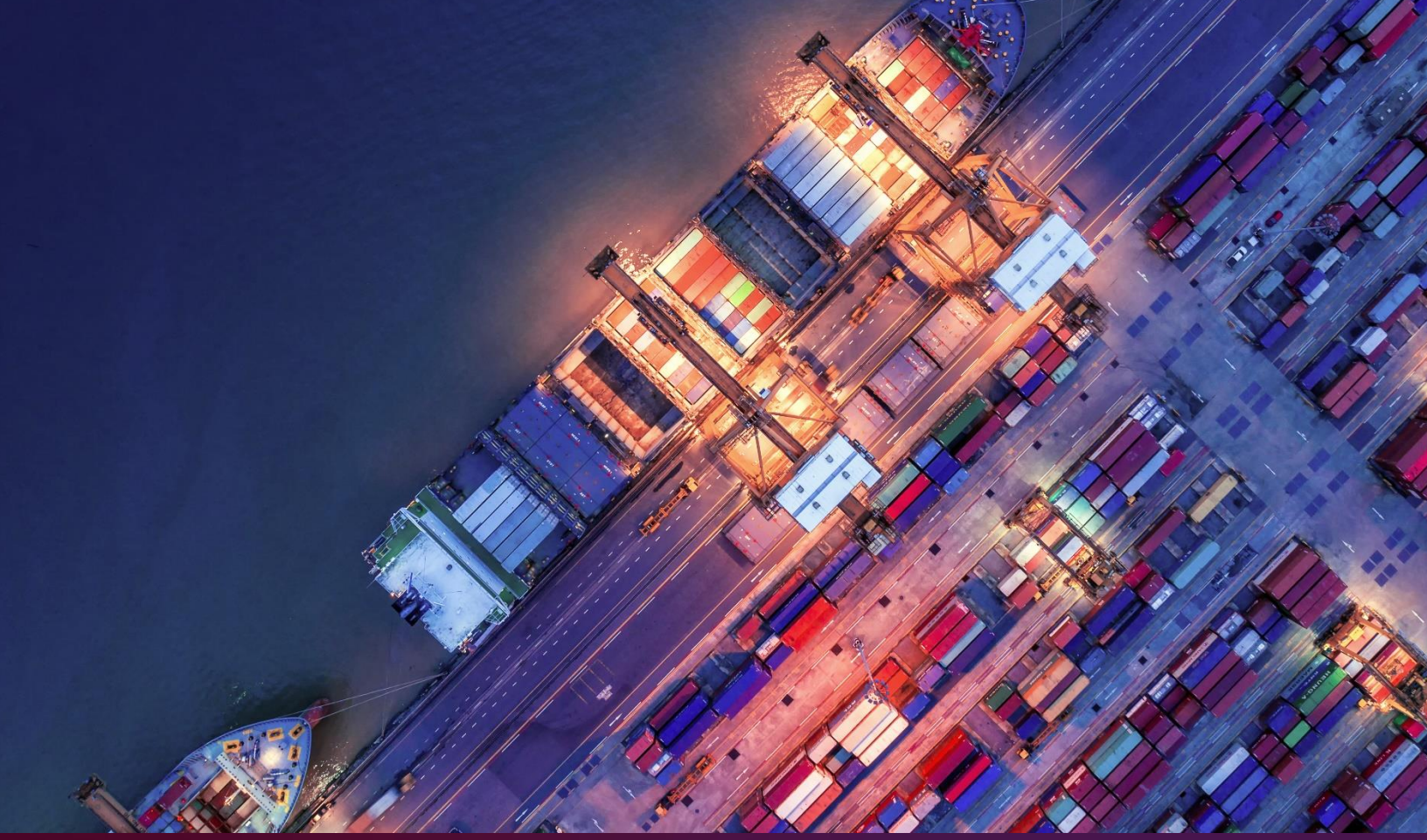


Secure, Reliable, Transparent

Lenovo Global Supply Chain

Smarter technology for all

Lenovo

Table of Contents

Introduction

Information technology is increasingly interconnected, and our dependency on it continues to grow. Advancements in technology provide numerous advantages for everyone as we live in an increasingly digital world. More systems are connected through complex, critical networks which create new exposures to evolving threats. The increasing sophistication of threats that poses a greater risk to our customers and shareholders. Therefore, the task of continuously safeguarding this critical infrastructure becomes increasingly complex. At Lenovo, it's our goal to ensure that our products are safe, highly resilient, and trustworthy before they enter our customers' environment. We attest to the integrity of each device right down to the system levels that require administrator access.

Lenovo's Global Supply Chain

Lenovo's global supply chain is an embodiment of the customer-centric approach that defines its success. Lenovo's commitment to delivering innovation, efficiency, and resilience to customers worldwide is underpinned by its resilient supply chain. It's not just about being a technological powerhouse; it's about ensuring that cutting-edge products reach customers securely and on time. Lenovo takes pride in maintaining a world-class supply chain, consistently recognized among the industry leaders with 30+ manufacturing sites located across 10 geographies serving 180+ markets globally. Lenovo's supply chain remains highly resilient, ready to adapt swiftly to mitigate a wide variety of disruptions. Lenovo's world-class Global Supply Chain has again been named in the Gartner Supply Chain Top 25[1] for 2023, ranking #8 in this list of global companies with supply chains(a rank up from its position in 2022). The Gartner Supply Chain Top 25 identifies, celebrates and profiles supply chain excellence on a global scale, and by target region and industry. This is followed by ranking #1 in the Gartner® Asia/Pacific Supply Chain Top 10[2] for 2023. This marks the second consecutive year that Lenovo has received this recognition. Lenovo also ranked #3 in Gartner 2023 Supply Chain Top 25[3] High Tech Category. At its core, Lenovo's Global Supply Chain is committed to resilience, addressing the uncertainties of the global market. Lenovo's multi-sourcing approach is pivotal, ensuring customer success by diversifying sources for critical components, strategically diversifying suppliers to fortify against risks. By avoiding dependence on a single source for essential components, Lenovo insulates itself from disruptions, ensuring a consistent and reliable supply. Lenovo's strategy showcases foresight and adaptability helps the company navigate natural disasters, geopolitical tensions, and pandemics. Lenovo's dedication to customer success is evident in its proactive risk management. Understanding that product dependability hinges on a reliable supply chain, the company strategically deploys multiple suppliers for critical components. This approach not only safeguards Lenovo's interests but, more importantly, allows customers to receive products without compromise

"Lenovo is dedicated to driving supply chain security thought leadership, so we remain in front of the supply chain evolution."

-Doug Fisher, Chief Security Officer, Lenovo

1 Lenovo Press Release: Lenovo ranks eighth in the Gartner Supply Chain Top 25 for 2023
2 Lenovo Press Release: Lenovo Ranks No.1 in the Gartner Asia/Pacific Supply Chain Top 10 for 2023
3 Top High Tech Supply Chains for 2023

Global Supply Chain's key objectives

Security

Security is paramount in Lenovo's supply chain operations. From the start of the design phase all the way through to customer delivery, Lenovo assures customers of the integrity of our products and services. It's a commitment to customer trust that's backed by substantial investments in security measures.

Resiliency

Lenovo operates 30+ manufacturing sites across 10 markets. This extensive global manufacturing network isn't just about reliable production; it's also about being closer to the customer. It means swift responses to local demands, lower shipping costs, and potentially shorter wait times. The advantage of Lenovo's in-house manufacturing strategy allows us to deploy and enforce stricter security controls resulting in products with higher reliability and a better customer experience.

Transparency

Lenovo focuses on component transparency and has undergone extensive audits conducted by customers and various third parties. These evaluations, which explored various aspects of our operations, were an opportunity for us to successfully demonstrate our commitment to transparency, quality, IT security, compliance, product security, corporate ethics, and more.

Security at Lenovo

At Lenovo, security is a top priority, with a committed top-down management approach, ensuring that every employee understands and embraces the principle that security is everyone's responsibility. Lenovo's Global Security Organization is led by our Chief Security Officer, who reports to Lenovo's Chief Executive Officer. Our CSO is one of Lenovo's top 18 senior executives and is a member of our Leadership Executive Committee. The CSO manages alignment of all security efforts across Lenovo with a mission to position Lenovo as a leader and enabler of intelligent transformation through a comprehensive and cohesive global security program. Lenovo's Global Security organizational structure provides a sturdy foundation beginning with our security strategy, corresponding policies, and standards to drive security requirements across our enterprise. Lenovo's Security First Culture starts with the shared focus that "Security is Everyone's Responsibility." Lenovo's four main security functions are:

- IT Infrastructure Security
- Products & Services Security
- Supply Chain Security
- Physical Asset Security

Each of Lenovo's security functions serves to strengthen Lenovo's commitment to Data Privacy and Security. Lenovo's Privacy Program ensures that global operations, as well as products and services, comply with regulations in the 180 markets in which we operate.

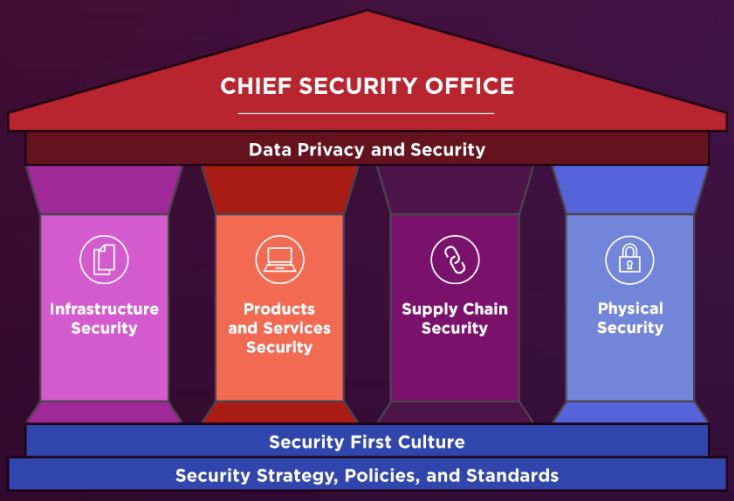


Figure 1

Lenovo Global Supply Chain Security

Lenovo's dedication to supply chain security focuses heavily on the prevention of tainted products, counterfeit goods, and software vulnerabilities. Our secure supply chain process implements rigorous measures to lock down the entire manufacturing supply chain, ensuring that suppliers, components, and processes meet stringent security standards. Every step of the manufacturing process is meticulously controlled, audited, and made tamper-proof, demonstrating that customers can rely on secure devices from the outset.

At Lenovo, our unwavering commitment to security and integrity is integrated throughout our product portfolio. In every product and service, we prioritize the safety and trust of our customers by embedding robust security measures into every facet of our supply chain. Figure 2 illustrates Lenovo's supply chain security framework:

VISION

Security in our Value Chain | Integrity in our Ecosystem

MISSION

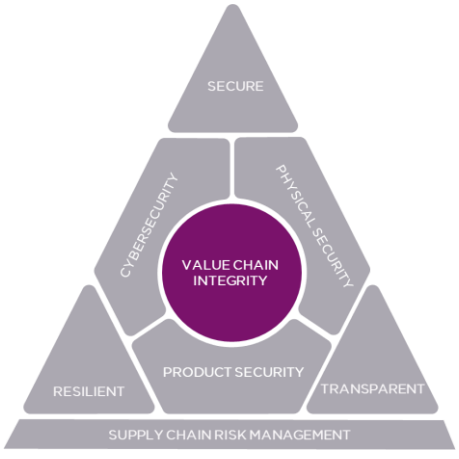
Securing the Future of our Products, Services & Customers

STRATEGIC OBJECTIVES

- Differentiate Lenovo as a trusted and secure IT partner
- Develop a One-Lenovo GSC security mindset
- Align with CSO Vision, Mission, and Strategic Objectives

Figure 2

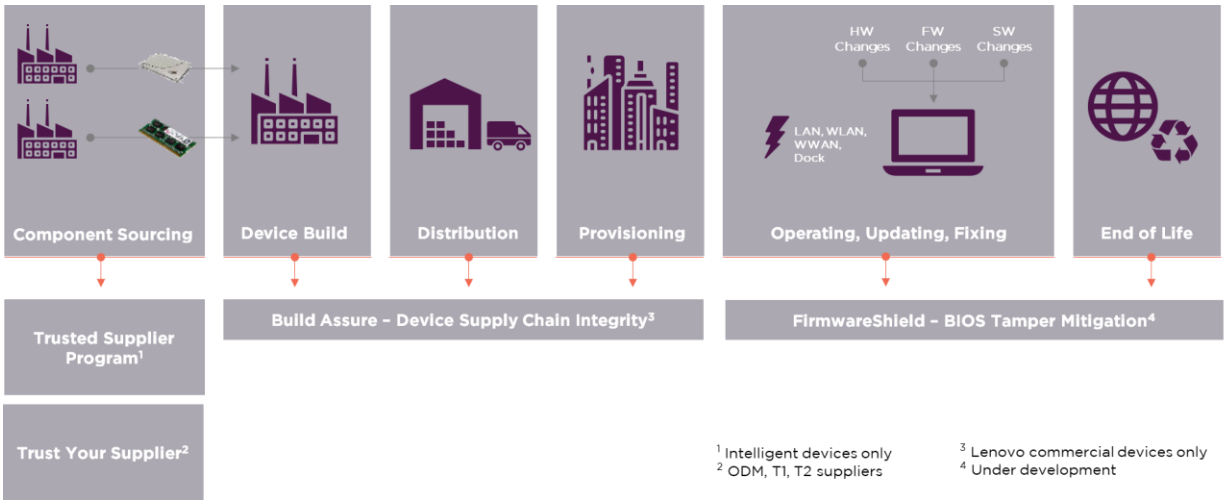
Security is a non-negotiable priority across our devices, from consumer devices to enterprise infrastructure and everything in between. Lenovo takes immense pride in delivering products that prioritize security and integrity from inception to delivery, giving our customers the peace of mind, they deserve in today's complex digital landscape. Lenovo's supply chain security approach is built on a foundation of prevention. We rigorously vet suppliers and components, embed security by design, and strive for transparency and accountability. Our commitment to security extends from product development through to end-of-life asset management. By taking a proactive stance against backdoors, tainted products, counterfeits, and hardware/software vulnerabilities, Lenovo safeguards its products and sets a high industry standard for supply chain security.



Value chain integrity

Lenovo's dedication to value chain integrity goes beyond mere compliance; it embodies a comprehensive approach that covers its operations from cradle to grave. In this section, we delve into Lenovo's robust strategy for global supply chain security, outlining the principles and practices that underscore our unwavering commitment to upholding the integrity of its value chain. Lenovo's ThinkShield solution secures critical data and business technologies with comprehensive end-to-end cybersecurity protection. From the moment we envision a new platform, we incorporate a security-by-design approach throughout the R&D process that extends to our Supply Chain to deliver on our vision of Platform Security. Lenovo's ThinkShield solutions seamlessly integrate with our industry-leading Lenovo devices to give our customers

peace of mind. Our Platform security is built into our ThinkShield security solutions that come standard on industry-leading Think devices. Features such as our Self-healing BIOS, Firmware Security, and Physical Attack Mitigation provide critical protections in the evolving threat landscape. Lenovo products built in this supply chain environment coupled with ThinkShield security features such as Self-Healing Bios, Firmware security, etc. allow Lenovo to deliver on our promise to provide customers with secure and reliable products.



The Trusted Supplier Program (TSP): A commitment to security

A backbone to Lenovo's supply chain security and resiliency is our Trusted Supplier Program. Lenovo recognizes that in an interconnected world, the security of each component is pivotal to the overall security of the final product. Thus, the TSP extends its reach to suppliers providing Intelligent components (CPU, memory,etc) that are integrated into products sold to customers. Lenovo diligently vets, selects, and maintains relationships with trusted suppliers who meet stringent criteria for quality, security, and compliance. We prioritize these relationships with trusted suppliers who share our commitment in utilizing strong security practices and possess a track record of delivering high-quality, genuine components for our customers. By forging strong partnerships with these trusted suppliers, we lay the groundwork for the continued success of Lenovo's supply chain. At its core, the program aims to instill good security practices among suppliers while fostering a sense of ownership in securing their products.

Defining intelligent components

The TSP hinges on the concept of "Intelligent Components," which encompasses any software, hardware, or services that hold the potential for security vulnerabilities. In the eyes of Lenovo, it is essential to scrutinize and secure these elements comprehensively, as their security directly affects the integrity of the entire supply chain. Recognizing the significance of this broad definition, Lenovo extends the program's coverage to any component that fits this description, minimizing gaps in the security process.

Expansion and growth

As of September 2023, the Trusted Supplier Program has made significant progress. The program has onboarded a remarkable 928 suppliers with a YoY increase of 152% in supplier partners. This growth highlights the success of the TSP and reinforces Lenovo's dedication to supplier integrity. The increasing number of suppliers embracing this program signifies a collective acknowledgment of the critical role played by suppliers in safeguarding the security and integrity of the entire supply chain. By promoting security practices and requiring suppliers to take ownership of their product security, Lenovo is forging a robust and resilient supply chain that prioritizes the security of Intelligent Components. The program's impressive growth is a testament to its relevance and success, and it serves as a compelling model for the industry to prioritize supplier integrity. Lenovo, through the TSP, is paving the way for a more secure and resilient future in the global supply chain.

Supplier quality assurance

Lenovo enforces security requirements through commercial contracts or quality agreements signed with suppliers. These critical documents form the foundation of secure and high-quality supply chain operations. Within the system or parts business transactions, We have seamless alignment with suppliers on product and part level RFQ (Request for Quotation) documents and quality agreements. These documents are meticulously crafted and contain detailed requirements for quality targets and solutions for addressing critical quality issues. This dedication to security underscores Lenovo's commitment to safeguarding our products and trust of our partners and customers.

Component supply assurance

One of our primary strategies in component supply management is the utilization of "Vendor Managed Inventory (VMI)" for major commodities whenever possible. In this system, VMI supplier partner have ownership and responsibility for the supply until it's needed to fulfill an order. This approach streamlines our inventory management and provides an exceptionally high level of assurance against counterfeit components infiltrating our supply chain. Moreover, we meticulously inventory and physically control and secure all components within Lenovo's manufacturing facilities. This process includes stringent tracking and verification of expected part numbers, serial numbers, quantities, and other critical details. This level of scrutiny demands that every component entering our production line meets the exact specifications and quality standards we demand.

Component integration excellence

In Lenovo manufacturing, the integration of components into our systems follows a rigorous and standardized process to maintain quality and security. Some key aspects of this process include:

- **First Article Inspections (FAIs):** Both internal and external customer FAIs are integral components of our end-to-end quality process. These inspections help us verify that the initial components and systems meet the expected quality standards before they proceed further in the manufacturing process.

- **Precise component tracking:** We maintain meticulous inventories that include detailed records of each component's serial number and its installation location within a system. Lenovo-specific or supplier-provided component barcodes capture vital data, enabling us to track the journey of each component through our production process. Additionally, this process contributes to the Intel Transparent Supply Chain's as-built product bill of materials, as more fully described below.

- **Stringent testing:** Systems undergo thorough inspections and testing to validate their functionality, performance, and configuration. Any failures are rigorously analyzed, creating a focused inspection point for counterfeit detection and other quality issues. This requires that only products meeting our stringent standards progress to the next phase of manufacturing.

- **Comprehensive record keeping:** Once the testing phase is complete, product serial numbers and test records are stored as part of the product manufacturing record. This meticulous documentation is crucial for traceability, quality control, and post-production monitoring.

ISO certifications

Lenovo's pursuit of quality is further exemplified by its extensive ISO certifications. ISO 9001:2015[4], ISO 14001:2015[5], ISO 27001:2022 and ISO 45001:2015[6] attest to Lenovo's commitment to robust quality management, environmental responsibility, information security and occupational health and safety. These certifications set the standard for excellence in their respective domains, emphasizing Lenovo's dedication to quality and security throughout its operations. By adhering to these stringent international standards, Lenovo assures customers, partners, and stakeholders that it maintains the highest levels of quality and security throughout its product lifecycle. As is standard practice in the computer hardware industry, Lenovo Infrastructure Solutions Group (ISG) firmware and software are developed globally. Differing from standard practice, however, our CSP ecosystem firmware and software source code is stored, compiled, and digitally signed in a secure “clean room” Isolated Computing Environment located

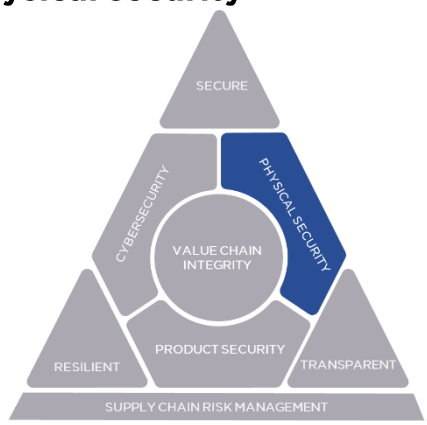
4. Lenovo ISO 9001 Certification
5. Lenovo ISO 14001 Certification
6.Lenovo ISO 45001 Certification
7.Lenovo Press Release: Introduction to Intel Transparent Supply Chain on Lenovo ThinkSystem Servers
8. Lenovo Press Release: Lenovo's Infrastructure Solutions Group Earns its ISO 27001:2022 Information Security Management System (ISMS) Certification

in Morrisville, NC, USA, by explicitly authorized personnel. (Applicable to Lenovo-developed ThinkSystem, ThinkEdge, ThinkAgile products).This facility is ISO 27001:2022 Information Security Management System (ISMS) certified and has been granted a certification for TAPA Facility Security Requirements (FSR) with IT and Cyber Security Threat Enhancement. It is physically partitioned from Lenovo's corporate network, with security-sensitive functions such as access approvals, management, operations, compilation, and signing performed by US Nationals that have undergone NACLC equivalent criminal and credit background checks.

Intel Transparent Supply Chain

Lenovo offers an unparalleled level of supply chain transparency and security with the Intel Transparent Supply Chain program. Lenovo has forged a strong partnership with Intel® to enhance supply chain security. Through the Intel® Transparent Supply Chain, Lenovo can provide attested device integrity from manufacturing to customer deployment. This unique initiative provides traceability at both the component and system levels, with Intel's digital signature process attesting to authenticity. More information can be found in the Lenovo article "Introduction to Intel Transparent Supply Chain on Lenovo ThinkSystem Servers[7].

Physical security



Secure development

Lenovo follows a secure development approach, aligning with NIST's recommendation for secure software development. Our Lenovo Security Development Lifecycle (LSDL) integrates industry standards and practices, including those from Microsoft, SAFECode, and ISO 27034. The Security Review Board (SRB), located in North Carolina, US plays a pivotal role in LSDL, ensuring that security is ingrained throughout the product lifecycle. This aligns with NIST's emphasis on secure software engineering. Security training for employees, specific to their roles, further strengthens our commitment to secure development, in line with NIST's focus on personnel security.

Lenovo's Secure Development Lab is ISO 27001:2022 Information Security Management System (ISMS) certified and has also earned a 2020 TAPA Facility Security Requirements (FSR) Level C with IT and Cyber Security Threat Enhancement certification. This secure development lab is located in the US, managed by US Nationals, with restricted access based on need. It houses ThinkSystem, ThinkEdge, ThinkAgile and Cloud Service Provider (CSP) ecosystem 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 for a secure, trusted boot-up.

Secure facilities

Lenovo places a significant emphasis on facility security at its manufacturing sites, both in support of new site implementations and in the ongoing maintenance and enhancement of existing sites. For new site support, Lenovo carefully devises staffing plans, optimal equipment layouts, and security systems to enable the security and efficiency of operations. This meticulous planning extends to master process designs, encompassing a comprehensive approach to facility security. Existing site support is equally comprehensive, with Lenovo conducting internal audits and facilitating customer audits. These audits serve to continuously evaluate and strengthen the security measures in place. Lenovo also prioritizes

equipment upgrades and maintenance, encompassing the installation of digital cameras and conducting global in-house plant asset validation across our servers and workstations. Training forms a crucial component of Lenovo's facility security strategy, with a particular focus on cybersecurity training to keep staff well-versed in the latest security protocols and practices. For site-specific security, dedicated efforts go into equipment setup and security guard deployment, ensuring that the physical aspects of security are well-tailored to site needs. The existing site support extends to enhancing e-security systems and conducting both internal audits and customer audits/questionnaires. Continuity plans are actively improved through initiatives and rigorous testing, including cyber resilience measures and risk self-evaluation. Certain key Lenovo locations are TAPA certified, which helps meet our corporate responsibility and enhance our competitive strength. TAPA certification demonstrates standard security protections against some of the most common supply chain physical security and information security threats.

Employee awareness and training

Lenovo places a strong emphasis on educating our workforce across several security areas. Regular training programs prepare employees to be well-informed and vigilant, making them the first line of defense against insider threats, social engineering, and bribery. With a focus on all pillars on security, Lenovo keeps staff informed on the latest security protocols and practices through annual mandatory training.

Secure talent integration and transition

Stringent background screening is conducted before granting access to sensitive information or facilities within the supply chain. Structured termination procedures swiftly revoke access upon an employee's departure, reducing post-employment insider threats.

Physical security and surveillance

CCTV surveillance practices and vigilant monitoring of suspicious activities maintain the security of our facilities. Security personnel are trained to identify and respond to unusual behavior.

Access controls and policies

To minimize the risk of insider threat, Lenovo implements a policy of Separation of Duties and utilizes Single Sign-On (SSO) and Active Directory (AD) systems by dividing responsibilities and requiring multiple authorizations for critical actions. Comprehensive policies and controls guide employee behavior, with regular audits and compliance checks.

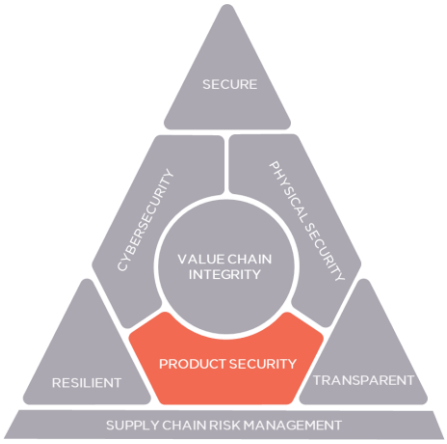
Secure logistics

Lenovo's Global Logistics Security strategy integrates personnel, perimeter, in-transit, storage, packaging, and contractual cascading of security measures to all Suppliers/Carriers to align with NIST's supply chain security principles globally. Lenovo has been a US Customs and Border Patrol (CBP) Tier 3 Customs-Trade Partnership Against Terrorism (C-TPAT) validated company since 2007 and utilizes Suppliers that adhere to Transported Asset Protection Association (TAPA) Transportation (TSR) and Facility (FSR) security requirement certifications. Personnel/staff security elements include background screening, risk reviews, security awareness and education for employees and suppliers, effective communications, and Business Management Systems (BMS) strategies adhering to NIST's focus on personnel security. Facility and Perimeter/Secure Yard security elements to include pre-route screening, advanced alarm systems, fenced perimeters, CCTV, lighting, and access controls align with NIST's recommendations for access control and perimeter protection. Transportation (in-transit) security practices, such as the "No Stop" rules (within certain distance from destination), team drivers, route risk analysis, armored trucks, security escorts with armored vehicles, advanced GPS capabilities, active monitoring, and remote engine stop capabilities reflect an emphasis on secure transportation, load theft/tampering prevention and anti-hijacking. Lenovo's security program focuses on loss prevention, risk mitigation, and loss recovery as equal elements.

Secure asset maintenance and disposal

Lenovo provides the secure maintenance and disposal of assets, in alignment with NIST's asset management principles. Secure disposal practices safeguard sensitive information and reduce security risks associated with retired assets.

Product security

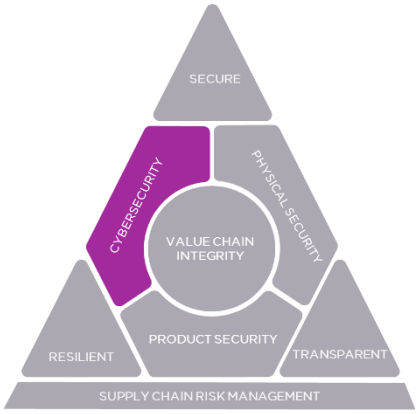


Lenovo prioritizes security across all our products, to elevate protection for our customers. The latest offerings, ThinkSystem and ThinkAgile v3 provide advanced features that safeguard against attacks, detect any anomalies, and facilitate recovery in the rare instance of tampering or corruption. These improvements include fortified platform protection, incorporating the latest security standards like FIPS 140-3 (validation in process), robust password storage, heightened compliance with NIST SP800-193 Platform Firmware Resiliency (PFR), and CNSA Suite Quantum-resistant cryptography. With Lenovo System Guard, we've implemented a vigilant hardware inventory monitor that shields against supply chain attacks or hacking throughout a server's lifecycle. By digitally assessing critical components such as CPUs, DIMMs, PCI Adapters, drives, risers & backplanes, we can identify any unauthorized changes made during manufacturing, shipping, delivery, or deployment. System Guard offers configurable responses, alerting administrators or blocking boot-up in the event of a component alteration. Lenovo's immutable hardware Root of Trust (RoT) uses a silicon-based chip, to ensure the server only boots with trusted firmware. The carefully orchestrated "chain of trust" in the boot process verifies the correct digital signature for critical below-OS components, signaling any tampering. Failure triggers a non-boot state, and administrators are promptly notified. Additionally, we have enhanced redundancy for critical firmware support, ensuring swift and reliable recovery in the unlikely event of tampering or corruption.

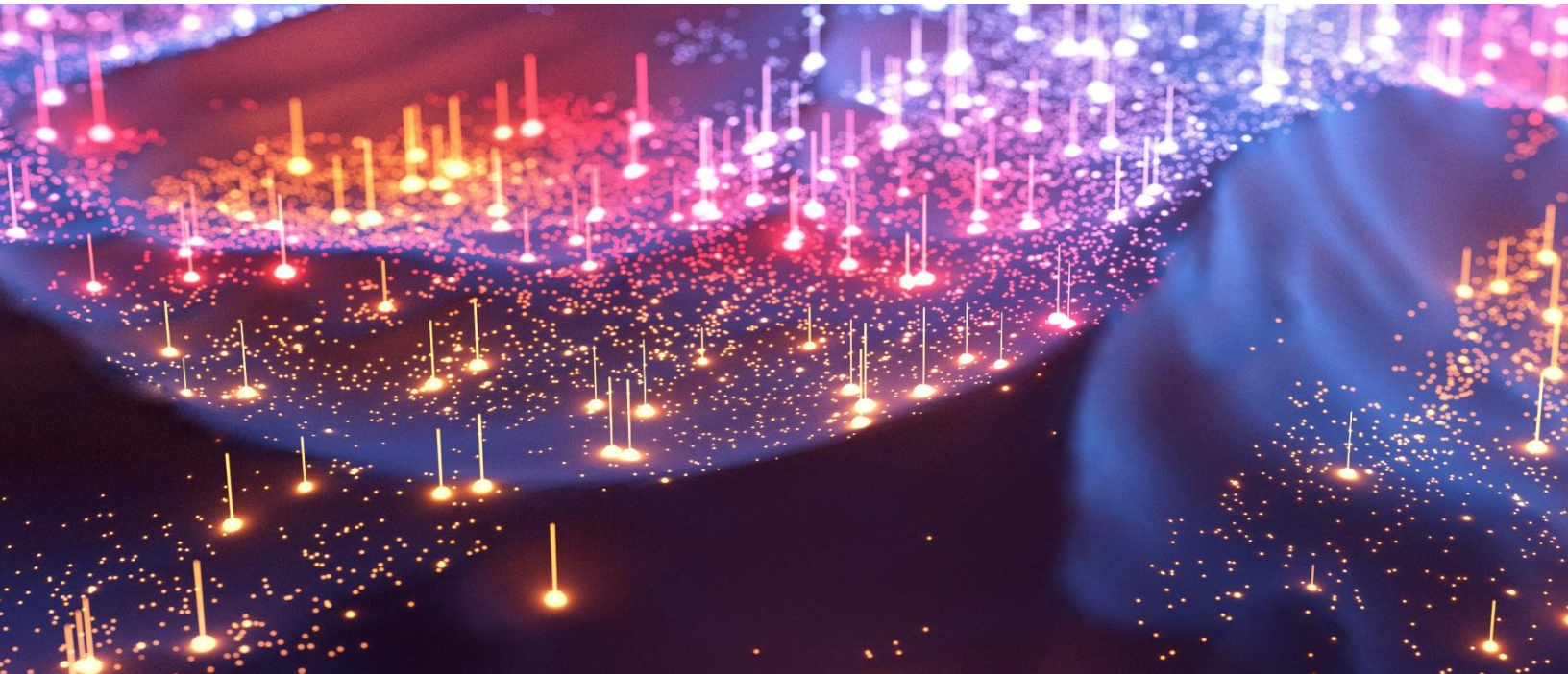
Our Product Security Incident Response Team (PSIRT) is dedicated to enhancing customer trust and awareness in the security of Lenovo products. The PSIRT collaborates with various stakeholders, including customers, suppliers, and researchers, to promptly address security vulnerabilities. This aligns with NIST's emphasis on incident response and coordination. Lenovo actively participates in the Coordinated Vulnerability Disclosure (CVD) process, encouraging researchers and suppliers to do the same. We publish security advisories transparently, providing customers with essential information to protect their systems, adhering to the NIST principle of timely disclosure. Lenovo can assign a CVE identifier per our CVE Number Authority Information Sharing and Embargo Policy. Common Vulnerabilities and Exposures (CVE®) is a dictionary of publicly known information security vulnerabilities and exposures and is maintained by The MITRE Corporation. A CVE identifier represents a single security vulnerability and allows vendors, researchers and customers to talk about that specific vulnerability. Lenovo assigns CVE identifiers for Lenovo product vulnerabilities[9] even if vulnerability information will remain private for an unpredictable amount of time. This helps the security community to plan for and mitigate current information security threats. Additionally, Lenovo is a member of the Forum of Incident Response and Security Teams (FIRST), promoting international collaboration to promote internet safety, which aligns with NIST's focus on global cybersecurity efforts.

9 Lenovo assigns CVE identifiers for Lenovo product vulnerabilities

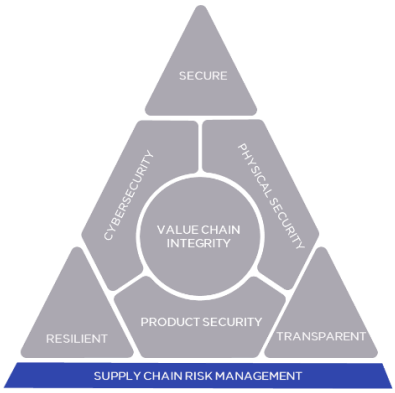
Cybersecurity and information security



Lenovo's IT operations cybersecurity practices align with industry standard frameworks such as IS027001, NIST Cybersecurity Framework (CSF) and AICPA (American Institute of Certified Public Accountants) SOC2 critical controls. The fundamental tenant of our mission is to protect and respect our customers' data. Lenovo's policies, processes and controls extend to our supply chain sites. Practices include: Board level and executive sponsorship, governance, funding for improvements, policies, practices, confidentiality, background checks, regular risk assessments, threat intelligence, regulatory awareness training, incident response, tabletop exercises, access controls, multi-factor authentication, system hardening, patching, advanced network protection, advanced endpoint protection, proactive monitoring, continuous improvement plans, third party assessments, project security reviews, privacy reviews, and dedicated security staff. Lenovo binds its supply chain partners through contractual commitments that leverage industry standards such as the ISO27001. Focus areas include privacy, cyber security, physical security along with extensive assessments.



Continuous risk assessment and improvement



Lenovo has embraced a proactive and comprehensive approach to supply chain security by implementing a robust Supply Chain Risk Management (SCRM) model. Lenovo's commitment to ensuring supply chain security is evident through continuous risk assessment and improvement, outlining the strategies, tools, and governance mechanisms employed to mitigate risks and enhance resilience. Lenovo's commitment to continuous improvement is evident in the expansion of our certificates, 3rd party assessments, internal security programs like TSP, Supply Chain Assurance and Thinkshield Solutions.

Lenovo's Proactive Approach: SCRM Model and Governance

At the heart of Lenovo's continuous risk assessment and improvement strategy lies the Supply Chain Risk Management (SCRM) model. This model is bolstered by a governance workgroup closely aligned with the Chief Security Office. This synergy is vital in proactively identifying and addressing strategic risks that could jeopardize key Global Supply Chain (GSC) objectives.

The SCRM model operates by systematically developing impact and likelihood assessments, leading to the formulation of proper controls and action plans. This methodical approach facilitates better resource allocation and governance, allowing Lenovo to take proactive measures to minimize the adverse impact of potential risks.

The GSC risk council: A holistic enterprise-wide framework

The GSC Risk Council forms a vital component of Lenovo's strategy for continuous risk assessment and improvement. It offers an enterprise-wide framework for exploring all risks, considering their severity, and evaluating associated costs to Lenovo's GSC. This council serves as a single platform that offers continuous guidance and in-depth expertise to enhance the organization's risk management capabilities and development of business-critical action plans.

ISO Certifications: An assurance of security and resilience

Lenovo's commitment to supply chain security extends to attaining globally recognized ISO certifications. Lenovo has an ISO 27001:2022 certification coverings its Global IT Operations and is on target to obtain an ISO 22301:2019 certification of its business continuity practices for its Global IT Operations in 2024. In addition to other locations, these certifications cover IT operations in Lenovo key manufacturing sites and demonstrate a resilient approach to supply chain security and continuity, assuring customers and partners of Lenovo's commitment to safeguarding their interests.

Third-Party Supply Chain and business process security assessments (ISG)

Lenovo Infrastructure Solutions Group' (ISG) most recent milestone of earning its ISO 27001:2022 Information Security Management System (ISMS) certification[8] for the Isolated Computing Environment (ICE) Lab in Morrisville, North Carolina, where ThinkSystem, ThinkEdge, ThinkAgile and CSP ecosystem firmware and software are securely stored, built, and signed. ISO 27001 is a globally recognized standard for managing information security. Certification provides evidence that an organization manages information security appropriately and adheres to strict guidelines. This underscores the company's commitment to providing secure solutions and products to businesses of all sizes. The company's clean audit results are a testament to the best-in-class security practices implemented and adhered to.

Implementing a strong security culture is a continuous task, not an isolated one. As the amount of data businesses hold continues to grow exponentially, propelled further by increased adoption of AI and analytics, security capabilities must expand in conjunction. And

with a greater emphasis on security solutions rather than just products, combined with difficulties finding the right security personnel, organizations are looking to unified, autonomous solutions to empower them to safeguard their data. Lenovo ISG's ISO 27001:2022 ISMS certification demonstrates that the people, processes and technologies that process protected data address stringent security controls such as threat intelligence, physical security monitoring, data leakage prevention, and secure coding, to name a few. Lenovo has a long history of security testing by independent third parties. Those tests are routinely performed as part of our development process, consisting of a mix of Grey Box* and White Box** testing. As of March 2023, we have more than 20 third party assessments by multiple security auditing firms including Synopsys, Atredis, KoreLogic and others. Attestation letters are available from most of these assessments.

Multi-Sourcing and hybrid manufacturing: Strengthening resilience

To mitigate operational risks and enhance resilience, Lenovo has adopted a multi-sourcing strategy. This approach reinforces local manufacturing and multi-sourcing capability, minimizing the potential impact of disruptions in the supply chain. Additionally, Lenovo is actively working to synergize multi-tier sourcing management, thereby optimizing supplier networks and diversifying sources.

Comprehensive risk management and security enhancement

Lenovo's continuous risk assessment and improvement strategy goes beyond risk identification and mitigation. Scenario planning is employed to analyze major risks, considering inputs from all related functions. Furthermore, Lenovo has increased upstream supplier risk visibility through in-house and third-party digital platforms. Security enhancement is another critical component of Lenovo's approach. Lenovo strives to maintain business continuity by implementing practices aligned with ISO 22301:2019 Security and Resilience – Business Continuity Management Systems and ensuring product traceability via ISO 20243 standard alignment. ISO 20243-1:2023 is an international standard that addresses the threat of maliciously tainted products in the supply chain.. This commitment also extends to physical asset security and collaboration with certified logistics partners to protect and track products throughout the end-to-end shipping process.

Quality in Lenovo Global Supply Chain

Quality within the Lenovo global supply chain is integral to security, as it drives reliability and integrity of components used in their products. Lenovo has developed an Intelligent Quality Ecosystem that focuses on full life-cycle management, protecting products and customers The Intelligent Quality Ecosystem acts as a robust defense mechanism, minimizing the likelihood of vulnerabilities that could compromise the integrity of products. In essence, the emphasis on quality directly safeguards the security of Lenovo's supply chain by mitigating potential risks and bolstering the overall resilience of their products. Managing the design, manufacturing, and materials of products through quality management is a key component within the security of Lenovo's global supply chain.

Design quality assurance

Lenovo's quality department works collaboratively with various key departments, including product development, validation, and the CSO, to conduct security reviews at crucial checkpoints by the SRB and leadership located in Morrisville, NC during the product development phase. Our design process allows both hardware and software solutions to meet security requirements right from the inception of product design. Security review is a non-negotiable component for every project, and only after successfully passing this security review can a project advance to the next phase. Lenovo's emphasis on security at the design stage is a proactive measure to preempt security issues and strengthen the foundation of product quality.

Manufacturing & assembly quality controls

As part of a vertically integrated supply chain, Lenovo has ownership of our motherboard factories and processes. In these factories, we define a consistent controlled process that will verify components are on our AVL(Approved Vendor List) and meet the required quality standards. We require our mechanical suppliers to meet our expected standards and our QMS allows us to block or quarantine parts before they enter our factories if required. The introduction of digital checklists streamlines the process, providing a

systematic and traceable approach to quality control. The "Unit review in media build" Final assembly inspection stage further bolsters quality control measures. The Manufacturing and Product Quality Performance Dashboard is an essential tool showcases a spectrum of key metrics, including VLRR (Verified Line Reject Rate) Commodity Performance, NPI (New Product Introduction) Delivery, PRR (Part Replacement Rate) Commodity Performance, Executive Summaries, and Continuous Improvement Reviews. This provides enhanced visibility of our manufacturing and assembly process to our customers.

Product testing & packaging

Quality control extends seamlessly into the testing and packaging phase, offering flexibility to accommodate various products and form factors. Various testing and packaging inspections, validations, defect recordings such as CSA (Customer Simulation Audit) Inspection with pictures, OOB (Out of Box) Inspection with pictures, visual pack Inspection, process audits, digital checklists, RAI (Rack Assembly Inspection) Inspection with pictures, EOLA (End of Line Audit) Inspection with pictures are rigorously executed so our products are packaged flawlessly and delivered to customers as expected.

Transformation – 4IR technologies

Lenovo's Hefei factory, LCFC, has proudly joined the prestigious Global Lighthouse Network at World Economic Forum 2023 in Davos[10]. This network, now with 132 leading manufacturers globally, acknowledges those at the forefront of the Fourth Industrial Revolution (4IR). LCFC, integrating cutting-edge technologies like AI, 3D-printing, and big data analytics, exemplifies the transformation imperative for a secure and transparent.

supply chain. These innovations enhance efficiency, competitiveness, and signal a profound shift in business models, fostering economic growth, workforce augmentation, and environmental protection. Lenovo's commitment to security, reliability, and transparency aligns with the 4IR principles, allowing us to meet evolving customer expectations. As part of the Global Lighthouse Network, Lenovo leads in innovation, trust, and resilience, setting new standards in the global manufacturing landscape. Lenovo is strategically placing a strong emphasis on AI/ML technologies as pivotal drivers in its transformation journey. Through these advanced capabilities, Lenovo is enhancing operational efficiency and competitiveness, leading the way by increasing our adaptability and resilience within the Fourth Industrial Revolution. Through a proactive investment in AI/ML, Lenovo is positioning itself at the forefront of technological innovation, reinforcing its commitment to delivering cutting-edge solutions and setting new benchmarks in the global manufacturing standards.

Industry collaboration and security ecosystem

With the ever-changing threat landscape to Supply Chain security, Lenovo continues to stay ahead of these threats by developing and enhancing strong partnerships with security partners and industry standard groups. Lenovo's security ecosystem is comprised of some of the most innovative, industry leading security partners in the business. Lenovo continues to build a collaborative security ecosystem as it is critical we stay ahead of the complex and ever-changing security and privacy environment in areas such as data sovereignty, evolving global regulatory requirements, standards, and best practices. We sit on the boards and are a respected member of numerous industry standards groups and greater cybersecurity communities, maintaining constructive relationships with key organizations such as:

- UEFI Forum
- Trusted Computing Group
- Fast ID Online (FIDO) Alliance (Holding a Board seat)
- Storage Networking Industry Association (SNIA)
- Wi-Fi Alliance

We continue to strengthen, cultivate, and evolve our security ecosystem through increased partner outreach to collaborate on industry-wide best practices, benchmarks, evolving topics and issues.

Highest standards of compliance

Lenovo ISG offers Trade Agreements Act (TAA)-compliant manufacturing of globally sourced components in Mexico and the US. Additionally, non-TAA manufacturing is available in China. Primary North American manufacturing occurs in Monterrey, Mexico and primary European manufacturing occurs in Ullo, Hungary.
Lenovo ISG products comply with the requirements of Section 889 of the US FY2019 National Defense Authorization Act (NDAA). Lenovo products are not designed, developed, or manufactured using

10 Lenovo Press Release: Lenovo Recognized for Global Manufacturing Leadership

hardware or software developed by or procured from any company or subsidiary thereof listed in Section 889 of the Act.

Secure the future – Advancing security programs and technology

In alignment with the Supply Chain Security mission to fortify the future of Lenovo's products, services, and customer experiences, there is significant investment in expanding our industry-leading security programs like Supply Chain Assurance, and a global network of Cybersecurity Innovation centers. We aim to elevate our capabilities in prevention, detection, response, and recovery. As we navigate an ever-evolving digital landscape, Lenovo's dedication to securing the technological forefront underscores our commitment to delivering trust, reliability, and resilience to our customers worldwide.

Investments in cutting-edge technologies, platforms, and people

Lenovo's approach to supply chain security is grounded in substantial investments in advanced technologies, robust platforms, and a highly skilled workforce. This comprehensive strategy not only fortifies our defenses but also embeds security into every aspect of our operations. By continuously evolving our technological infrastructure, we create a resilient foundation that adapts to the ever-changing cybersecurity landscape.

Expanding the Trusted Supplier Program

Lenovo acknowledges that a secure supply chain requires a collaborative effort. Hence, we are expanding our Trusted Supplier Program by broadening its scope and onboarding new suppliers every quarter. This program provides a platform for our partners to share our commitment to security, creating a unified front against potential threats.

Lenovo Cybersecurity Innovation Center (LCIC)

Our ongoing efforts to combat cyber threats are exemplified through the Lenovo Cybersecurity Innovation Center (LCIC)[11]. This center serves as a hub for cutting-edge research and development, enabling us to stay at the forefront of cybersecurity innovation and proactively address emerging challenges.

ThinkShield Supply Chain Security Platform

The ThinkShield Supply Chain Assurance, powered by Intel Transparent Supply Chain (Intel TSC), establishes a secure hardware foundation for Lenovo systems. It verifies the authenticity of components, collecting and securely storing data files during manufacturing. The customer can use the system to confirm that the product delivered is authentic and unmodified, providing transparency and trust in the system's security.

Conclusion

Lenovo continues to be a trusted supplier to governments, financial services, 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. The strength of our commitment to security is evidenced not only by third-party assessments and attestations but also by the result, the security of our products—as demonstrated, for example, by ITIC's 2023 global security survey finding that "Lenovo ThinkSystem servers achieved the best security scores among all x86 server distributions for the fifth year in a row." Lenovo's global supply chain is not just a logistical framework; it's our ability to design, manufacture, and deliver trusted technology solutions to our valued customers. Our commitment to Security, Resilience, and Quality extends beyond products; it embodies our ambition to create a global technology ecosystem rooted in trust and reliability. Together with our trusted industry partners, we continue to build a more innovative, secure and sustainable supply chain. Lenovo's commitment to supply chain security excellence is a pledge to shape the future of technology while upholding the values of trust, integrity, and reliability. We believe that securing our supply chain is essential to ensuring our customers receive cutting-edge technology that they can trust and rely on today and in the future.

11 Lenovo Press Release: Lenovo Cybersecurity Innovation Center Established

Resources

Lenovo recognized for Global Manufacturing Leadership at world Economic Forum -2023

Introducing ThinkShield by Lenovo, Complete End-to-End Security Solutions that Keep Companies Safer - Lenovo StoryHub

Platform Firmware Resiliency Guidelines (NIST.SP.800-193)

Lenovo ISO 9001:2015 Certification

Introduction to Intel Transparent Supply Chain on Lenovo ThinkSystem Servers

Vulnerability Disclosure Policy - Lenovo Support US

Lenovo Security by Design: Foundational Security from Edge to Cloud > Lenovo Press

Secunet Customer Story | Lenovo Tech Today US