AI Security and Threat Management

# Smarter AI powered security and threat management

Trusted, built-in security turns intelligence into a secure foundation for the future

## Business resiliency is critical — and AI is redefining the enterprise by automating tasks, streamlining workflows, and driving efficiency at every level.

The adoption of GenAI alone, across all industries, **grew by 6x over the past year.**[1] 88% of organizations now report regular AI use in at least one business function.[1]

Cyber threats are evolving fast, exploiting gaps in data flows, model pipelines, and distributed environments. IT leaders are fighting back with advanced AI models to identify anomalous and malicious behavior, sorting through threat logs to uncover previously unknown attacks before they cause damage. AI models handle real-time analytics and response, sorting through massive threat logs to send alerts for human attention where it matters most.

From retail loss prevention, secure data handling, and fraud detection to patient data protection in healthcare, AI security adoption in any industry requires a comprehensive approach to securing the data, hardware, and software that powers your business. This is especially true in highly regulated industries.

**Lenovo has you covered with security embedded at every layer.** With built-in device-level safeguards like Lifecycle Device Manager (LDM), secure user experiences, and AI-powered software and infrastructure management tools like Lenovo XClarity — all working together to detect, protect, and respond proactively across the entire AI lifecycle. Add in Lenovo AI Services, including Premier Support Plus, and you get end-to-end protection and lifecycle management.

This is the Lenovo synergy that gives enterprise confidence to innovate without compromising trust. With Lenovo, your business remains resilient, compliant, and trustworthy — **now and in the future.**

## Lenovo's AI-enabled security approach turns risk into opportunity

Lenovo AI-enabled solutions are designed for security, built for hybrid AI environments, and engineered to deliver faster detection, faster response, and lower operational cost.

73% of IT security professionals say their organization is more likely to consider a security solution that uses AI.[2] While AI offers tremendous value, security and governance need to be in lockstep. 70% of IT security professionals also favor a consolidated security platform to streamline their workflows.[2] Lenovo helps your enterprise simplify the complexities with a consolidated security platform that:

- **Streamlines your workflows** for data and cost efficiency with rapid response of detected anomalies to avoid costly data breaches
- **Avoids unauthorized use of AI tools** that compromise your business and its data integrity
- **Provides AI-driven automated reporting, logging, and governance insights** to avoid data loss, compliance breaches, and business disruption to help satisfy audit requirements and build audit maturity
- **Supports regulatory frameworks** (GDPR, NIST, industry standards)
- **Offers built-in, continuous monitoring protections** from manufacturing through disposal

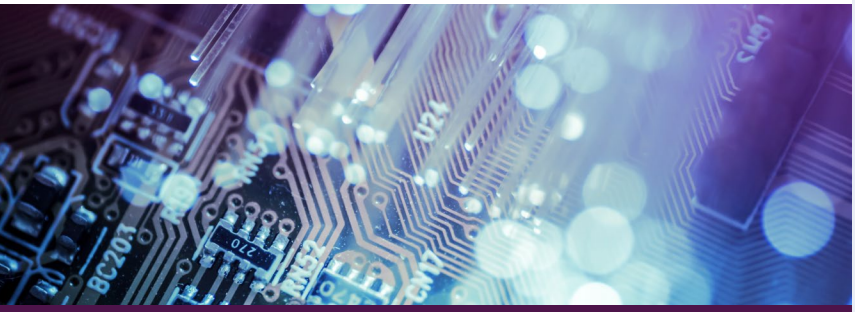
Lenovo

# Easily unify security across environments

Modern AI workloads don't live in a single place. They travel across laptops, edge sensors, data centers, and multi-cloud environments. Lenovo's AI Security and Threat Management ensures organizations can **deploy AI solutions anywhere, without sacrificing control of data.**

Lenovo provides a single operational model for AI security — covering endpoints, edge, data center, and cloud — backed by Lenovo managed services, unified telemetry, and SLA-driven response.

Lenovo delivers an end-to-end AI security architecture, supported by Lenovo AI Services. **Prevention, detection, response, and recovery are unified across environments** — enabling consistent enforcement, faster response, and reduced operational complexity throughout the AI lifecycle.



## Keeping vital business systems running smoothly

Working with Lenovo, Hisense Group deployed an AI-powered monitoring and alerting solution — improving operational efficiency and enabling 50% faster issue investigation across thousands of IT systems.

"Lenovo helps us to aggregate monitoring metrics, events, and other information automatically, delivering a full-stack observability solution that helps us keep our systems running 24/7."

**SUN WENGUANG**
IT MANAGER, PROCESS IT AND DATA MANAGEMENT DEPARTMENT, HISENSE GROUP

READ MORE >

## Reduce risk and prevent incidents

Lenovo reduces risk through a secure, transparent supply chain, firmware-level protections, and hardware-rooted trust. Zero Trust devices, backed by Lenovo ThinkShield, enforce continuous verification. Built-in data protection and sovereignty controls help organizations keep regulated or proprietary data where it belongs, which is critical for AI workloads operating across hybrid environments.

## Detect threats traditional tools miss

Lenovo addresses increasingly sophisticated threats with AI-driven analytics across an XDR data lake, correlating signals from devices, edge systems, servers, and cloud workloads. Behavior-based detection helps identify attacks, while advanced anomaly detection monitors suspicious activity in AI pipelines for true threats. Shadow AI discovery further surfaces unsanctioned tools and models operating outside governance.

## Contain threats at the speed of AI

When incidents occur, response time determines impact. Lenovo enables automated containment and guided remediation. With Lenovo Managed XDR (MxDR), organizations gain 24/7 monitoring, expert-led response, and rapid isolation or rollback of affected systems. Golden snapshots and ransomware-specific recovery workflows help stop attacks from spreading while preserving business continuity.

## Build long-term AI resilience

Lenovo's Cyber Resiliency as a Service (CRaaS) supports immutable, tamper-proof backups, detailed incident forensics, and rapid restoration. Beyond technical recovery, Lenovo helps organizations mature their AI governance posture through Responsible AI assessments, continuous adversarial testing, and ongoing governance services. This ensures AI systems remain compliant, explainable, and resilient as regulations, models, and threats evolve.

Lenovo

# Lenovo's security-by-design

Lenovo builds protection into every step. This security-by-design philosophy ensures that devices, infrastructure, and software are secured from the moment silicon is manufactured to the moment workloads run. These built-in protections are operationalized through Lenovo Services, enabling security policies, telemetry, and response workflows to extend consistently across devices, infrastructure, and AI workloads.

- Hardware-rooted trust to prevent tampering, spoofing, and unauthorized access
- End-to-end supply chain transparency ensuring components are verifiable and secure
- Platform integrity features that protect firmware, BIOS, and runtime execution
- Zero Trust-aligned controls that enforce least privilege across distributed architectures

## Comprehensive protection for AI-enabled devices

AI dramatically increases both the value of endpoints and their vulnerability. Every device becomes a critical security boundary. Lenovo ThinkShield provides the multilayer defense needed to secure AI-driven workflows.

- Faster detection and response through intelligent threat monitoring, AI-powered risk scoring, and automated remediation
- Reduced breach impact with BIOS-level protection, device-anchored identity, and real-time policy enforcement
- Improved compliance and governance by ensuring data, models, and interactions remain protected across the full user session
- Proactive defense through continuous updates, advanced authentication, and protection against evolving AI-enabled attacks

## Extending security and AI governance

As enterprises scale AI, operational complexity quickly becomes a barrier. Lenovo Managed Services act as the control plane for AI security, integrating telemetry, response, governance, and recovery across the full AI lifecycle into a unified operating model.

- Empower IT and security leaders to scale AI securely without scaling risk or overhead
- Reduce the burden on internal teams, enabling IT and security leaders to focus on strategic AI initiatives instead of day-to-day threat management
- Continuously monitor endpoints, edge devices, servers, and cloud workloads, detecting threats in real time and accelerating responses
- Support for meeting regulatory mandates, maintaining audit readiness, and enforcing responsible AI usage across the enterprise

## Validating the integrity of employee devices

Meta is working with Lenovo to validate the provenance, security, and authenticity of employee devices. The core of this Zero Trust approach is provided by Lenovo ThinkShield Supply Chain Assurance.

"Simplification is the key here. By rolling out Lenovo ThinkShield Supply Chain Assurance to more employee devices and moving away from traditional authentication and authorization workflows, we will simplify and improve the efficiency of the entire process."

**RUBEN RECABARREN VELARDE**
SECURITY ENGINEER, META

READ MORE >

# Empowering security with hybrid infrastructure and intelligent devices

Lenovo delivers AI security as an integrated, service-led operating model that reduces reliance on fragmented security tools, accelerates incident response, and lowers ongoing SecOps overhead. By unifying advisory, deployment, protection, and recovery across the AI lifecycle, organizations gain clearer ownership, faster decision-making, and the operational confidence to move AI from pilot to production without adding complexity.


Lenovo ThinkStation®
P8 Workstation


Lenovo ThinkEdge™
SE455i V3 Server


Lenovo ThinkSystem®
SR650 V4 Server

## Detect earlier and act faster

Rapidly detect and address threats to minimize security risks and downtime. Gain earlier visibility into AI-driven threats and shadow AI activity across the environment.

- Lenovo ThinkShield and SentinelOne deliver behavior-based detection for fileless and memory-resident attacks.
- Lenovo MxDR correlates signals across endpoints, edge, data center, and cloud with SLA-backed response. Lenovo MxDR is purpose-built as the industry's only Trusted Behavior Registry™ within our Zero Trust Analytics Platform™.
- Lenovo ThinkEdge enables real-time anomaly detection closer to where data and AI inference occur.
- Lenovo AI Security Assessments evaluate your current operations and pinpoint opportunities for improvement.

## Protect with AI as you grow

As AI initiatives expand from pilots to enterprise-wide deployments, you can scale securely without increasing complexity or governance issues. Security policies, controls, and visibility must remain consistent as AI workloads grow across hybrid environments.

- Lenovo AI Discover and Advisory Workshops align leadership on scalable AI risk and governance.
- Lenovo AI Factory Services meet you wherever you are in your AI journey to help you rapidly define, deploy, secure, and drive real value from AI.
- Secure infrastructure and hybrid solutions, including Lenovo ThinkSystem and Lenovo ThinkAgile, deliver protected scalability, when organizations require predictable performance with full data sovereignty.
- Secure endpoint and edge solutions, including Lenovo ThinkStation, ThinkPad® P Series workstations, and Lenovo ThinkEdge provide secure, local, high-performance compute when needed to speed up model development, prototyping, and fine-tuning. Lenovo ThinkStation PGX unlocks additional compute capacity for demanding AI development workloads, delivering secure, on-desk flexibility.

Lenovo

## AI Security and Threat Management

### Prevent and contain threats

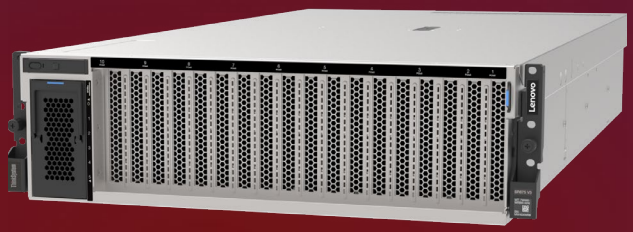
Reduce the likelihood and impact of breaches by preventing threats before they take hold and containing incidents instantly when they occur. AI-driven workflows, endpoints, and user interactions are protected by default, minimizing disruption even in highly distributed environments.

- Lenovo Aura Edition AI PCs keep your users productive and elevate the employee experience — all while acting as Zero Trust endpoints for AI initiatives.
- Lenovo ThinkShield offers foundational protection for firmware, identity, and access from day one.
- Lenovo AI Fast Start rapidly integrates SecOps workflows, MxDR, and governance controls — establishing secure operational foundations early in the AI journey.
- Lenovo Hybrid AI Advantage™ delivers business value fast with validated and pre-integrated enterprise AI factory solutions, infrastructure platforms, and services to help businesses deploy scalable and flexible AI across environments with built-in security at every layer.

### Recover fast and cost-efficiently

Lower the cost and complexity of security operations while strengthening resilience and compliance. Recovery is faster and more predictable, operational overhead is reduced, and AI governance becomes easier to manage.

- Lenovo Cyber Resiliency as a Service (CRaaS) delivers immutable backups, ransomware recovery, and forensics. CRaaS uses Lenovo device telemetry and Microsoft security software, including Microsoft Copilot for Security and Defender for Endpoint.
- Lenovo Responsible AI and governance services support your organization with properly vetted solutions and the guidance needed for compliance.
- Lenovo ThinkAgile and Lenovo ThinkSystem servers enable isolation, rollback, and golden snapshots for peace of mind.



Lenovo ThinkSystem® SR675i V3 Server

# Secure from the supply chain to the cloud

Lenovo builds hybrid technology that spans client devices, edge computing, private cloud, and public cloud. From the factory floor to users' hands, Lenovo's comprehensive, end-to-end security provides built-in platform, data, and device protection and management.

## Supply chain

- #8 on Gartner Supply Chain Top 25[3]
- AI-driven processes for faster detection and resolution times
- ThinkShield Build Assure tracks critical device information such as hardware, firmware, system components, and platform certificates validating components against tampering
- Backed by a team of 75 researchers, including 22 PhDs, across 30+ manufacturing sites[4]

## Below the OS

- ThinkShield Firmware Assurance enables deep visibility and protection by embracing Zero Trust Architecture (ZTA) component-level visibility
- Governance of critical components with a dedicated embedded controller (EC) that attests critical components and configuration during boot time to provide platform root of trust
- Prevent software and firmware components from being installed unless signed with recognized and approved certificates
- Unauthorized changes in BIOS policies can be prevented while providing automatic recovery of BIOS policies

## OS to cloud

- SentinelOne endpoint protection, detection, and response
- ThinkShield Extended Detection and Response (XDR), powered by SentinelOne, unifies and extends detection and response across multiple security layers, including endpoint, cloud, identity, network, and mobile
- ThinkShield XDR can be deployed on-premises, in the cloud, or as a hybrid solution — all with a centralized management console
- End-to-end enterprise visibility, powerful analytics, and automated responses across the technology stack
- Secure backup, patented solution to protect browser, password-less authentication, data defense, and automated BIOS patching

Lenovo

# Why Lenovo for security and threat management?

With Lenovo, your AI-driven security initiatives are backed by experienced experts, proven solutions, and a massive partner ecosystem.

**#1**
in x86 server **reliability** for 11 consecutive years[5]

**#1**
in x86 server **security** for 6 consecutive years[5]

**#1**
PC provider

**#1**
Microsoft Windows AI PC provider

**30+**
years of trusted partnership with IT leaders to transform AI vision into value

**165+**
enterprise AI solutions from our AI partner ecosystem with validated use cases

**50% faster**
outcomes achievable with our AI Library of proven accelerators and network of AI Innovators[6]

## Experience end-to-end visibility and control for the AI era

As AI adoption accelerates, security, governance, and resilience can't fall behind. Lenovo delivers end-to-end AI protections that reduce risk, speed response, and lower cost.

Contact us to see a demo of our AI solutions or explore how we can help secure your AI initiatives starting today.

**www.lenovo.com/us/en/ai/security-threat-management**

**Sources**
1 OpenAI, "The State of Enterprise AI," December 2025
2 Foundry, "Security Priorities Survey," November 2025
3 Gartner, "Gartner Announces 2025 Rankings of the Global Supply Chain Top 25," June 2025
4 Lenovo, "Lenovo ranks 8th in the Gartner® Supply Chain Top 25 for 2025," June 2025
5 ITIC, "ITIC 2024 Global Server Hardware, Server OS Reliability Report," November 2024
6 Lenovo, "Lenovo Hybrid AI Solutions," October 2025



Smarter technology for all

Lenovo