Adversaries seek out and exploit any security vulnerability they can; servers and storage remain prime targets. Here are three best practices on how to strengthen your server and storage infrastructure to make your IT foundation more secure, resilient and highly available.

Security attacks continue to take a substantial toll on enterprises across all industries. New threats and vulnerabilities are being identified in real time, while many other attacks often infiltrate an enterprise's firewalls. Make no mistake: The consequences of a security breach are staggering. And the financial implications aren’t the only concerns: Security breaches also bring significant operational and reputational risks.

The 2017 U.S. State of Cybercrime report points out that 39% of survey respondents experienced more cybersecurity events during the past year, with the average financial impact on enterprises for a single cybersecurity event rising to nearly $900,000 in 2017. That figure is almost double the amount reported just two years ago.¹ And, research from Accenture puts the average cost of a malware attack at $2.4 million.²

These and other sobering statistics have caught the attention of IT and security leaders—as well as their C-suite executives and boards of directors. As a result, many organizations are looking for server and storage solutions that address potential security problems with integrated, designed-in defenses and features that make them more resilient against both internal and external threats. In particular, organizations should plan for enterprise-wide security defenses, including server and storage design, firmware and software security tools.

¹ “2017 U.S. State of Cybercrime,” IDG, October 2017
² “2017 Cost of Cyber Crime Study,” Accenture and Ponemon Institute, 2017
New approaches to securing vital IT infrastructure are needed, such as security by design, silicon root of trust and highly secure encrypted storage. Fortunately, technology companies are introducing new ways to fortify their server and storage infrastructure to protect, detect and recover from threats.

**Security challenges to server and storage infrastructure**

In an environment increasingly marked by virtualization and cloud computing, on-premises servers remain a critical part of the overall IT modernization effort. The expanding attack surface, along with the frequent lack of visibility and control, leaves organizations vulnerable to a wide range of attacks.

The more virtualized an organization becomes—and the fewer physical servers an organization uses to support large numbers of VMs—the more those servers need to be cyber resilient to avoid downtime caused by data breaches. Failure to do so often creates serious problems resulting from data loss, exposure of sensitive customer data and related downtime in the event of a compromise.

**Bottom line**: As enterprises become more connected across platforms, devices and geographies, being cyber resilient becomes a mission-critical requirement.

For storage infrastructure issues, a big risk factor is the increased use of pools. Storage pools are very efficient and represent a big step forward in capacity utilization and CapEx reduction; but they also are a potential vulnerability for IT operations since they house mission-critical data.

Stricter requirements for compliance and legal issues also are important in securing compute and storage infrastructure. One prime example is the much-discussed General Data Protection Regulation (GDPR), governing the protection of personal data of European Union residents. GDPR takes effect on May 25, 2018, and it has raised the stakes when it comes to data security. For example, organizations that discover a data breach have strict notification obligations to affected individuals and/or EU supervisory authority (usually within 72 hours for a serious data breach). Failure to meet those obligations could result in substantial financial penalties that can range as high as 4% of global annual turnover or 20 million Euros (whichever is higher).

One threat in particular that has grabbed both headlines and the attention of IT, security and business leaders is ransomware, a type of malicious software designed to block access to a computer system until a sum of money is paid. The WannaCry global ransomware attack impacted hundreds of thousands of users across more than 150 countries in 2017. One report indicates that, as of October 2017, more than 6,300 dark web marketplaces were selling ransomware, creating a 2,500% increase in the underground economy for ransomware in just the past year.

What does this mean for IT and security professionals? IT and security personnel should consider building or refreshing their IT infrastructure with products aligned with the five functions (identify, protect, detect, respond and recover) of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. Dell EMC recommends a three-phased approach that is aligned with the NIST framework: protect, detect and recover.

With servers and storage functioning as the foundation of IT operations for traditional, virtualized and cloud computing architectures, the modern IT security platform should be engineered and integrated as an entity, not bolted on as an afterthought. An IT infrastructure built from the ground up with security as an essential element is more likely to enable true cyber resiliency.

The modern IT security platform should also include software solutions such as encryption, identity management and access controls, which definitely play valuable roles in securing infrastructure. But even more is needed in protecting these valuable assets. What steps should be taken?

Security and IT professionals should ask tough questions about their organizations’ readiness against infrastructure vulnerabilities, including:

- How can we detect and respond to malicious attacks around the clock?
- What types of access control techniques are being deployed, and are they sufficient for emerging threats?
- Are we taking the right steps to protect data both at rest and in motion?
- Are our server and storage defense frameworks providing comprehensive, end-to-end coverage—both on premises and in virtualized environments?
- Should we rethink how we securely decommission servers?

---

Security by design
An integrated security framework, rather than a collection of disparate security tools for each infrastructure component, ensures that servers and storage are fully protected as part of an end-to-end security approach in an effective and cost-efficient manner. Also, by treating server and storage security as part of a total framework, rather than as potential flashpoints, organizations move from a “secure perimeter” mindset to a “secure architecture” philosophy.

IT modernization has become an important goal for organizations embracing digital transformation. Whether they are re-engineering data centers, distributing compute and storage resources to remote offices or repurposing older but still functional servers and storage systems, IT decision makers need to consider the security ramifications of re-deploying or even retiring servers and storage to ensure they can protect, detect and recover from attacks. Successful strategies designed to ensure cyber resilience require organizations to think ahead as the future becomes increasingly unpredictable.

First, infrastructure needs to be “secure by design.” Specifically, security features must be designed into servers and storage from the ground up, and they must be available and continuously improved from the initial deployment through upgrades, and even during repurposing and retirement.

Embedded security ensures that only valid, signed updates are permitted for the server BIOS and peripherals, specifically storage devices.

IT and security decision makers look to establish a silicon root of trust, where firmware updates are authenticated to prevent malware from taking hold on compute and storage systems.

Also, security for storage infrastructure needs to implement hardware-based encryption rather than software, in the form of self-encrypting drives (SEDs). Using hardware-based encryption offers a number of benefits over software-based encryption, including more effective restriction of access from outside sources and significant performance improvements.4

With SEDs, the encryption key is generated on the drives by a random number-generation process, and the authorization key is encrypted inside the drive. New SEDs support the ability to erase the old key and replace it with a new encryption key. For the decommissioning or repurposing of legacy storage systems, this provides an added layer of secure sanitization before storage devices are reallocated, redeployed or retired.

Cyber-resilient servers: Enabling better security
Initiatives such as digital, IT and workforce transformation not only create tremendous opportunities, but also greatly expand the attack surface. There is much more data being captured, stored and shared outside the confines of the traditional data center. That’s an important reason why Dell EMC took an innovative approach toward security with the latest PowerEdge™ server generation—one that also supports a longer-term, sustainable approach to managing and reducing risk.

Cyber Resilient Architecture is a vital aspect of the latest PowerEdge server portfolio. It is designed to protect servers wherever they reside, including traditional data centers, remote office facilities and as part of software-defined data center architectures. Under the umbrella of cyber resiliency, IT and security professionals need to consider all the issues that occur before, during and after a threat has been uncovered or an adverse event has taken place. This requires a holistic approach to security that merges a wide set of security initiatives, including continuous monitoring, data protection, business continuity and ensured availability of critical cyber assets.

Integrated security, engineered into the server design beginning at the factory, delivers enhanced silicon root of trust that enables the three phases of cyber-resiliency: protect, detect and recover. When organizations embrace and enact the “protect, detect and recover” framework, they begin to take the most effective and efficient steps toward achieving cyber resiliency, which is often the final goal of modern IT security.

Dell EMC provides a number of essential security tools and functionality built into its PowerEdge servers, each aligned with different categories of the protect/detect/recover paradigm:

**Protect**
- Silicon root of trust: authentication of BIOS, integrated Dell Remote Access Controller (iDRAC) and OS booting
- Cryptographically signed firmware: enforces a secure platform environment.
- Self-encrypted disks (SEDs) to protect data at rest
- Always-on iDRAC: agent-free management that enforces security throughout the server.

**Detect**
- Drift detection: continuous detection of configuration and firmware changes with rapid remediation
- Physical intrusion detection: detect physical tampering of servers whether in transit to your data center or operating in remote locations

4 “Commonly asked questions and answers on self-encrypting drives,” Trusted Computing Group, January 2011
• Alerts and logging: logs every event and provides alerts, including recommended actions

Recover

• BIOS recovery: seamless, automatic recovery to a protected, trusted BIOS image after an attack
• Easy restore to trusted state: automatic restoration of server configuration after part or motherboard replacement
• System Erase: erase sensitive data securely and instantly using cryptographic techniques

These and other integrated security features are designed to protect enterprises by preventing unauthorized or inadvertent changes, securing the data center through a fully cyber-resilient architecture and ensuring privacy by quickly erasing user data from drives when a server is retired. Systems engineered with the three-phase approach integrated into an overall security framework are more likely to avoid and resist attacks, and to return to normal operation faster and more reliably.

Toshiba SSDs for enhanced reliability and security

Storage is another potential point of attack for security vulnerabilities—which is potentially catastrophic, considering that storage systems house an organization’s most vital data. This is a key reason why Dell EMC chose Toshiba self-encrypting solid-state drives (SED SSDs)—including Toshiba’s PX05SV Series 12Gbs SAS and HK4E Series 6Gbs SATA SSD products—for their PowerEdge server line.

Toshiba has been a pioneer in data storage for decades and is the principal inventor of NAND flash. The company is one of the major suppliers of storage for data centers and has led the charge on the development of SSD technology, which is now mainstream in many enterprise data centers, as well as in new infrastructure formats such as converged and hyperconverged systems. Because SSDs do not use moving parts, they offer enhanced reliability over traditional hard drives.

Importantly, Toshiba SAS-based, self-encrypted SSDs offer greater security and resilience because they have passed rigid certification testing under the U.S. Federal Information Processing Standard (FIPS) 140-2 encryption guidelines. Additionally, Toshiba SED drives secure data at rest because encryption is designed into the hardware itself, not implemented via software. And, using hardware-based encryption allows the drives to operate without performance penalties normally associated with software-based encryption. Toshiba’s SED-based SSDs also offer Instant Secure Erase (ISE) for fast and secure decommissioning and, if necessary, disposal of SSDs. It is designed to work in harmony with Dell EMC’s System Erase feature, another robust security function that safeguards data during system repurposing or retirement.

Toshiba’s SED-based SSDs are available in both SATA and SAS interfaces, with throughput rates of up to 6 Gbps and 12 Gbps, respectively.

Conclusion

Security is top of mind for executives in IT, security and business roles, and it carries a big impact for all users, including customers, suppliers and partners. Security and business interruption threats represent critical financial, reputational and operational challenges for enterprises with server and storage infrastructure.

Organizations now demand new IT infrastructure solutions that are integrated within, rather than bolted onto systems in the form of disparate tools and point products that are not optimized to work together for maximum efficiency.

Solutions built on “security-centric” infrastructure such as Dell EMC PowerEdge servers and Toshiba’s highly reliable and secure SED SSDs—optimized for use in Dell EMC servers—represent a major step forward in delivering integrated security across the infrastructure stack.

IT and security professionals looking to protect their infrastructure and make those assets more resilient, highly available and secure should evaluate, select and implement servers and storage with integrated security features. Servers and storage must support the goals of protecting, detecting and recovering from threats that inevitably put their enterprises in jeopardy.

For more information on integrated security infrastructure solutions from Dell and Toshiba, please visit:

www.Dell.com/Poweredge
www.Dell.com/Toshiba