Lenovo

Leveraging Data Management to Fight Security Breaches

Cybersecurity threats are mounting every day, creating untold operational, financial, regulatory and brand problems for organizations. Ransomware, malware, identity theft and other security challenges must be identified, prevented and remediated before extensive damage can be done and essential data is compromised. This paper looks at why and how a defensive framework based on data management should be built to lock down cyber threats and protect against data loss.

TechTarget | Custom Media

Lenovo.com/Data Center Group

Every minute of every hour of every day, organizations are under cyberattacks. In fact, hackers attack somewhere every 39 seconds.[1] The threat of cyberattacks such as ransomware, zero-day attacks and mobile malware are growing at alarming rates as cyber criminals become more persistent and resourceful, and utilize the collective capabilities of other attackers and machine learning algorithms.

In 2020, the average cost of an enterprise data breach will exceed $150 million.[2] But, at least as important are the economic, operational and reputational impacts of compliance violations brought about by things like compromised personally identifiable information.

Protecting data, identities and other digital assets requires a combination of innovative, intelligent and automated data management techniques. Organizations also should insist resilient and "secure-from-the-factory" storage and compute infrastructure.

This paper looks at what organizations can and should do about mitigating cybersecurity threats and why data management is an essential element in addressing malware, advanced persistent threats, ransomware and other attack formats. It also offers some concrete suggestions for teaming with a trusted and proven technology partner for data management solutions.

What enterprises should do today

Enterprises have become more resourceful in their fight against security threats, committing hundreds of billions of dollars annually to everything from threat monitoring subscriptions and data breach remediation services to next-generation firewalls and malware-resistant servers. And yet, attacks continue to proliferate, intensifying pressure on organizations to shore up their data protection efforts from the core to the edge to the cloud.

When "doing what has always been done" no longer works, it's time for new ideas, new strategies and new

[1] "15 Alarming Cyber Security Facts and Stats," Cybint Solutions, September 23, 2019.
[2] "Business Losses to Cybercrime Data Breaches to Exceed $5 Trillion by 2024," Juniper Research, August 27, 2019.

tools. At the heart of a rock-solid, efficient and flexible cybersecurity and data protection framework is data management. There are many elements of a data management architecture that contribute to a smart, automated and responsive cybersecurity posture. For instance, backup and archiving are integral to data protection and fast, reliable data restoration, while snapshots, de-duplication and compression all improve storage optimization. Data management also is critical for business continuity, data visibility, auditability for compliance and governance in the event of an attack. This is particularly true in an increasingly hybrid cloud and multi-cloud IT environment, where data is often migrated from on premises to the cloud, and to/from different storage systems.

Data management is an invaluable part of cybersecurity attack detection and mitigation, and should be an integral part of IT infrastructure such as storage to ensure management is done easily without a lot of manual monitoring and intervention.

One proven industry leader with demonstrable data management expertise is Lenovo, a global leader in IT infrastructure, software and services. Lenovo's broad array of storage, compute, software and service/support capabilities help organizations build a comprehensive security framework based upon state-of-the-art data management.

Lenovo's cybersecurity defense strategy is built upon several core principles, including the primacy of data management to automatically spot and prevent potentially damaging attacks without having to rely upon armies of security analysts. Lenovo's storage and software solutions also are built on the foundation of "secure by design," where products and services are created from the start with security as a core function, rather than being added on after infrastructure has been deployed and threats have emerged.

How Lenovo data management, infrastructure and software fortify your defenses

For the past decade-and-a-half, Lenovo has built a reputation for IT infrastructure leadership from the endpoint to the data center. Its desktops, notebooks, servers and storage are widely recognized for enterprise requirements such as performance, scalability, resilience and security.

Lenovo storage and compute solutions are key parts of an organization's cybersecurity defense framework. Its DM and DE series of all-flash and hybrid flash storage, combined with the ThinkSystem server lineup, help detect and mitigate the impact of security breaches at multiple levels, including:

- Multi-factor authentication
- Lightweight access points
- Monitoring of privileged accounts and groups
- Network segmentation
- Role-based access
- Volume encryption
- Aggregate encryption
- Secure purge
- Storage encryption
- Onboard Key Manager secure boot

Lenovo storage hardware and software detect and mitigate the impact of cyber threats on several levels, including:

- Snapshotting to ensure no data is lost on core workloads.
- Fast, simple and reliable data restores.
- Replication to move data off-site to restart workloads in the event of a data breach or service interruption.
- Secure-by-design architecture that starts at the component level in the factory.

Organizations are spending large sums of money on backup tools, threat-detection services, malware protection and next-generation firewalls. But if—or when—those steps fail, organizations still must have the ability to fully, reliably and securely back up production data regardless of its movement or location. And data from backup copies must be validated to ensure that IT and storage administrators are not booting up bad data.

Additionally, Lenovo storage infrastructure security is further fortified by the company's tight partnerships with leading backup storage software vendors. Lenovo's partnerships help organizations withstand the impact of data breaches with easy-to-deploy, yet powerful encryption to provide foundational backup capability, validated backups and easy testing of restore processes.

Lenovo DM storage arrays leverage industry-leading storage management software to battle threats through powerful encryption, snapshots and SnapLock technology to create non-writable, non-erasable data on storage media to prevent files from being altered or deleted until a pre-determined or default retention date.

These and other security tools are integrated into Lenovo storage solutions from the start, ensuring that organizations can take advantage of proven defenses immediately without having to "bolt on" security tools.

Conclusion

Cyberattacks are surging, and no organization is immune to those attacks. Enterprises of all

sizes, geographies and industries must address the root causes of cybersecurity risks with a multi-level, multi-tiered approach. The key to securing critical data before hackers can penetrate systems and exfiltrate data is a well-planned and tightly executed data management strategy to ensure essential data is always available and can be easily restored if systems are compromised.

Storage infrastructure solutions from Lenovo have been designed from the ground up for resiliency, scalability and performance—and to help organizations withstand cyberattacks and to mitigate their impact.

For more information on how Lenovo solutions help organizations in their fight against cyber threats, please go to:

https://www.lenovo.com/us/en/data-center/storage/c/storage

This content was commissioned by Lenovo and produced by TechTarget Inc.