TechChannel

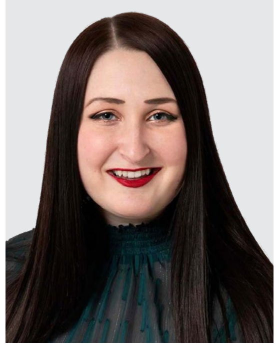
How to Create a Security Strategy That’s Built to Last

→ Security expert Chad Mead on building a reliable security strategy

→ ITIC survey reveals zSystems, LinuxONE III and Power Systems security and reliability strengths

SPONSORED BY BLAIR TECHNOLOGY SOLUTIONS + FLAGSHIP SOLUTIONS GROUP + CONVERGE ENTERPRISE CLOUD contents

Building and Bolstering an Effective Security Strategy



Security through obscurity—hiding security flaws and vulnerabilities—was once a common and safe approach to securing data. Today, hackers take a broadcast approach to attacks rather than targeting specific systems—meaning security through obscurity is no longer viable.

More accessible, faster technology; economic and political volatility; and evolving hacking techniques mean that security personnel face different challenges than they did five years ago. As a result, organizations must develop a reliable security strategy to keep up with data security needs.

Part of this strategy begins with the security basics: assess your environment, implement end-user education, enforce password policies, develop a Zero-Trust design. In this e-book, Chad Mead, vice president, global mainframe and security consulting, Ensono, shares his thoughts on these and other elements to include in your security strategy.

Amping up security also means choosing the most secure platforms on the market—starting with the zSystems, LinuxONE III and Power Systems platforms, which posted the best across-the-board reliability scores in the 2022 ITIC Global Server Reliability survey for the 14th consecutive year. This e-book also explores other findings from the survey and highlights these platforms' greatest security and reliability strengths.

Security trends simply constitute a new normal—meaning your plan should be built to adapt and evolve based on these changing needs.

Keelia Estrada Moeller, Senior Editor

Patch the Hole Before You Bail Water: Implementing a Reliable Security Strategy

Security expert Chad Mead on how to build a reliable security strategy in any industry, on any platform

BY DAVA STEWART

Chad Mead, vice president, global mainframe and security consulting, Ensono, has witnessed an increase in technology speed and accessibility during his career. While this is good for users and business, it is also good for hackers.

At one time, **security through obscurity** was a relatively safe approach. Hiding security flaws and vulnerabilities offered protection from hackers who gained access through known vulnerabilities. Today, hackers have largely abandoned targeted attacks for a broadcast approach so security through obscurity no longer works. “Hackers can attack anyone, anywhere, anytime,” cautions Mead.

More accessible, faster technology; economic and political volatility; and evolving hacking techniques mean that security personnel face a new set of challenges compared to even five years ago. Organizations seeking to build or reinforce a reliable security strategy need to consider the pieces of the security puzzle that are often overlooked.

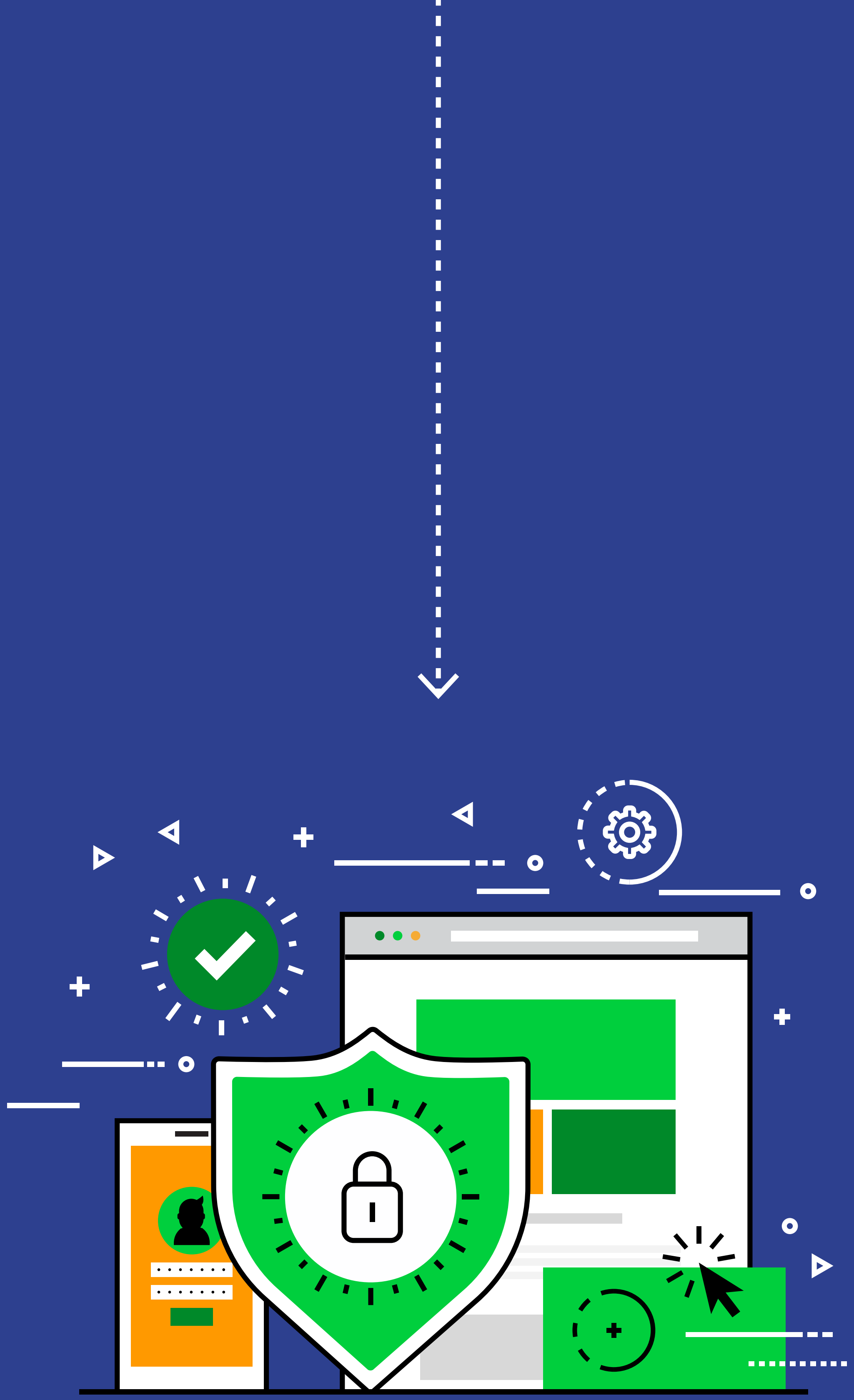
Begin With the Security Basics

“People are bailing water out of a boat with a hole in it and not trying to fix the hole,” says Mead. Even though so much has changed in IT, the fundamentals of a solid security strategy remain the same:

1. **Assess the environment regularly.** Plenty of tools exist, regardless of industry, architecture or other variances. Regular risk assessments provide information on current threats, as well as emerging threats. Assessments also provide a sort of scorecard for tracking improvements.

2. **Implement end-user education.** Phishing schemes have become incredibly sophisticated, and although most people have been using the internet for decades, end users are still not generally aware of cyberattacks or the need for cybersecurity protocols.

3. **Develop and enforce password policies.** The 2021 Data Breach Investigations Report by Verizon found that compromised passwords were responsible for more than 80% of hacking-related breaches. The National Institute of Standards and Technology (NIST) password guidelines, designed for federal agencies, provides a highly credible and reliable framework for developing password policies.



> **“Find a security methodology and a framework that fits the business, and regularly check against it to find out if you’re making progress.”**
>
> —Chad Mead, vice president, global mainframe and security consulting, Ensono

4. **Enforce a Zero Trust design.** “The Zero Trust model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity,” according to the **National Security Agency.**

5. **Create a plan for vulnerability management.** Make sure this plan is aligned with organizational needs and structured as another vital part of a functional security strategy. **Gartner recommends** approaching vulnerability management based on the threat landscape of the individual organization, rather than “a mythical standard.” Mead notes that one of the challenges of vulnerability management is that it often bounces between applications and infrastructure.

There Is No Silver Bullet for Security Issues

No single vendor solution will solve all security issues. Rather than seeking a vendor solution, Mead suggests that security professionals use a maturity assessment to determine where the organization needs to improve. This assessment should be revisited regularly. “Find a methodology and a framework that fits the business, and regularly check against it to find out if you’re making progress,” he says.

If you think of security as a scale from zero to five, figure out where the business needs to be on that scale. It may not need to be a five. Some industries require significantly more secure IT operations than others. Once the goal is identified, begin making progress toward it.

The task of securing IT operations is daunting, but thinking of it as a journey rather than a destination helps. Consistent, continual improvement of security throughout the journey is something Mead believes many teams overlook. Continually elevating security and improving the effectiveness and remediation around the security program makes the task more manageable than only thinking about reaching the goal. “You should always look at how to get better,” advises Mead.

Consistency is an important part of the path to better security. “Having all of those policies in place is useless without doing them consistently,” says Mead. Assessing the IT environment now and then doesn’t make the system more secure, much like changing the oil in your car inconsistently doesn’t protect the engine. Changing it after three months, then not again for two years is not going to keep things running smoothly.

Mead notes that there are many existing frameworks and maturity assessments to use within those frameworks. “Having an independent third party come in and help is a good way to show the executive team or the board of directors that you’re making progress,” Mead says. It’s one way to verify progress. An annual or biannual check against the framework reveals increasing maturity—or not.

Static Strategy, Variable Implementation

The elements of a good security strategy don’t differ regardless of platform, according to Mead, but the implementation approach will vary. “By default, generally, mainframes are more secure,” says Mead. Yet, more controls don’t overcome human nature. “I can make a mainframe just as vulnerable as any other platform,” he says.

Some of the increased security of the mainframe is thanks to the fact that not too many hackers are familiar with zSystems, but that isn’t something to rely on. “As bad guys continue to figure out how to do things and where the better value is, they’ll invest,” Mead predicts.

The solution to increasing security on any architecture, including the mainframe, is people. Increasing awareness and concern is crucial. “Start with, and spend the most time on, the most vulnerable assets, then move through the environment,” Mead advises.

Ransomware: Growing, But Not New

Ransomware is a growing threat, but it’s certainly not a new one. Mead points out that ransomware has been around for at least 20 years, but currently, much more publicity is devoted to high-profile cases.

Other technology experts agree. “While ransomware is not a new cybersecurity risk, it is a threat that received attention at the highest levels of government,” according to a TechTarget article titled “**Ransomware Trends, Statistics and Facts in 2022.**” Ransomware **doubled in frequency** in 2021 and is now part of 10% of all breaches. More than **130 different strains** of ransomware have been detected since 2020, and **14 of the 16** critical infrastructure sectors in the United States have been hit by ransomware attacks.

BLAIR
TECHNOLOGY SOLUTIONS

How well are you protected from cyber threats on your IBM Power Systems platform?

Configuration of IBM i Security

- ✓ User authority settings
- ✓ Controlling access to System Service Tools
- ✓ System values settings (QSecurity System Value, QALWOBJRST, QFRCCVNRST,...)
- ✓ IBM i server-configuration settings (FTP, Telnet,...)
- ✓ Staying current on OS releases and PTFs

Physical Protection

Files and Fields Security

- ✓ Encryption
- ✓ Tokenization of field data
- ✓ Anonymization
- ✓ Object-level authority management

Security of System Access

- ✓ Password management
- ✓ Multi-factor authentication
- ✓ Network-access control
- ✓ Command control

Database Security

- ✓ TCP/IP address and port
- ✓ Session start and end times
- ✓ Object names (for example, tables or views)
- ✓ SQLSTATEs
- ✓ Job and job numbers
- ✓ SQL statements and variables

Network Security

Application Security

- ✓ Query strings
- ✓ Requests and answers
- ✓ Scripts
- ✓ Memory leakage
- ✓ Cookies and session handling
- ✓ Authentication
- ✓ Execution of third-party components
- ✓ Data injection

Take the first step in protecting your IBM Power Systems by understanding your risk. Let us help you:

- ✓ **Discover** security vulnerabilities and gaps
- ✓ **Get advice** on best practices from our experienced IBM security experts
- ✓ **Gain confidence** knowing you’re moving in the right direction to cyber resilience

Request Your IBM i Security Assessment

Platinum Business Partner IBM

www.blairtechnology.com/microsite/IBM-Power

Mead recommends having a good asset inventory as an element of securing against the risk of a ransomware attack, noting, “It’s hard to rebuild if you don’t know what you have.” He also says that keeping an up-to-date asset inventory is a bit like painting the Golden Gate Bridge: as soon as you finish, it’s time to start over.

“Preserve an older backup—six months to one year,” suggests Mead. Ransomware attacks can lay dormant until they are activated, so keeping an older backup is essential. “If you get hit with an attack, would you rather have the newest and best, or would you rather be up and running?” he asks.

4 Final Security Tips

Four final tips from Mead for covering the most often overlooked pieces of a reliable security strategy include:

1. **Consider what happens if the power goes out** for days or even weeks, both in terms of data centers and remote workers. Events such as the ice storms in Texas in 2021, for example, mean that security programs must consider how business can continue to operate without power for extended periods of time. Look at solutions such as generators for data centers or alternative locations for workers.

2. **Keep older threats in mind.** DDOS attacks were prevalent for a period of time as a main threat. Now that ransomware attacks are the focus, some companies seem to forget about the older risks.

3. **Make your attack surface as narrow as possible.** It’s easier to attack a sheet of plywood than it is a two-by-four.

4. **Start an initiative to protect middleware immediately.** Figure out who is responsible for what and follow all the tendrils associated with middleware.

FAQs on the Log4Shell Security Vulnerability

BY JESSE GORZINSKI

You've likely heard of the Log4Shell (aka "LogJam") security vulnerability that was recently published. It has gotten a lot of press, and understandably so; it can be easy to exploit, and it can allow an attacker to perform remote code execution. Here are answers to a few FAQs on the Log4Shell vulnerability:

Q: Where can I find the official documentation on this vulnerability?

The vulnerability has been assigned an ID of CVE-2021-44228. As with most security vulnerabilities, it's recorded in the National Vulerability Database (NVD). The official documentation at NVD can be found here.

Q: What OSes does the Log4Shell vulnerability affect?

This is a Java vulnerability, so it impacts Java applications running on any OS. It does not impact any particular OS per se, just the Java programs running within.

Q: What about Java programs that aren't "mine?"

For IBM impacts from this vulnerability, please **see this blog post** on the most up-to-date information regarding IBM products and services, including any exposures and remediation steps. For any third-party software that uses Java, contact the software vendor for information.

Get answers to more Log4Shell FAQs

IBM, Lenovo, HPE and Huawei Servers Remain Reliable and Secure

The zSystems, LinuxONE III and Power Systems platforms posted the best reliability scores in the ITIC Global Server Reliability survey for the 14th consecutive year

BY LAURA DIDIO

For the 14th consecutive year, the zSystems (formerly IBM Z), LinuxONE III and the Power Systems platforms posted the best across-the-board reliability scores in the **2022 ITIC Global Server Reliability survey** (which polled approximately 1,200 corporations across 28 vertical market segments worldwide on the reliability, performance and security of the most popular server platforms). They were closely followed by Lenovo's ThinkSystem servers, which recorded the best uptime among all x86 hardware distributions. These distributions recorded the least amount of unplanned downtime and the lowest percentage of unplanned server outages exceeding four hours annually.

This enabled the IBM, Lenovo, Huawei, HPE and Cisco servers (in that order) to deliver the most economical total cost of ownership (TCO) among all mainstream distributions in data centers, at the network edge and in hybrid cloud environments. The top performers—led by IBM, Lenovo, HPE and Huawei mission-critical servers—also delivered the strongest security and suffered the fewest number of successful data breaches.

2022 ITIC Reliability Survey Results

Unplanned server downtime

The IBM z14 and z15 and the LinuxONE III boasted their personal best and industry best reliability scores, recording just 0.55 seconds of per server unplanned downtime (see Figure 1).

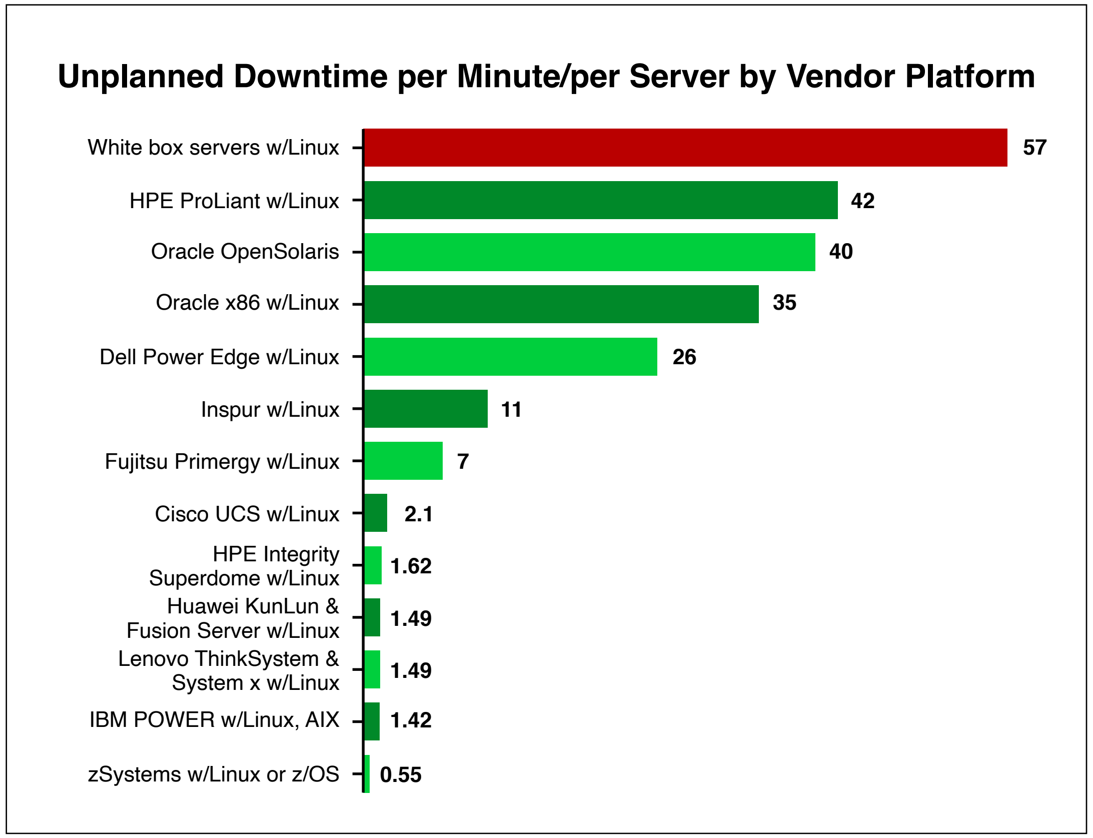


Figure 1. IBM, Lenovo, Huawei and HPE servers score top reliability marks

The IBM Power models also achieved their best uptime scores, with just 1.42 minutes of unplanned per server downtime, down from 1.49 per server/ per annum minutes in ITIC's 2021 Reliability study. The Lenovo ThinkSystem and Huawei KunLun platforms followed closely, notching the highest uptime among all x86-based servers: 1.49 minutes of unplanned per server outages, down from 1.51 per minutes in ITIC's prior reliability survey in 2021.

HPE's Superdome recorded 1.62 per minute/per server of unplanned downtime while the Cisco UCS hardware had 2.1 minutes of unplanned per server outage, down from 2.3 minutes a year ago. Inspur scored in the midrange of server platforms notching the same 11 minutes of unplanned per server, per annum downtime as they experienced in 2021. The Dell PowerEdge servers likewise registered the same 26 minutes of unplanned downtime per server unavailability as they recorded last year. Unbranded white box servers (which often run unlicensed or pirated software) again were the least reliable servers, holding steady at 57 minutes of unplanned per server downtime compared to ITIC's 2021 findings.

Reliability and continuous availability

The zSystems servers and the LinuxONE III platform are in a class by themselves: A 96% majority of zSystems customers said their businesses achieved unparalleled fault tolerant levels of seven nines (99.99999%) reliability and continuous availability, the best among all server distributions. The IBM Power distributions also garnered high reliability ratings; 93% of corporate enterprises said the POWER9 and latest Power10 models, which began shipping in September 2021, deliver a minimum of five and six nines availability/uptime, respectively.

The Lenovo ThinkSystem, Huawei KunLun and HPE Superdome servers also had high reliability ratings. Some 93% of Lenovo ThinkSystem enterprises said their businesses achieve a minimum of five and six nines server reliability, followed by 92% of respondents who estimated the HPE Superdome and Huawei KunLun hardware delivered five and six nines of uptime. Cisco Systems UCS servers—many of which are deployed at the network edge—continue to gain ground on the leaders as Cisco keeps fortifying security. Some 90% of Cisco UCS

customers said the platform delivered 99.999%, or five nines, of uptime.

Reliability metrics have a direct correlation to productivity, system and network security and corporate enterprises' overall TCO and return on investment (ROI).

Downtime charges

As Figure 2 shows, IBM z14 and z15; IBM LinuxONE III; and the POWER9 and Power10 servers deliver the most economical TCO and near immediate ROI. A single minute of per server unplanned downtime on an IBM z14 or z15 server, calculated at a rate of $100,000, now costs enterprise customers $919 (USD), down $83 compared with $1,002 in the prior survey.

Unplanned downtime of 1.42 minutes on a single IBM POWER9 and Power10 server calculated at $100,000 an hour now costs $2,371; this is a decrease of $117 compared with $2,488 per server based on 1.49 minutes per server charges in ITIC's 2021 reliability poll. These results underscore that reducing per server downtime by seconds per week, month or year delivers tangible gains in user productivity, reliability and security. Uninterrupted access to crucial

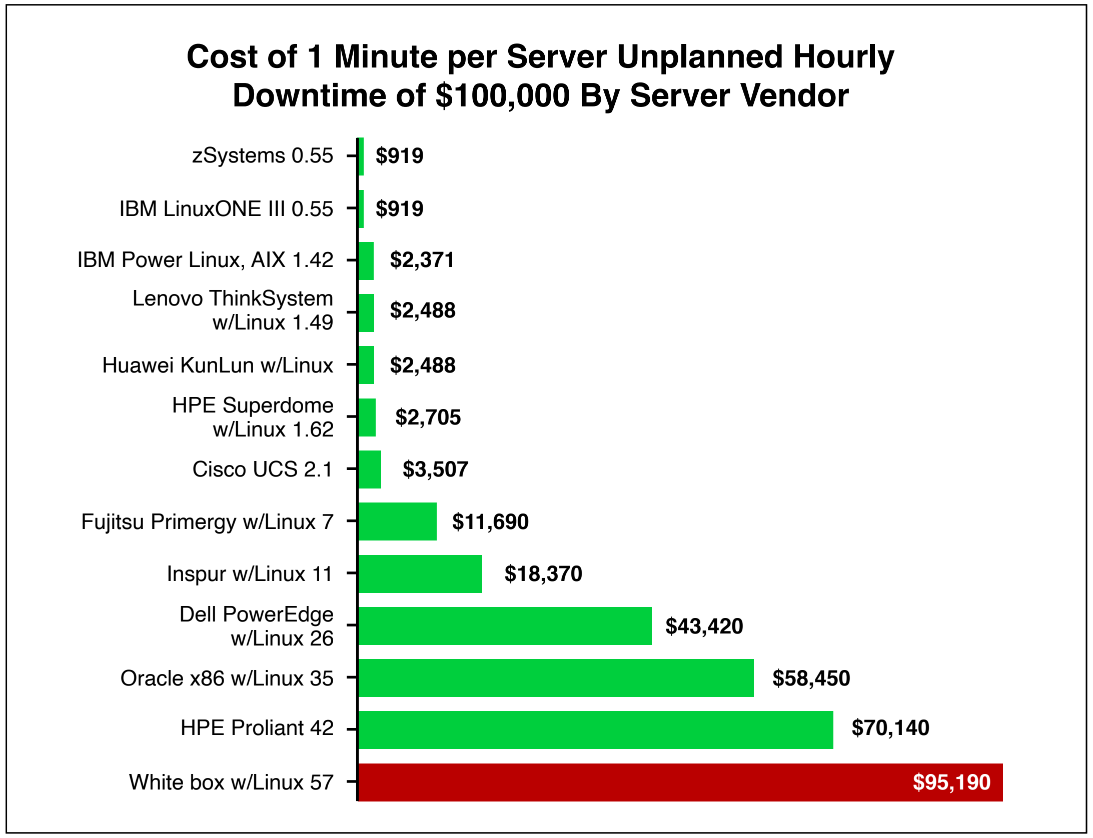


Figure 2. IBM, Lenovo, Huawei, HPE are the most reliable and economic servers

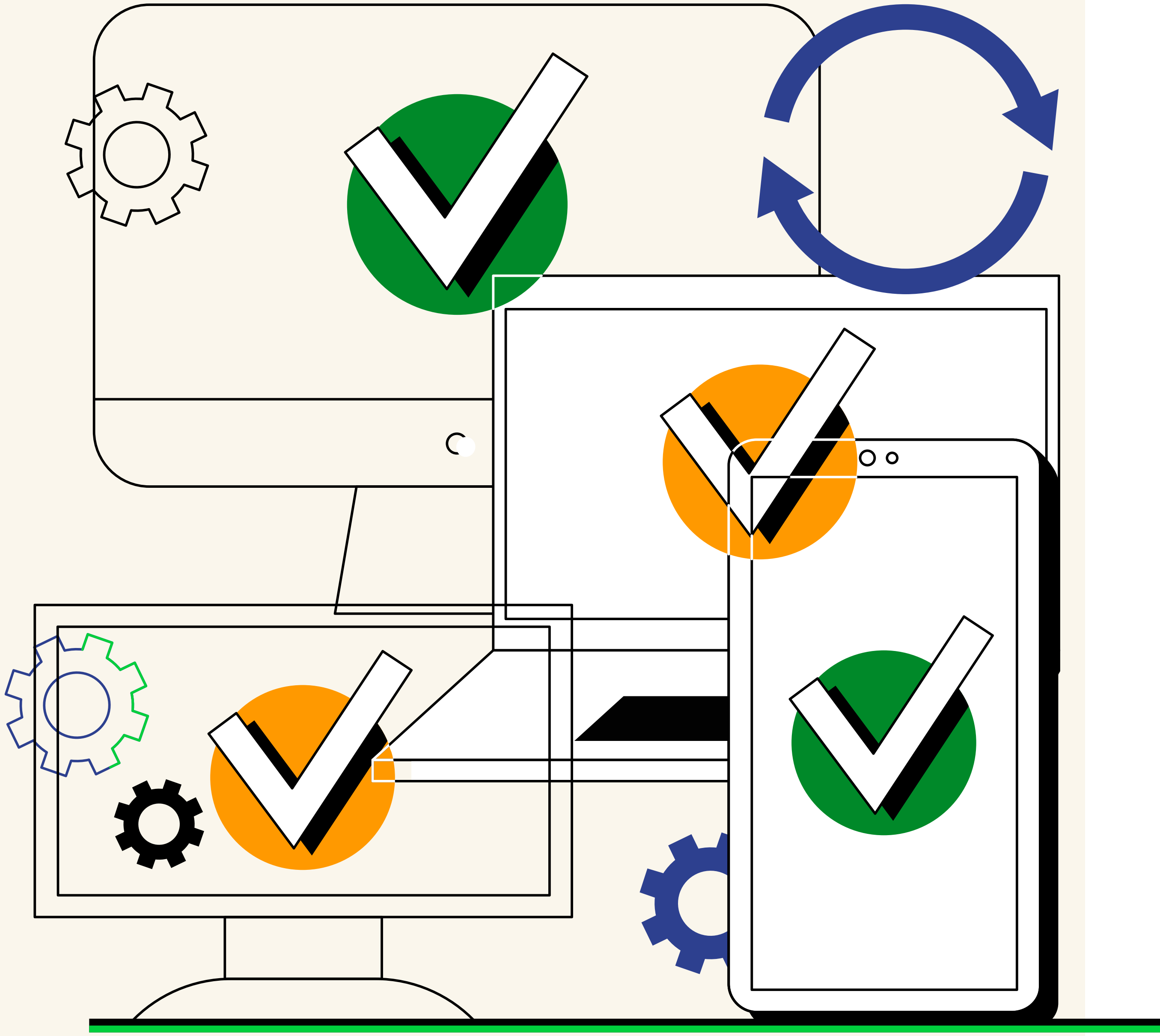
data and applications also bolsters customer satisfaction and retention and protects the organization's revenue stream.

The Lenovo ThinkSystem and Huawei KunLun and Fusion offerings averaged 1.49 minutes of unplanned per server outages. That equates to per server/per minute downtime charges of $2,488, down from $2,521 in last year's poll. Unbranded white box servers were the least reliable, with 57 minutes of unplanned per server downtime. This could cost corporations $95,190 based on $100,000 hourly downtime losses.

Server reliability directly correlates to lower TCO. For example, the $117 a zSystems or LinuxONE III enterprise saves with improved uptime of 0.04 seconds on a single server potentially delivers annual cost savings of $1,170 for an enterprise with 10 zSystems or LinuxONE III servers and $11,700 annually for a firm that has 100 servers (assuming one hour of

downtime calculates to $100,000). The savings rise exponentially for companies that estimate a single hour of downtime costs $300,000, $500,000 or $1 million or more.

ITIC's latest 2021-2022 Hourly Cost of Downtime survey indicates a single hour of server downtime totals $301,000 or more for 91% percent of mid-sized enterprises (SMEs) and large enterprises. And 44% of corporate respondents indicated their hourly outage costs exceed $1 million to over $5 million.



Security, User Error and Remote Work Are Top Downtime Causes

Other notable findings in the 2022 ITIC's Reliability Survey include:

- **Security hacks, data breaches surge.** Since the beginning of the COVID-19 pandemic two years ago, security hacks and targeted data breaches have surged by 51%, according to ITIC's latest survey data. A 75% majority of survey respondents cited security as the chief cause of unplanned downtime.

IBM z14 and z15 and the LinuxONE III boasted personal-best and industry-best reliability scores this year, recording just 0.55 seconds of per server unplanned downtime. IBM Power models also achieved their best uptime scores, at only 1.42 minutes of unplanned per server downtime.

- **Server security by vendor platform.** High-end mission-critical IBM, Lenovo, Huawei and HPE systems exhibited the strongest security. ITIC's latest Global Reliability poll similarly found that IBM, Lenovo, Huawei and HPE mission-critical servers experienced the lowest percentages of downtime due to successful security hacks and data breaches. A miniscule 0.1% of zSystems high-end enterprise servers and IBM LinuxONE III experienced a successful data breach. Just 4% of IBM Power Systems and Lenovo ThinkSystem users reported their systems were successfully hacked. And only 5% of Huawei KunLun and HPE Integrity Superdome servers suffered a security breach. Once again, unbranded white box servers had the highest percentage—51%—of successful security hacks and data breaches.

- **Human error.** Nearly two-thirds of respondent companies (65%) said human error (i.e., misconfiguration and provisioning mistakes) caused unplanned server outages.

- **IT management challenges.** Some 63% of survey participants attributed increased downtime to management and security issues related to issues like remote working and remote academic learning.

These trends are the "new normal." The ongoing shift to public, private and hybrid clouds and intelligent edge computing will accelerate. Many organizations will continue to pursue hybrid office and remote work models, making server and application reliability imperative. ■

LAURA DIDIO is principal analyst at ITIC, a research and consulting firm based in the Boston area.

New FlashSystem Storage Offerings Target Ransomware, Defend Against Cyberthreats

BY NEIL TARDY

Managing and maintaining storage networks was never easy, but over the past two years, the responsibilities and challenges that come with the job have multiplied and diversified.

Administrators must provide secure access to networks that extend beyond virtual corporate boundaries to serve an ever-growing work-from-home user base. Ransomware and other threats to data are constant, with bad actors seemingly running multiple steps ahead in their inscrutable, wearying games.

In its efforts to help customers move toward cyberresilience, IBM recently unveiled new, next-generation flash storage offerings: the IBM FlashSystem Cyber Vault and two new ultra-performant enterprise storage array models, the FlashSystem 7300 and FlashSystem 9500.

These solutions contribute to "a consistent and secure architecture. Whatever you do at the data center edge, in the core of the data center or in the cloud is exactly the same," notes Scott Baker, CMO, IBM Storage. That creates a consistent set of operations in terms of how you store, safeguard, protect and manage the data.

Learn more about the new FlashSystem offerings

This e-book was published by

TechChannel 953 Westgate Drive, Suite 107, St. Paul, MN 55114 // (612) 339-7571

staff list

Senior Editor: Keelia Estrada Moeller

Copy Editor: Emma Pitzl

Art Director: Kelsey Hanscom

Senior Marketing Manager: Noelle Heaslip

Audience Development Director: Linda Holm

Publishing Director: Mari Adamson-Bray
(612) 336-9241 // mbray@techchannel.com

Account Executive: Darryl Rowell
(612) 313-1781 // drowell@techchannel.com

Sr. Strategic Account Manager: Lisa Kilwein
(480) 428-9780 // lkilwein@techchannel.com

This e-book could contain technical inaccuracies or typographical errors. Also, illustrations shown herein may show prototype equipment. Your system configuration may vary slightly. This e-book may contain small programs that are furnished by MSPC as simple examples to provide an illustration. These examples have not been tested under all conditions. MSPC, therefore, cannot guarantee or imply reliability, serviceability or function of these programs. All programs contained herein are provided to you “AS IS.” IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED.

All customer examples cited represent the results achieved by some customers. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

The articles in this e-book represent the views of the authors and are not necessarily those of MSPC or TechChannel.