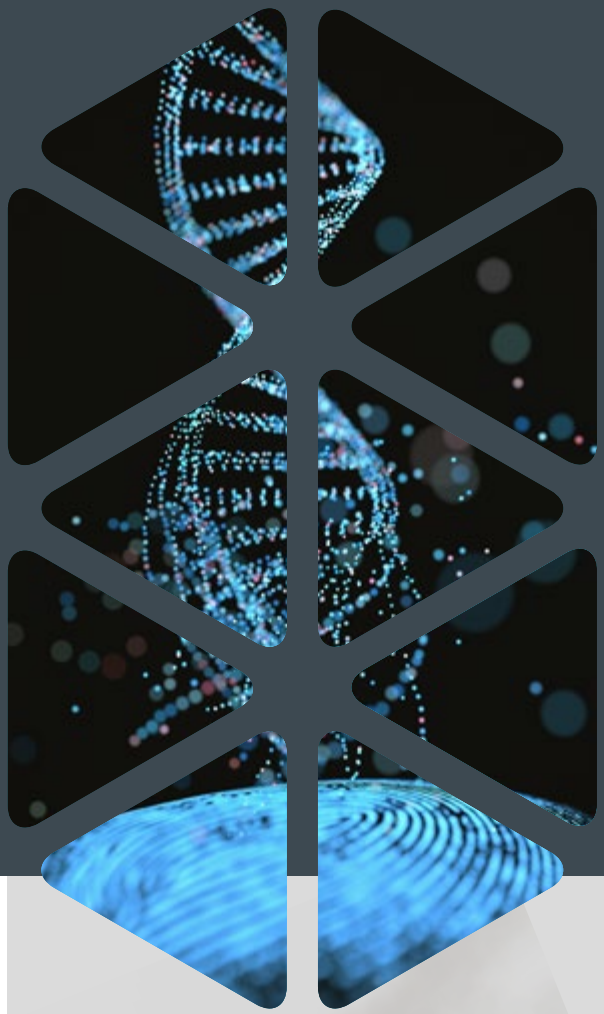
ThinkShield

Security Is in Our DNA

Protect your data and fortify your business against cyberattacks with a foundation of built-in security for the infrastructure.



Lenovo

Intensifying Business Risks

Traditional approaches to platform security are no match as cyber criminals up the ante, exploiting vulnerabilities in data center servers and IoT devices. Cyberattacks are becoming the No. 1 risk to business, brand, operations, and financials.[1] Your data is among your most valuable assets and data breaches can cost you dearly.

13%
Of security professionals have a FULLY implemented security program that includes Firmware[2]

50%
Of enterprises report at least one incident of firmware infection

8%
of enterprise administrators feel the infrastructure is prepared for firmware related attacks

Unfailing Platform Security

In an unpredictable threat landscape, a secure infrastructure is your first line of defense. Lenovo data center solutions shield your business with built-in hardware security to help prevent, detect, and recover from cyberattacks.

- Configured with components from known, trusted suppliers
- Built in secure manufacturing facilities
- Designed to prevent compromised firmware from loading

A Strong Foundation for Future-Ready IT

Exacting Security Practices

Lenovo's business processes are based on proven security practices to meet the most rigorous requirements.

- 100% of CFIUS audits passed with zero infractions
- Source codes stored, compiled, and digitally signed in the U.S.
- Transparent security development processes reviewed and approved by the U.S. government

Trustworthy Product Design

Lenovo's product design helps ensure your server won't introduce security vulnerabilities at a hardware level.

- Built-in, standards-based security
- Secure software development lifecycle
- Ongoing product security assessments and penetration testing
- Unauthorized firmware code blocked from launching

Secured Supply Chain

Lenovo's supply chain protects your servers from unauthorized entry at any point in the manufacturing process.

- Highest security level achieved for supply chain audit: C-TPAT Tier 3[5]
- Trusted suppliers with annual assessments
- Lenovo-owned and controlled manufacturing plants
- Option to specify complete manufacturing in U.S.

Did You Know?

1 100% of Lenovo stock is publicly traded and the company manufactures in each major geography around the world.

2 Lenovo has held a GSA schedule for more than 10 years, supplying trade-compliant products that have passed 100% of audits with zero infractions.

3 Lenovo supports critical infrastructure customers in energy, banking, healthcare, large retail, education, manufacturing, telecom, IT/technology, and other key industries.

Learn More

Discover how industry-leading platform security helps move your business forward with Lenovo ThinkAgile software-defined infrastructure and Lenovo ThinkSystem server, storage, and networking solutions.

www.lenovo.com/us/en/product-security/landing

ThinkShield

Lenovo

[1] 2018 SonicWall Cyber Threat Report, March 2018
[2] isaca.org/firmware
[3] isaca.org/firmware
[4] isaca.org/firmware
[5] Customs-Trade Partnership Against Terrorism (C-TPAT) audits supply chain; certifies manufacturing points, origination, and consolidation points; and provides enhanced cargo screening