MATRIX INTEGRATION

WHITE PAPER

# 3 Ways to Safeguard Hybrid IT Using Server Security and Access Control

Technology infrastructure is playing a pivotal role in the market. Companies of all sizes—across all sectors—must be able to transform ideas into market-ready innovations faster than their competitors. This capability of infrastructure to expedite workflows and speed collaboration has put a strain on legacy infrastructures built on rigid, hardware-defined, last-generation technology ill-equipped to keep pace. The challenge of infrastructure to optimize disparate systems to deliver services from IT to the business is well documented: As many as 80 percent of surveyed companies report dissatisfaction with the way IT services are integrated, and they are concerned about where and how tools and resources are connected.[1]

## Hybrid IT for On-Demand Capacity

Hybrid IT, in which companies can tap into cloud and on-premises infrastructure capacity to scale and accelerate the distribution of IT resources, is becoming a competitive advantage for SMBs and enterprise-scale companies. They are embracing resource consolidation and software-defined management to reduce IT costs while improving agility. The ability of hybrid infrastructures to give companies the choice to provision from the data center or a public or private cloud provides a flexible, adaptable infrastructure well-suited for today's business demand. Solutions such as HPE Nimble Storage, powered by Intel® Xeon® processors, combine the best of on-premises and public cloud storage for hybrid IT deployments. The trend is on the rise, as demonstrated by the fact that only 18 percent of SMBs are adopting a cloud-only infrastructure, while 80 percent of SMBs use a mix of public and private cloud or their own private cloud.[1]

Along with the scale of hybrid infrastructure comes the IT challenge of securing workloads that flow from the data center to the cloud—with access across many different endpoints. As many as 45 percent of companies say they have struggled with security

### Benefits of Hybrid Adoption

**Of those companies that adopt hybrid IT:**

- **92% could better meet customer expectations[2]**
- **91% gained an edge over competitors[2]**
- **89% saw increased selling opportunities[2]**

challenges when implementing a hybrid strategy.[2] A surprising 50 percent of companies avoid using public clouds because of security concerns.[1] Other challenges include complexity as the migration and operating concerns involved in cloud-based deployments consume too much IT resource time and expertise.

### Hybrid Insecurity: Evaluating Risk

The infrastructure consolidation that makes hybrid IT an attractive and efficient way to scale resources also makes it a target for cyber thieves looking for big payloads. No longer are cyberattacks leveraging end users as a gateway into corporate networks; they are now targeting data center components at the core. Some ransomware attacks go after databases directly, while others leverage weak configurations and credentials to attack the data center components. Other infrastructure vulnerabilities include:

**Core vulnerability:** Security threats are moving past applications and operating systems and targeting hardware itself; this includes the targeting of servers. It's easy to understand why. The data center houses corporate servers and storage devices that contain mission-critical and highly valuable data and applications, making these high-value targets for cybercrime. Considering the average cost of a data center outage can be upwards of $7,900 per minute, corporate entities might be motivated to pay ransomware to limit those losses.[3]

**Cloud vulnerability:** Security in the public cloud isn't as transparent as companies would think. While there are service-level agreements related to uptime, the security of a company's applications and data aren't necessarily assured. One doesn't need to look any further than the Amazon Web Services DDoS attack of 2016 that left customers offline for hours to understand the vulnerability of cloud-based workloads.[4] The nature of cloud deployments that include multi-tenancy, VMs, shared databases, integration, APIs, and multi locations make for a highly dispersed attack surface ripe for cybercrime.

**Edge vulnerability:** Malware attacks are getting smarter, and it's believed that as many as 90 percent of malware today is designed to attack a single system, thus bypassing traditional security controls.[5] Among those targets: endpoints often left vulnerable because of security policy lapses of mobile and IoT devices. Among the biggest challenges of endpoint protection is the inability to automate detection of security threats, leading as many as 23 percent of IT professionals to regularly reimage infected endpoints.[6] What's more, as many as 19 percent of IT professionals say it's the lack of integration and automation between endpoint security tools that leads to manual management that contributes to security gaps.[6]

**HPE ProLiant DL380 Gen10 Servers, powered by Intel® Xeon® Scalable processors, the world's most secure industry standard server, is configured with a silicon root of trust.[7]**

### Three Server and Storage Advances for Hybrid Security

#### 1 Secure Servers

Today's malware is going undetected for an average of 99 days, during which time it sits within a server's operating environment where it's harder to detect.[8] Only 8 percent of enterprise companies have the capacity to defend against these firmware attacks.[8] New servers are being architected with built-in security to prevent ransomware and cyberattack at the hardware level. Products like HPE ProLiant Gen10 Servers are designed with firmware anchored to the silicon, along with a silicon root of trust to prevent firmware attacks. It validates and verifies firmware code every 24 hours and prevents compromised code from being executed upon boot up. In the event of a BIOS attack, firmware rolls back to the last known good state or factory settings.

#### 2 Predictive Storage

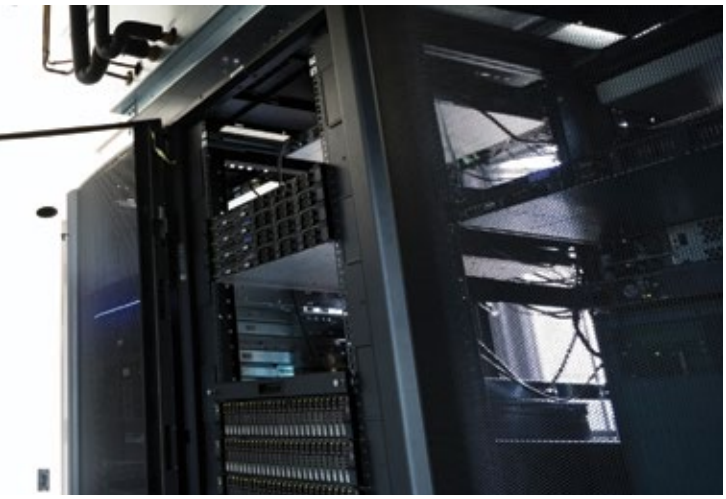
Storage backups aren't just for due diligence anymore. It seems storage backup is an essential component to recovering from a malware attack or breach—that includes backup of data on premises or the cloud. In fact, many ransomware attacks can be thwarted with an updated backup of import databases. Therefore, backups and snapshots should be performed frequently—especially for mission-critical business data.

- **Proactive Protection:** New storage advances like HPE Nimble, powered by Intel® Xeon® processors, are configured to ease the management of hybrid storage volumes using HPE InfoSight to predict and prevent 86 percent of storage problems. This includes mitigation of the 54 percent of problems that arise outside of storage infrastructures.[9] The

process uses machine learning and analytics to eliminate the manual intervention that otherwise might open the door to storage vulnerabilities and downtime.

- **Ease of recovery:** HPE Nimble flash and adaptive-flash arrays, powered by Intel® Xeon® processors, are configured with built-in snapshots and replication and are integrated with backup

**More than 50% of cybersecurity professionals reported at least one incident of malware-infected firmware in 2016.[10]**



software. Additional security comes in the form of fault-tolerant drives, encryption, and secure data shredding, all of which can be used to safeguard storage volumes. HPE Nimble secondary flash arrays provide a single platform for backup and disaster recovery with near-instant restores and failover from primary storage to secondary flash arrays.

## 3 Automated Access Control

For many companies, access control is out of control. There is an inability to monitor and manage access privileges and a lack of insight into the granting of administrative rights. Not knowing who has access to what or being able to control access to infrastructure components based on roles, devices, and users can put hybrid environments at risk. The capability to identify user access and privilege levels and to ensure no rights are approved to those who don't need them and that privileges are reviewed and updated regularly is essential.

IT managers can automate hybrid IT access control and security with Aruba ClearPass policy manager from Aruba, a Hewlett Packard Enterprise company. It is designed to automate the task of discovering, profiling, and authorizing any network access, on wired or wireless networks, including for BYOD and IoT

**It's estimated that less than 20 percent of IoT data is secure, and the rest is exploitable.[8]**

---

**Aruba ClearPass is the first in the cybersecurity industry to be awarded Common Criteria certification and is the industry's first NAC solution to receive certification as an authentication server.[11]**

devices. This automated policy manager tool tackles access control on two levels; it uses automation for attack detection and automates the setting of granular policy controls across users and devices. Here again, machine learning is leveraged to provide the analytics into vulnerabilities and policy breaches, helping to ensure secure device access and compliance.

## Conclusion

Hybrid IT delivers infrastructure agility and accelerates IT service delivery with the consolidation of on-premises and cloud-based capacity to scale to meet resource demand. With this highly interconnected

infrastructure comes the need to protect the edge, core, and cloud-based components. Hybrid IT servers and storage, like the HPE ProLiant DL380 Gen10 Server, and HPE Nimble, powered by Intel® Xeon® processors, leverage advanced security features, machine learning, analytics, and automation to safeguard infrastructure hardware from today's persistent threats. When combined with policy management tools, these hardware advances ensure secure hybrid IT environments and eliminate much of the manual security management tasks.

Matrix Integration is an HPE Platinum Partner and technology solutions provider with 37 years of experience helping companies advance infrastructure capacity. With nearly 75 employees, including engineers, solution architects, and business professionals, Matrix has the expertise and resources to advise companies on hybrid IT configuration, security, and automation. The company is a certified Women's Business Enterprise, an active member of many business associations, and has received numerous national accolades and certifications for business and IT excellence.

**For more information, contact Matrix Integration at (812) 634-1550.**

Matrix Integration | 417 Main Street, Jasper, IN 47546 | (812) 634-1550 | matrixintegration.com

Hewlett Packard Enterprise
Platinum Partner

intel XEON inside™

1. HPE, "Harvard Business Review Survey Finds Companies Say Yes to Hybrid IT," June 22, 2017.
2. Forrester, "Hybrid IT Insights: Composable Infrastructure and Business Breakthroughs," Feb. 2018.
3. Silverback Data Center Solutions, "Ransomware and Data Centers: Avoiding a Worst-Case Scenario," accessed April 5, 2018.
4. Moor Insights, "Hybrid IT Helps Businesses Navigate Through Digital Transformation," June 2017.
5. Security Intelligence, "Global IoT Security Spending to Reach $1.5 Billion in 2018, Report Reveals," April 3, 2018.
6. CSO, "Endpoint Security Suites Must Detect/Prevent Threats and Ease Operations," March 6, 2018.
7. Based on external firm conducting cyber security penetration testing of a range of server products from a range of manufactures, May 2017.
8. Moor Insights, "Demystifying Server Root of Trust," Aug. 2017
9. HPE web page, HPE Nimble Storage, accessed April 5, 2018.
10. Press release, "HPE Unveils the World's Most Secure Industry Standard Servers," June 5, 2017.
11. CSO, "Aruba Achieves Cybersecurity First with Common Criteria Certification for Network Access Control Solutions," Jan. 29, 2018.

Hewlett Packard Enterprise specializations include Platinum: Converged Infrastructure, Networking.