IBM Z, IBM POWER SYSTEMS & LENOVO THINKSYSTEM SERVERS MOST SECURE - TOUGHEST TO CRACK

November 30, 2022 • ITIC • Laura DiDio

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.

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 mid-November 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.

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. Security is and will continue to rank as the number one cause of unanticipated downtime for the foreseeable future.
Any organization that ignores security does so at its own risk. Ask yourselves: what does my organization have to lose and how much is my company willing to risk?