Smarter technology for all

# Sichere Lösungen für Ihr Datacenter

## Hardware – Daten – Betrieb – Security by Design

Miroslav Peic – Technical Solution Architect

2025 Lenovo. All Rights Reserved.

# Warum “Security”

1. **Schutz vor Cyberangriffen**
   * Rechenzentren sind zentrale Angriffspunkte (Ransomware, DDoS, Supply-Chain-Attacken)
   * Angriffe auf Datacenter können ganze Unternehmen oder kritische Infrastruktur lahmlegen

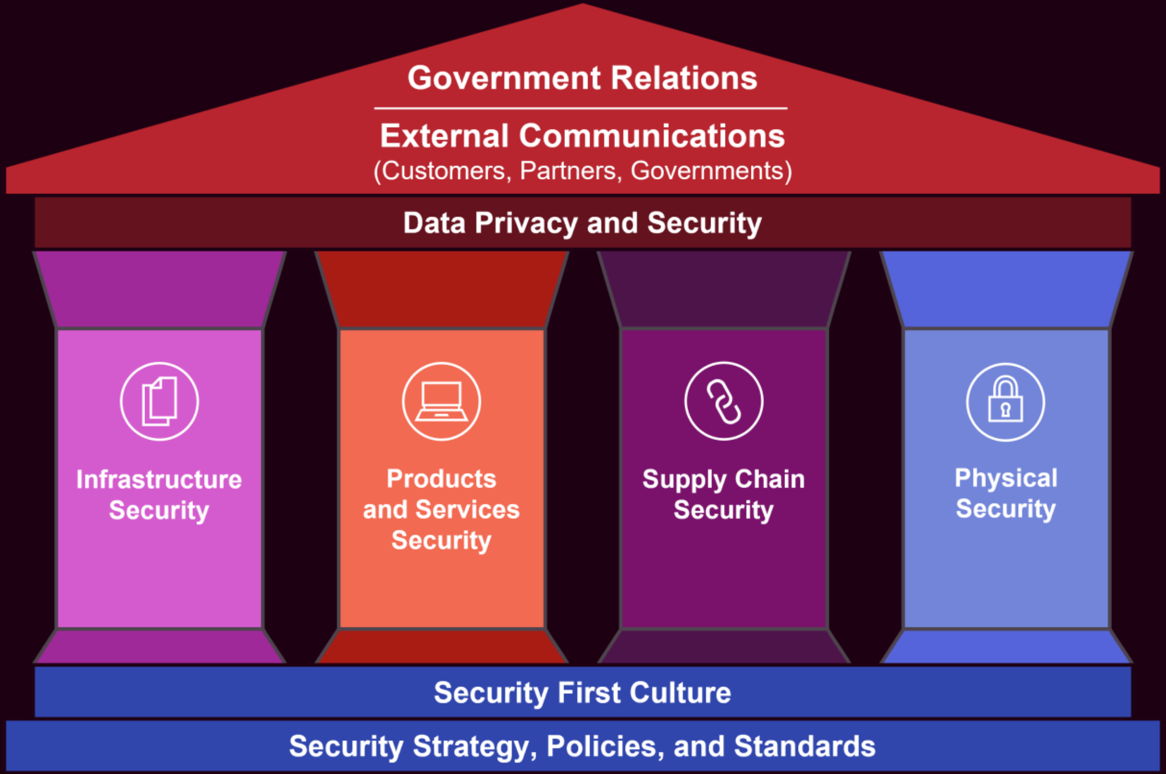
2. **Verfügbarkeit & Geschäftskontinuität**
   * Sicherheitsmaßnahmen schützen die Betriebsfähigkeit (24/7 Verfügbarkeit)
   * Notwendig für SLAs, Betriebsverträge und Kundenzufriedenheit

3. **Vertraulichkeit & Datenschutz**
   * Besonders relevant bei sensiblen personenbezogenen Daten
   * Verbindung zu DSGVO und branchenspezifischen Datenschutzbestimmungen

4. **Regulatorische & gesetzliche Anforderungen**
   * Sicherheitsanforderungen sind heute gesetzlich verpflichtend
   * DSGVO / NIS2 / DORA / BSI / ISO 27001 / ...

2025 Lenovo. All rights reserved.

# Global Security Organization


Government Relations
External Communications
(Customers, Partners, Governments)
Data Privacy and Security
Infrastructure Security
Products and Services Security
Supply Chain Security
Physical Security
Security First Culture
Security Strategy, Policies, and Standards

CSO Reports Directly to CEO

Aligns all security efforts

Foundation for all security work

Pillars support data privacy and security

Lenovo 2025 Lenovo. All Rights Reserved.

# Infrastructure Security

Safeguarding customer data

### Identify

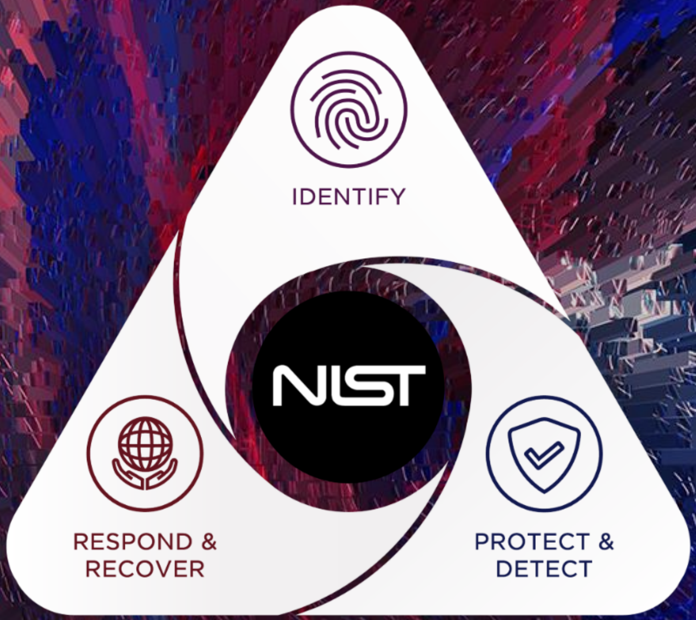
Identification of critical assets and threats

### Protect and Detect

Layers of advanced protection and detection on our networks and endpoints

### Respond and Recover

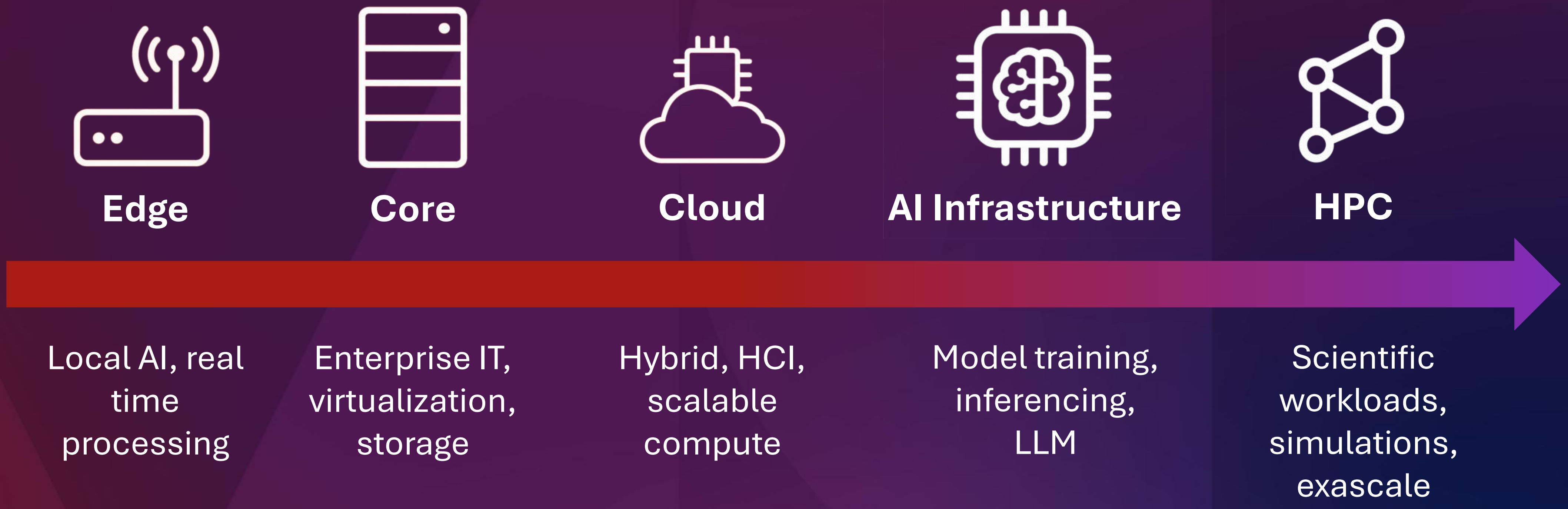
Proactive incident response processes to assure cyber resiliency



Lenovo 2025 Lenovo. All Rights Reserved.

# One Portfolio – Every Workload

Lenovo delivers the broadest and most reliable infrastructure portfolio in the industry, engineered to handle everything from AI at the edge to super compute.



**Edge**

Local AI, real time processing

**Core**

Enterprise IT, virtualization, storage

**Cloud**

Hybrid, HCI, scalable compute

**AI Infrastructure**

Model training, inferencing, LLM

**HPC**

Scientific workloads, simulations, exascale

Lenovo 2025 Lenovo. All rights reserved.

# Security without Compromise

## Compliance:

Supports FIPS 140-3, enhanced NIST SP800-193 Compliance, CNSA Suite 1.0 Quantum-resistant cryptography

## Lenovo System Guard:

monitors a server's internal hardware inventory to detect and protect against supply chain attacks or hacking

## Trusted platform Module(TPM) 2.0:

hardware-based security which provides user authentication, remote access, and data protection

## Protection:

Hardware-assisted encryption, physical intrusion switches and secure boot

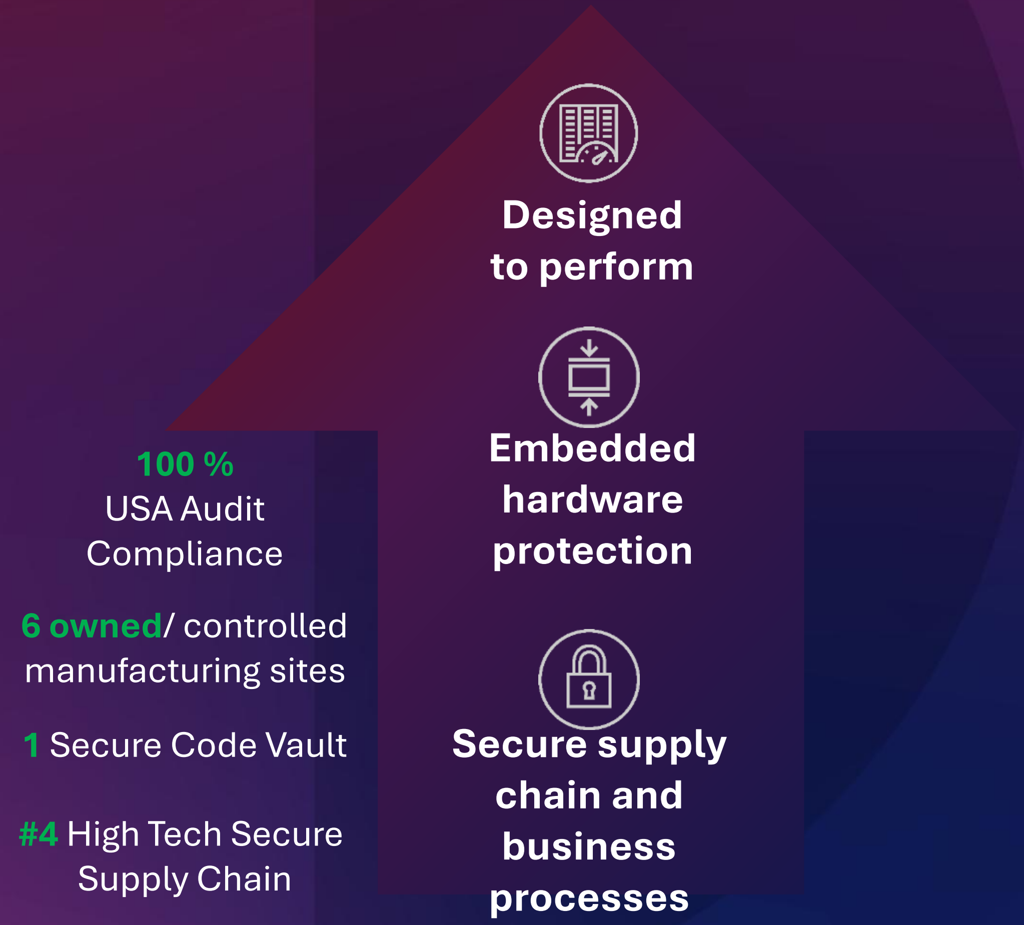
## Lenovo Immutable Root of Trust:

provides an embedded, silicon-based chip that ensures that the server can only be booted with trusted firmware

## Secure Development Lifecycle:

drives security into products and services throughout the lifecycle including digital signatures on products, secure development processes and incident response teams

ThinkShield



Designed to perform

Embedded hardware protection

Secure supply chain and business processes

**100 %** USA Audit Compliance

**6 owned**/ controlled manufacturing sites

**1** Secure Code Vault

**#4** High Tech Secure Supply Chain

Lenovo 2025 Lenovo. All rights reserved.

# Secure Product Design – Security Modes

## Enterprise Strict Security Mode

- Strict Security Mode is the most secure mode.
- All cryptography algorithms used by XCC are CNSA compliant.
- XCC operates in FIPS 140-2/140-3 validated mode.
- Requires CNSA grade certificates.
- Only services that support CNSA level cryptography are allowed.
- Requires XCC platinum license key to enable.

## Standard Security Mode

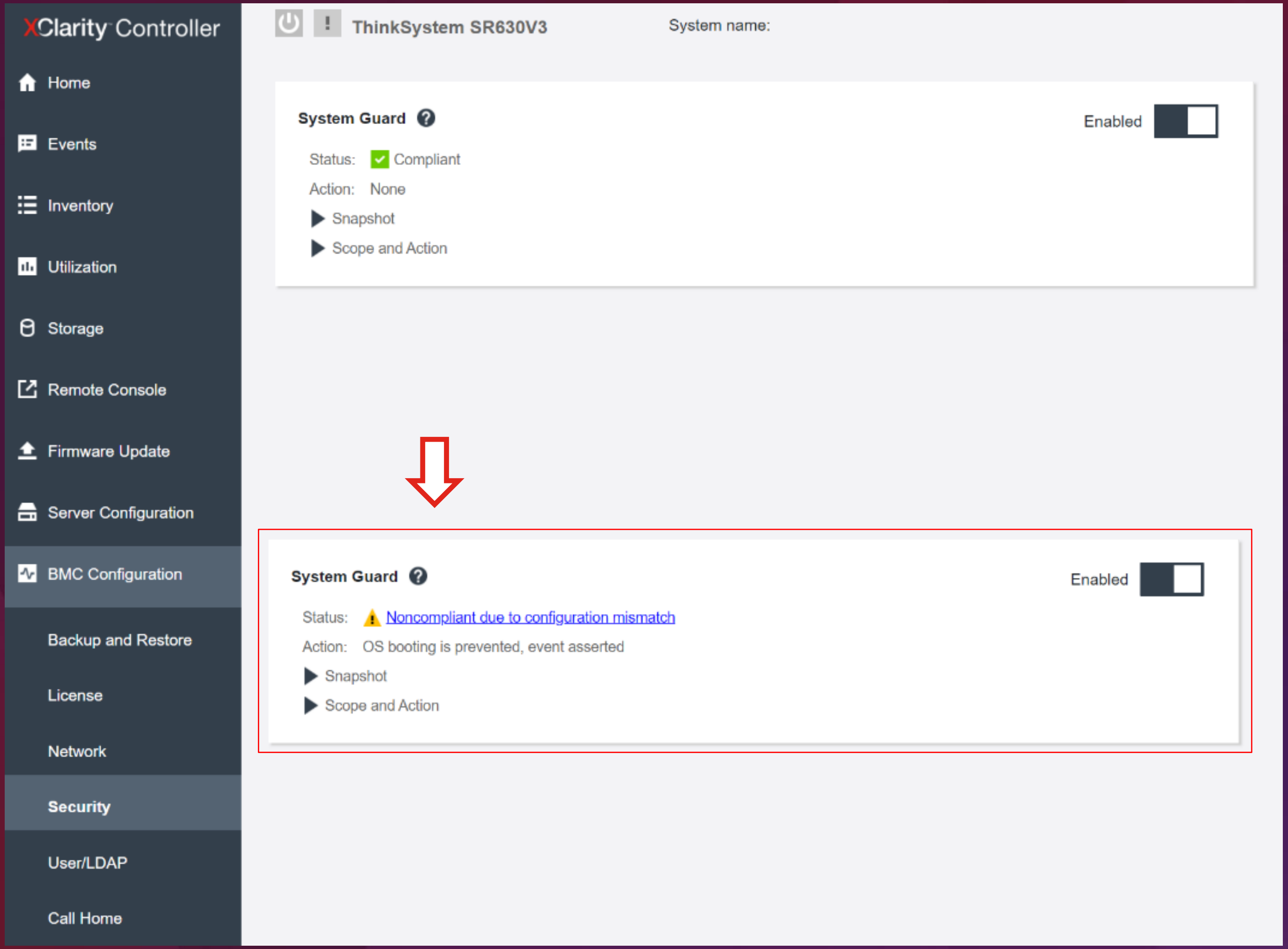
- Standard Mode is the **default** security mode.
- All cryptography algorithms used by XCC are FIPS 140-3/FIPS 140-2 compliant
- XCC operates in FIPS 140-2/140-3 validated mode.
- Requires FIPs grade certificates.
- Services that require cryptography that do not support FIPS 140-2/FIPS 140-3 level cryptography are disabled by default.

## Compatibility Security Mode

- Compatibility Mode is the mode to use when services and clients require cryptography that is not CNSA/FIPS compliant.
- A wider range of cryptography algorithms are supported.
- When this mode is enabled XCC is NOT operating in FIPS-validated mode.
- Allows all services to be enabled.

Lenovo 2025 Lenovo. All rights reserved.

# Secure Product Design – System Guard



ThinkSystem SR630V3    System name:

**System Guard** ?    Enabled

Status: ✓ Compliant

Action: None

▶ Snapshot

▶ Scope and Action

⇩

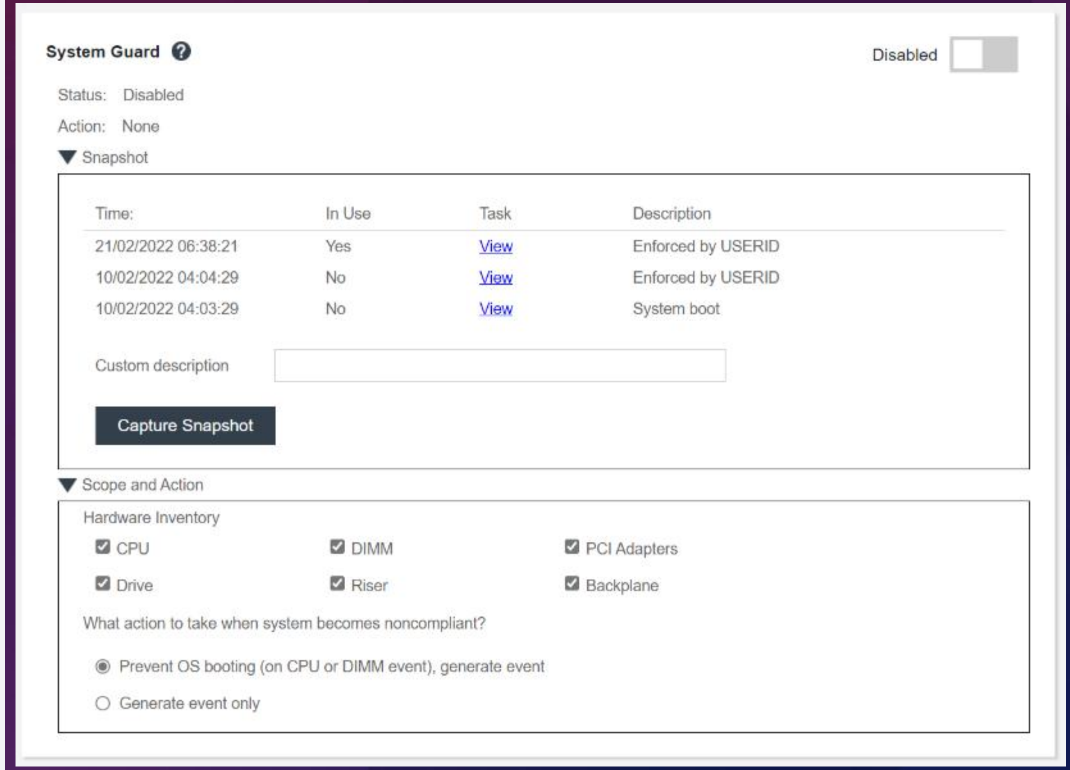
**System Guard** ?    Enabled

Status: ⚠ Noncompliant due to configuration mismatch

Action: OS booting is prevented, event asserted

▶ Snapshot

▶ Scope and Action



**System Guard** ?    Disabled

Status: Disabled

Action: None

▼ Snapshot

| Time: | In Use | Task | Description |
|---|---|---|---|
| 21/02/2022 06:38:21 | Yes | View | Enforced by USERID |
| 10/02/2022 04:04:29 | No | View | Enforced by USERID |
| 10/02/2022 04:03:29 | No | View | System boot |

Custom description

▼ Scope and Action

Hardware Inventory

☑ CPU    ☑ DIMM    ☑ PCI Adapters

☑ Drive    ☑ Riser    ☑ Backplane

What action to take when system becomes noncompliant?

● Prevent OS booting (on CPU or DIMM event), generate event

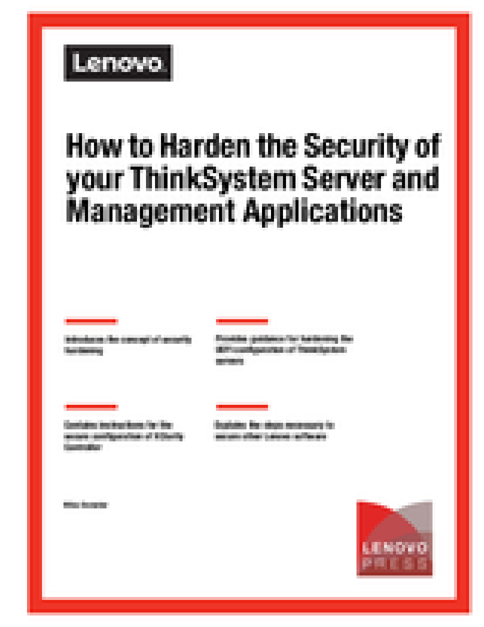
○ Generate event only

**Monitor hardware inventory for unexpected changes (CPU, DIMM, PCI, HDD, etc.), log event or prevent booting**

Lenovo 2025 Lenovo. All rights reserved.

# High quality technical publications

- Introduces the concept of security hardening
- Provides guidance for hardening the UEFI configuration of ThinkSystem servers
- Contains instructions for the secure configuration of XClarity Controller
- Explains the steps necessary to secure other Lenovo software



Lenovo

How to Harden the Security of your ThinkSystem Server and Management Applications

Introduces the concept of security hardening

Provides guidance for hardening the UEFI configuration of ThinkSystem servers

Contains instructions for the secure configuration of XClarity Controller

Explains the steps necessary to secure other Lenovo software

[illegible]

LENOVO PRESS

https://lenovopress.lenovo.com/lp1260.pdf

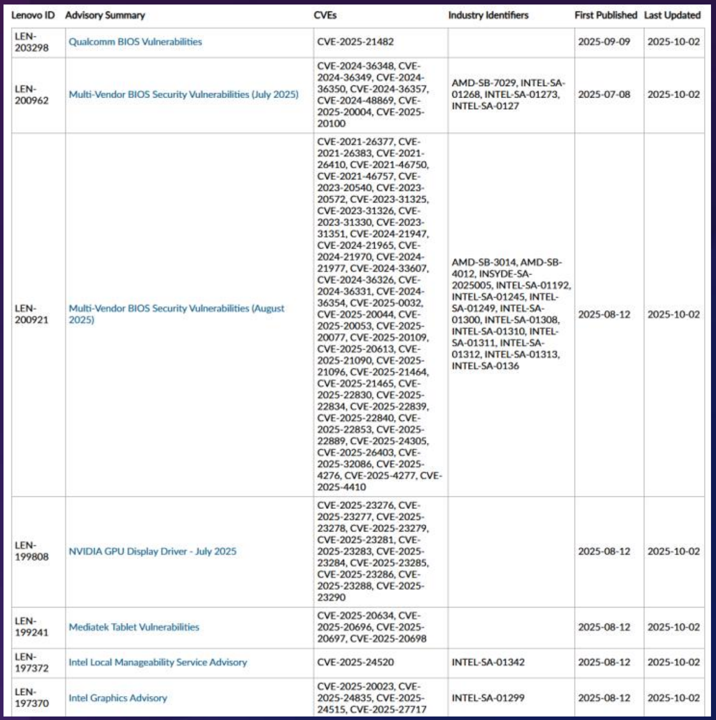
Lenovo 2025 Lenovo. All rights reserved.

# Lenovo Product Security Advisories and Announcements

**Lenovo hat es sich zur Aufgabe gemacht, Produkte und Services zu entwickeln, die den höchsten Sicherheitsstandards entsprechen, um unsere Kunden und ihre Daten zu schützen.**

- **Das Lenovo Product Security Incident Response Team (PSIRT) untersucht gemeldete Schwachstellen und stellt Informationen zur Verfügung, indem es Sicherheitsempfehlungen veröffentlicht.**

- **Lenovo veröffentlicht auch Ankündigungen, die sicherheitsbezogene Ratschläge, reaktive Aussagen oder zusätzliche Details zur Ergänzung einer Empfehlung enthalten können.**



| Lenovo ID | Advisory Summary | CVEs | Industry Identifiers | First Published | Last Updated |
|---|---|---|---|---|---|
| LEN-203298 | Qualcomm BIOS Vulnerabilities | CVE-2025-21482 | | 2025-09-09 | 2025-10-02 |
| LEN-200962 | Multi-Vendor BIOS Security Vulnerabilities (July 2025) | CVE-2024-36348, CVE-2024-36349, CVE-2024-36350, CVE-2024-36357, CVE-2024-48869, CVE-2025-20004, CVE-2025-20100 | AMD-SB-7029, INTEL-SA-01268, INTEL-SA-01273, INTEL-SA-0127 | 2025-07-08 | 2025-10-02 |
| LEN-200921 | Multi-Vendor BIOS Security Vulnerabilities (August 2025) | CVE-2021-26377, CVE-2021-26383, CVE-2021-26410, CVE-2021-46750, CVE-2021-46757, CVE-2023-20540, CVE-2023-20572, CVE-2023-31325, CVE-2023-31326, CVE-2023-31330, CVE-2023-31351, CVE-2024-21947, CVE-2024-21965, CVE-2024-21970, CVE-2024-21977, CVE-2024-33607, CVE-2024-36326, CVE-2024-36331, CVE-2024-36354, CVE-2025-0032, CVE-2025-20044, CVE-2025-20053, CVE-2025-20077, CVE-2025-20109, CVE-2025-20613, CVE-2025-21090, CVE-2025-21096, CVE-2025-21464, CVE-2025-21465, CVE-2025-22830, CVE-2025-22834, CVE-2025-22839, CVE-2025-22840, CVE-2025-22853, CVE-2025-22889, CVE-2025-24305, CVE-2025-26403, CVE-2025-32086, CVE-2025-4276, CVE-2025-4277, CVE-2025-4410 | AMD-SB-3014, AMD-SB-4012, INSYDE-SA-2025005, INTEL-SA-01192, INTEL-SA-01245, INTEL-SA-01249, INTEL-SA-01300, INTEL-SA-01308, INTEL-SA-01310, INTEL-SA-01311, INTEL-SA-01312, INTEL-SA-01313, INTEL-SA-0136 | 2025-08-12 | 2025-10-02 |
| LEN-199808 | NVIDIA GPU Display Driver - July 2025 | CVE-2025-23276, CVE-2025-23277, CVE-2025-23278, CVE-2025-23279, CVE-2025-23281, CVE-2025-23283, CVE-2025-23284, CVE-2025-23285, CVE-2025-23286, CVE-2025-23288, CVE-2025-23290 | | 2025-08-12 | 2025-10-02 |
| LEN-199241 | Mediatek Tablet Vulnerabilities | CVE-2025-20634, CVE-2025-20696, CVE-2025-20697, CVE-2025-20698 | | 2025-08-12 | 2025-10-02 |
| LEN-197372 | Intel Local Manageability Service Advisory | CVE-2025-24520 | INTEL-SA-01342 | 2025-08-12 | 2025-10-02 |
| LEN-197370 | Intel Graphics Advisory | CVE-2025-20023, CVE-2025-24835, CVE-2025-24515, CVE-2025-27717 | INTEL-SA-01299 | 2025-08-12 | 2025-10-02 |

Lenovo 2025 Lenovo. All rights reserved.

# XClarity One – Advanced IT Operations

Critical updates to firmware

The firmware on 3 of your devices have should be updates to resolve outstanding critical issues.

New firmwar

There firmware c complies with

New updates available

You may wish to update 9 devices with the latest firmware

XClarity One

**Security** →

Built on Zero Trust with MFA for better protection

**Simplicity** →

Intuitive interfaces and automation reduce complexity

**Scalability** →

Cloud deployment allows flex up and down on demand

**Efficiency** →

Optimized utilization lowers costs and environmental impact

**Reliability** →

Continuous monitoring and self-healing capabilities ensure uptime

**Manage your environment, not your tools**

With XClarity One you can Simplify IT Operations, Secure your infrastructure, and Scale your success with unparalleled ease and confidence!

# Full-spectrum Data Protection for ThinkSystem DG/DM Series

## Protect

### Policy Engine

Automatically block known malicious file types

### Immutable WORM Primary Data & Tamper-Proof Snapshots

Prevent data destruction with immutable and indelible snapshots

### Multi-Admin Verify

Block rogue admins and malicious users

### End-to-End Encryption

Secure data access, end-to-end

## Detect

### Autonomous Ransomware Protection

Automatically detect and respond to file system anomalies that may signal a ransomware attack – builtin

## Recover

### SnapRestore

Restore data in minutes from secure snapshots

Lenovo 2025 Lenovo. All Rights Reserved.

# Made in Europe for Europe

- Lenovo delivers customized solutions in the heart of Europe from our manufacturing plant in Ullo, Hungary.
- Our Ullo plant shipped one million workstations & servers in its first year, enabling deeper collaboration, transparency, and understanding with Lenovo customers across the EMEA region.

2025 Lenovo. All rights reserved.

Lenovo 2025 Lenovo. All rights reserved.

Smarter
technology
for all

Lenovo

# thanks.