Lenovo Security by Design: Foundational Security from Edge to Cloud

Article

Cybersecurity has become a major concern for all organizations, large and small. The frequency, severity and cost of data breaches accelerates daily, as the cyber attack surface expands and the breadth of attacks grows to compromise new and different areas. C-Suite executives and Boards want to partner with IT providers that truly understand security and can help them guard against the impact of security breaches. Lenovo ISG's product security program "bakes in" foundational security to our products in order to minimize security risks and to help customers guard their data and infrastructure.

The Magnitude of the Security Problem

The costs associated with security breaches—both tangible and intangible—are alarming:

In March 2022, the release of the annual FBI Internet Crime Report 2021 revealed the total money lost to cybercrime increased 64% to $6.9 billion last year and that the number of cybercrime complaints to the FBI rose seven percent (7%) to 847,376. The average cost of a data breach increased 2.6% from USD 4.24 million in 2021 to USD 4.35 million in 2022. The global cost of cybercrime topped $6 trillion in 2021!

ITIC's 2022 Global Server Hardware Security survey shows that 78% of corporate enterprises rank security as the leading cause of unplanned server and application downtime, and that 80% of survey respondents fear their organizations will fall victim to a targeted attack over the next 12 to 18 months.

> "Lenovo ThinkSystem servers achieved the best security scores among all x86 server distributions for the fourth year in a row. "
>
> "In 2022, only 2% of Lenovo ThinkSystem servers experienced downtime due to a hack attack. This is down from 4% of Lenovo ThinkSystem servers that suffered unplanned downtime due to a security attack in 2021."
>
> —ITIC 2022 Global Server Hardware Security Report

Furthermore, security breaches from issues associated with supply chain and third-party suppliers made an unprecedented jump in the US in 2021, rising 297% year over year and representing about a fourth of all security breaches, making supply chain security crucial.

Lenovo ISG's Product Security Program

Lenovo Infrastructure Solutions Group's (ISG) security program (ThinkShield) has a long heritage, with its roots in System x security foundations. With a goal of being our customers' most trusted partner, Lenovo ISG equips our customers with secure solutions from edge to cloud. We build security into our products from development through delivery. In a world where bad actors are constantly attacking servers and networks and seeking to steal critical data, Lenovo ISG is committed to programs and actions which will minimize security risks in our products and to our customers.

Lenovo ISG encourages customers to scrutinize all IT suppliers and ask each supplier questions about code origin and security controls, independent product security assessments, security response, and product security governance. Our industry leadership position provides us with significant market insight, which demonstrates that Lenovo ISG's product security practices exceed industry norms.

A Strong Foundation for Future-Ready IT

Lenovo ISG's product security program begins with our award-winning secure supply chain and continues with secure business processes throughout the development life cycle, resulting in products that have security built in to help our customers protect their infrastructures from cyberattacks.

 **Secure Supply Chain**	 **Secure Business Processes**	 **Secure Product Design**
Lenovo owns and controls our manufacturing to ensure security is built into our products from the beginning of development • Lenovo Supply Chain ranked #3 High Tech Supply Chain and #9 Global Supply Chain by Gartner for 2022 • Trusted suppliers with periodic assessments • Highest security level achieved for supply chain: C-TPAT Tier 3 • "…Lenovo's implementation[s] meet or exceed industry standards from a supply chain and product development security perspective and likely are at or above the level of its peers…" – *Chain Security* independent assessment	Lenovo's business processes are based on proven security practices to meet the most rigorous requirements • Secure Development Lifecycle drives security into products and services throughout the lifecycle • Source code is stored, compiled, and digitally signed in an air-gapped facility in the U.S. • Transparent security development processes are reviewed and have been audited by customers and third-party consultancies • Incident response team works with customers, suppliers, researchers, and even competitors to address security vulnerabilities as they arise	Lenovo's product design builds security into our products, and we continuously enhance our products to meet the latest security standards • Built-in, standards-based security • Enhanced platform protection with an increased number of the latest security standards • Lenovo System Guard monitors server internal hardware inventory to protect against supply chain attacks or hacking throughout the life cycle • Lenovo's immutable hardware Root of Trust ensures that the server can only be booted with trusted firmware and enables recovery in the unlikely event of tampering or corruption

Secure Supply Chain

Lenovo builds security into our products from the very beginning of development. Lenovo owns and controls our manufacturing, unlike many of our competitors. Our **award-winning supply chain** is ranked by Gartner as the #3 High Tech Supply Chain for 2022 (in the Top 7 since 2015), and #9 Global Supply Chain (in the Top 35 since 2013). This ranking is across **all** firms and industries evaluated by Gartner.

Through our **Trusted Supplier Program** we specify supplier security requirements and carefully evaluate and qualify all our suppliers to ensure they meet our security standards, and we periodically audit their compliance on a risk basis. This program covers all Intelligent Components (any executable component, memory, semiconductors, etc.)—and their suppliers—that could adversely affect the security of our products.

Lenovo was the first Tier 1 manufacturer to offer **Intel Transparent Supply Chain (TSC)**, which provides a "Birth Certificate" for Intel-based ThinkSystem Servers and ThinkAgile Solutions. This birth certificate provides traceability at the system and component level and a statement of conformance, digitally signed by Intel®, to guarantee the authenticity of the systems.

Lenovo augments our secure supply chain with **secure logistics**. We ensure that our products remain secure from the time they leave our manufacturing facilities to the time they are delivered and operationalized in customer environments. Once the products are built and tested, they are packaged and prepared for shipping with tamper-evident materials so that any problems can be noticed immediately, en route, and the incident investigated. After packaging, Lenovo works with qualified logistics suppliers to safely deliver products to end customers. Protection throughout the shipping process includes secure facilities, trucks and conveyances, and thoroughly-screened employees, visitors, and drivers. Shipments are tracked from the time they leave Lenovo buildings until they are received at a customer's location.

Beyond our supply chain security, we assist customers with security for their product lifecycle management. For those customers who are interested in secure disposal, Lenovo offers an end-of-life program through our **Asset Recovery Services (ARS)**. Through ARS, Lenovo can securely wipe hard drives and securely recycle parts utilizing industry recognized data sanitization standards such as NIST SP 800-88 R1 and Commission Regulation (EU) 2019/424, compliant with privacy laws such as HIPAA, GDPR, CCPA, Sarbanes Oxley, Gramm-Leach-Bliley, and others.

Lenovo adheres to the World Customs Organization (WCO) SAFE Framework of Standards to Secure and Facilitate Global Trade and Authorized Economic Operators (AEO) requirements. We are committed to strengthening international supply chains and improving United States border security. We are a C-TPAT Tier III partner ("Certified, Exceeding" all minimum criteria), the highest rating provided by the U.S. Customs and Border Protection.

Secure Business Processes

Lenovo has established a governance structure to drive security across products and services development. Our **Lenovo Secure Development Lifecycle (LSDL)** guides products and services security efforts throughout our business units to reduce risk. We draw from the BSIMM ("Building Security In" Maturity Model) and will be compliant with Cybersecurity Executive Order 14028 "Improving the Nation's Cybersecurity." The cornerstone of this LSDL process is the **Software Security Review Board (SSRB).** The Security Review Board engages with products and services development teams throughout the entire product lifecycle to ensure a secure design and to further review security before release.

Lenovo's Secure Development Lab is located in the US, managed by US Nationals, with restricted access based on need. It houses ThinkSystem general purpose server firmware and software source code, build, and signing functions. Lenovo firmware is maintained, built, and digitally signed on logically isolated servers in this facility to protect against tampering and ensure secure, trusted boot-up. Our development security enablement embeds security tooling into development teams to enable faster issue identification and remediation.

Lenovo ensures that **Security assessments** are routinely performed for processes and product offerings. These have included annual third-party (external) security process audits, third-party (external) assessments for major development milestones of core products, and first-party (internal) assessments for each software / firmware release. We have longstanding relationships with third-party security partners, most of whom are approved for use by the US Government.

Our security support for our customers extends throughout the lifecycle. Lenovo's **Product Security Office** exists to improve customer trust and awareness in the security of Lenovo product offerings. Our **Product Security Incident Response Team (PSIRT)** works with customers, suppliers, partners, and researchers to investigate, resolve, and report security vulnerability information related to Lenovo products. We publish security advisories that transparently describe vulnerabilities affecting Lenovo products and provide information on how customers can protect their systems.

Secure Product Design and Continuous Innovation

Lenovo ISG builds security into all our ThinkSystem and ThinkAgile products and continuously enhances our products to increase security for our customers. Our ThinkSystem and ThinkAgile v3 offerings incorporate significant new capabilities to protect against attacks, detect attacks if they occur, and recover from attacks in the unlikely event of tampering or corruption. These include enhancements to our platform protection with an increased number of the latest security standards such as FIPS 140-3 (validation in process), stronger password storage, enhanced compliance with NIST SP800-193 Platform Firmware Resiliency (PFR), and CNSA Suite Quantum-resistant cryptography.

Lenovo now offers Lenovo System Guard, which monitors a server's internal hardware inventory to protect against supply chain attacks or hacking throughout the life cycle. By taking digital "measurements" of critical components such as CPUs, DIMMs, PCI Adapters, drives, risers & backplanes, we can detect if these components are removed or swapped with a different component after shipment from the manufacturing plant, through shipping and delivery, and after deployment in our customers' infrastructure. In the event a component change is detected, System Guard can be configured either to send an alert to an administrator or to block boot-up.

Lenovo's immutable hardware Root of Trust (RoT) provides an embedded, silicon-based chip which ensures that the server can only be booted with trusted firmware. Through a carefully choreographed "chain of trust," the boot process ensures that each of the critical below-OS components has the correct digital signature from our manufacturing plant and has not been tampered with. If any component fails this test the server will not boot, and the administrator is notified of the issue. We have also built in increased redundancy for critical firmware support, which means faster and more reliable recovery in the unlikely event of tampering or corruption.

Summary

Lenovo is committed to programs and processes to deliver products and solutions that not only have the functionality our customers want, but also meet or exceed industry standards for security. We build in security from the beginning of development through our secure supply chain, manufacture our products in Lenovo-owned factories, and ensure security throughout the product lifecycle. The strength of our commitment to security is evidenced not only by third-party assessments and attestations but also by the end result, the security of our products—as demonstrated, for example, by ITIC's 2022 global security survey finding that **"Lenovo ThinkSystem servers achieved the best security scores among all x86 server distributions for the fourth year in a row."**

Lenovo provides provably secure solutions via independent audits by customers and third-party consultancies. We support our customers not only with secure products but also through our Product Security Incident Response Team to publish advisories of any potential exposure and help customers with remediation if needed.

Lenovo ISG continues to be a trusted supplier to governments, critical infrastructure industries, and many other security-sensitive customers around the world. Our servers are used in wide-ranging critical applications such as powering more supercomputers than any other supplier to solve some of humanity's greatest challenges, to supporting critical infrastructure workloads, to serving as a foundational capability for 8 of the top 10 global cloud providers. As a result, robust security is an integral part of our product development process.

About the author

Bob Nevins is a Senior Consultant at Lenovo with a focus on Infrastructure Security.

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2023. All rights reserved.

This document, LP1116, was created or updated on October 14, 2022.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP1116
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP1116.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
System x®
ThinkAgile®
ThinkShield®
ThinkSystem®

The following terms are trademarks of other companies:

Intel® is a trademark of Intel Corporation or its subsidiaries.

Other company, product, or service names may be trademarks or service marks of others.