INFORMATION TECHNOLOGY
INTELLIGENCE CONSULTING

Information Technology Intelligence Consulting

ITIC

ITIC 2022 Global Server Hardware, Server OS Security Report

August/September 2022

Table of Contents

Executive Summary

For the fourth straight year, enterprises ranked mission critical servers from IBM, Lenovo, Huawei and Hewlett-Packard Enterprise (in that order) as the most secure platforms which experienced the least amount of successful data breaches and proved the most formidable for hackers to crack.

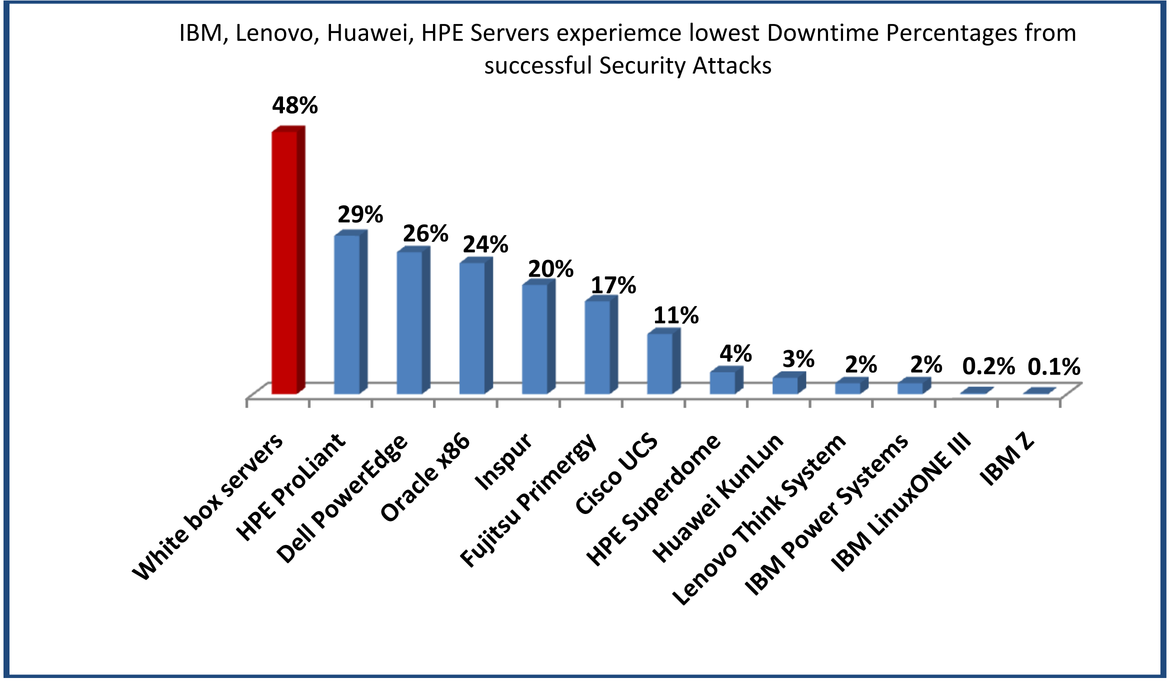
Only a miniscule 0.1% of IBM Z mainframes suffered unplanned downtime due to a successful data breach. And just two percent (2%) of IBM Power Systems; two percent (2%) of Lenovo Think Systems; three percent (3%) of Huawei KunLun and four percent (4%) of HPE Superdome servers experienced downtime, application inaccessibility and productivity disruptions due to security attacks (**See Exhibit 1).**

Those are the results of ITIC's 2022 Global Server Hardware Security survey which compared the security features and functions of 18 different server platforms. ITIC's independent Web-based survey polled 1,550 businesses worldwide across 30 different vertical market sectors from January through June 2022.

ITIC's latest study found that strong security enabled IBM, Lenovo, Huawei and HPE corporate enterprises to lower annual IT operational costs related to cyberattacks by 27% to over 60%, compared to the least secure server hardware distributions. .

IBM, Lenovo, Huawei, HPE and Cisco hardware (in that order) recorded the top overall scores in every security category, successfully solidifying and improving their top positions as the most secure and reliable server platforms despite a significant 86% spike in security hacks and data breaches over the past two and a half years.

Exhibit 1. IBM, Lenovo Servers Most Secure, Toughest to Crack



Source: ITIC 2022 Global Server Hardware, Server OS Security Survey

The top servers led by the IBM Z; IBM POWER; the Lenovo ThinkSystem; the Huawei KunLun and HPE (in that order), all scored their respective best security performances in the latest poll. These vendors achieved the best security results among 18 mainstream server hardware platforms in every security category, including:

- The fewest number of ***successful*** security hacks/data breaches.
- The least amount of overall unplanned server downtime for ***any*** reason and the least amount of unplanned server downtime due to a data breach incident.

- The fastest Mean Time to Detection (MTTD) from the onset of the attack until the company isolated and shut it down.
- The fastest Mean Time to Remediation (MTTR) to restore servers, applications and networks to full operation.
- The least amount of lost, stolen, destroyed, damaged or changed data as a direct consequence of a security data breach (e.g. Ransomware, phishing scam or CEO fraud).
- The least amount of monetary losses due to a successful security hack.
- The highest confidence in the embedded security of the server hardware to deliver alerts/warnings and repel security attacks and data breaches.

The IBM Z mainframe outperformed all other server distributions – delivering near foolproof security and true fault tolerant seven nines or better (99.9999999%) uptime and reliability. Only a minuscule – 0.1% - of IBM Z mainframes and 0.2% of IBM LinuxONE III systems experienced a successful security breach.

IBM standalone Power Systems and the Lenovo ThinkSystem servers were in a statistical tie; with only two percent (2%) of respondents reporting a successful hack over the last 12 months. Only a minuscule – 0.1% - of IBM Z mainframes and IBM LinuxONE III systems experienced a successful security breach. The IBM Power8, Power9 and Power10 servers again delivered top notch security among all mainstream hardware distributions with 95% of survey respondents reporting their firms were able to identify and thwart attempted security penetrations immediately or within the first 10 minutes of detection.

The Lenovo ThinkSystem servers achieved the best security scores among all x86 server distributions for the fourth year in a row. Lenovo ThinkSystem servers similarly delivered the best MTTD rates among all Intel x86-based servers. A 95% of majority of Lenovo ThinkSystem survey respondents said their IT and security administrators detected and repelled attempted hacks and data breaches immediately or within the first 10 minutes of the penetration.

Huawei's KunLun mission critical platform was close behind with three percent (3%) of customers experiencing a successful hack and four percent (4%) HPE Integrity Superdome customers said they had a successful security breach over the last year.

Just over one-in-ten or 11% of Cisco UCS servers were successfully hacked. Cisco's hardware performed extremely well, particularly considering that a large portion of UCS servers are deployed in remote locations and at the network edge. Inexpensive unbranded White box servers again proved the most porous – nearly half - 48% - of survey respondents said their businesses were hacked. This is a four percent (4%) increase compared to ITIC's 2021 survey.
Security is, and will remain the number one issue that either fortifies or undermines the reliability of mission critical server hardware, server operating system and applications.

Businesses that hope to keep their data assets secure and ensure continuous, uninterrupted operations are well advised to deploy the most secure server hardware, server OS and application infrastructure. Any organization that ignores security does so at its own risk.

Introduction

ITIC's 2022 Global Server Hardware Security survey shows that 78% of corporate enterprises rank security as the leading cause of unplanned server and application downtime and inaccessibility. And over 80% of survey respondents classify security breaches as the biggest potential threat to the stability and uptime of their on-premises, cloud and network edge infrastructures and ecosystems. This is in stark contrast to ITIC's 2013 Global Server Hardware, Server OS Reliability poll when only 22% cited security issues as a top cause of server outages.

To reiterate, security will remain the largest pain point and potential vulnerability for the core infrastructure, networks, the cloud and the network edge for the foreseeable future.

Hackers are organized and their hacks are targeted and sophisticated. The hacks themselves are more precise, pervasive and pernicious. A single security breach of even a few minutes duration can interrupt daily operational transactions and prove expensive.

While COVID-19 is past its peak, corporate enterprises are still feeling the pain. The effects caused by the pandemic reverberate to the present day. These include:

- Supply chain shortages and delays across a wide range of consumer and high tech component parts.
- Hybrid work environments which increase the attack surface and the number of potential vulnerabilities.
- Inflationary pricing on products and services.
- Added stress on IT and security administrators to oversee vast, complex on-premises, cloud and network edge environments.
- A persistent shortage of skilled IT and security administrators.

Additionally, the increasing number of interconnected standalone and Internet of Things (IoT) devices spanning data centers, the network edge and virtualized cloud deployments has commensurately amplified the number of potential vulnerability points. Attack surfaces or vectors are virtually unlimited; new and more damaging security attacks appear with regularity.

Overall, ITIC's latest survey findings indicate that the security and reliability chasm among the **most secure** and the **most insecure** servers continues to widen. The global pandemic sparked a wave of COVID-19 related data breaches, Ransomware, phishing, Business Email Compromise (BEC), CEO fraud and other scams that continue unabated.

ITIC's most recent survey results further underscore that the reliability and security of the core infrastructure server hardware are inextricably intertwined and symbiotic. The data losses and productivity losses associated with successful security penetrations are expensive. They compromise businesses' intellectual property (IP) and heighten the threats for business partners, customers and suppliers. Hacks also expose employees' personal data and commensurately raise corporations' risk of litigation and regulatory non-compliance.

No one and nothing is immune.

It is no coincidence that the top five most reliable server platforms: the IBM Z, the IBM LinuxONE III, the IBM Power Systems, Lenovo ThinkSystem, Huawei KunLun and Fusion Servers, the HPE Superdome Integrity and Cisco UCS (in that order) provide the most formidable security.

The global pandemic sparked a wave of COVID-19 related data breaches, Ransomware, Phishing, Business Email Compromise (BEC), CEO fraud and attacks that continue unabated to the present. Security attacks target myriad corporate and consumer devices and software across businesses of all sizes, spanning every vertical industry.

ITIC's latest poll also revealed that 80% of survey respondents fear their organizations will fall victim to a targeted attack over the next 12 to 18 months. This is up from 73% of businesses concerned about a successful breach a year ago.

ITIC's latest security survey findings are bolstered by various U.S. Federal government agencies which ramped up their security initiatives. Since the start of the global COVID-19 pandemic in early 2020, government agencies have issued an increasing number of cybersecurity risk alerts and recommendations. The Federal Bureau of Investigation (FBI); the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) that issued dozens of alerts during the first seven months of 2022. CISA[1] alone has issued over two dozen security alerts in 2022.

In March, 2022 the release of the annual FBI Internet Crime Report 2021[2] revealed the total money lost to cybercrime increased 64% to $6.9 billion last year and that the number of cybercrime complaints to FBI rose seven percent (7%) to 847,376. In 2021, the FBI's IC3

[1] Cybersecurity & Infrastructure Security Agency (CISA) 2022 Alerts. URL: https://www.cisa.gov/uscert/ncas/alerts/2022

[2] Federal Bureau of Investigation (FBI) Internet Crime Report 2021. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

received 19,954 business email compromise (BEC)/email account compromise (EAC) complaints resulting in adjusted losses of nearly $2.4 billion (USD).

The FBI 2021 Internet Crime Report also detailed how cyber crooks exploit organizations' use of remote work and virtual meetings resulted in a rise in online scams, noting: "…One new technique involved scammers inviting company employees to a virtual meeting and then using 'deep fake' simulated audio of an executive's voice to instruct employees to transfer money to a fraudulent account."

According to the FBI, "almost all cybercrime metrics have increased dramatically since 2017 — money lost increased by 393% and the overall number of complaints increased by 191%, while reports of phishing — in which a scammer sends an email pretending to represent a reputable company in order to trick the victim into revealing passwords or other information — were up by a whopping 1,178%."

A July 2022 article in Wired magazine, "The Worst Hacks and Breaches of 2022 So Far," chronicles some of the most recent egregious attacks in 2022, to date.

Among the most high profile and well documented security breaches this year are:

- The Russia/Ukraine hacking war began even before Russia invaded the Ukraine. Both countries are engaged in an ongoing series of attacks and counterattacks aimed at destroying each other's computer systems and various institutions and IT infrastructure.
- In early 2022, the international digital extortion gang Lapsus$, based in the United Kingdom, launched a series of successful phishing attacks against a wide array of high technology firms. The Lapsus$ hacking group stole and leaked proprietary source code from Microsoft, Nvidia and Samsung, in an apparent extortion attempts.
- In April, the Conti cybercrime hackers, who have been linked to Russia, attacked Costa Rica's Ministry of Finance, crippling that country's import/export business for months.
- In June, Shields Health Care Group based in Massachusetts, reported it got hit by a near month-long hack that impacted nearly two (2) million subscribers.
- In August, BlackFog a global cybersecurity company, headquartered in Cheyenne, Wyoming said it recorded 39 ransomware attacks, the second highest month since it began tracking data breaches in 2015. According to BlackFog, healthcare organizations were particularly hit hard with 10 different incidents recorded, including an attack on the UK's National Health System (NHS_ as well as an attack on a French hospital which resulted in a $10 million (USD) ransom demand. Education, government and utilities were also high on cybercriminals' hit list.

The aforementioned security attacks are the ones that make the news. For every one of them there are scores more, that disrupt daily operations at small, midsize and large enterprises that we never hear about, but are just as deadly and expensive.

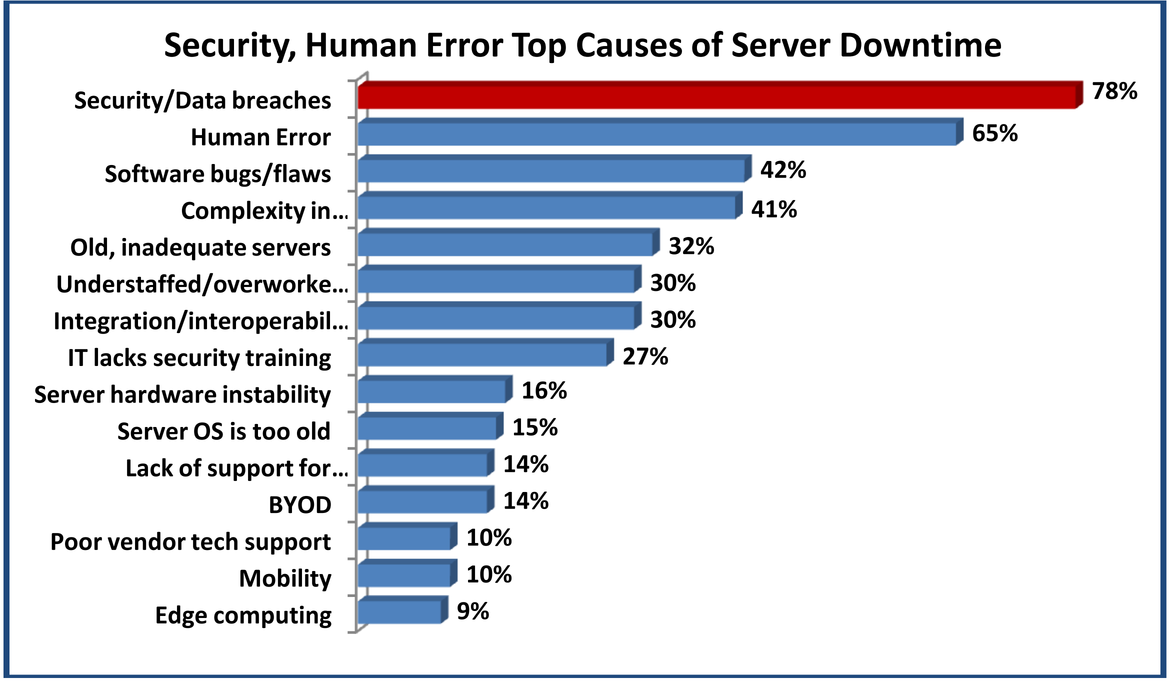
Strong Infrastructure & Network Security is Imperative

The ongoing solid security results posted by IBM, Lenovo, Huawei, HPE and Cisco (in that order) are especially noteworthy. Each of the top performing vendors has a long history of prioritizing security and being at the forefront of delivering advanced security technologies. The top five server distributions have maintained – and improved - those high levels of security despite the increasing frequency, ferocity and increasingly targeted nature of the security attacks. On average, 46% of all ITIC survey respondents reported their servers, operating systems and critical business applications suffered successful security hacks since the outset of COVID-19 in early 2020 – over two-and-a-half years ago. This is an increase of 11 percentage points from 41% in just the last year and a hike of 32 percentage points based on the 19% of organizations that said their servers were successfully penetrated in ITIC's 2020 Global Server Hardware, Server OS Security poll, two years ago.

By contrast, only a very small percentage in the single digits - of IBM Z (0.1%); the IBM LinuxONE III (0.2%); the IBM Power Systems (2%); Lenovo ThinkSystem (2%); Huawei KunLun (3%) and HPE Superdome Integrity (4%) mission critical server respondent customers said their firms had a successful data breach within the last year.

Security is a technology and business issue that impacts all enterprises. To reiterate, a 78% majority of 1,550 survey respondents cited security and data breaches as the greatest threat to server, application, data center, network edge and cloud ecosystem reliability **(See Exhibit 2)**. The hacks are more targeted, pervasive and pernicious. They are designed to inflict maximum damage and losses on their enterprise and consumer victims.

Exhibit 2. Security is the Top Cause of Server, Application Downtime



Source: ITIC 2022 Global Server Hardware, Server OS Security Survey

Average Data Breach Costs Top $4 Million

Data breaches are big business and a primary business for the burgeoning professional hacking community. A successful hack is expensive on many levels. In 2021, the average cost of a data breach rose by nearly 10% to $4.24 million (USD) up from $3.86 million in 2020 according to the 2022 Cost of a Data Breach Study jointly conducted by IBM and the Ponemon Institute[3]. This is a 20% increase since 2015.

Additionally, the latest Verizon 2022 Data Breach Investigations Report [4] compiled in conjunction with 87 partner organizations confirmed the rise in security attacks with the

[3] "2022 Cost of a Data Breach Study," IBM and the Ponemon Institute. URL: https://www.ibm.com/security/data-breach

[4] "Verizon 2022 Data Breach Investigations Report," Verizon. URL: https://www.verizon.com/business/resources/reports/dbir/

banking/finance, government, healthcare and retail organizations being among the hardest hit markets. Verizon's 2022 DBIR study detailed data from 23,896 security incidents, including 5,212 confirmed data breaches. Some 849 of the security incidents (approximately 18%) analyzed in the report were experienced by healthcare businesses; some 571 of the incidents reported by healthcare organizations resulted in confirmed data breaches.

The Verizon 2022 DBIR report also confirmed that ransomware attacks spiked by 13% in 2021. This percentage is more than the combined increases over the previous five years from 2016 - 2021. The Verizon study found that ransomware attacks accounted for 25%, or one-in-four, data breaches last year. The greatest common denominator in overall ransomware attacks was the use of stolen credentials which were causal in 40% of hacks; they are primarily utilized in desktop sharing software. Phishing was the second most common vector in security breaches and provided initial, illegal access in 35% of ransomware attacks; this was followed by the exploitation of vulnerabilities in web applications and direct installs. The high percentage of remote desktop software and email attacks underscores the necessity of locking down RDP and securing email which are among the most used daily applications.

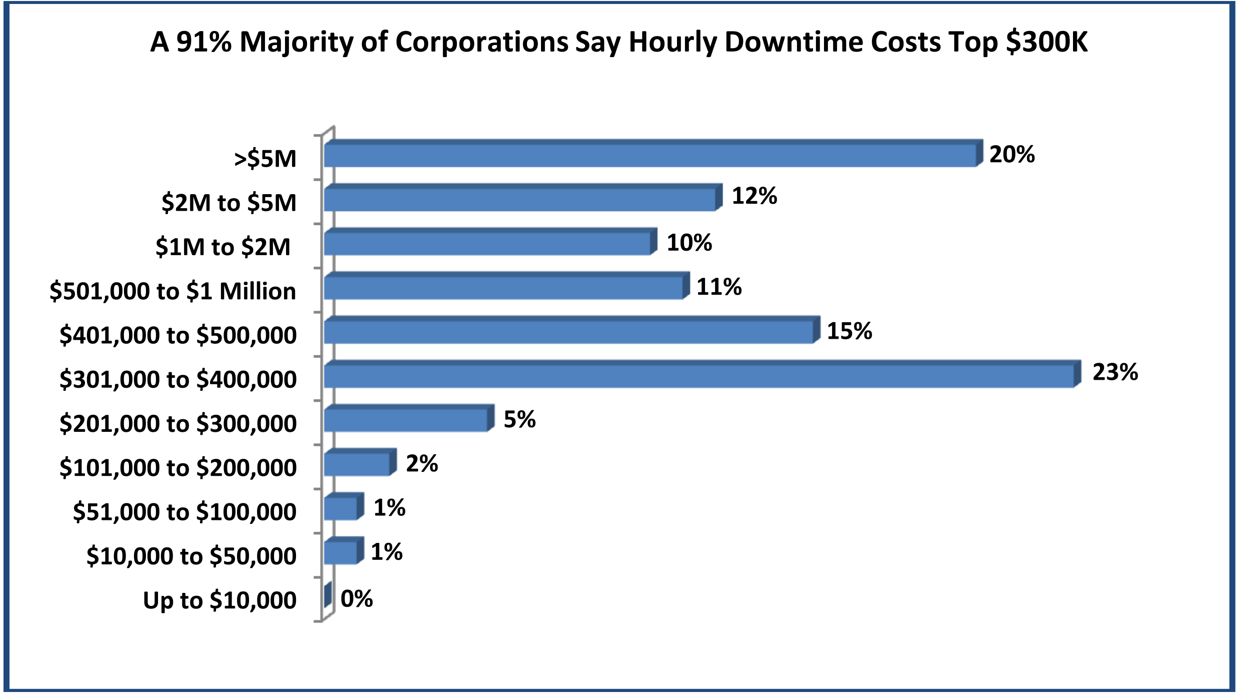
Another worrisome trend identified in the Verizon 2022 DBIR study is the escalation in supply chain attacks, which were responsible for 62% of successful penetrations last year. Hackers exploit supply chain vulnerabilities for financial gain; disruption to local, national and global markets to manipulate prices and espionage.

A DTEX Systems Report found that "only 30% of organizations were prepared to secure a complete shift to remote work." The DTEX Systems study also found that almost 75% of organizations are concerned about the security risks were introduced by users working from home and 73% of businesses admitted they have partial or no visibility into user activity if their VPN is disabled by remote workers. Another alarming (though unsurprising) finding is that teleworkers use their work laptops for personal use; with 25% of respondents acknowledging this increases the risk of drive-by-downloads, with 15% saying their firms are more susceptible to Phishing attacks.

Hourly Server, Application Downtime Costs Climb

ITIC's most recent study also revealed that the Hourly Cost of Downtime now exceeds $300,000 (USD) for 91% of SME and large enterprises; this is up from 81% of survey respondents who calculated the same loss figures in 2018 **(See Exhibit 3).** And 44% estimate hourly downtime causes their firms to lose from $1 million to over $5 million.

Exhibit 3. Hourly Cost of Server Downtime Tops $1 Million for 42% of Enterprises



Source: ITIC 2022 Global Server Hardware, Server OS Reliability Survey

These statistics represent ***average*** hourly outage costs. In a worst-case scenario a data breach that occurs during peak usage hours and interrupts crucial business operations can cost businesses millions per minute. Any organization that suffers a protracted outage of hours or days as the result of targeted Ransomware attack will almost certainly incur many millions in damages. There is also no guarantee that a hacker or hacking group will be true to their word and provide the key to unlock the data once the ransom is paid.

Monetary and data losses are always uppermost on corporate minds' due to productivity and disrupted operations. But businesses must also calculate the amount of employee manpower hours lost as well as the number of IT and security administrators and their associated time spent performing remediation efforts and full return to operation. Firms must also determine whether any data or intellectual property (IP) was lost, stolen, damaged, destroyed or changed.

Organizations must also consider the cost of any litigation as well as potential civil or criminal fines/penalties associated with security incidents and data breaches. Some costs, like damage to an organization's reputation, are incalculable and may result in lost business. A full and thorough accounting of all remediation efforts, costs and the impact of lost, stolen, damaged, changed and destroyed data, along with any litigation fees, lost business, civil and criminal fine and penalties, may take a company months or over a year to perform. In the process, it can cost millions to find the original source(s) of the hack and the affected server hardware and software.

Hackers pick and choose their targets with great precision and they are extremely opportunistic. Cybercriminals are especially skilled at honing in on so-called “soft targets” like teleworkers and remote learning students taking online and Zoom classes; local and state municipalities; small and mid-sized school districts, hospitals, health care clinics, doctors’ offices and branch bank offices. The reason: students and remote workers often fail to implement security because it’s too much of a nuisance. Many remote and network edge sites lack onsite security administrators.

Inherent, embedded server infrastructure security is crucial in order to identify, thwart and repel hacks from both company and employee or student owned desktop and mobile devices that continually access server-based data and assets.

- As always, ITIC emphasizes that individual companies’ experiences and costs will vary depending upon the type, duration and severity of their specific data breach. Additionally, the monetary costs associated with security breaches, increase annually. Enterprises must consider other, often hidden consequences of a security attack. These include but are not limited to:
- Stolen, lost, damaged, destroyed, changed data and sensitive data and Intellectual Property (IP).
- Disruptions to daily operational transactions and employee productivity, to the business, its customers, business partners and even suppliers.
- Increased risk of litigation.
- Increased risk of regulatory non-compliance with federal, state, local and international security and privacy laws. If found guilty, the company could face serious penalties including fines, civil penalties and even jail time for some executives.
- Increase in insurance premiums
- Damage to the corporation’s brand and reputation. This could result in lost business and in worst case scenarios cause the company to go out of business.

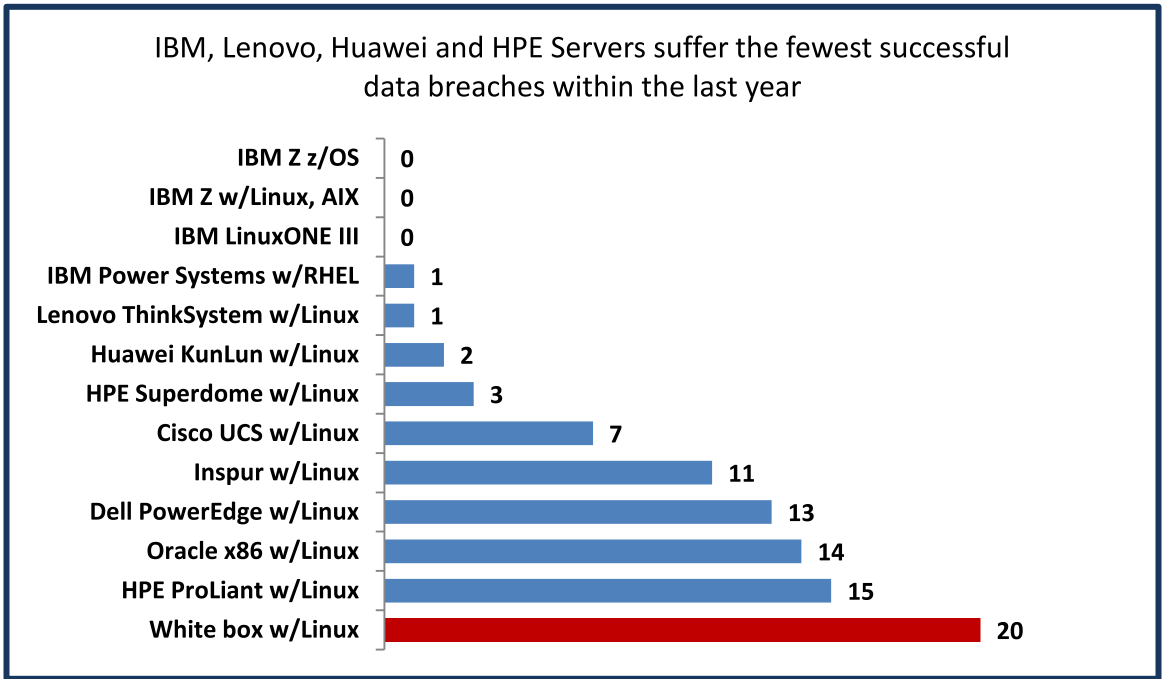
Data & Analysis: Vendor Security Results

IBM, Lenovo, Huawei and HPE perennially achieve top server reliability ratings because they have the most secure hardware platforms with the best embedded security technologies and capabilities. These vendors, and more recently Cisco, have made server security – and in Lenovo's case PC, laptop and server security – a top priority. All of the aforementioned vendors, particularly IBM, Lenovo and Huawei significantly upped R&D spending in the last several years – particularly with regard to security.

IBM for example, is at the vanguard of Quantum safe cryptography research to stay ahead of cybercriminals by significantly raising the degree of difficulty it takes to hack into systems. And Lenovo has doubled down on its pioneering Product Security Program for servers and ThinkShield portfolio to enable customers with end-to-end security across the IT stack on PCs and mobile devices.

As **Exhibit 4** indicates, the most secure server hardware platforms experienced the fewest successful security breaches. The IBM Z running the z/OS and Red Hat Enterprise Linux (RHEL) and IBM LinuxONE III respondents all said those platforms had no successful security hacks over the 12 months. They were followed by the IBM Power Systems and Linux ThinkSystem servers with one each; Huawei KunLun which averaged two hacks; the HPE Integrity with three successful penetrations and Cisco's UCS servers with seven data breaches. The unbranded White box servers were the most porous, averaging 20 successful data breaches in the past year.

Exhibit 4. IBM, Lenovo, Huawei and HPE Servers Suffer Fewest Successful Hacks



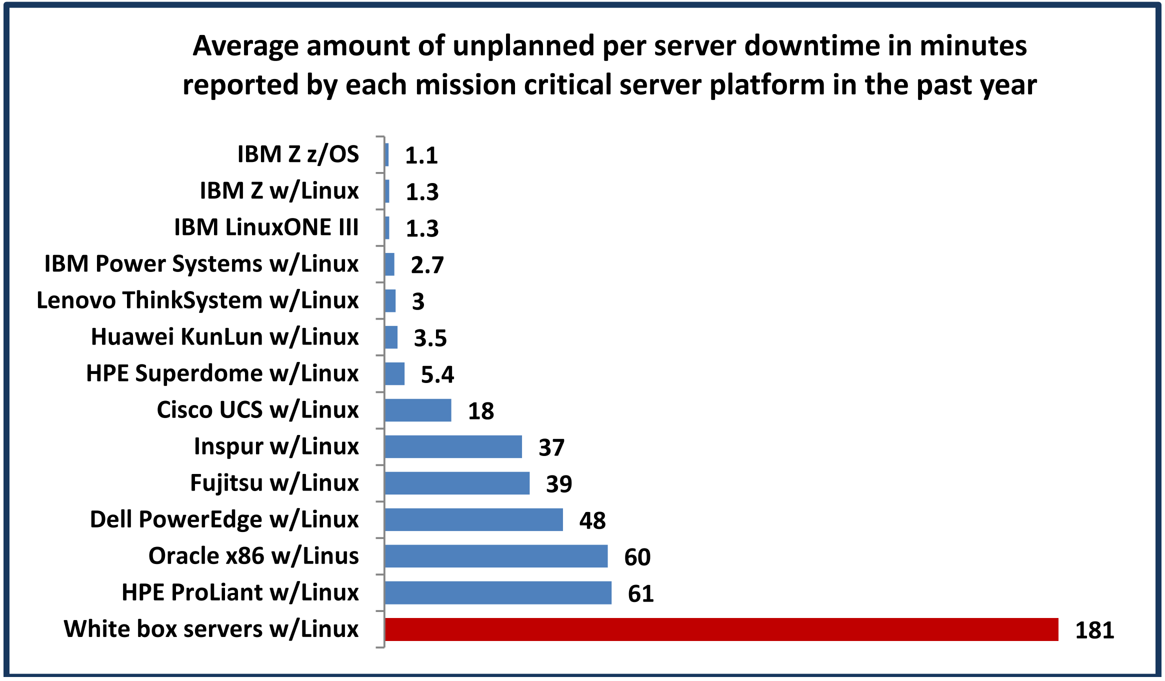
Source: ITIC 2022 Global Server Hardware, Server OS Security Survey

To reiterate, ITIC's 2022 Global Server Hardware Security survey once again found that the IBM Z, IBM LinuxONE III, IBM Power Systems, Lenovo ThinkSystem and Huawei KunLun and Fusion servers (in that order) achieved the best results in every security category including:

- The fewest number of ***successful*** security hacks/data breaches.
- The least amount of overall unplanned server downtime for ***any*** reason and the least amount of unplanned server downtime as the result of a security incident.
- The fastest Mean Time to Detection (MTTD) from the onset of the attack until the company isolated and shut it down.
- The fastest Mean Time to Remediation (MTTR) to restore servers, applications and networks to full operation.
- The least amount of lost, stolen, destroyed, damaged or changed data as a direct consequence of a security data breach (e.g. Ransomware, phishing scam or CEO fraud).
- The least amount of monetary losses due to a successful security hack.
- The highest confidence in the embedded security of the server hardware to deliver alerts/warnings and repel security attacks and data breaches.

As **Exhibit 5** depicts, the IBM Z, the IBM Power Systems, the Lenovo ThinkSystem, Huawei KunLun and HPE Superdome mission critical servers (in that order) experienced the least amount of unplanned downtime as the direct consequence of either successful or attempted security attacks.

Exhibit 5. IBM, Lenovo, Huawei Experience Lease Amount of Security Downtime



Source: ITIC 2022 Global Server Hardware, Server OS Security Survey

This is significant from a productivity, cost and risk mitigation perspective.

The IBM Z and IBM LinuxONE III both averaged under two (2) minutes each of per server unplanned downtime associated with each individual security occurrence. They were followed closely by IBM's POWER8, POWER9 and Power10 servers which experienced just under (3) minutes of per server unplanned outages as the result of a security issue; the Lenovo ThinkSystem x86 servers recorded approximately three (3) minutes of per server downtime followed closely by the Huawei KunLun and Fusion servers and HPE Superdome Integrity high end servers which each experienced an average of 3.5 minutes of per server unplanned downtime associated with security incidents. Once again, unbranded White box servers racked up 181 minutes or nearly three (3) hours each of downtime as a direct consequence of security-related issues. That makes the most secure IBM Z servers as much as 90x more secure and reliable than the least secure White box hardware. The IBM Power8, Power9 and Power10 offerings are up to 60x more secure than unbranded White box servers. The Lenovo ThinkSystem platforms are likewise nearly 60x more secure than White box servers.

Fast Mean Time to Detection is Critical

Security hacks and data breaches are a fact of doing business in the digital age. At some point, every organization and its critical main line of business servers, server OSes and applications will be the victims of an attempted or successful data breach.

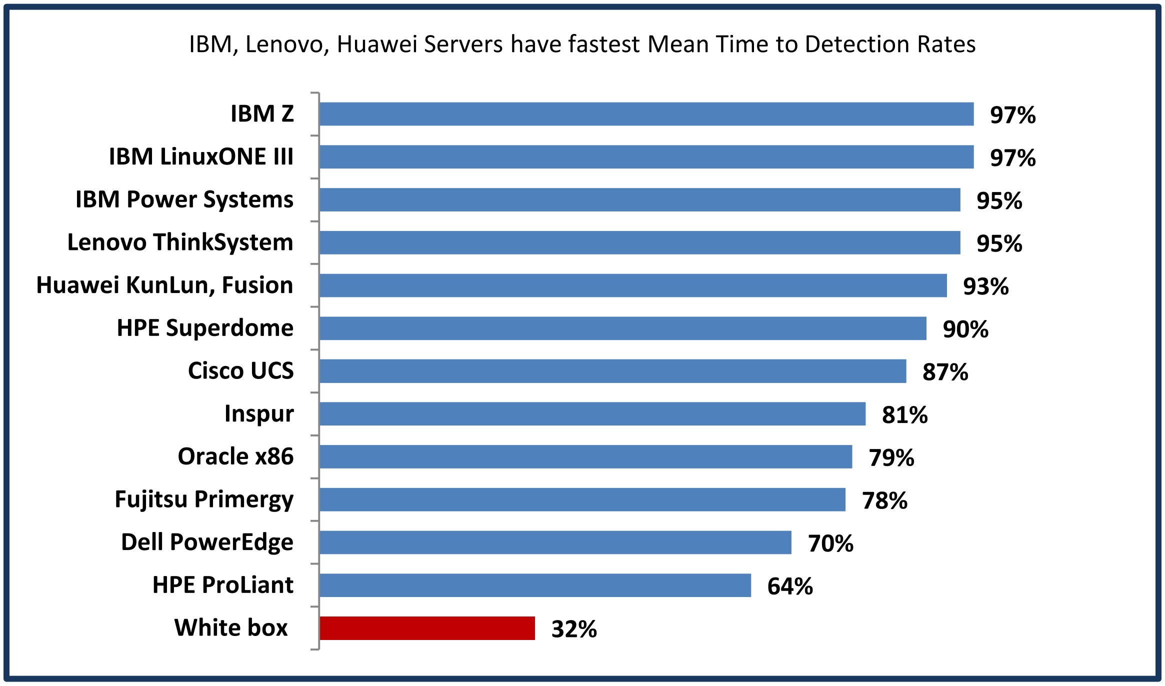
Companies that fail to detect data breaches in a timely manner (and the faster the better) will almost assuredly suffer the very costly consequences. Once again, the average cost of a data breach in 2022 is now over $4 million according to the Ponemon Institute's 2022 Cost of a Data Breach study. The more quickly the company's servers and software can detect a security issue and respond to it, the greater the chances of thwarting the attack ***before*** it can infiltrate the network, interrupt transactions and daily operations and access sensitive data and IP.

This reinforces the need for strong embedded server and infrastructure security that recognizes the danger, sends alerts and alarms and has the ability to isolate the threats. Strong preparedness on the part of the corporation and having a well trained staff of security professionals and IT administrators are also of paramount importance.

Exhibit 6 shows that once again, the IBM Z, the IBM LinuxONE III, the IBM Power Systems, Lenovo ThinkSystem, Huawei KunLun and Fusion Servers, HPE Superdome Integrity and Cisco UCS Servers (in that order) excelled in thwarting hacks. These servers had the best Mean Time to Detection (MTTD) percentages among all server platforms.

An overwhelming 97% of IBM Z, IBM LinuxOne III survey respondents indicated their servers were able to detect an attempted security breach "Immediately or within the first 10 minutes" of the hack and shut it down. They were followed in order by the IBM Power Systems (95%); the Lenovo ThinkSystem (95%); Huawei KunLun and Fusion distributions (93%) and HPE Superdome Integrity (90%) of each of those platform users, said their firms were able to recognize and repel a security breach "immediately or within the first 10 minutes." The faster the critical core infrastructure servers, operating systems and mission critical applications can identify and repel a hack, the better the chances the business will experience little to no downtime or fall victim to stolen, changed, damage or compromised data and IP theft.

Exhibit 6. IBM, Lenovo & Huawei Servers have Fastest Mean Time to Detection Rates



Source: ITIC 2022 Global Server Hardware, Server OS Security Survey

Just under one-third or 32% of businesses running unbranded white box servers were able to detect, isolate and thwart security attacks. Once again, a hallmark of unbranded white box servers is that they often lack even basic security mechanisms. This makes them especially susceptible to cyberattacks.

Server Vendor Security Initiatives

Maintaining server security is a daunting and complex task.

Cybercriminals only have to be right once to invade and compromise server hardware and software security. The server vendors have to be right ***all the time*** to avoid being hacked.

There's no such thing as 100% foolproof, perfect security. However, top technology combined with trained, proactive security administrators and best computer security policies and procedures can mitigate risk to acceptable levels.

IBM Security Overview/Initiatives

IBM has been a leader in computer security for decades and it shows. IBM Z servers continue to achieve top grades for security as well as overall reliability, accessibility and performance among all server platforms. The IBM Z family — the "Z" stands for zero downtime — consistently outperforms **all** competitors in every security and reliability category. Consequently, the Z family mitigates risk of data, IP, operations, productivity and monetary losses to an acceptable level. The Z server platform also delivers the lowest total cost of ownership (TCO) and fastest return on investment (ROI). The z13, z14 and z15 mainframes scored the best reliability/uptime, application availability ratings and security across the board in terms of actual minutes of unplanned per server/per annum downtime. The newly released IBM z16, the industry's first quantum-safe system[5], is expected to further improve security.

The centerpiece of IBM's security lineup is its Quantum Safe computing initiative, which was first introduced in 2020. Simply put, it utilizes advanced algorithms to make cracking IBM hardware virtually impossible. IBM is also making it possible for customers to make their own applications quantum safe. As part of its initiatives, IBM is also delivering continuous compliance capabilities. Misconfigurations are a significant factor for introducing risk; IBM's z Security and Compliance Center (zSCC) allows clients to gain visibility in compliance risk as means to reduce risk.

On July 5, 2022, NIST announced the first four algorithms selected to become part of NIST's post-quantum cryptographic standard[6]. Three of the four selected standards were developed IBM, collaborating with industry and academic partners. Two of those algorithms, CRYSTALS-Kyber public-key encryption and the CRYSTALS-Dilithium digital signature algorithms, were chosen as primary standards[7].

At its most recent Think conference in May, IBM unveiled an updated and detailed roadmap for its quantum computing and 4,000+ qubit system over the next three years (2022 – 2025). The roadmap calls for IBM to build new modular architectures and networking that will allow its quantum systems — developed in-house — to have qubit counts that scale up to hundreds of thousands of qubits. IBM will rollout three new scalable architectures to enable a new class of

[5] IBM z16 with the Crypto Express 8S card provides quantum- safe APIs providing access to quantum-safe algorithms which have been selected by NIST to become part of its post-quantum cryptographic standard. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
refers to efforts to identify algorithms that are resistant to attacks by both classical and quantum computers, to keep information assets secure even after a large-scale quantum computer has been built. Source: https://www.etsi.org/technologies/quantum-safe- cryptography." These algorithms are used to help ensure the integrity of a number of the firmware and boot processes. IBM z16 is the industry-first system protected by quantum-safe technology across multiple layers of firmware.

[6] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
[7] https://research.ibm.com/blog/nist-quantum-safe-protocols

modular and networked quantum processors. The hardware will complement IBM-built intelligent software to distribute workloads “across quantum and classical resources,” to avoid traditional infrastructure challenges and limitations. These new technologies will be leveraged towards IBM's 2025 goal: a 4,000+ qubit processor built with multiple clusters of modularly scaled processors. To date, the company has shipped the IBM Eagle, a 127-qubit processor with quantum circuits that cannot be reliably simulated exactly on a classical computer and a 120x speedup in the ability to simulate a molecule using Qiskit Runtime, compared to a prior experiment in 2017. Later this year, IBM will unveil its 433-qubit processor, IBM Osprey, as well as IBM Condor, the world's first universal quantum processor with 1000+ qubits in 2023.

- **IBM Z** illustrates how IBM’s ongoing commitment to security technology and R&D has yielded tangible results. The IBM Z mainframe and the IBM LinuxONE distributions both exhibit true fault tolerance experiencing just 0.0043 minutes or just 3.15 seconds of unplanned per server downtime **annually** of ***unplanned*** per server downtime due to server flaws, compared to the 0.0055 minutes the Z and LinuxONE platforms averaged in ITIC’s 2021 Global Server Reliability poll. This is a 58% reduction in unplanned per server monthly downtime compared to the IBM Z and IBM LinuxONE III reliability scores in ITIC’s 2019 survey. The improved monthly uptime in turn, lowers the TCO of the IBM Z and LinuxONE from $12.32 per server/per minute in 2019 to $7.18 per server/per minute in the latest ITIC 2022 Global Server Hardware Security study. Overall, the IBM Z registers just 0.259 seconds of near imperceptible monthly downtime. Equally important, given the ongoing surge in security hacks and data breaches, is the IBM Z server’s superlative security. Additionally, IBM Z and LinuxONE III survey respondents also reported the quickest Mean Time to Detection (MTTD) with 97% of ITIC enterprise respondents stating their security and IT administrators were able to detect and shut down hacks on these platforms. Singularly and collectively, these results underscore the success of IBM Z and LinuxONE III offerings. The platforms have also been bolstered by IBM’s 2019 acquisition of Red Hat; this has resulted in a significant uptick of Linux workloads on the Z and LinuxONE platforms. IBM executives publicly stated the company has seen a 55% increase in Linux MIPS in the last two years and noted that 92 of IBM’s top 100 IBM Z clients run Linux workloads. Building on this strong foundation, the new IBM z16, the industry’s first quantum-safe system available on May 31, 2022, leverages CRYSTALS-Dilithium and CRYSTALS-Kyber for its key encapsulation and digital signature capabilities. Its quantum-safe secure boot technology helps to protect IBM Z firmware from quantum attacks through a built-in dual signature scheme. IBM z16’s new Crypto Express8S hardware security module (HSM) provides APIs so that their clients can integrate this quantum-safe cryptography into their applications now. IBM z16 also adds transparent memory encryption. When it comes to the cost of a data breach, Ponemon Institute’s 2022 report identifies compliance failures as one of the top three cost amplifiers of a data breach. Introduced with IBM z16, the IBM Z Security and Compliance Center is aimed at simplifying and streamlining compliance tasks. IBM z16 offers a new capability called IBM Flexible Capacity for Cyber Resiliency to help clients proactive avoid outages. With this offering, clients are able to shift production capacity between IBM z16's at different sites within seconds. Just two of the use cases for this capability are the ability to proactively avoid outages due to severe weather threats or rolling power outages and simplify disaster recovery testing which can help demonstrate business continuity compliance.

- **IBM's LinuxONE III** is based on the IBM Z platform. It specifically addresses hybrid cloud environments and utilizes the IBM Z's pervasive encryption. The LinuxONE III platform and the IBM z15 confidential computing enhancements include IBM Secure Execution for Linux, a hardware-based Trusted Execution Environment (TEE) to protect applications and data in use against insider and external threats. Both platforms also support IBM Hyper Protect Virtual Servers, which helps protect data and applications throughout the development lifecycle and incorporate the IBM Hyper Protect Data Controller, which delivers transparent, end-to-end, data-level protection and privacy. The IBM Hyper Protect Data Controller enables corporations to encrypt data, grant and revoke access to it, and maintain control of it — even as it moves off the system of record**.** The result: IBM LinuxONE III shared the highest security and reliability rankings in ITIC's 2022 poll with 97% of LinuxONE III enterprises detecting and shutting down data breaches "Immediately or within the first 10 minutes" of the attack. IBM LinuxONE III (and the upcoming LinuxONE IV) is the foundation for the IBM Cloud Hyper Protect Services suite of offerings in the IBM Cloud including a IBM Cloud Hyper Protect Crypto Services, cloud data encryption with Keep Your Own Key capability backed by a dedicated cloud HSM service enabling multicloud key management

- **IBM Power** a 95% majority of IBM Power customers reported their IT and security administrators were able to detect and thwart attacks "Immediately or within the first 10 minutes" of a breach. IBM Power9 scale-out systems have been out three years. The latest generation Power10 servers began shipping in September 2021. And they provided customers with a big boost in security and reliability. In ITIC's latest 2022 Global Server Hardware, Server OS Reliability Report, the IBM Power servers cut downtime by 42 seconds per server, per month — from 1.42 minutes of downtime down to just one minute of unplanned downtime per server on a monthly basis. Those reliability improvements enabled IBM Power customers to lower the cost of a single minute of per server downtime calculated at $100,000 hourly down to $1,670 per server, per minute in 2022. This is a reduction of 42% or $701 compared to the $2,371 of per server, per minute costs the IBM Power servers registered in ITIC's 2021 Global Server Hardware Server OS Reliability study. With the Power10 models, IBM made support for mission critical workloads, advanced analytics, in-memory databases and embedded security top priorities. All of the IBM Power models are hybrid cloud ready. IBM Power has security built in at all layers in the stack — processor, systems, firmware, OS and hypervisor. With accelerated encryption built into the chip, data is protected in motion and at rest. IBM claims that its PowerVM hypervisor has no reported security vulnerabilities. The IBM Power10 is designed for energy efficiency and performance in a 7nm form factor. IBM estimates this will yield improvements of up to 3x greater processor energy efficiency, workload capacity, and container density than the Power9. The latest Power10 servers incorporate a variety of advanced capabilities including support for multi-petabyte memory clusters which will expand cloud capacity to support memory-intensive workloads. IBM Power10 offers hardware-enabled security capabilities like transparent memory encryption for end-to-end security. The IBM Power10 processor is engineered to achieve significantly faster encryption performance with quadruple the number of AES encryption engines per core compared to IBM Power9 for today's most demanding standards and anticipated future cryptographic standards like quantum-safe cryptography and fully homomorphic encryption. It also brings new enhancements to container security.

Lenovo Security Initiatives

Lenovo ThinkSystem Security Results

- **Lenovo ThinkSystem** servers tied with the IBM Power Systems and were first among all Intel x86-based servers in achieving the best security MTTD rates. An overwhelming 95% of Lenovo survey respondents said their firms' IT and security administrators detected and shut down attempted hacks and data breaches immediately or within the first 10 minutes of the penetration. This is no accident. Lenovo has made security a priority in the development of its servers, and Lenovo's technical service and support is also first-rate. Lenovo's ThinkSystem servers recorded reliability improvements in ITIC's 2022 Global Server Hardware Security survey achieving their best uptime to date: 1.10 minutes of unplanned monthly per server downtime due to hardware and security related issues. The Lenovo ThinkSystem servers' high rate of between "five and six nines" of reliability and uptime improves security, lowers TCO and increases ROI. In monetary terms, a business that assumes losses of $100,000 for one hour of downtime on a Lenovo ThinkSystem server running a mission critical business application could potentially lose $1,854 per minute/per server. By contrast, Dell PowerEdge server customers, who average 26 minutes of unplanned monthly per server downtime, could see potential monetary losses of $43,420. This makes Lenovo ThinkSystem servers over 23x more cost effective than rival Dell PowerEdge servers.

Lenovo's Latest Servers Span Network Edge to Hybrid Cloud

Lenovo also continues to upgrade the features and functions of its servers to address organizations' requirements for security, sustainability, manageability and scalability regardless of location – from on-premises data centers; to remote offices; to the network edge; the cloud and hybrid work situations.

- In March 2022 Lenovo unveiled a suite of edge-to-cloud IT infrastructure solutions optimized to address remote and hybrid work situations. The latest offerings include the single-socket ThinkSystem V2 Servers, which are flexible, energy-efficient, and low-noise solutions designed to allow customers to manage constrained spaces inside. They are also well suited for network edge deployments. The single-socket ThinkSystem ST50 V2, ST250 V2 and the SR250 V2 servers offer companies simple solutions that are easily tailored for running their business, including support for business-critical applications in retail, manufacturing, and financial services.
- The line also includes the ThinkEdge SE450, Lenovo's latest AI server for the network edge which delivers optimal bandwidth. The Lenovo SE450, bolsters security with both physical and electronic features and capabilities[8] all aimed at protecting data assets and improving reliability. The SE450 has 10 to 36 server cores with up to 1TB of memory; it supports broad-wired and wireless connectivity and it can continuously operate at temperatures between 5°C and 45°C. Lenovo is also targeting midrange and high end enterprises with its SR630 V2 Rack server which supports data analytics, hybrid cloud, hyperconverged infrastructure, video surveillance and high performance computing.

Overall, Lenovo has constructed and executed an excellent and effective tactical and strategic security strategy. During the height of the COVID-19 global pandemic (from 2020 through 2021), many organizations shifted to a remote workforce for workers and students alike. Overburdened IT and security administrators were extremely challenged to maintain security and protect data assets. ITIC's survey data indicates that security and data breaches are the top cause of unplanned downtime, according to 78% of respondents. This is a 22% increase from the 56% of corporations who identified security issues as the main source of downtime three years ago in 2019.

The improvements have fortified the embedded security of ThinkSystem servers during the past four years even as security attacks soared by double digits.

ITIC's latest 2022 Global Server Hardware Security Lenovo-specific survey results show:

- Out of an estimated 60 ***attempted*** data breaches against Lenovo ThinkSystem servers in the last 12 months, the Lenovo survey respondent corporations only reported one (1) successful penetration.
- In 2022, only two (2%) percent of Lenovo ThinkSystem servers experienced downtime due to a hack attack. This is down from four (4%) percent of Lenovo ThinkSystem servers that suffered unplanned downtime due to a security attack in 2021.
- On average Lenovo ThinkSystem server customers said they experienced approximately three (3) minutes of unplanned per server downtime on their mission

[8] Lenovo ThinkEdge SE450 Edge Server. URL: https://lenovopress.lenovo.com/lp1540-thinkedge-se450-edge-server#security

critical servers due to security issues experienced by mission critical systems in the past year. This is the best result among all x86 server vendors.

- And 95% of Lenovo ThinkSystem server customers reported they were able to identify and thwart attempted security penetrations "immediately or within the first 10 minutes." This is an increase of three (3%) percent up from the 92% of Lenovo server respondents who said they identified and thwarted security attacks in 2021.

Overall, Lenovo's Product Security Program has had a net positive impact on thwarting security attacks and mitigating risk to an acceptable level**.**

Cisco UCS Security Survey Highlights

- **Cisco's Unified Computing System (UCS)** continues to score well and it bested the 2.3 minutes of per server downtime that it first achieved in ITIC's 2020 Global Server Hardware, Server OS Mid-Year Update Survey. From January through August 2022, Cisco's servers experienced two (2) minutes of unplanned per server monthly downtime. This is no mean feat considering that many Cisco UCS servers are positioned at the network edge which is on the front line of security attacks. Despite this, 87% of Cisco UCS survey respondents said they were able to detect, isolate and shut down security hacks "immediately or within the first 10 minutes." Cisco UCS survey respondents also reported that the servers experienced seven (7) successful security hacks each over the last 18 months. In response to the increase in data breaches, Cisco began publishing the Cisco UCS Hardening Guide. The document is available for free download. It contains detailed information to help users secure Cisco UCS platform devices to improve network security. Structured around the three planes by which the functions of a network device are categorized, this document provides an overview of each Cisco UCS Software feature and references related documentation. Additionally, Cisco introduced a number of management and performance upgrades aimed at improving TCO and accelerating installation and deployment. Cisco claims its UCS will allow an 86% reduction in cabling, and allow provisioning in a matter of minutes (rather than days or weeks), while reducing capital expenses by more than 40%. Manufacturers assure users of 100% compatibility between and among components. And load balancing is a non-issue.

HPE Security Survey Highlights

- **HPE's Superdome** line of servers (including the Integrity and Flex models) also exhibit high reliability of five and six nines for a 92% majority of its customers. And 89% of HPE survey respondents said their firms discovered and shut down security breaches "Immediately or within the first 10 minutes." The ITIC survey data shows that HPE Superdome servers each experienced three (3) successful security hacks within the last 18 months. This puts the HPE hardware platforms in the top five most secure systems. The Superdome portfolio also benefits from the inherently strong stability of the HPE hardware. HPE has made security, feature/performance innovation and after-market technical service and support, its top priorities. All of this is critical in the increasingly insecure, complex and interconnected Digital Age. HPE is well entrenched in corporate enterprises from SMBs to the largest multinational businesses. The HPE Superdome Flex Server features RAS capabilities and end-to-end security to protect vital workloads. The HPE Superdome Flex Server, for example delivers scalability of up to 32 sockets. This is 2.3x the scalability of prior generation servers. It also features an In-memory design and memory capacity of 768GB - 48 TB in a single platform. HPE Superdome Flex Server has a modular design that scales flexibly from 4- to 32-sockets in 4-socket increments. HPE also says the Superdome Flex server has a more cost efficient entry point for mission-critical workloads at 4 sockets, it delivers up to 45% lower acquisition cost compared to previous models. HPE also emphasizes reliability claiming that the Superdome Flex Server embedded RAS capabilities deliver five nines - 99.999% - of single-system availability. HPE also asserts that the Superdome Flex server reduces human error via its predictive fault handling Error Analysis Engine. Security and human error are two issues that are closely linked and undermine security and reliability. This engine predicts hardware faults and initiates self-repair with no need for human intervention or “operator assistance.” It contains errors at the firmware level, including memory errors, before any interruption can occur at the Operating System layer with HPE's “Firmware First” approach. HPE also provides continuity for Linux workloads with its HPE Serviceguard for Linux (SGLX) high availability and disaster recovery clustering solution. This enables businesses to safeguard their servers running Linux against a multitude of infrastructure and application faults across physical or virtual environments over any distance.

Huawei Security Survey Highlights

Over the last five years Huawei, headquartered in Shenzhen, China has emerged as one of the top five server hardware vendors worldwide with its high end KunLun mission critical server and its general purpose FusionServer x-86-based servers.

- Based on ITIC’s 2022 Global Server Hardware, Server OS Reliability Survey and the ITIC 2022 Global Server Hardware Security Survey, the Huawei KunLun and Fusion Servers are also among the top three most reliable and secure hardware platforms. A 91% majority of Huawei survey respondents noted their IT and security administrators detected and shut down attempted breaches “Immediately or in under 10 minutes.” Huawei survey respondents indicated that the KunLun and Fusion servers each experienced 1.5 hacks during the last 18 months. Since 2015, Huawei fortified the advances features, inherent security and overall performance of its servers. To successfully compete with rivals including Cisco, Fujitsu, HPE, IBM, Inspur, Lenovo and others, Huawei’s server family includes general purpose rack and blade servers to mission critical hardware to address high performance computing (HPC). Huawei has also imbued its servers with advanced capabilities to support emerging compute intensive applications like AI, big data analytics, deep learning and machine learning. Huawei is emphasizing security via best practices documents on “How to Build a Proactive Defense

System" via its HiSec solution which enables more intelligent threat detection, threat response, security operations and maintenance. Huawei says HiSec improves the threat prevention capabilities of enterprise networks and the telecom infrastructure, thus increasing security O&M efficiency and reducing O&M costs. In addition, Huawei offers a number of new security offerings for its various server solutions in the data center, the cloud and the network.

Conclusions

Security is the number one issue that negatively undermines the reliability and availability of server hardware, server operating systems and business critical applications. It will almost certainly remain so for the foreseeable future. Security hacks and organized hacking groups are organized; the attacks themselves are increasingly dangerous, stealthy and effective.

To combat and thwart the ever-growing threats, the server hardware vendors and their customers – from small businesses to the largest enterprises, must counter with strong, inherent security technology coupled with security best practices, procedures and enforcement.

ITIC's 2022 Global Server Hardware and Server OS Reliability Survey findings indicate that the IBM Z mainframe, IBM Power Systems, followed closely by Lenovo ThinkSystem, Huawei KunLun and HPE Integrity Superdome servers continue to solidify and improve their status as the most reliable server hardware offerings. The IBM Z enterprise platform stands alone in delivering consistent security and fault tolerant reliability of seven nines – 99.99999% reliability for upwards of 97% of its enterprise users. Excluding super computers and high availability (HA) hardware no server platforms come close to achieving the Z's level of reliability, availability and near-flawless uptime and security.

Nine-in-10 survey respondents affirmed that the IBM Power Systems and Lenovo ThinkSystem solutions both registered five and even the vaunted six nines - 99.999% and 99.9999% - of reliability and availability. The IBM Power Systems and Lenovo ThinkSystem platforms are up to 40x more reliable and as much as 36x more cost effective and economical than the worst performing unbranded White box servers.

In another notable achievement, IBM and Lenovo captured first or second place rankings in every reliability and availability category or, they tied for first or second place in every uptime, security or manageability metric in the survey.

All organizations, irrespective of size or vertical market must make security a priority and work closely with their vendors to mitigate security risks to an acceptable level.

Every added second and minute of server downtime and application unavailability negatively impacts business operations, employee productivity and revenue.

Server security (and by association, server operating system, application and networking device), like reliability are fluid, not static. No server, no component part – hard drive, memory or CPU; operating system; application, device or connectivity mechanism is immune from inherent problems or failures.

Servers are the bedrock upon which the entire network infrastructure and extended network ecosystem rests. When servers fail, data access is denied. Business stops. Productivity ceases. Revenue suffers. Some 88% of all corporations now require a minimum 99.99% reliability for their firms' server hardware, operating systems and main line-of-business applications to ensure productivity and deliver uninterrupted data access. High reliability and availability also safeguards the corporation's daily operations, data assets and intellectual property (IP), employees' personnel information, business processes and revenue stream.

In 2022 and for the foreseeable future, security, human error and end users will continue to present the biggest potential threats to undermine the reliability and availability of servers, operating systems and applications.

The negative effects and impact of the global pandemic will likely persist for years – especially with regards to security and data breach threats.

This is the new normal: organized hackers are here to stay. They will continue to use this pandemic to exploit vulnerabilities. Hackers will continue to seize every opportunity to exfiltrate corporate and employee data assets for profit. Every added second and minute of server downtime and application unavailability negatively impacts business operations, employee productivity and revenue.

A significant portion of enterprise servers and applications now reside in virtualized cloud environments and at the network edge. In post-pandemic 2022, a substantial amount of organizations continue to support and adhere to a hybrid work environment in which employees and independent contractors work remotely for two, three and even four days a week. Therefore, organizations and their IT departments and security administrators still face substantial challenges to manage far-flung employees and devices to ensure the uptime and availability of all sensitive data assets.

Security is extremely crucial. Vendors must continue to fortify embedded server security; quickly supply fixes and patches when flaws are found and work with customers to provide prescriptive guidance. Corporate enterprises must also assume responsibility to ensure the reliability and security of the entire server and network infrastructure and key business applications in datacenters and the cloud. It's critical that companies implement and enforce strong security policies and procedures for **all employees,** particularly teleworkers and students and any fulltime or temporary employee, that use their personal devices to access the corporate network. Security and reliability are core foundational elements of the network infrastructure. Both are necessary to ensure uninterrupted daily operations, defend IP assets, secure, continuous data access and to protect the revenue stream.

ITIC's 2022 Global Server Hardware, Server OS Security Survey emphasizes the need for **all** organizations, irrespective of size and vertical industry to proactively and continually strive to identify and thwart the growing array of increasingly sophisticated and targeted cyber attacks.

That means implementing all appropriate security measures. Enacting and enforcing strong computer security policies and procedures for **all company employees** – from C-suite executives down to company contract workers and interns is imperative. Businesses must allocate adequate budgets for purchasing security products and devote the necessary time and appropriate internal and external third party resources to provide end users and IT administrators and security professionals with the security tools and security training.

There is no such thing as 100% foolproof security. However, multi-layer security defenses, bolstered by vulnerability testing and security awareness training can thwart the number of data breaches and Ransomware hacks and mitigate risk to an acceptable level.

In addition to IBM and Lenovo, mission critical systems HPE, Huawei and Cisco all performed extremely well and continued to improve security, reliability and uptime.

Cisco's UCS servers maintained the security and reliability gains in ITIC's latest 2022 Global Server Hardware, Server OS Security Survey. This is critical. A significant portion of Cisco's UCS servers are deployed at the network edge - long considered to be among the most vulnerable points of the ecosystem.

No vendor can rest on its laurels. Competition in the worldwide global server hardware market is intense. It is, and will remain a buyer's market. While many companies, particularly SMBs, make their purchasing decisions based on price, a significant portion of enterprises choose to purchase more robust hardware, equipped with embedded security, advanced management, AI and big data analytics functionality.

The survey data shows that corporate enterprises place an extremely high value on after-market vendor technical service and support. Companies increasingly rely on their server and cloud vendors to bolster the manpower and expertise of their own internal corporate IT and security administrators who find themselves increasingly challenged to monitor end-to-end security vulnerabilities throughout their ecosystems. Corporations require vendors to act quickly if and when problems arise. Vendors should provide customers with realistic recommendations and prescriptive guidance for server-based security configurations.

As always, ITIC maintains that vendors also bear the responsibility to deliver patches, fixes and updates in a timely manner and to inform customers to the best of their ability regarding any known incompatibility issues that may potentially impact performance. Vendors should also be honest with customers and notify them of problems or delays in delivering replacement parts.

Recommendations

No server platform, server OS or business application will provide foolproof security. However, IBM, Lenovo, Huawei, HPE and Cisco which are among the most reliable server platforms also provide the greatest levels of inherent security. This enables customers to achieve the greatest economies of scale and safeguard their sensitive IP and data assets. Security is a 50/50 proposition. While vendors must deliver robust security, corporations are responsible for maintaining the reliability of their server and overarching network infrastructure. ITIC strongly advise businesses to:

- **Take Inventory.** Know what's on your network. This means cataloguing ***all*** servers, crucial main line-of-business applications; network devices (firewalls, routers) across the entire network ecosystem including the datacenter, remote offices, public, private and hybrid clouds, IoT devices and the network edge.
- **Right size server hardware**. Server hardware must be robust enough to accommodate current workloads as well as anticipated increased workloads and larger applications.
- **Regularly replace, retrofit and refresh server hardware.** This means keeping up-to-date with the necessary patches, updates and security fixes ***as needed*** to maintain system health and achieve peak system performance.
- **Update Software.** Whenever possible, never stay more than two revisions behind on server operating systems and key server-based firmware and applications.
- **Produce regular firmware and software updates with security fixes**
- **Test all security products.** This should be done an as needed basis.
- **Establish a Product and Business Security Incident Response Team (PSIRT).** The team should keep a detailed record of all incidents and activities including attempted and successful hacks and the length, duration and remediation costs, where applicable.
- **Validate the security of all business partners and suppliers.** Ideally, organizations should do this on a quarterly or as-needed basis.
- **Vendors should provide product security hardening guidance to customers.** Ideally, vendors should provide at least once a year.
- **Implement strong security policies and procedures.** It is imperative that companies of all sizes and across all vertical market segments construct corporate wide security

policies and procedures. Disseminate them via hard copy and email to all employees. The computer security policies should be an integral part of the overall corporate guidelines and should contain specific provisions and penalties for first, second and third offenses. Companies are also advised to have all employees attend mandatory computer security training, similar to sexual harassment training.

- **Closely Monitor Service Level Agreements (SLAs).** Pay close attention to SLA contracts to ensure that your firm's hardware, software vendors and cloud vendors meet or exceed the terms of SLAs to deliver agreed upon responses and remediation to security and data breaches.
- **Both customers and server vendors should conduct security vulnerability testing of their products.** Given the continuing spike in all types of security hacks and data breaches e.g., Ransomware, Phishing attacks and CEO Fraud to name a few, all corporate enterprises should conduct vulnerability testing at least once a year and as-needed. ITIC recommends that corporations work with independent third party experts.
- **Construct a Governance and Remediation plan.** Have a remediation and governance plan in place to quickly respond in the event your firm is successfully hacked. Designate a hierarchy of who's in charge in the event of a data breach or network outage. The Governance and Remediation plan should also assign and designate specific tasks for specific groups and individuals. Make sure the plan also includes the pertinent contact information for all vendors and third party service providers.
- **Train and certify Security and IT Administrators.** Ensure that Security and IT professionals receive adequate training and have the necessary security certifications.
- **Train End users.** Ensure that end users as well as contract workers and temporary employees receive adequate security awareness training on the latest e~~E~~mail and Phishing scams and Ransomware threats.

Methodology

ITIC's *2022 Global Server Hardware Security Reliability Survey*, polled C-level executives and IT managers at over one thousand corporations worldwide from January 2022 through June 2022. The independent Web-based survey included multiple choice questions and one Essay question. To maintain objectivity, ITIC accepted no vendor sponsorship. No survey participants received any remuneration. ITIC analysts also conducted two dozen first person customer interviews to obtain valuable anecdotal data and gain deeper insights and contextual knowledge of the impact and implications of security vulnerabilities and data breaches on the reliability of the corporate server and network infrastructure. Respondents included C-suite executives, IT and security administrators and end users. ITIC employed authentication and tracking mechanisms to prevent tampering and to prohibit multiple responses by the same parties.

Survey Demographics

ITIC polled 1,550 companies of all sizes and across 28 vertical markets for the survey. Corporations of all sizes were well represented. Respondents came from companies ranging from small and medium businesses (SMBs) with fewer than 50 workers, to multinational enterprises with over 100,000 employees.

All market sectors were equally represented: SMBs with one-to-100 employees accounted for 24% of the respondents. Small and medium enterprises (SMEs) with 101-to-1,000 workers represented 28% of the participants. The remaining 43% of respondents came from large enterprises with 1,001 to over 100,000 employees. Survey respondents hailed from 49 different vertical markets. Approximately 65% of respondents hailed from North America; 35% were international customers who hailed from 22 countries throughout Europe, Asia, Australia, New Zealand, Central/South America and Africa.

Appendices

This section provides links to the various ITIC statistics and surveys cited in this Report.

ITIC Website and links to survey data and blog posts:

https://itic-corp.com/security-data-breaches-top-cause-of-downtime-in-2022/

https://itic-corp.com/ibm-lenovo-hpe-and-huawei-servers-remain-reliable-and-secure-as-security-hacks-data-breaches-surge/

https://itic-corp.com/44-of-enterprises-say-hourly-downtime-costs-top-1-million-with-covid-19-security-hacks-and-remote-working-as-driving-factors/

https://itic-corp.com/itic-2021-global-server-hardware-server-os-reliability-survey-results/

https://itic-corp.com/blog/2019/08/itic-poll-human-error-and-security-are-top-issues-negatively-impacting-reliability/

http://itic-corp.com/blog/2017/07/ibm-z14-mainframe-advances-security-reliability-processing-power/