with. For data infrastructure, this translates into multi-factor authentication and role-based access control - which have long been table stakes capabilities for practitioners.

Today's era of cyber-resilience ups this ante, necessitating the requirement for multiple administrators to verify potentially destructive actions, such as the deletion of entire storage volumes, in the event that a malicious actor is able to gain access.

Along the vein of preparing for the inevitability of a breach, the ability to identify and automatically block known malicious file types also becomes table stakes. Specifically, it is important to be able to detect anomalous and potentially malicious activity in real time and with the utmost precision, given the evolving and innovative nature of attackers.

Furthermore, end-to-end encryption and multi-tenant key management become more critical than ever in the quest for cyber-resilience. End-to-end encryption helps to ensure the confidentiality and integrity of data in the event of potentially malicious access. It ensures that data remains encrypted from creation, transmission, storage, and access, inhibiting

unauthorized interception or tampering. What's more, it prohibits data from being further manipulated if it is encrypted by ransomware, or if it is stolen or exfiltrated. Multi-tenant key management ensures the secure creation, storage, control, and deletion of encryption keys. Isolating keys reduces risks inherent in centralized key management, enabling finer-grained control over data access.

Facilitating Recoverability of Data

Data breaches are an unfortunate inevitability for organizations of all sizes, industries, and global regions. With this in mind, organizations need to ensure that data can be recovered in the event of a broad range of incidents, from ransomware to insider threats. Cyber resilience is also about protecting data from unintentional data loss such as human error and natural disasters. Fortunately, the tools that protect against malicious actors can help protect against these threats to data.

The first step in facilitating recoverability is creating data copies that retain integrity, can be authenticated, and can be recovered. Doing so necessitates the creation of snapshots that are immutable (read-only and unchangeable) and indelible (undeletable, in addition to being unchangeable - even by an administrator). This practice, coupled with the multi-administrator verification, protects against credential vulnerabilities and spoofing, in addition to ransomware and data extortion.

Finally, the ability to identify and automatically recover from the last known good snapshot becomes more important for fast, reliable recovery. The Futurum Group consistently hears that mitigating downtime and data loss following an attack is the number one priority when it comes to optimizing cyber-resilience, in order to minimize any business disruption. In instances of recovering from a cyberattack, this becomes more difficult. It is difficult to know when the breach first occurred and how it spread across the network, and then quickly restore the most critical data and systems, especially when an entire storage volume was compromised. This is true considering the potential for human error in crisis situations.

Beyond Software: End-to-End Resilience

Cyber-resilience begins before data infrastructure systems are even deployed. It starts at the point of manufacturing at the factory and continues through the supply chain, ensuring the security of every component, from origin through its shipping and operation. The infrastructure hosting the data must be built and delivered to incorporate the following elements in order to prevent vulnerabilities that could be exploited by attackers.

A secure supply chain protects hardware and software components against tampering, counterfeiting, and unauthorized modifications. Implementing

Key Features for Cyber-Resilience:

- MFA
- RBAC
- Multi-admin verify
- Identify and automatically block known malicious files
- Anomaly detection
- End-to-end encryption
- Multi-tenant key management
- Immutable, indelible data copies
- Identify and automatically recover from the last known good data copies
- Secure supply chain
- Software, firmware, and BIOS security

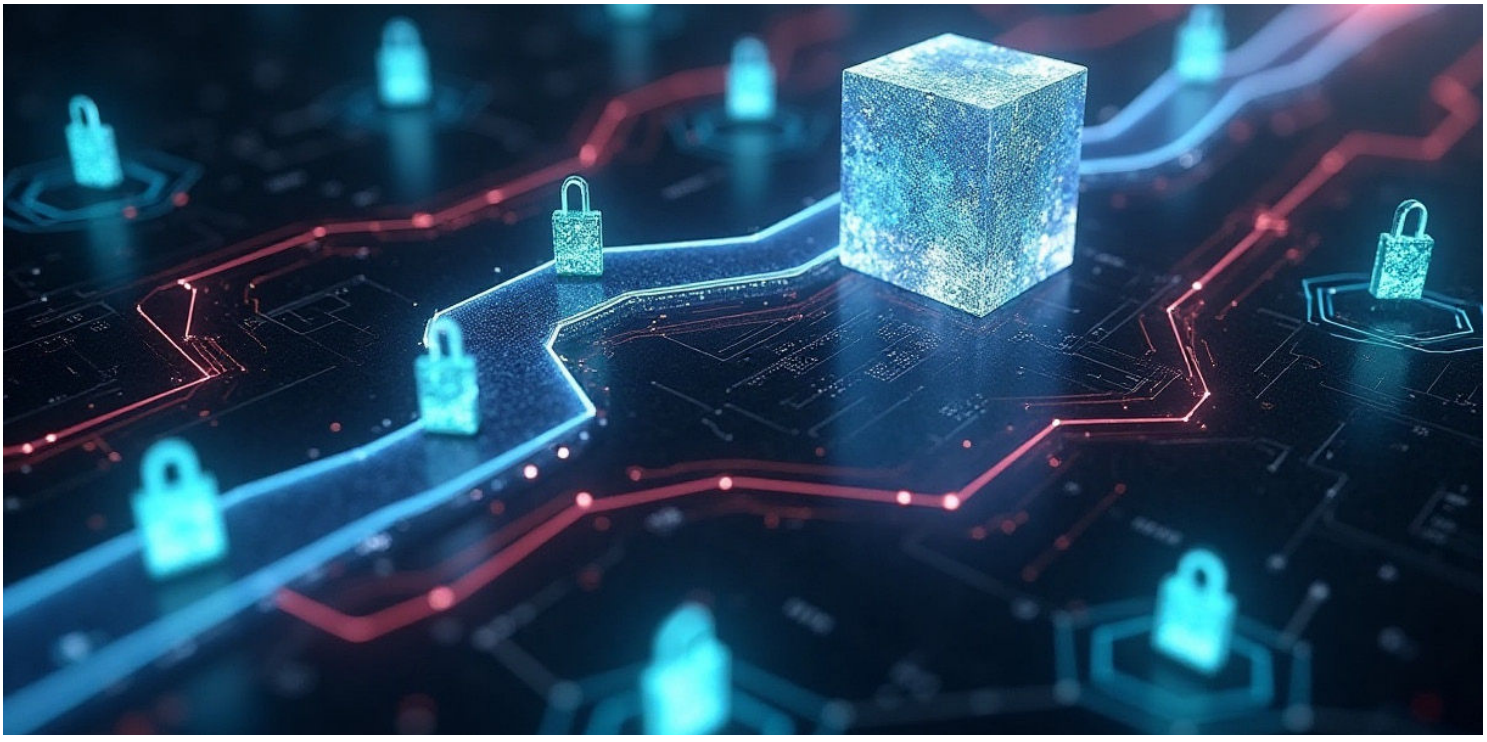
protocols such as secure manufacturing facilities, tamper-evident packaging, and careful auditing and evaluation of third-party suppliers reduces the potential for attackers to introduce malicious components or backdoors before a system even reaches an organization's data center.

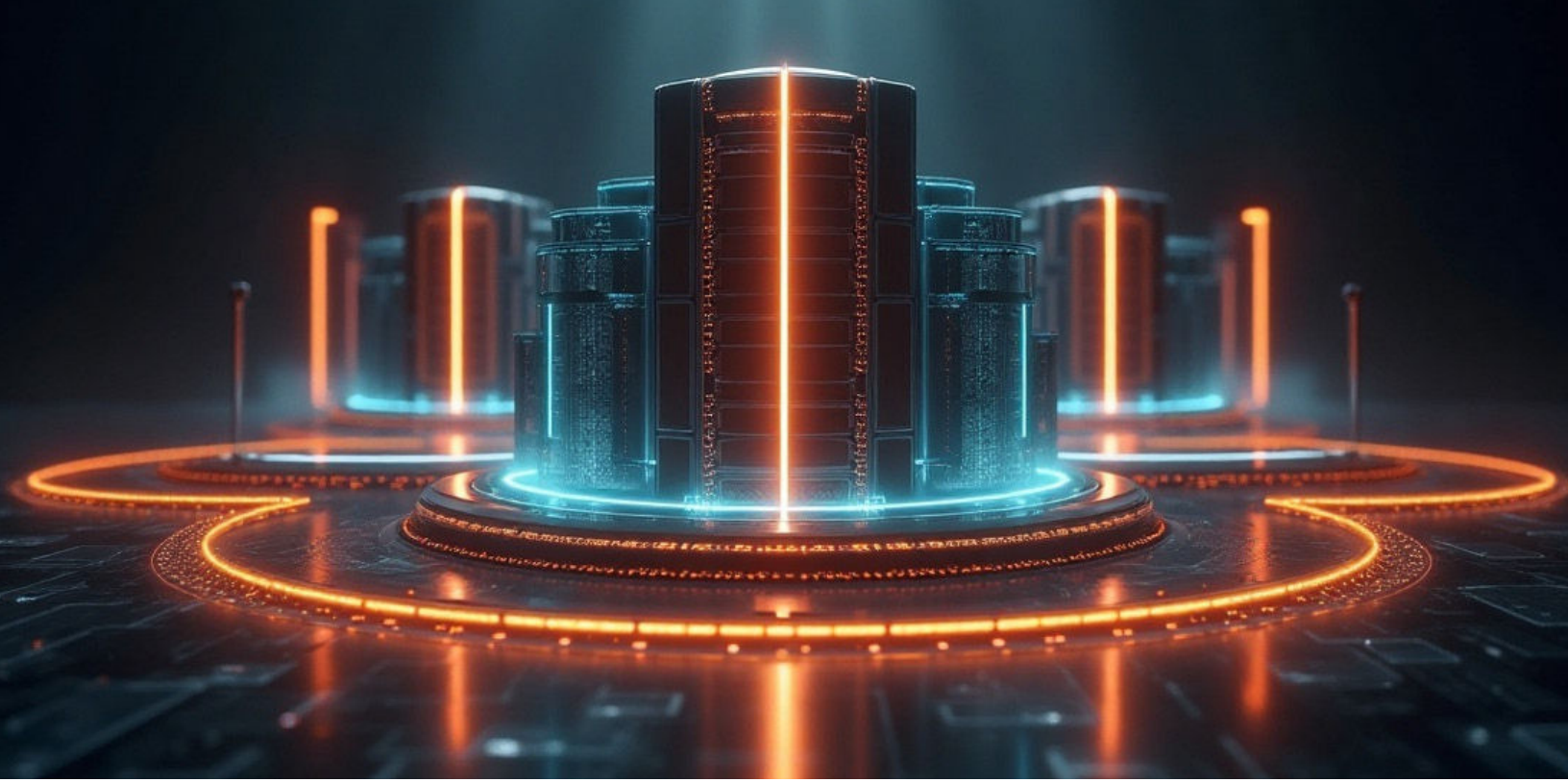
Cyber-resilience extends beyond hardware to the software and firmware. A secure and transparent software development cycle, coupled with a secure code repository, ensures that firmware, drivers, and management software are protected from unauthorized modifications and malicious injections. Furthermore, strict access controls, cryptographic code signing, and continuous integrity checks help prevent attackers from embedding vulnerabilities at the source, ensuring only trusted code is deployed on critical infrastructure.

Firmware and the system BIOS are of particular importance, given that they serve as the foundation for system security, controlling the lowest levels of hardware operation. What's more, attackers target these components because they can persist undetected even after operating system reinstalls or data restoration occurs. Locking down the firmware and BIOS - for example, through secure boot, signed firmware updates, and hardware-based attestation - prevents unauthorized modifications that could compromise system integrity. This ensures that servers and storage arrays boot securely and remain resistant to firmware-level attacks.

Regular security audits are required to identify vulnerabilities before they can be exploited. These audits should include supply chain assessments and firmware integrity checks to uncover potential weaknesses and reduce their exposure to supply chain attacks, firmware compromises, and unauthorized modifications.

Requiring multiple tools and products from multiple vendors adds costs and complexities, costing the organization time and budget resources that they cannot afford. It also increases the potential for human error. Working with a data infrastructure provider that offers a comprehensive stack of cyber-resilience capabilities that are easy to integrate is a compelling advantage.





Integrated Security and Resiliency Features in Lenovo's Data Storage and Management Offerings

For its part, Lenovo has integrated key data security and resiliency features into its ThinkSystem storage arrays and ThinkAgile SDI Series appliances and nodes. Specifically, ransomware attacks can be proactively detected and mitigated via AI-driven autonomous ransomware protection capabilities in Lenovo's ThinkSystem DG and DM storage arrays. In addition, features such as tamper-proof snapshots and end-to-end encryption with multi-tenant key management protect data from unauthorized access and malicious attacks. Finally, Lenovo's XClarity and XClarity One software provides secure end-to-end systems management. It is important to also note that Lenovo designs security best practices comprehensively across the lifecycle of its hardware offerings, from design to decommissioning, to ensure Lenovo delivers trusted data storage solutions with comprehensive security.

Conclusion

Data infrastructure, including primary data storage and data protection, plays a critical role in organizations' ability to minimize the amount of data loss and downtime that occurs in the event of a successful breach. Given the onslaught of ever-more varied and sophisticated data breaches, the data infrastructure must evolve to play a leading role in preventing such malicious access to begin with.

Like all organizations, SMBs and smaller enterprises are at risk, but they often also contend with more security gaps and less in-house expertise. A multi-layered approach to cyber-resilience that is not only reactive to common threats such as ransomware but also helps the organization adopt a more preventative stance against emerging threat vectors is critical. For smaller-scale organizations with limited resources, integrated and easy-to-use features are also important. This necessitates incorporating a variety of measures within the data infrastructure to inhibit unauthorized access, mitigate risks, and ensure rapid recoverability in the event of a breach.

Important Information About This Report

AUTHORS

Krista Case
Research Director, Cybersecurity | The Futurum Group

Camberley Bates
Vice President & Practice Lead, Data Infrastructure | The Futurum Group

PUBLISHER

Daniel Newman
CEO | The Futurum Group

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Lenovo

ABOUT LENOVO

Lenovo is a US$57 billion revenue global technology powerhouse, ranked #248 in the Fortune Global 500, and serving millions of customers every day in 180 markets. Focused on a bold vision to deliver Smarter Technology for All, Lenovo has built on its success as the world's largest PC company with a full-stack portfolio of AI-enabled, AI-ready, and AI-optimized devices (PCs, workstations, smartphones, tablets), infrastructure (server, storage, edge, high performance computing and software defined infrastructure), software, solutions, and services. Lenovo's continued investment in world-changing innovation is building a more equitable, trustworthy, and smarter future for everyone, everywhere. Lenovo is listed on the Hong Kong stock exchange under Lenovo Group Limited (HKSE: 992) (ADR: LNVGY). To find out more visit https://www.lenovo.com

Futurum

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.