
Your framework for end-to-end cyber resiliency.
Lenovo’s unified approach to strengthening security across your organization in the AI era.
Smarter technology for all
Lenovo

Strength in a single framework.

Organizations need a new, holistic approach to cyber resiliency to resist today's AI threats.

AI brings enormous potential, but it also exposes the limits of many organizations' current security models. At the same time, attackers are using these technologies to increase the speed and sophistication of attacks. Many organizations recognize the risk yet remain underprepared to manage AI-driven threats across their environments.

90%

aren't very confident they can address the risk of cyber criminals using AI.[1]

Over 60%

aren't confident they can address internal AI threats like misuse of AI by employees.[2]

54%

of IT leaders feel their data protection tools, process and staff capabilities aren't fully sufficient to address AI risks.[3]

This gap between risk and readiness has real consequences. Security now determines whether AI initiatives can move forward at all. Without strong foundations, risk accumulates quickly and progress slows. This is no longer just a technical concern. Regulatory expectations are tightening, with secure-by-design practices becoming a baseline requirement for digital and AI systems.

To navigate this shift, organizations need a cyber resiliency framework that is continuous, end-to-end and designed to help them adapt to evolving threats and absorb disruption when incidents occur. In this eBook, we explore what Lenovo's Cyber Resiliency Framework includes, alongside practical recommendations, real-world use cases and the outcomes organizations can expect.

"A single-framework approach to cyber resiliency is critical to combating today's AI threats. It helps organizations think bigger and more holistically while ensuring every layer is protected not only today, but continues to be as risks evolve."

Rakshit Ghura

Vice President & General Manager, Lenovo Digital Workplace Solutions.

Core components of Lenovo's Cyber Resiliency Framework.

How to build the best defense against new AI threats with a unified, end-to-end model.

Modern security programs are often built in layers that don't fully connect. Tools, teams and processes are introduced over time, but without a unifying model, gaps emerge and complexity grows. Lenovo's Cyber Resiliency Framework brings these layers together by aligning Assessment & Consulting with Implementation, Configuration and Managed Services.

Built around a set of core components, the framework brings security together across the entire digital estate, from users and endpoints to applications, AI and on-premises and cloud environments. With secure access and strong posture management, organizations can establish continuity and control across their security architecture.

Our framework enables:

- Constant risk reduction and protection of digital assets.
- Faster recovery time.
- Reduced IT complexity.
- Stronger regulatory alignment.
- Greater trust in AI systems.
- Secure digital transformation.

Lenovo's Cyber Resiliency Framework delivers an adaptive, end-to-end security architecture that covers every layer of infrastructure.

Assessment & Consulting

Analysis of current security posture to identify gaps, prioritize risk and guide where controls and services should be applied.

Access & Trust Management

Continuous, identity-led access controls that verify users and devices in real time and limit risk across every interaction.

Digital Data Protection & Resiliency

End-to-end safeguards that protect sensitive data and AI assets throughout their lifecycle, wherever they're created or used.

Managed Extended Detection & Response (MxDR)

AI-driven monitoring and response that contains threats quickly, limits impact and supports rapid recovery when incidents occur.

Visibility & Risk Management

Clear insight into the digital estate to identify exposure, prioritize risk and reduce vulnerabilities before they're exploited.

Security for AI

Security solutions that protect AI systems and support responsible use.

Read more about each component below.

Assessment & Consulting

Clarity before control.

Many organizations invest in security without a clear view of where risk sits. As environments change, assumptions about posture and coverage quickly fall out of date. Assessment & Consulting provides an independent view of readiness across users, data, systems and AI.

By identifying gaps and validating controls, organizations can prioritize risk, focus investment where it matters most and align security decisions with business and regulatory expectations.

82%

of IT leaders say vulnerability and threat analysis is critical for managing AI risk, yet many still lack the insight needed to understand their true exposure.[4]

Recommendations

How to establish a clear security baseline:

- **Conduct structured assessments** to understand current security posture across identity, data, infrastructure and AI use.
- **Identify gaps, overlaps and areas of elevated risk** that may not be visible through tooling alone.
- **Prioritize remediation based on business impact,** regulatory exposure and operational risk.
- **Use expert insight** to guide implementation, configuration and managed services decisions.

Access & Trust Management

Dynamic zero-trust models are imperative.

In hybrid environments, traditional defenses such as firewalls and network boundaries are no longer sufficient. As users, devices, applications and AI agents operate across many locations and platforms, identity has become the new perimeter. But static zero-trust models cannot keep pace with today's risk. Trust must be evaluated continuously, using real-time signals to adjust access as conditions change. Moving from "verify always" to "verify continuously" enables adaptive protection across every interaction, without introducing friction or delay.

70%

of organizations will have zero trust as a starting point for security by 2027, up from less than 20% in 2025.[5]

Recommendations

How to implement adaptive zero-trust access controls:

- **Authenticate and authorize** every human and non-human identity before granting access to enterprise applications or critical resources.
- **Establish trust dynamically** using real-time signals such as user behavior, device posture and contextual risk.
- **Adopt an identity-led security posture** that limits lateral movement and reduces access-related exposure.
- **Work with a trusted partner** to keep privileged access controls effective as environments evolve.

Digital Data Protection & Resiliency

Surge in sensitive data from AI use requires new safeguards.

Enterprise data is being created, shared and reused in new ways as AI becomes part of everyday workflows. Sensitive information now moves across systems and models in patterns traditional controls were not designed to manage, so protection needs to be built into how data is governed and accessed. Secure-by-design approaches define clear boundaries around AI use, helping to reduce leakage risk and support responsible adoption. Resiliency means building these protections so critical services can continue to run even during an incident, rather than stopping and recovering later.

Over half

of IT leaders feel their data protection isn't fully sufficient to address AI risks despite 83% seeing it as 'critical' or of 'high importance'.[6]

Recommendations

How to protect data across AI-driven environments:

- **Define clear guardrails** for AI use to limit data leakage through prompts, outputs and model interactions.
- **Use privacy-aware architectures** to reduce exposure as data moves between systems and AI models.
- **Apply consistent governance** to sensitive data wherever it's stored, shared or used across the organization.
- **Validate data protection controls continuously** to maintain confidence as volumes and usage patterns change.
- **Build data protection for continuity**, ensuring critical systems remain online even when data or AI services are under attack.

Managed Extended Detection & Response. (MxDR)

Responding faster to modern threats.

AI now plays a dual role in cybersecurity, acting as both an attack tool and a defensive capability. Adversarial techniques increase the speed and scale of reconnaissance, exploitation and social engineering, placing greater pressure on detection and response teams.

Many organizations are already constrained by security skills shortages, making it harder to investigate alerts and respond quickly. To remain effective, detection and response must reduce alert noise through intelligent platforms and advanced MxDR capabilities, allowing analysts to focus on meaningful incidents rather than false positives.

90%

of routine security triage will be handled by autonomous AI agents in 2026, freeing analysts to focus on the threats that matter.[7]

Recommendations

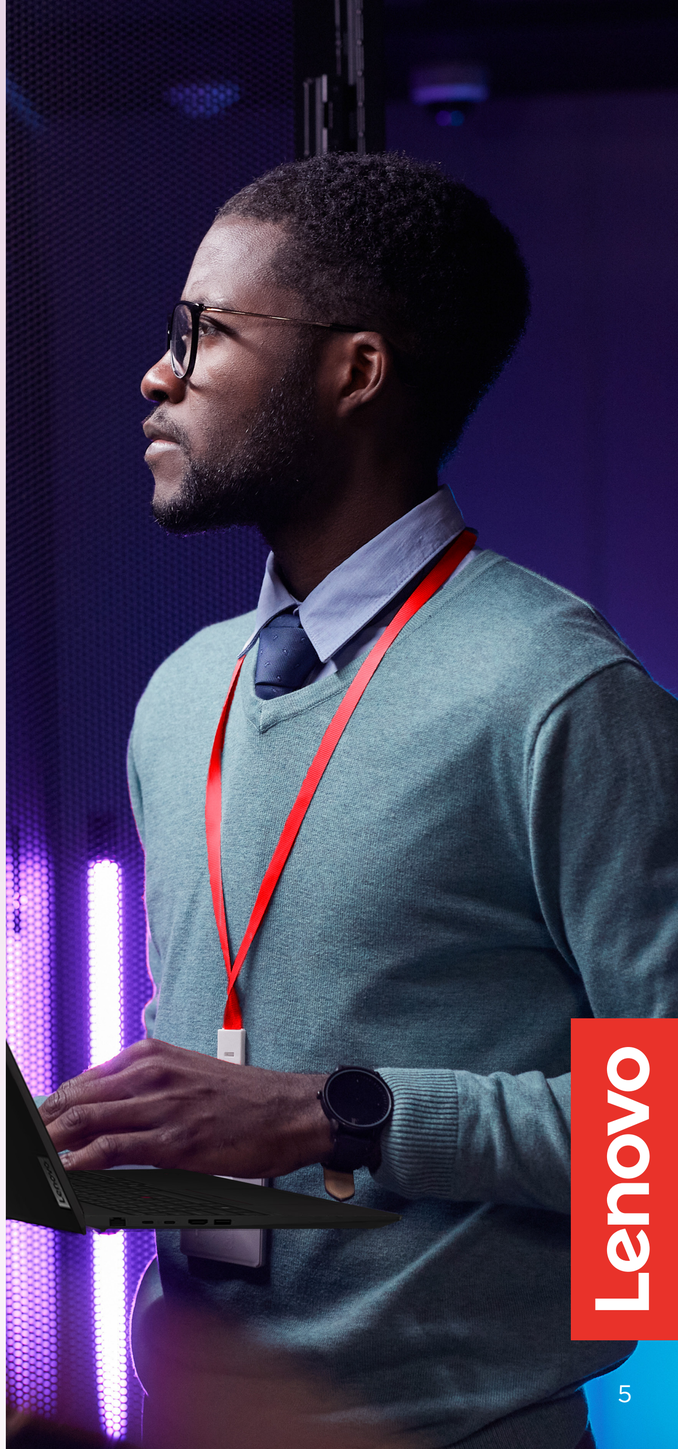
How to modernize detection and response:

- **Shift detection toward AI-driven monitoring** to surface credible threats earlier and reduce alert noise.
- **Design response around rapid containment** to limit spread and shorten recovery.
- **Adopt MxDR services** to close internal skills gaps and maintain continuous coverage.
- **Use automation** to support investigation and response as environments and alert volumes grow.

“Security teams are overwhelmed by alert volume and skills shortages as threats are becoming more automated. Effective detection and response depend on combining intelligent, technology-driven controls and automation with the ability to extend teams through trusted managed support.”

Tiago Da Costa Silva

Cyber Security Services Director, Digital Workplace Solutions, Lenovo.



Visibility & Risk Management

Continuous insight across a borderless digital estate.

As organizations expand across cloud, on-premises, edge, API- and agentic-driven environments, the digital estate becomes harder to track. Assets change constantly, making it difficult to maintain a clear view of risk. Visibility & Risk Management helps organizations move beyond periodic assessment to ongoing awareness across the environment.

65%

of IT leaders feel their vulnerability and threat analysis aren't fully sufficient to address AI risks.[8]

Recommendations

How to maintain visibility and reduce exposure:

- **Establish continuous discovery of assets and dependencies** across cloud, on-premises and edge environments.
- **Prioritize vulnerabilities** based on business impact rather than volume or severity scores alone.
- **Validate security posture regularly** to identify drift as environments change.
- **Use ongoing testing, scanning and simulation** to confirm controls remain effective against emerging threats. Drive an impact containment strategy where appropriate.

Security for AI

Building trust into AI adoption.

AI introduces new risks, including prompt injection, hallucination, model poisoning and data exposure. These persist beyond deployment and increase security, regulatory and executive pressure. Without strong governance, integrated controls and continuous monitoring, managing AI risk at scale is difficult. Security for AI treats cloud and AI as one system, from code to runtime. It embeds controls across infrastructure, AI platforms, applications and agents, so they are built in rather than bolted on.

More than 30%

of organizations see lack of governance and risk management as the top barrier to adopting AI.[9]

Recommendations

How to secure AI with confidence:

- **Establish clear governance of AI systems,** defining ownership and acceptable use from the outset.
- **Apply security controls across the AI lifecycle** to protect data, models and outputs.
- **Monitor AI behavior continuously** to identify changes in model behavior, unexpected outcomes or policy violations.
- **Align AI security practices with evolving regulatory expectations** to support responsible and compliant use.

Total cyber resiliency in action.

Use cases you can achieve within the framework.

Autonomous threat containment and recovery

Limiting business impact when incidents occur

Inbound threats are contained immediately using AI-driven systems that isolate affected endpoints or workloads and prevent lateral movement. Compromised systems are rolled back to a trusted state, then restored from clean, verified snapshots. Automated response playbooks support containment and speed recovery, helping limit disruption while maintaining operational integrity.

Key outcomes:

- Minimized downtime.
- Threats contained before they spread.
- More efficient security operations.

Primary component:	Supported by:
Managed Extended Detection & Response	Visibility & Risk Management Digital Data Protection & Resiliency

Resilient identity and access controls

Preventing identity compromise at scale

When identity is compromised or unusual behavior is detected, adaptive controls are applied immediately to limit risk. Access is adjusted dynamically based on real-time risk signals, with suspicious sessions restricted or reverified. Throughout the process, AI-driven monitoring evaluates user and device posture to maintain secure, trusted access without unnecessary disruption.

Key outcomes:

- Prevention of account takeover.
- Privilege misuse stopped from escalating into serious incidents.

Primary component:	Supported by:
Access & Trust Management	Visibility & Risk Management

Cloud and data resiliency

Recovering critical operations after disruption

In multi-cloud environments, data is protected through built-in recovery guardrails that safeguard information wherever it resides. Clean, untampered copies are maintained through immutable backups and secure vaulting, with integrity verified continuously. When disruption occurs, critical workloads can be restored quickly using built-in recovery mechanisms that support continuity across environments.

Key outcomes:

- Secure and rapid recovery from even the most serious cyber events.
- Reduced risk of permanent data loss or corruption.
- Greater confidence in recovery readiness.

Primary component:	Supported by:
Digital Data Protection & Resiliency	Visibility & Risk Management

AI model integrity protection and autonomous recovery

Maintaining trust in AI-driven decisions

AI models can be compromised through poisoning, corruption or manipulation that is difficult to detect after deployment. Continuous monitoring helps identify anomalous behavior early, triggering automated safeguards that restore models to trusted states. By validating training data and reverting to clean datasets when needed, organizations can maintain confidence in how AI systems operate.

Key outcomes:

- Trusted and reliable AI model behavior.
- Reduced risk from manipulation or unintended model drift.

Primary component:		Supported by:
Security for AI	→	Digital Data Protection & Resiliency

Intelligent incident forecasting and self-healing security

Avoiding disruption before users are affected

Patterns across telemetry, logs and identity signals can reveal where incidents are most likely to emerge. By identifying risk early, organizations can apply preventative changes before issues escalate. When degradation or compromise is detected, self-healing actions help restore stability and maintain continuity without waiting for manual intervention.

Key outcomes:

- Reduced likelihood of disruptive security incidents.
- Improved operational stability through automated recovery.

Primary component:		Supported by:
Managed Extended Detection & Response	→	Visibility & Risk Management

Continuous threat exposure management

Reducing risk before attackers can act

Threat exposure is reduced through continuous assessment of vulnerabilities across cloud, on-premises and edge environments. Risks are prioritized based on business impact, while testing and simulation help validate how weaknesses could be exploited. This enables organizations to confirm controls remain effective and shift from reactive response to proactive defense.

Key outcomes:

- Reduced exposure to emerging threats.
- Greater confidence in security controls and posture.

Primary component:		Supported by:
Visibility & Risk Management	→	Assessment & Consulting

Interested in learning more?

Discover how Lenovo’s holistic Cyber Resiliency Framework can keep your business secure from evolving threats.

Every organization should address the core components outlined in this eBook, but no two approaches look the same. With experience supporting organizations across 180+ markets, Lenovo brings a practical perspective on applying a consistent Cyber Resiliency Framework across different environments. If you’d like to explore how this approach could work for you, let’s talk.

Speak to our cyber resiliency experts today.

The vision is yours. Get there with Lenovo DWS.

1, 2, 3, 4. Lenovo, Work Reborn, Reinforcing the modern workplace, 2025.
5. Gartner, Zero Trust: Rethinking Security for a perimeterless world, 2025.
6. Lenovo, Work Reborn, Reinforcing the modern workplace, 2025.
7. SentinelOne, Key Cyber Security Statistics in 2026.
8. Lenovo, Work Reborn, Reinforcing the modern workplace, 2025.
9. IDC, From Risk to Reward: The Business Case for Responsible AI, 2025.