Lenovo—Building Trusted, Secure Data Center Products

Infrastructure Security Matters

The impact of a security breach can be devastating in terms of customer trust, legal actions, regulatory costs, and more. The Ponemon *2015 Cost of a Data Breach Study*[1] showed the average cost of a data breach to a company was $3.8 million; an average cost of $154 for each stolen sensitive or confidential data record.

While most (if not all) data center security breaches occur in the software stack — unauthorized access, malicious software and viruses, etc. — IT managers should also be concerned about the security of the hardware and firmware used to run the software. How does one know if the products and appliances used in the infrastructure can be trusted? Are you sure your servers won't inject a security fault, or allow an entry point for malicious software?

Data Center Security Built-In

At Lenovo, we take extraordinary measures to build security into our products, and gain and keep our customer's trust in Lenovo as a respected data center provider. If fact, we are confident we go above and beyond what other x86 vendors do for system security, and are more open and secure in how we develop and manufacture our products than any of our competitors.

Lenovo's Data Center Group (DCG) employs rigorous business processes, product design, and supply chain controls. These measures help to ensure our products are built with components from known, reliable suppliers, guard against hijacking, and protect against compromised firmware updates once the servers are deployed.

Business Processes

Lenovo's acquisition of IBM's System x business was subject to an exacting review and approval process conducted by the U.S. Government (the Committee on Foreign Investment in the United States or "CFIUS"). As a part of that process, Lenovo agreed to maintain and *strengthen* the same rigorous development, supply chain processes, and controls used by IBM. And because Lenovo believes security is

[1] *2015 Cost of Data Breach Study: Global Analysis*; Ponemon Institute, May 2015

enhanced through transparency, Lenovo agreed to allow the U.S. government and independent auditors to review these processes at any time. As a result, Lenovo believes this to be the most transparent, auditable, and secure supply chain in the server industry.

Lenovo has implemented a rigorous governance model. A product security office works closely with EBG leadership, and provides expertise, focus and oversight for all aspects of product security. At the top is a board-level Security Director; this individual holds a U.S. Government security clearance. At the operational level, the product security office is led by a Security Officer, backed by a team of security experts.

This office has implemented security policies based on widely recognized industry best practices and international standards, including ISO 27000, NIST, and EU Data Privacy. The office continually monitors and reports on compliance with the policies and helps ensure they are always up to date and are responsive to the latest threats.

Lenovo is transparent with our customers as well regarding any security incidents that could affect our products, whether identified by Lenovo, industry, government, or customers. Lenovo maintains a team responsible to drive closure of all validated incidents. This team is also responsible to notify customers, and communicate risk and remediation plans. Security advisories, vulnerabilities and their corrective actions are posted to Lenovo's website and are available to anyone.

Server Product Design

Lenovo's System x server products have security built in by design. To ensure that System x server firmware is not compromised, Lenovo's firmware requirements, architecture, and design are performed by U.S. based teams that ensure compliance with Lenovo product requirements, design practices, and industry standards. Code developed by third parties is inspected by the U.S. teams for quality control.

Lenovo System x server source code is maintained on U.S. based Code Retention Servers, and all code changes are tracked and auditable. Build servers, also based in the U.S., are where source code is compiled and converted into executable code. Before the code is released, it is digitally signed on secure signing servers. The signing servers, used only for digital signing of code, are also based in a secure U.S. data center with limited and auditable access.

The output of this process is digitally signed and verified firmware, which is made available to customers behind a secure firewall, and is ultimately included in the systems that we deploy in the field.

Lenovo has incorporated the Secure Software Development Life Cycle (S-SDLC) into all of our business units, so that all software is verified, vetted and validated to reduce the risk of any holes, open doors, back doors, malware, spyware, etc.

In addition, Lenovo performs ongoing threat assessments, including threat modeling and ethical hacking of firmware to continually assess security protection.

System x servers also include a secure system execution process designed to ensure that only genuine, trusted firmware is able to load and execute. System x servers have two dedicated Trusted Security Zones. One is dedicated to the out-of-band systems management interface and the other to the host system. These features protect against unauthorized code being loaded during a system update or while the operating system boots. The digital signature of all firmware is checked every time it is loaded and before it executes—in order to protect the system against low level attacks—and helps establish the integrity for upper layers of software.

Secure Supply Chain

Lenovo tightly controls its supply chain and manufacturing processes to ensure the integrity of the components used in its server products.

Lenovo owns the manufacturing plants where its servers are made. This gives us greater control over supply chain operations, including control over the facilities' physical and IT security, and employees, to a much greater extent than the contract manufacturers or leased facilities that are used by our competitors. Lenovo also manufactures servers in the US, and offers products built completely within a secure end-to-end process located entirely in the U.S. by verified U.S. persons, for those customers who require this level of assurance.

Additionally, only selected, trusted suppliers participate in Lenovo's supply chain, promoting end-to-end security. Lenovo Trusted Suppliers are held to high standards for security and must allow periodic inspections and security audits. To become a Trusted Supplier, a lengthy questionnaire is used to validate a supplier's general, hardware, and software security practices. Those suppliers that do not provide enough evidence in any of these three areas cannot become Trusted Suppliers.

The last leg is to ensure that products are not tampered with and modified after shipment. Lenovo has contractual requirements with transport companies to use GPS technology, security escorts when required, counter-surveillance, and background screening of its employees in order to protect shipments. Products also go through a comprehensive inspection and sealing process that includes a layered approach, with over-packs, banding, stretch wrap, seals and tamper tape—all designed to ensure the integrity of products during shipment and aid in tamper detection.

As proof, Lenovo has maintains the highest security level—Tier3—awarded by U.S. Customs and Border Protection (part of the Department of Homeland Security) under the Customs-Trade Partnership Against Terrorism (C-TPAT), which audits the supply chain from end-to-end, and certifies manufacturing points, origination and consolidation points, and provides enhanced cargo screening.

Summary

To gain approval to acquire the System x business from IBM, Lenovo passed a US Government (CFIUS) review process, which included a stringent review of Lenovo's supply chain and product development processes. In fact, Lenovo has satisfied this review process 5 times since 2005. We have held a GSA schedule for nine years and counting. We supply trade-compliant products, and have sold over $1 billion in PC hardware to the U.S. federal government.

Lenovo's Data Center Group, specifically, has been reviewed by the U.S. government, and is subject to validation by third-party audits to measure the effectiveness of security processes and controls at each touch point in the supply chain, and to test for vulnerabilities in the firmware and software used on our products.

Lenovo is proud of the ways it has improved upon the foundation established by IBM. We believe that our servers are produced with transparent and secure development, supply chain and manufacturing processes that are second to none.

Lenovo White Papers

Lenovo—Building Trusted, Secure Data Center Products

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. This information could include technical inaccuracies or typographical errors. Changes may be 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.