Threatwise™

Defending data from cyber threats: Why early warning matters

A SNAPSHOT OF DATA PROTECTION TODAY

Data protection stakeholders sit at the core of every company, ensuring data availability for the entire business. Conventionally perceived as the last line of defense, data protection admins focus their day on ensuring critical data is backed up and recoverable in the event of a data incident. Proactive measures can be taken when managing backup infrastructure, regularly testing backups, and implementing disaster recovery plans. However traditional data protection processes are largely reactionary—waiting for an incident to happen before reacting to it. A sprint to recover all impacted data starts with data compromise to win the race to full operability and meet recovery SLAs. As ransomware gangs evolve, the stakes have never been higher. From double and triple extortion to direct attacks targeting backup infrastructure themselves, sitting idle, waiting to recover, doesn't cut it. Instead of expecting the next data incident to hit, data protection must start early before the damage is done.

TRANSFORMING DATA PROTECTION: THE POWER OF EARLY WARNING

With data-minded cyber deception, companies of every size get modern ransomware protection and early warning. Threatwise, from Commvault®, offers advanced detection measures that intelligently safeguard assets and data and alerts businesses of zero-day and unknown attacks the moment they happen—before it's time to recover. Using decoys, Commvault blankets tripwires across on-prem, cloud, and SaaS environments to shield business data and systems from malicious intent and activity across the organization. Starting by protecting data at the source, Threatwise uses an inward-out approach, proactively spotting threats along the path to your data using decoys that replicate real network assets. First, Threatwise masks the backup infrastructure, hiding it from threats directly targeting them to ensure backup and recovery utilities remain resilient from zero-day and unknown threats. Next, the data and workloads being protected are surrounded to detect and divert malicious activity targeting your crown jewels. Finally, decoys are scattered in strategic places across the organization, reaching perimeter borders to create an end-to-end protection strategy that spots threat actors early before they reach your data.

PROACTIVE DATA SECURITY

Monitor and backup environments
Ensuring the integrity of your backup infrastructure

Enhance cyber recovery
Reacting faster by streamlining your disaster recovery plans and early warning

Stay ahead
Expose silent threats along the paths of your data

Safeguard critical workloads
Protecting your data beyond backup environments

Ensure availability and recoverability
Sealing your backup environments from malicious activity

PROTECTING YOUR BUSINESS: DATA-MINDED CYBER RESILIENCE

Adopting data-minded threat detection capabilities enables businesses to focus, unearth, and engage threats early during recon, discovery, and lateral movement. With Threatwise, businesses get intelligent early warning that proactively masks, secures, and diverts attacks against real data and assets. Using patented deception technology, Commvault delivers advance visibility before damage is done, to reduce risk, limit recoveries, and eliminate downtime.

To learn more about Threatwise, visit **commvault.com**

Commvault®

commvault.com | 888.746.3849