Insight

Long Live Tape — And Other Data Protection Trends for a New Threatscape

Cybercriminals have refined their attack strategies and are now targeting data protection environments. To stay ahead of the bad actors, consider incorporating these 11 data protection trends we're seeing across modern data protection environments.

The lifecycle of a cyberattack

Before you can effectively prevent a breach, it's important to understand the lifecycle of a cyberattack:

Reconnaissance:
Bad actors identify potential targets, assess the target's defenses and choose their method of attack.

Initial compromise:
Hackers bypass perimeter defenses and gain access to the network.

Command & control:
The attackers use the compromised device to gain further access to the environment and set up long-term control.

Lateral compromise:
With access established, the cybercriminals attempt to compromise additional users and machines.

Target attainment:
Multiple access points and hundreds of compromised users provide the hackers with in-depth information about the environment.

Exfiltration, corruption & disruption:
The attackers now have full access to sensitive data, intellectual property or other mission-critical systems, potentially costing the organization hundreds of thousands of dollars — or more.

11 trends in modern data protection

From data isolation solutions that logically or physically isolate data storage to mitigate risk to the modern infrastructures and strategies redefining the state of data protection, these 11 trends make secure data management more attainable.

#1 Magnetic tape

Tape storage — a form of completely offline, air-gapped backups — isn't going away anytime soon. **New technology has increased magnetic tape storage capacity, making magnetic tape an extremely cost-effective method for storage and backup. Because air gapping is offline, this type of data protection is nearly 100% secure.**

#2 Immutable storage

Historically known as the "nuclear option," immutability has become an appealing option for security teams. Immutable storage lets organizations take a snapshot of their data and set policies on its expiration, knowing that the data is unaffected and completely restorable until that time, regardless of any unintentional or intentional breach of the environment.

The result? It's completely impervious to ransomware attacks.

#3 All-flash

All-flash storage is growing in popularity due to its ability to **minimize recovery point and recovery time, provide fast or synchronous replication and automatic failover, and be easily integrated with cloud and hybrid cloud environments.**

#4 Vault solutions

Enabling total recoverability, vault solutions don't just protect your data — **they account for business-critical services and infrastructure, too.** Vaults can be leveraged on-premises, in a colocation or in the public cloud, enabling your business to secure, isolate and recover with ultimate confidence.

#5 Cloud archive

For files you don't need to access frequently, cloud archive options offer a form of backup that frees up storage resources for active data while adding the security layers needed for resilience and compliance. **Cloud archive now supports object lock, which brings immutability to archive backups for added protection against ransomware.**

#6 Two- or multi-factor authentication

Two- or multi-factor (MFA) authentication validates users prior to granting access to data. **Research shows that 57% of organizations that offer MFA use either push notifications via phone/email or one-time passwords. This helps guard against automated attacks, bulk phishing attacks and targeted attacks.**

#7 At-scale test restores

To test the strength of your data protection strategy, consider performing at-scale test restores. **This type of testing exercise restores the entire environment, as opposed to single files, apps or machines,** and is conducted under the premise that the primary data center is encrypted to replicate a ransomware attack.

#8 Cloud-connected storage

As storage moves out of the traditional data center to the edge and into the hybrid cloud, **teams are ensuring they only work with top cloud providers and are actively searching for ways to properly secure data in the cloud.**

#9 Data discovery & classification

When organizations provide employees access to more data than they need, data breaches can occur. A clear data classification policy and restricted data access position companies to be better protected against this risk. You also can't protect what you don't know exists. **Performing regular data discovery and classification is key to highly effective cloud data protection and storage.**

#10 As-a-service consumption models

The global Storage as a Service (STaaS) market was valued at $34 billion in 2022 and is expected to reach $396.5 billion by 2032, indicating that enterprises are identifying the STaaS model as a cost-effective, scalable and secure option for data management.

#11 A shift in the security team mindset

And finally, IT security teams are **expanding their understanding of security** to include storage and data protection roles not previously included.

The best teams view data protection through a business continuity lens, constantly testing and refining their strategies — all while playing a key role in cybersecurity and awareness training across the organization.

If you're ready to modernize your approach to data protection, Insight can help you determine the best options for your unique environment.

Learn more at insight.com.

Sources:
Allied Market Research. (October 2023). Storage as a Service Market: Global Opportunity Analysis and Industry Forecast, 2023–2032.
CRI Team. (2022, July 5). Global Small and Medium-Sized Businesses Slow to Move to More Secure Multi-Factor Authentication Account Access Method; New Cyber Readiness Institute Survey Finds. Cyber Readiness Institute.