Security

A Strong Foundation for Secure Infrastructure

As cyberattacks become more frequent and more costly, businesses are working harder to secure their infrastructure.

In fact, data quality, sovereignty and compliance are all ranked number one amongst IT decision makers when it comes to secure IT infrastructure.

Lenovo stands strong with you by building modern, smarter, security into their solutions. Lenovo are recognized as an industry leader by ITIC and are committed to security from design to decommission. Learn about the next generation of security features in Lenovo's ThinkSystem V4 & ThinkAgile V4 portfolio.

$4.88 million

cost of a data breach for enterprises

Ponemon Institute, 2024[2] Average

$2.2 million

cost savings using security AI & automation

Ponemon Institute, 20242 Average

#1 on ITIC's x86 global server security survey for 6 years running.[1]

Modernize Security with Enhanced Data Capabilities & Quality

Learn more about Lenovo Security

Security innovation is fundamental in Lenovo product design, providing built-in capabilities that meet or exceed industry standards.

In 2024, Lenovo became one of the first technology leaders to sign the Secure by Design Pledge announced by the US Cybersecurity & Infrastructure Security Agency (CISA).

Read “Lenovo Security by Design: Foundational Security from Edge to Cloud” at Lenovo Press.

Lenovo is named in the Gartner Global Supply Chain Top 25 for 2024.

Built-in security to protect sensitive data and become AI ready

Lenovo’s best-in-class Security by Design commitment protects ThinkSystem and ThinkAgile solutions. With Lenovo’s secure supply chain and business processes, you can protect your infrastructure and minimize security risks. Additional layers of security, including locking bezels, embedded hardware protections, and built-in software controls secure the product throughout its lifecycle.

Validate firmware with platform firmware resiliency (PFR)

Enhanced PFR, with NIST SP800-193 compliant hardware root of trust, monitors firmware for corruption or compromise. If an unauthorized firmware update or change is detected, firmware is automatically restored using a trusted, unchangeable image.

Detect incidents with Lenovo System Guard Lenovo System Guard monitors every server's internal hardware inventory to protect against supply chain attacks and hacks throughout the system’s life cycle. System Guard digitally identifies critical components, from CPUs and DIMMs to risers and backplanes. If these components are removed or changed, System Guard can alert administrators and even block boot-up.

Speed disaster recovery with XClarity Controller 2.0

Save time in disaster recovery situations, with Neighbor Groups in Lenovo XClarity Controller 2.0 software. A single administrator can easily remediate every server in the Neighbor Group from a single instance.

New Innovative Security

Early in 2025, Lenovo announced the ThinkSystem Emulex® Secure Fibre Channel host bus adapters (FC HBAs) by Broadcom, designed to deliver the highest level of security, performance, and manageability for mission- critical infrastructures.

The Emulex Secure HBAs integrate the most robust quantum-resistant algorithms to ensure that encrypted data remains encrypted even as quantum computing and AI put legacy encryption at risk.

Learn more about Lenovo's foundational approach to security. Read "Lenovo Security by Design: Foundational Security from Edge to Cloud" at Lenovo Press.

© Lenovo 2025. All rights reserved. Lenovo, the Lenovo logo are trademarks or registered trademarks of Lenovo. All trademarks are the property of their respective owners.

1. ITIC (2024). IBM Z, IBM Power Systems & Lenovo ThinkSystem Servers Most Secure, Toughest To Crack.

2. Ponemon Institute (2024). Cost of a Data Breach Report 2022.

3. Gartner (2022, May 26). Gartner Announces Rankings of the 2022 Global Supply Chain Top 25.

Detect incidents with Lenovo System Guard

Lenovo System Guard monitors every server' s internal hardware inventory to protect against supply chain attacks and hacks throughout the system's life cycle. System Guard digitally identifies critical components, from CPUs and DIMMs to risers and backplanes. If these components are removed or changed, System Guard can alert administrators and even block boot- up.

Secure infrastructure from design to decommission

Security shouldn't start and end with the physical server. All Lenovo ThinkSystem and ThinkAgile with ThinkShield offerings are developed in accordance with the Lenovo Secure Development Lifecycle (LSDL) - built-in security that protects even the most sensitive data throughout the solution lifecycle. Lenovo continuously review their security approach with customers and independent experts.

Lenovo suppliers are validated through the Trusted Supplier Program, a documented and auditable supply chain security program that is designed to minimize customer risk. Lenovo's supply chain is also augmented with secure logistics, to ensure products are secure from data to decommission.

Standardized data protection

Lenovo Infrastructure Solutions enhance data protection with support for the latest security standards*

- Lenovo XClarity Controller 2.0 leverages FIPS 140-3 certified cryptography in process
- Trusted Computing Group Trusted Platform Module (TPM) version 2.0
- UEFI Forum standards for secure UEFI boot
- NIST SP800-131A rev 2 "Transitioning the Use of Cryptographic Algorithms and Key Lengths"
- NIST SP800-147B "BIOS Protection Guidelines for Servers"
- NIST SP800-193 "Platform Firmware Resiliency Guidelines"
- ISO/IEC 11889 "Trusted Platform Module Library"
- CNSA 1.0 quantum-resistant cryptography support in XClarity Controller (XCC)
- European Union Commission Regulation 2019/424 ("ErP Lot 9") "Ecodesign Requirements for Servers and Data Storage Products" Secure Data Deletion
- Optional FIPS 140-2 validated Self-Encrypting Disks (SEDs) with external KMIP-based key management

*Certain features are supported in XCCv2 such as Neighbor Groups, System Guard and FIPS 140-3 crypto.

Industry-leading built-in security and reliability for a worry-free infrastructure

Modern IT infrastructure must adapt quickly to ensure security. Data breaches and cyberthreats are continuing to grow each year and could potentially disrupt your business with costly fines, loss of customers and damage to your brand. For example, the average cost of a data breach has increased 10% over the last year to $4.88M. Making it the highest increase ever!

Lenovo recognizes that security is one of the most critical requirements that organizations have today, and Lenovo build security processes and products from design to decommission.

ITIC ranks Lenovo as the industry leader in reliability and security among all x86 platforms. Lenovo ISG product security program begins with the award-winning secure supply chain. It continues with secure business processes throughout the development life cycle, resulting in infrastructure and services that have security built-in, helping organizations protect their infrastructures from cyberattacks.

Modernize with confidence

Together with Lenovo, we can help you modernize your infrastructure with built-in security, simplified management, and long-term reliability.
Let's discuss how the latest ThinkSystem and ThinkAgile solutions can strengthen your defenses and prepare your business for what's next.

Contact us today to start your modernization journey.

© Lenovo 2025. All rights reserved. Lenovo, the Lenovo logo are trademarks or registered trademarks of Lenovo. All trademarks are the property of their respective owners.

1. https://s7d1.scene7.com/is/content/Lenovoassetsprod/sustainability-rethinking-packaging-eBookpdf