VERTIV WHITE PAPER

How IT and Cyber Teams Can Work Hand-in-Hand to Strengthen Server Management Security

Vertiv™ Avocent® ADX Ecosystem Brings Clarity and Control to Reducing Server Security Risks

Adapting to Change

The past two years have placed incredible stress on IT teams at enterprises and small and medium-sized businesses (SMBs) around the world. However, they have rallied to enable a hybrid workforce and develop a digital platform to support long-term growth. Similarly, security teams have combatted an avalanche of attacks as cybercriminals turned their attention from networks to endpoints, which are far easier to penetrate.

However, maintaining business stability amidst market turbulence and constant setbacks has come at a cost. Both IT and security teams are experiencing diminished visibility into network performance and conditions at the same time they face soaring demand for services. These teams are responsible for maintaining the performance and security of distributed networks, while redesigning processes for a zero-trust world. As a result, IT networking and cybersecurity teams need to collaborate more intensively to improve server management security across corporate networks. The good news is that 89 percent of network managers say they are doing just that. Some 37 percent of organizations have fully converged network and security management teams, while 26 maintain separate teams but have integrated tools or processes.[1]

Servers are the workhorses of industry, providing invaluable compute processing capability for the torrents of data companies, users, and their customers produce. Along with other networking devices, servers power digital services and enable the digital experiences customers covet. Thus, maintaining continuous uptime and performance is obviously critical for IT and security. In addition, attackers that gain access to servers can manipulate, control, and steal or freeze access to data, crippling a company's business operations and impacting customers. The ransomware attack on Colonial Pipeline Co., which led to gas shortages on the U.S. East Coast, is an example of just how disabling and far-reaching these attacks can be.[2]

IT and Security Server Management Challenges and Opportunities

So, just what issues are IT and security teams faces as they try to protect servers located at enterprise data centers, colocation facilities, and edge sites, among other locations?

Digital businesses create digital sprawl: Today, almost everything is digital: employee work processes, customer interactions, product development, and supply chain operations. A survey of IT professionals found that 47 percent expect permanent change, while 13 percent said their business had completely transformed due to recent events.[3]

Companies have expanded cloud and edge investments to keep up, creating IT device sprawl. Servers placed at remote edge sites may not be as proactively managed as those at the core, but still present significant security risks. What IT and security teams need more than ever is to gain a centralized view into network performance. They also need to harness secure remote access and in-band and out-of-band management to keep networks up and running and free from performance issues.

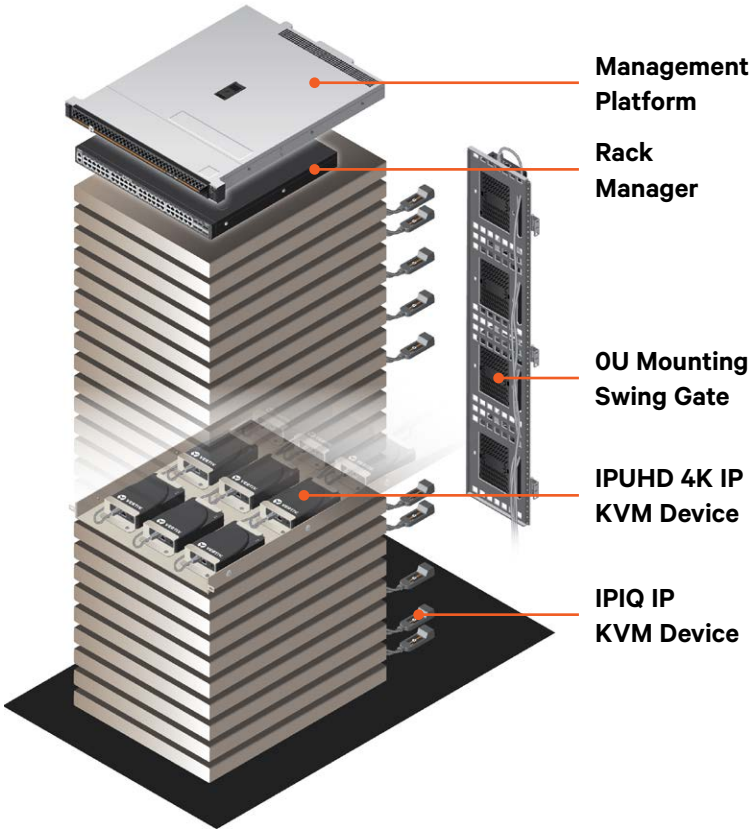
When more technology means more toolkits: As a result of digital growth, IT and security teams now are managing a larger number of servers and networking devices from a wide array of vendors. That means more toolsets, more policies, and more complexity unless IT consolidates network management duties in a single tool – and shares holistic data with security. While IT has made major strides to reduce management complexity, 64 percent of enterprises still use between four and 10 tools to manage their networks.[4] Many wish to consolidate further. The good news is that IT can manage more of their IT devices than ever on a centralized platform. Security, too, benefits from being able to integrate physical, environmental, and device monitoring into a single view.

Centralizing IT Device Management with One Platform

The Vertiv™ Avocent® ADX Ecosystem helps IT and cybersecurity teams centralize monitoring and management, improving the security of servers and other networking devices.

Servers - Production, development, and test servers; non-essential servers.

Other IT Devices - Administrative desktops, storage devices, networking equipment, remote rack power distribution units (rPDUs), remote uninterruptible power supplies (UPSs) and sensors, rack door locks, cameras, and more.



Security lacks visibility into policies:
IT and security teams want to manage the condition of all servers, wherever they're placed. However, because these teams are using multiple vendors and toolsets, devices likely have inconsistent security policies, and some may not provide granular visibility and control. That's a non-starter in a world of constant risks and threats. Security will want to partner with IT on defining and managing granular access privileges based on user roles and jobs to be done. Examples include controlling who can update firmware, attach virtual media to devices, and reboot servers. By so doing, the teams can reduce excessive access privileges, which can be exploited by cybercriminals to launch devastating attacks.

IT needs to streamline firmware management:
Automating firmware upgrades is rising importance as cybercriminals target kernel, memory, and other vulnerabilities in servers and other devices. For example, attackers can use malware such as Trickbot to scan devices for vulnerabilities, then reading, writing or erasing UEFI BIOS firmware.[5] Another threat, the new iLOBleed rootkit targets HP Enterprise Servers, manipulating firmware and wiping data off systems.[6] Further, security teams report that they are still spending 41 percent of their time on manual firmware patches that could be automated.[7] Automating these upgrades eliminates the risks created by out-of-date firmware and gives IT and security time back for strategic work.

"More than 80 percent of enterprises have experienced at least one firmware attack in the past two years, finds a Microsoft report. However, only 29 percent of these firms' security budgets are focused on protecting firmware."[8]

Providing greater functionality: IT and security could use separate networking monitoring and automation platforms. However, why not converge these capabilities? Both IT and security benefit by obtaining a holistic view of the network performance and sharing and acting on real-time data. That includes the ability to jointly set access privileges, review anomalies, plan incident response, and implement best practices like automation.

Vertiv™ Avocent® ADX Ecosystem - A Centralized Platform IT and Security Can Use to Collaborate

So, server management and security challenges are growing. However, the good news is that IT and security can work together cooperatively to address these issues and strengthen security, contributing to their firms' goals of creating zero-trust architectures. They can do so by deploying and sharing a centralized management platform and implementing a simple four-step roadmap.

The Vertiv™ Avocent® ADX Ecosystem provides IT and security with the centralized platform they need to improve server management and security. It provides the single view, management tools, and automation capabilities both teams need to bring clarity and control to networking and security. The Avocent ADX Ecosystem includes:

- A management platform for secure remote access, control, and automation
- A rack manager that physically connects to interface modules or directly to service processors, rack PDUs, or network equipment
- Interface modules that connect to aggregation appliances and the end target

Avocent ADX Ecosystem, which is based on a common digital architecture with an open platform and APIs, allows up to 100 simultaneous users to monitor and manage devices. Multi-level security ensures that authorized users only have access to the devices and privileges they need to do their jobs.

These users have options with how they access and manage devices. IT and security administrators can use serial consoles and Vertiv™ Avocent® ADX IPIQ 4K KVM devices to manage enterprise devices physically connected to the rack manager. Alternatively, they can use Vertiv™ Avocent® ADX IPIQ IP KVM devices as a fast, low-cost Zero U solution to manage devices without the need for the rack manager.

Vertiv™ Avocent® Core Insight – Standardize IT management with open-source firmare IT teams want to standardize management of devices, eliminating security gaps and increasing code quality and speed to market. Vertiv™ Avocent® Core Insight (ACI) provides a commercial-ready implementation of the OpenBMC project for baseboard management controllers (BMCs). Engineers can use ACI firmware to build secure, scalable, leading-edge embedded management systems for any device.

Developers have flexible options and can choose among:

- Open-source firmware that's ready to build upon
- Advanced ACI application modules that can be added to an existing stack
- A subscription service, that provides an enterprise ready-ACI bundle, including full source code access, tools, and premium support

Vertiv ACI provides premium runtime security, eliminating an entire vector of memory-based vulnerabilities.

Implement This Roadmap to Strengthen Server Security Today

Now that IT and security can see and share data and execute processes together, how should they proceed? Here is a simple roadmap to improve server security, starting now.

- **Connect devices physically for greater security:** IT can connect devices to the Avocent ADX Rack Manager – and hide them from network view and access by putting them on a private network. The private network is then accessible only via a rack management interface to authorized individuals, decreasing the risk of human error or internal sabotage.
- **Use secure protocols to communicate with devices:** IT and security teams can't always control device security. They may need to use legacy devices or new vendor devices that don't have the most up-to-date protocols and ciphers. However, these teams can place these less-secure devices behind the Avocent ADX Rack Manager for greater protection. By so doing, IT and security teams can reap more value from older devices or trial new innovations, without compromising network or site security.
- **Keep firmware updated on service processors:** System administrators can use the Avocent ADX Management Platform to automate server firmware upgrades using RESTful APIs and software development kits (SDKs), bringing consistency and standardization to this necessary task. Finally, the Avocent ADX Management Platform simplifies upgrades, avoiding device downtime and reducing security risks.
- **Strengthen device security with granular controls:** With the Avocent ADX Management Platform, it's easy to allocate, manage, and control privileges, avoiding the risk that excessive administrator privileges create. Individuals that do initial builds of servers can have one set of privileges, such as installing operating system images and software and rebooting servers. IT staff that troubleshoot servers can be authorized to launch KVM or serial sessions and complete key actions, such as installing firmware.

In addition, IT can standardize these actions across different device types. For example, system administrators can be authorized to reboot multiple device types. The platform also provides auditing capabilities, enabling IT and security to review these privileges on an ongoing basis to make sure individuals aren't performing unauthorized actions.

Conclusion

Improving server management security is a top priority for enterprises and SMBs today. Servers power the critical processes that make digital business run. However, they are increasingly at risk, due to network sprawl, excessive administrative privileges, out-of-date firmware, memory vulnerabilities, and other issues.

IT and security teams can proactively identify and eliminate server security gaps by working together, using a centralized monitoring and management platform and automated processes. Vertiv Avocent ADX Management Platform provides these essential capabilities, enabling IT and security to work hand-in-hand to safeguard these mission-critical devices both now and in the future.

[1] Shamus McGillicuddy, The Convergence of Network and Security Operations, EMA White Paper, April 2021, page 1, https://www.enterprisemanagement.com/research/asset.php/4037/The-Convergence-of-Network-and-Security-Operations

[2] "Hackers Breached Colonial Pipeline Using Compromised Password," article, Bloomberg, June 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[3] 2022 Tech Trends, Research Report, Info-Tech Research Group, slide 3, https://www.infotech.com/research/ss/2022-tech-trends

[4] EMA: Network Management Megatrends, 2020, Kentik, page 1, https://www.kentik.com/resources/ema-network-management-megatrends-2020-report/

[5] "Assessing Enterprise Firmware Security Risk in 2021," article, January 14, 2021, Eclypsium, https://eclypsium.com/2021/01/14/assessing-enterprise-firmware-security-risk-in-2021/

[6] Ravie Lakshmanan, "New iLOBleed Rootkit Targeting HP Enterprise Servers with Data Wiping Attacks," article, The Hacker News, December 30, 2021, https://thehackernews.com/2021/12/new-ilobleed-rootkit-targeting-hp.html

[7] New Security Signals, ibid.

[8] "New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats," article, Microsoft, March 30, 2021, https://www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/

Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

SL-70977 (R05/22)