SECURITY, CONTROL, AND PROTECTION

SCALE ENTERPRISE AI WITH TRUST BUILT IN

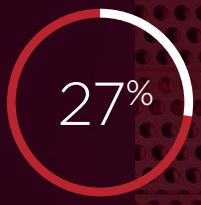
PROTECT DATA AND AI ASSETS WITH SECURITY, RESILIENCE, GOVERNANCE, AND CONTROL ACROSS THE AI LIFECYCLE

As AI gains access to more of what makes an organization valuable — enterprise data, intellectual property, applications, models, and business processes — the need for comprehensive governance grows.

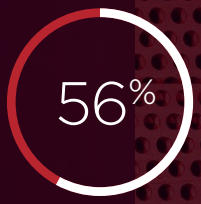
Agentic AI raises the stakes further. Systems that can reason, take action, and interact with enterprise applications create new requirements for visibility into what AI accesses, how it operates, and where sensitive information moves.

For IT leaders, scaling AI confidently means maintaining control across the environment — protecting data and infrastructure, governing access and AI behavior, supporting regulatory compliance across geographies, and maintaining sovereignty over data, models, and workloads.

Lenovo Hybrid AI Advantage™ with NVIDIA brings security, control, and trust into the enterprise AI foundation across AI-ready workstations supporting iterative development and local inference to shared enterprise infrastructure, data, models, and lifecycle services.



Only 27% of organizations have comprehensive AI governance frameworks in place.[1]



of countries are still developing comprehensive policies for AI governance, security, privacy, and data sovereignty.[1]

NVIDIA

Smarter technology for all

Lenovo

KNOW WHAT YOU NEED TO CONTROL

DATA AND OPERATIONAL PROTECTION ACROSS THE AI LIFECYCLE

For enterprises, sovereignty means more than choosing where infrastructure is located. It means retaining authority over where data is stored and processed, how models are developed and deployed, who can access AI systems, and which laws and policies govern operations.

These enterprise controls can also support broader national sovereign AI initiatives, which focus on a country's capacity to develop and operate AI using domestic infrastructure, data, talent, and business ecosystems.

As AI environments become more distributed, organizations need a clear view of the controls that apply at each stage.

DATA AND LOCATION

Determine where sensitive data is stored and processed, and which environments AI workloads can access. Lenovo enterprise storage, data management, and workload placement options help organizations maintain greater control over data residency and reduce unnecessary movement of sensitive information.

MODELS

Maintain visibility into how models are trained, customized, deployed, and governed. **Lenovo AI Services** can help establish governance practices across the model lifecycle, reducing the risk of unmanaged models or inconsistent controls as AI adoption expands.

ACCESS

Control who and what can interact with enterprise AI systems, data, and applications. The **Lenovo ThinkShield platform** and ThinkSystem security-by-design capabilities help strengthen protection across users, devices, and infrastructure — reducing the risk of unauthorized access to sensitive AI assets.

AI BEHAVIOR AND OUTPUTS

Establish policies and processes for monitoring, validating, and governing AI interactions and results.

NVIDIA NeMo GUARDRAILS

Apply configurable guardrails across AI interactions to validate user inputs, filter retrieved content, govern agent actions, and evaluate model outputs. **NVIDIA NeMo Guardrails** can help enforce topic boundaries, detect jailbreak attempts, protect sensitive information, and ground responses in approved evidence — giving organizations more direct technical control over AI behavior.[2]

OPERATIONS AND RECOVERY

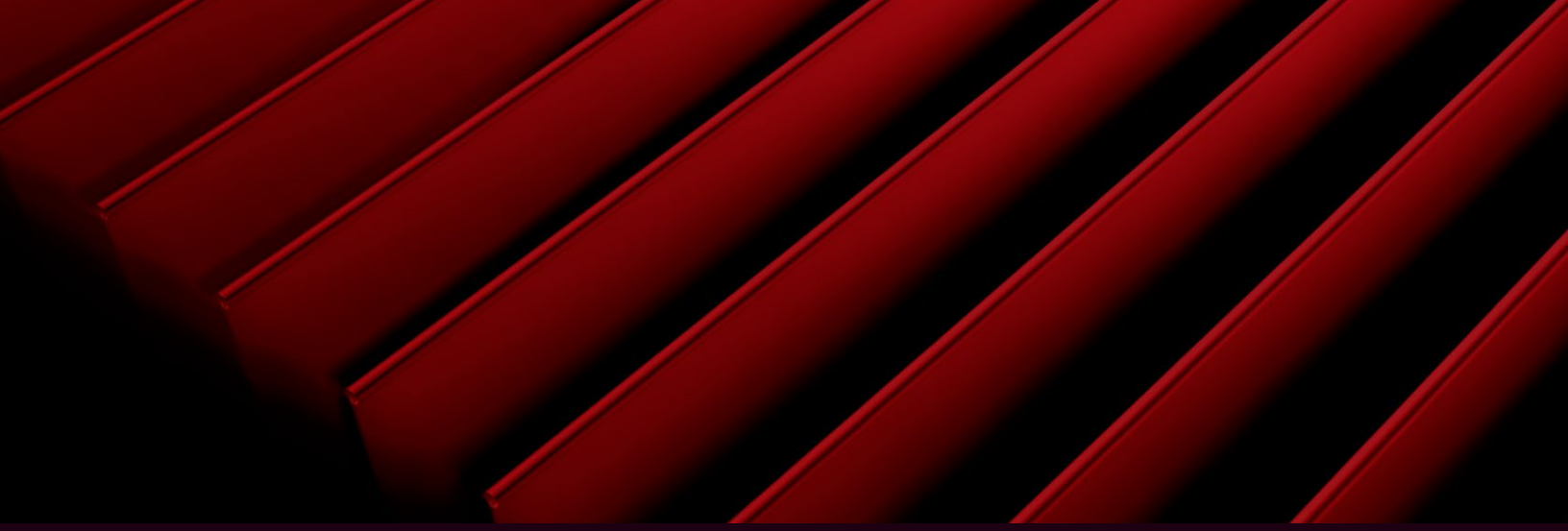
Protect AI workloads throughout their lifecycle and plan for resilience, recovery, and continued operation. **Lenovo xIQ Hybrid Cloud Platform** provides visibility and operational oversight across hybrid and multicloud environments, while **Lenovo XClarity One** centralizes management and lifecycle control for Lenovo infrastructure — helping reduce operational blind spots as environments become more distributed.

PUT DATA CONTROL AT THE CENTER

From workstation to data center, AI relies on fast access to trusted information, but moving sensitive data indiscriminately can increase risk and complicate sovereignty requirements. Protecting data only at rest and in transit leaves a gap while data and models are being processed; confidential computing helps address that exposure by isolating workloads in a trusted execution environment.

For workstation-based AI development and inference, keeping appropriate workloads close to users and data can reduce unnecessary data movement and help maintain greater control over sensitive enterprise data, models, and intellectual property.

Workload placement and data architecture can help organizations keep selected data and AI workloads within enterprise-controlled environments while supporting requirements for where information is stored and processed. Data protection and recovery controls can further strengthen that foundation. Lenovo data protection capabilities can help organizations protect critical information with immutable data protection, policy-based controls, multi-admin verification, end-to-end encryption, ransomware detection and response, and rapid recovery capabilities.



BUILD TRUST ACROSS THE AI ENVIRONMENT

STRENGTHEN PROTECTION AND GOVERNANCE FROM INFRASTRUCTURE THROUGH AI OPERATIONS

Enterprise AI security must account for more than a single device, application, or data repository. Trust depends on protections that work across the infrastructure, data, models, users, and operations supporting AI.

Lenovo and NVIDIA bring complementary capabilities together to help organizations address those requirements as AI expands across production environments and the enterprise.

PROTECT PEOPLE, DEVICES, AND DATA

The Lenovo ThinkShield platform helps protect people, devices, and data across the AI environment.

STRENGTHEN INFRASTRUCTURE TRUST

Lenovo ThinkSystem infrastructure incorporates security-by-design capabilities such as TPM-based cryptography, Secure Boot, administrator and power-on passwords, AES-NI encryption acceleration, and chassis-intrusion detection. Combined with #1-ranked x86 server reliability for 12 consecutive years[3] and a Lenovo-owned global supply chain spanning PC through data center, these capabilities help strengthen protection and assurance across the infrastructure lifecycle.

PROTECT MODELS AND DATA WHILE IN USE

Within Lenovo Hybrid AI Advantage™ with NVIDIA, supported Lenovo Hybrid AI Factory configurations use NVIDIA Confidential Computing to help isolate sensitive AI models in hardware-based trusted execution environments — helping protect against unauthorized access and support Zero Trust principles across shared, hybrid, and sovereign AI environments.[4]

SUPPORT GOVERNANCE ACROSS THE LIFECYCLE

Lenovo Hybrid AI Services help organizations address privacy, governance, and compliance from advisory and implementation through ongoing management — helping controls and operating practices evolve alongside AI adoption.

PROTECTION REQUIRES SECURITY AND SOVEREIGNTY

Security protects AI systems and information from threats. Sovereignty extends control over where data and workloads reside, who can access them, and how the AI environment is governed and operated.

Together, those capabilities help organizations pursue AI innovation while maintaining the enterprise controls needed for sensitive data, intellectual property, regulatory requirements, and mission-critical operations.

CONFIDENCE TO SCALE STARTS WITH A CONNECTED FOUNDATION

SECURITY, CONTROL, AND PROTECTION SUPPORT THE PATH FROM AI OPPORTUNITY TO ENTERPRISE OPERATIONS

Operationalizing enterprise AI also requires valuable use cases and infrastructure that can run them efficiently.

Lenovo Hybrid AI Advantage™ with NVIDIA connects these requirements in one enterprise AI approach — helping organizations accelerate valuable AI use cases, build infrastructure for production workloads, and maintain control as adoption expands.



ACCELERATE AI INNOVATION — LENOVO AI LIBRARY

Use ready-to-customize agents and use cases to turn business opportunities into working AI.



OPTIMIZE AI INFRASTRUCTURE — LENOVO HYBRID AI FACTORY WITH NVIDIA

Bring together validated compute, networking, storage, software, orchestration, and services to operate AI with better performance and economics.



SECURE AND TRUST ENTERPRISE AI — SECURITY, CONTROL, AND PROTECTION

Protect data and AI assets while supporting governance, compliance, sovereignty, and control across the AI lifecycle.

SCALE AI WITH GREATER CONFIDENCE

Lenovo and NVIDIA combine secure workstations and enterprise infrastructure, lifecycle services, and data management with NVIDIA accelerated computing, NVIDIA Confidential Computing, and NVIDIA NeMo Guardrails to help organizations protect data and models, govern agent behavior, and retain control over workload placement as AI adoption expands.

READY TO BUILD GREATER TRUST INTO ENTERPRISE AI?

Connect with Lenovo to align security, governance, data, infrastructure, and sovereignty requirements to your AI strategy.

Book an AI Discover workshop today

Explore secure AI infrastructure from Lenovo

Sources

1 Lenovo, "CIO Playbook 2026: The Race for Enterprise AI," Lenovo, January 2026
2 NVIDIA, "NVIDIA Releases NIM Microservices to Safeguard Applications for Agentic AI," NVIDIA Blog, January 2025
3 ITIC, "ITIC 2025 Global Server Hardware, Server OS Reliability Report," ITIC, December 2025
4 NVIDIA, "Confidential Computing for AI," NVIDIA Enterprise AI Factory Design Guide White Paper, updated May 2026

© Lenovo 2026. All rights reserved. v1.00 September 2026.

NVIDIA

Smarter technology for all

Lenovo