Why Lenovo ThinkSystem Servers are the Best Choice for Security

Designed from the ground up with the latest security features and practices

December 2017

Mark T. Chapman

Lenovo.com/systems

Executive Overview

For many organizations, security is the #1 concern today. The sophistication of cyber threats and the skill of the attackers continually increase. Whether it's a hacker trying to steal credit card numbers and other sensitive and valuable information, a rival company looking for competitive advantage, a "hactivist" bringing down a site for political reasons, or a rogue nation looking to create chaos, organizations cannot afford to be underprotected. The growing prevalence of social, mobile, cloud, and virtualization technologies presents a profound security challenge. Threats now also include boot firmware and even a server's systems management subsystem. More sophisticated threats and higher risk drive the need for more responsive, context-aware approaches to security management. Hardware/firmware-level attacks are just as—or more—effective at stealing information as OS- or hypervisor-level attacks.

Unfortunately, many servers, and indeed entire datacenters, lack the tools needed to protect their businesses and their customers' data, as we've seen recently. A major retailer was hacked in 2014, and 40 million credit card numbers were stolen, along with customer addresses and phone numbers. This not only hurt the customers but the reputation of the retailer as well, potentially costing untold millions in lost revenues and loss of customer loyalty. In 2017 a major credit reporting agency suffered a massive data breach, exposing the sensitive personal information of up to 143 million people in the U.S., U.K., Canada, and other countries. Similar security breaches have occurred at an arts & craft chain, a national department store, a network provider, an auction house, a restaurant chain, and many others. No organization can assume it's safe from attack.

The problem is widespread and growing—and expensive. For every *hour* that a commercial site is down, whether due to security breaches or other causes, it costs 98% of businesses at least $150,000 (USD) according to a 2017 ITIC study.[1] Thirty-one percent of companies say their hourly cost due to downtime is as much as $400,000, and another 33% say their cost is in the $1M to $5M range. (And the costs will only increase in 2018 and beyond.) Even for noncommercial sites, the economic costs of loss of trade secrets, lawsuits, and fines for noncompliance can be extensive. For certain government agencies the losses could be measured in lives (witness protection, confidential informants, undercover agents, etc.).

Antivirus/antimalware software only protects at the OS level. (*Figure 1,* below.) By then, the threat is already inside the server. What's needed are servers with built-in security that starts at the hardware level and extends all the way to the launch of the operating system. Platform-level security closes the most dangerous security holes and complements top-down security (firewalls, antivirus, and others).

[1] 2016-2017 Global Hardware, Server OS Reliability Report, ITIC, October 2016; and ITIC Reliability Study 2016 – 2017 Mid-year Update, May 2017.

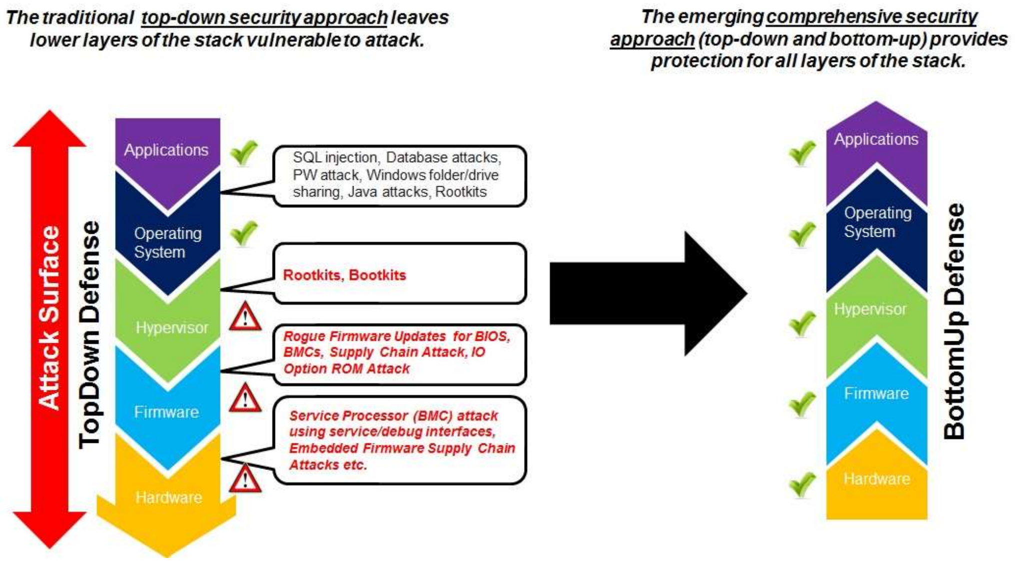
The traditional top-down security approach leaves lower layers of the stack vulnerable to attack.
The emerging comprehensive security approach (top-down and bottom-up) provides protection for all layers of the stack.
Attack Surface
TopDown Defense
Applications
Operating System
Hypervisor
Firmware
Hardware
SQL injection, Database attacks, PW attack, Windows folder/drive sharing, Java attacks, Rootkits
Rootkits, Bootkits
Rogue Firmware Updates for BIOS, BMCs, Supply Chain Attack, IO Option ROM Attack
Service Processor (BMC) attack using service/debug interfaces, Embedded Firmware Supply Chain Attacks etc.
Applications
Operating System
Hypervisor
Firmware
Hardware
BottomUp Defense

Figure 1. *Top-down protection vs. bottom-up protection*

Very few servers fully offer this level of protection, however. In fact, ThinkSystem servers from Lenovo are the *only* x86 systems that offer a level of protection capable of stopping many of these attacks.[2] Rather than trying to retrofit legacy servers with new hardware-level security features, Lenovo chose to architect the entire ThinkSystem product line from scratch with enhanced security built in.

The security capabilities include not only industry standards, but also system-unique hardware innovations and practices that go beyond industry standards technologies. Many of these features and practices are interlocked, creating a complete “chain of trust” that is not possible without them.

This paper explores customer security pain points, the limits of industry-standard technology, and how ThinkSystem servers are the only ones to address these security weaknesses. When reading the following, ask yourself whether your current server provider provides these security capabilities. If not, are they really the best server vendor for your data center?

[2] As of November 2017, based on internal research of publicly available information.

Industry-Standard Security

Industry standards necessarily form the foundation for ThinkSystem security. For example, the Intel Xeon Scalable Family processor series adds a number of new or enhanced built-in security features:

- **Near-zero encryption overhead** enables higher performance on all secure data transactions
- **Intel Key Protection Technology** (Intel KPT) with Integrated Intel QAT and Intel Platform Trust Technology (Intel PTT) enables hardware-enhanced platform security by providing efficient protection for both keys and data, whether at rest, in-use, or in-flight
- **Intel Trusted Execution Technology** (Intel TXT) with One-Touch Activation provides enhanced platform security, while providing simplified and scalable deployment for Intel TXT

The integrated industry-standard Trusted Platform Module (TPM) 2.0 is based upon standards set by the Trusted Computing Group (of which Lenovo is a contributing member). The TPM chip securely generates and stores inside the chip artifacts that are used to authenticate the server platform. Artifacts can include passwords, certificates, and encryption keys. Working together with the server BIOS, TPM forms a "root of trust." This combination of the TPM, BIOS, and operating system working together allows applications to operate with a reasonable level of confidence that the system hasn’t been compromised.

In addition, the National Institute of Standards and Technology (**NIST**) provides a Cybersecurity Framework, consisting of standards, guidelines, and practices that computer vendors, governments, and datacenters alike can use to strengthen the security of critical infrastructure. ThinkSystem servers are compliant with a number of NIST and other industry-standard security protocols and certifications, including:

- **NIST SP800-131a** — Cryptographic algorithms and key lengths
- **NIST SP800-147b** — BIOS protection guidelines
- **Trusted Computing Group (TCG)** — Industry security standards
- **PCI-DSS** — Credit/debit card data security standards

Most competitors’ systems incorporate some, but not all, of the above. Every one of these features, practices, standards, and chips are incorporated into ThinkSystem server design. And where most vendors stop at this point, these are merely steppingstones to even stronger security for ThinkSystem servers. No one layer of security is completely impervious to attack. The more layers and types of protection there are, the more kinds of attacks can be thwarted.

One of the biggest potential system vulnerabilities is in the systems management subsystem. There are no well-defined industry standards for systems management protection. This leaves systems management security up to platform vendors; however, many vendors have done little to address these security weaknesses.

Another vulnerability is through boot firmware. Because subcomponents are now manufactured worldwide, it is difficult to monitor them all for security. So systems management and boot firmware Core Root of Trust for Measurement (CRTM) code elements are established to serve that security-monitoring function. But if a CRTM can be corrupted, then an attacker can insert any desired code deep inside the system. This allows a vendor, disgruntled employee, or even a foreign entity to implant malware, viruses, or the like into system subcomponents, making detection difficult—if not impossible—without specialized methods.

Yet another potential vulnerability comes from the retirement, disposal, or theft of storage devices. What happens to your secure data after the storage devices leave your possession?

Within these categories, there are multiple weaknesses that can be exploited. ThinkSystem products offer protection against each of them.

- Systems Management
  - Systems management—controller integrity
  - Systems management—user ID and password control
  - Intrachassis communication links
  - Extrachassis communication links
  - Scripting and command line interface (CLI) application interfaces
  - Security object provisioning

- Boot Firmware
  - UEFI Firmware Rollbacks
  - Unified Extensible Firmware Interface (UEFI) code updates
  - UEFI attack by BMC

- Drive Retirement, Disposal, and Theft
- Supply Chain

ThinkSystem Security Features and Processes

ThinkSystem servers incorporate the industry-standard features described above, as well as a unique set of features that together create multiple layers of security. All security features are linked together into a “chain of trust.” via a combination of hardware and firmware support.

The following explains how ThinkSystem servers secure against the various types of attacks described above:

Systems Management

ThinkSystem servers include a number of features to secure systems management hardware from attack.

Systems Management Controller Integrity

Viruses, malware, and rootkits can enter the computational, storage, and network nodes through the systems management controllers. Because these controllers form the foundation for the entire system, they potentially could provide an unsecured path to attacking the system (OS) itself. To remain free of threatening software, systems management controllers must be able to boot to a secure state.

All ThinkSystem servers include a TPM 2.0 chip. The TPM helps protect the operating system and applications from attack through external communications (browsers, email, TCP/IP, WAN/MAN, Cloud, etc.). However, this still leaves room for potential attacks through the systems management controller itself. Therefore, all ThinkSystem servers include a second TPM chip, on the XClarity Controller. This chip protects the management subsystem from attack through the integrated management Ethernet port. Both TPMs individually verify code and are verified as genuine by third parties. Competitive servers that don't have a second TPM on their systems management controller are still vulnerable to attacks through this means, which provides an ideal target for Denial of Service (DoS) attacks.

In addition, on ThinkSystem servers both TPM chips implement the TPM 2.0 standard, which supports newer, more secure, versions of Microsoft Windows Server and encryption algorithms than the older TPM 1.2.

Each TPM chip in ThinkSystem servers is soldered to the planar to prevent it from being removed from the system (which would eliminate its protection). The TPM maintains a history of all running firmware that can be used for attestation or verification of authenticity by third parties that the firmware hasn't been changed. This history is sealed and stored securely, and can only be read or unsealed when the TPM is likewise in an unsealed state.

Another ThinkSystem competitive advantage that helps to secure firmware is unique measured boot. This feature indicates that all firmware is measured, recorded, and stored in the TPM for third-party verification prior to execution. A hash of every code module is calculated and stored in the TPM before it is executed. This way, you can be certain that the code hasn't been changed by anyone between the time the server was "flashed" in the factory and when it is delivered to you.

User ID and Password Control

User IDs and passwords across the entire systems management level are like the key system at a large hotel. Much as the hotel has a centralized system to manage keys and ensure security for each room, LDAP can now be used for centralized user ID and password control. There are a few master keys that can access any component, as well as numerous local user IDs and passwords that allow access only to specific systems management components. Local user IDs and passwords are often managed in an ad hoc fashion instead of being centrally controlled. This creates an opportunity for an attacker to introduce a rogue user ID and penetrate the system by cracking well-known local user IDs and passwords, weak passwords, and the like.

To prevent this sort of exposure, the Flex System Enterprise Chassis security policy blocks these local IDs on ThinkSystem blade servers. With password strength also controlled by the Flex System Enterprise Chassis security policy, executing a high level of security is no longer a serious administrative burden.

Secure Intrachassis Protocols

Communications *within* a blade chassis introduces another opportunity for malicious attacks and data interception. An attacker can monitor these links and collect protected credential information such as user IDs, passwords and keys from the data stream. Using this information, the attacker can then pose as a legitimate user, log in and attack the storage, computational and networking nodes, and I/O modules in the system.

Intrachassis communication links within each Lenovo Flex System chassis (containing ThinkSystem blade servers) are encrypted in “secure mode” to prevent unauthorized collection of sensitive information. Secure mode is used to provision, configure, and control the systems management components and compute nodes (servers). It prevents a management system attack from gaining access to login information and prevents attacks on compute nodes. In addition, insecure protocols are not allowed and unused or insecure ports are blocked from outside access.

Secure Extrachassis Protocols

Communication links that enable administrators to directly connect to a chassis’ systems management microcontrollers can be compromised. These links allow direct access to computational, storage, and networking nodes. If these links are not secure, attackers can monitor the traffic on these insecure links and extract legitimate credential information. Just as with the intrachassis communication links, the attacker can then pose as a legitimate user and log into, penetrate, and corrupt the system.

Customers can now directly connect to systems management controllers on compute nodes. Further, security policy and provisioning in the chassis allow these links to be centrally set up so they can be safely managed with minimal administrator intervention required. In addition, the Flex System Enterprise Chassis Management Module (CMM) configures the internal network so that each management controller can see and communicate with the CMM, but not with the management controllers on the other nodes.

Secure Scripting/Command Line Interfaces

Unsecure interfaces, such as telnet, permit a command line interface (CLI) to be accessed on systems management components. This provides an attacker an open interface to run scripts, search for and open password files, escalate privileges, and more. This can expose an entire system. For example, an attacker could execute programs from the command line to edit the system's firewall settings or open a known weakness. That would effectively open a backdoor through which the attacker could later reenter the system and corrupt it or extract sensitive data.

With high security mode set in the Flex System CMM, CLIs can be executed only over secure links and the logins used are centrally controlled by lightweight directory access protocol (LDAP).

Security Object Provisioning

Security object provisioning refers to the security functions necessary to define and start a system or component, or update the system or component due to changing system status. This includes the base user IDs and passwords to start core system functions, keys and their associated certificates to establish secure links, as well as security policies required by nodes to establish connections.

In the absence of a comprehensive security policy and provisioning, these essential security credentials are typically provided in an ad hoc fashion. Unless these objects are provisioned by the system or configured by people with in-depth system knowledge, it can be difficult to know if this has been done correctly and enormous security holes may exist.

With ThinkSystem, the customer sets the security policy, and then certificates and keys are automatically provisioned to the nodes and I/O modules. Rather than requiring highly-skilled personnel to manually provision the system security objects and provide ongoing security management monitoring, the system does this automatically and dramatically reduces the need for manual system administration.

Boot Firmware

Firmware presents a number of opportunities for security breaches. ThinkSystem servers offer many practices, processes, and features to prevent intrusions via firmware.

Lenovo’s Trusted Platform Assurance (TPA) program institutes rigorous security processes to all stages of firmware development, building, and validation to ensure that all firmware is secure.

There are two security processes within TPA. Both include comprehensive, industry-leading security validation and reporting cycles in which any discovered problems are immediately fixed and rolled back into the validated and signed firmware.

The development and build process uses comprehensive testing practices to create and validate digitally signed firmware as part of the secure development process. The build servers, based in the United States, 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 are highly controlled and are based in a secure U.S. datacenter with limited and auditable access and no connection to corporate networks. This firmware, designed, managed, compiled, signed, and stored in the U.S., is then used as the input to the secure system execution process, whereby the firmware is installed or updated in ThinkSystem servers.

In the system execution process, steps are taken to ensure the security of the firmware: First, the hardware is secured via locks placed on the TPM and FPGA modules. Then the firmware is secured by verifying its digital signature *every single time* before it executes. This securing of both the hardware and software creates a chain of trust. (Just as a chain is only as strong as its weakest link, a server is only as secure as its most vulnerable layer.) This secure layer of hardware and software creates a solid security layer for upper-layer workloads to depend on (trust), and protects the system from low-level attacks.

UEFI Firmware Rollbacks

Some competitive servers allow for easy rollback of firmware to previous versions in case of problems with the firmware. However, this leads to the possibility of unauthorized firmware rollbacks to a point before certain system vulnerabilities were corrected.

ThinkSystem servers provide secure UEFI firmware that prevents firmware updates to a previous authentic version, unless performed by a secure mechanism or authorized user. Also, firmware can only execute, boot, or be updated if digitally verified with public/private keys.

UEFI Code Updates

UEFI code updates are updates to the currently installed UEFI that fix known code problems or provide additional functionality. Because an update contains the entire UEFI BIOS image for the system, a compromised UEFI code update can introduce a major security breach into the system. Malicious firmware can be introduced accidentally or intentionally along the supply chain, somewhere between manufacturing and datacenter deployment: during transit, in a warehouse, during setup by a partner, during customer configuration, and elsewhere. The reason this type of supply chain attack is appealing to attackers is simple: If an intrusion is successful at these levels, it has full control over the system *below* the OS and hypervisor levels.

Because these attacks cannot be detected by current antivirus and anti-malware solutions, most likely the system owner won't even know the system has been compromised. Rootkits and other malware that can be inserted into "impostor" code updates can take control of the system at a very deep level and be extraordinarily difficult to detect.

Because of this, ThinkSystem platforms are designed to detect firmware supply chain attacks in the UEFI and the XClarity Controller. The ThinkSystem CRTM code element runs in the UEFI BIOS *before anything else*, scanning subsequent code for security breaches. Because the CRTM and the UEFI have different update requirements, for maximum security they are separately protected. Code signing is implemented separately for the entire UEFI code update as well as the embedded CRTM. The code update packages for the XClarity Controller and Flex System CMM are signed as well.

This process has expanded UEFI code signing from just the CRTM to the CRTM plus the entire separate UEFI code update—a key component in creating the system Trusted Computing Base (TCB). In addition, the new Lenovo XClarity Administrator virtual appliance helps you deploy ThinkSystem servers faster and more securely by allowing you to centrally manage firmware updates and compliance.

UEFI Attack by BMC

BMCs, such as the ThinkSystem XClarity Controller, have enormous control over the system and the UEFI. Because of this control, they are part of the TCB and must be hardened. A BMC can update UEFI code, update hardware firmware—such as field programmable gate arrays (FPGAs)i—and interrogate processors and memory, among other actions. Therefore, a BMC has the ability to implant threats in the UEFI, and from there into the system software. Also, since these controllers only run embedded Linux, the controllers have historically possessed only standard Linux security—no trusted computing and no trusted secure system management controller boot.

To keep any of this from happening, ThinkSystem provides the previously mentioned second TPM on the XClarity Controller, in addition to the CRTM. The TPM first establishes a static root of trust measurement (SRTM) for the BMC, as well as signed Uboot and Linux kernel images integrated into the XClarity Controller. This ensures that the XClarity Controller boots to a correct and trusted state. In addition, there are signed code updates for systems management (XClarity Controller, Flex System CMM, etc.), and the hardened XClarity Controller attack surface greatly enhances the ability of these systems management components to stop new threats from entering. Together, this provides three key security improvements for the system management components: 1) trusted secure boot, 2) trusted CRTM and TPMs, and 3) signed code updates.

In addition, the FPGA module that controls critical system hardware functions is locked at the hardware level in ThinkSystem servers. The FPGA is secure during runtime, preventing unauthorized updates. An

FPGA update is allowed only by trusted systems management firmware, and only after a successful verification of its digital signature.

Drive Retirement, Disposal, and Theft

At some point in the lifecycle of every drive, it becomes time to retire or dispose of it. This requires a painstaking and time-consuming process of either physically destroying the drives (by sledgehammer, for example), or erasing and overwriting the data many times. Even so, the data isn't necessarily unrecoverable, given enough time and effort. And what happens if a laptop containing confidential data is stolen? How confident are you that the user password won't be cracked or bypassed?

One way to protect this data is by encrypting it. Encryption software offers the ability to encrypt standard drives at the OS level. However, this comes with severe performance penalties (because the system processors must perform all of the encryption/decryption in addition to the business workload). In addition, there is still room for an operating system or firmware attack that circumvents the encryption. A better solution is to use drives that provide encryption at the hardware level.

Self-encrypting drives (SEDs) contain an onboard coprocessor (with dedicated memory) that offloads all of the drive encryption/decryption from the system processors. As a result, there is no performance penalty for enterprise-level encryption, and the encryption/decryption is completely transparent to the user, apps, and the OS. It also means that if the drives are stolen, *they cannot be read* without the encryption keys that are stored securely in the hardware. The instant the drive is removed from power, it automatically locks (Data at Rest protection) and the data is secured. This provides government-grade security that ensures Safe Harbor-compliance for data privacy.

The encryption keys are stored within the SED controller, rather than in system memory, which makes them invisible to attackers. Because encryption/decryption is factory-enabled, everything is encrypted and decrypted automatically. This eliminates the need for bulk encryption required by software-based full-disk encryption and saves hours of installation time.

Lockable doors and bezels do make it more difficult to remove hot-swap drives from the server. However, if the drive *is* removed there is nothing protecting your data if the drives aren't encrypted.

SEDs also aid with secure drive retirement and disposal, by eliminating the costly overwriting/wiping process normally necessary. An entire SED can be cryptographically erased in less than a second, simply by changing the internal encryption key. This makes it impossible to read the data encrypted using the missing key. Unfortunately, generating, securing, and managing thousands of encryption keys can be a pain point for many customers.

Lenovo certainly isn't the only vendor to offer SEDs; however, only Lenovo offers Secure Key Lifecycle Manager (SKLM). Combined with SEDs, SKLM provides a number of unique features:

- Efficient, simple, and transparent centralized local or remote encryption key management
- Addresses regulatory requirements calling for encryption key protection
- Reduces operating costs and speeds implementation
- Enables interoperability via Key Management Interoperability Protocol (KMIP) support
- No server performance impact

SKLM works seamlessly with self-encrypting drives. By combining these two capabilities, an organization achieves:

- Centralized authorization key storage
- Automated management of local and remote encryption keys
- A scalable solution to support large ThinkSystem environments that need to manage thousands of keys
- Simple and secure integration, with interoperability across solutions that include ThinkSystem as well as others

Supply Chain

Even if a server vendor maintains strict security control over its own products, vulnerabilities can occur via components sourced through the supply chain if suppliers are not as diligent about security. For example, in 2015, two security researchers found that certain automobiles could be remotely hacked, controlled, and even paralyzed on the road using vulnerabilities found in some of the OEM components used by the car manufacturer. The expense of recalling and patching 140 million vehicles worldwide—plus lost sales—was considerable, and the company’s reputation was tarnished.

In a server scenario, components infected at the hardware/firmware level could bypass all OS/software-level security measures on the server, thereby exposing customer data and leaving the server vendor subject to penalties and lost revenues.

To prevent this scenario, the server vendor must work with the suppliers to ensure that components are just as secure as the server hardware itself.

Lenovo closely controls the supply chain to ensure that suppliers follow industry-standard security practices for all active components used in Lenovo products. This includes security education and unannounced audits to verify compliance. If a supplier fails an audit, they are given an opportunity to correct the problem. Suppliers can be (and some have been) removed from Lenovo’s trusted supplier lists.

Whenever code is developed by third parties, U.S. teams perform rigorous inspections for quality control. All source code is maintained on United States-based code retention servers, and all code changes are tracked and audited.

Lenovo itself undergoes unannounced audits (related to the acquisition of IBM's x86 server business in 2014) of ThinkSystem business processes by the U.S. government and independent auditors, creating the most transparent, auditable, and secure supply chain in the server industry. Other server vendors undergo no such audits, leaving their processes far less transparent. Do you know what security measures your server vendor requires of its supply chain, if any?

Overseas Manufacturing

With servers manufactured across the globe, many customers worry that malware could be introduced intentionally into servers at the local level by competitors or those opposed to Western interests.

Like our competitors, Lenovo manufactures servers in locations all around the world. However, Lenovo is the only server vendor to manufacture servers in North America as well. The facility in North Carolina offers enhanced security capabilities and manufacturing for customers who require servers that are "Made in America". Competitors' servers are manufactured exclusively outside of North America, mainly in Asia, using third-party manufacturing facilities and employees for most or all of their servers.

In contrast, Lenovo owns most of its manufacturing facilities around the world (including North America). In addition, all personnel in these facilities are Lenovo employees who have been through an exhaustive screening and approval process.

This enables an end-to-end business model for vertical integration. By leveraging our own manufacturing capabilities and using employees who have a vested interest in keeping Lenovo servers secure, we can maintain greater control over product development, manufacturing, and supply chain operations.

Availability

Part of the security equation is avoiding the chaos and cost of downtime. Obviously, security breaches aren't the only reason for downtime. Hardware failure is another. Keeping your hardware online requires world-class reliability and availability. ThinkSystem servers from Lenovo fulfill that requirement as well.

A 2017 survey conducted by Information Technology Intelligence Consulting (ITIC) [3], found that 79% of corporate users demand at least "four-nines" (99.99%) availability from their servers, and 24% require *five*-nines or better

[3] 2016-2017 Global Hardware, Server OS Reliability Report, ITIC, October 2016; and ITIC Reliability Study 2016 – 2017 Mid-year Update, May 2017.

(99.999%) from their mission-critical and key line-of-business servers. The latter is equal to 5.25 minutes *per year* of unplanned downtime, or 43.7 seconds per month—essentially *no* downtime.

In that same survey, corporate enterprise users—for the *7th time in a row*—ranked Lenovo server hardware #1 in delivering the highest levels of reliability/uptime of any x86 servers in the industry. Lenovo servers (along with IBM POWER servers) finished first or second in *every* reliability category, including security. Among x86 servers, Lenovo had the highest levels of five-nines availability (68% of servers) in the course of the past year, with the fewest unplanned outages lasting over 4 hours (1%). In contrast to Lenovo's 1%, 7% of Dell servers failed for at least 4 hours, along with 10% of HPE and 13% of Oracle x86 systems.

Not surprisingly, Lenovo servers were also ranked #1 in a 2017 survey of *customer satisfaction* conducted by Technology Business Review (TBR), *finishing first in all 22 categories*.[4] The icing on the cake is industry-leading performance, as evidenced by the *88 current world records* achieved by ThinkSystem servers on industry benchmarks.[5]

Summary

In an environment where organizations consider security to be their biggest concern, no other servers provide as many ways to prevent security breaches as ThinkSystem servers do. We start with industry-standard security features and then add Lenovo-unique hardware-, firmware-, and systems management-level security capabilities no other vendor has. Our firmware is developed in the U.S. and kept on highly-secure air-gapped servers in the U.S., so there is no possibility of accidental or intentional corruption. We closely monitor and police our supply chain (and, in turn are monitored by the U.S. government and independent auditors) for adherence to security best practices. And we're the only vendor to offer servers manufactured in North America.

ThinkSystem servers combine the industry's best security with the best uptime, the best performance, and the highest customer satisfaction. They give you the greatest chance of keeping your servers online throughout daily operations as well as cyberattacks. i

You owe it to your organization—and your customers—to see whether Lenovo ThinkSystem servers are the right fit for you. For more information, contact your Lenovo representative or Business Partner.

[4] 2H16 Corporate IT Buying Behavior and Customer Satisfaction Study, TBR; July 2017.
[5] As of November 8, 2017. https://lenovopress.com/lp0810-lenovo-thinksystem-servers-88-performance-world-records

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.

Any performance data contained herein was determined in a controlled environment; therefore, the results 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.

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.