COHESITY

ActualTech MEDIA

Intelligent Data Security and Management

Lawrence Miller

- What Will You Do When Ransomware Hits You?
- Data Security and Management Use Cases
- Ransomware Data Protection and Recovery

IN THIS PAPER

In the digital era, data is crucial for businesses and a prime target for cybercriminals. Despite a slight decrease in ransomware incidents, the threat remains significant. Learn about the intelligent data security and management tools that are needed in the modern enterprise so your organization is ready to mitigate risk.

Highlights include:

- How ransomware threats are changing.
- Most common data security and management use cases.
- Key capabilities for ransomware data protection and recovery.

CONTENTS

In the digital economy, data is the most important asset for modern enterprises and a lucrative target for cybercriminals. While the rate of ransomware attacks dropped slightly in the past two years (59% of organizations being hit by ransomware in 2023), it's no time to let down your guard. Cybercriminals and ransomware gangs are increasingly targeting backups with an alarming 75% success rate and, in the absence of a secure, immutable backup, 56% of organizations are paying a ransom to recover their data.

An intelligent data security and management solution provides granular controls to help ensure compliance.

What Will You Do When Ransomware Hits You?

The enterprise data footprint—that is, your attack surface—is growing rapidly and becoming increasingly complex as organizations innovate, add more tools to their tech stack, and pursue multicloud strategies. Larger attack surface areas are more difficult to protect and leave organizations more vulnerable to attacks. Data management is the foundation for any effective security strategy. At the same time, cyberattacks are occurring more frequently. This is in part due to Ransomware-as-a-Service (RaaS) offerings, which have made it easy for anyone to launch an attack and use AI to gain intelligence and repeatedly attempt to compromise your last line of ransomware defense, your backups. Ransomware attacks are also becoming more

complex with double-extortion (attackers exfiltrate a copy of your sensitive data and threaten to expose it) and triple-extortion attacks (attackers launch a denial-of-service attack or directly target individuals whose data they have stolen) becoming more pervasive.

Data Security and Management Use Cases

An intelligent data security and management solution supports many enterprise use cases, including:

- **Cyber resilience.** A cyber resilient solution requires the foundational layer of backup and recovery with enhanced, built-in ransomware defenses to protect your data.
- **Ransomware protection, detection, and recovery.** Robust ransomware defense requires comprehensive data security and management capabilities, including immutable backup snapshots, AI-powered threat detection and user behavior analysis, and rapid recovery at scale.
- **Clean room recovery.** A clean room isolates compromised systems in a controlled environment where security operations teams can perform forensics to understand how an attack happened while completely separated from the network. Building a timeline of the incident allows them to devise a recovery plan that eradicates the threat and helps prevent reinfection in the future.
- **Data compliance.** Governance, risk, and compliance (GRC) establishes the data archival, retention, and sovereignty requirements that an organization must follow to align with regulations. An intelligent data security and management solution provides granular controls to help ensure compliance.
- **Data privacy laws.** Data privacy laws, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), are driving organizations to accurately identify and manage sensitive data containing personally identifiable information (PII), and prove compliance. EU regulations such as the Digital Operational Resilience Act (DORA) are creating additional penalties for organizations that don't comply.

An intelligent data security and management solution helps organizations strengthen their security posture, reduce the risk of unauthorized access, and minimize the impact of a ransomware attack.

Ransomware Data Protection and Recovery

An intelligent data security and management solution helps organizations strengthen their security posture, reduce the risk of unauthorized access, and minimize the impact of a ransomware attack. Key capabilities for ransomware data protection and recovery include:

- **Cyber vaulting and data isolation.** A cyber vault creates an isolated copy of production data. With a clean, separate, and protected copy of data always ready, organizations can rapidly recover data back to its original source, or alternate backup locations, in case of a ransomware attack or other incident that compromises production or primary backup systems.
- **Unlimited immutable snapshots.** Software-based, native immutable backup snapshots effectively throw up a wall against ransomware attacks because they can't be encrypted, modified, or deleted. Unlimited snapshots enable precise point-in-time recovery to a known good backup.
- **WORM lock.** Write once, read many (WORM) mechanisms provide another layer of protection against a ransomware attack, allowing IT teams to create and apply a time-bound lock to enhance immutability for protected data.

Intelligent data management helps organizations proactively identify, classify, and protect their most sensitive and valuable data, and prioritize their recovery efforts.

- **AI/machine learning (ML) threat detection.** A modern data security and management solution powered by AI/ML can accurately detect patterns and anomalies that may be indicative of an imminent cyberattack, while reducing alert fatigue and "noise" due to false positives.
- **At-rest and in-flight encryption.** Secure at-rest and in-flight backup data with robust Advanced Encryption Standard (AES)-256 encryption that is U.S. Federal Information Processing Standards (FIPS)-validated.
- **Granular role-based access control (RBAC).** Least-privilege access is key to reducing ransomware and insider threats. Granular RBAC provides an efficient and effective means to reduce the risk of unauthorized access to data while granting authorized users the minimum privileges required to do their work.
- **Strong authentication with multi factor authentication (MFA).** MFA has become a de facto standard for strong authentication. To protect your backup data from ransomware and other threats, ensure phishing-resistant asymmetric key cryptographic challenge-response authentication protocols (not text-based) MFA is enforced for access.
- **Separation of duties.** Administrative control (also known as Quorum Approval) used by organizations can prevent fraud, sabotage, theft, and other security compromises. It's the principle that no person, role, or group should be able to execute all parts of a transaction or process.
- **Data classification.** Intelligent data management helps organizations proactively identify, classify, and protect their most sensitive and valuable data, and prioritize their recovery efforts.

- **Automation.** The ability to configure regular backup schedules, policies, and reporting, as well as to perform automated testing to verify the integrity of backups. This automation helps ensure that backups are reliable and can be restored quickly when needed.
- **Actionable alerts.** Customizable, real-time alerts ensure that IT and security teams receive prompt notification of important events. Alerts allow you to build custom playbooks to streamline response operations.
- **Extensible application programming interfaces (APIs) and third-party integrations.** Customizable management APIs, pre-built workflows, and third-party integrations provide an extensible, future-proof solution that helps streamline operations and enhance data security.

Customer Story

Emerge IT Solutions Helps Client Recover from Ransomware Attack in Just 3 Days with Cohesity DataProtect

Founded in 2004, Emerge is committed to being the most trusted technology adviser in the Ohio Valley. The company accomplishes this with best-in-class technical knowledge and competency, leading technology, superior customer service, and a commitment to long-term relationships.

CHALLENGE

Emerge IT Solutions has been helping customers in the Midwest with their IT needs since the early 2000s. For several years Emerge has seen surging interest in its managed cybersecurity services. Some companies that Emerge works with face pressure from supply chain partners to meet more stringent cybersecurity policies, making compliance important for revenue attainment and retention.

Emerge offers managed data protection as part of its OmniWATCH suite of security offerings, which also include penetration testing, security auditing, and threat detection. Until 2022, Emerge used several popular backup technologies. But backing up several petabytes took 24 hours, and restoring large data sets sometimes took days.

SOLUTION

Emerge found its answer in Cohesity DataProtect, which it offers as a managed service. Running on Emerges private cloud, DataProtect reduces risk with immutable copies, multifactor authentication (MFA), and role-based access controls (RBAC). And it's fast. Today, Emerge uses Cohesity DataProtect to back up several petabytes of customer files, including virtual machines (VMs), virtual desktops, applications, and data. For extra protection, Emerge uses Cohesity's DataLock feature to create a backup snapshot that nobody can alter—not even an administrator—until the lock expires.

For a large manufacturer with multiple locations, Emerge's Cohesity-powered backup and recovery service paid for itself many times over in the first month. Weeks after Emerge implemented Cohesity DataProtect for backup and recovery, the manufacturer was hit by a targeted ransomware attack that encrypted nearly all of its 65 VMs and 500 virtual desktops.

Emerge quickly confirmed that certain production servers were encrypted, and that the problem was spreading. The manufacturer's security partner soon determined that the event was a large-scale attack by a nation-state threat actor.

Emerge sprang into action to restore clean files from the Cohesity backups, forming a team that worked around the clock for three days. The first step in recovery was identifying the most current backup copy that wasn't infected. The Emerge team used a third-party tool to identify the most recent backup without the attack signature.

Working from the clean copy, Emerge began restoring VMs and virtual desktops in the order the customer requested—most critical first. The recovery process was so straightforward that Emerge needed no help from Cohesity support despite having deployed DataProtect only one month earlier.

OUTCOME

Fast recovery had a significant impact on the bottom line. Recovering in three days instead of the 14 to 21 days typical of this type of attack saved approximately $12 million in downtime costs. No ransom was paid.

Now Emerge is putting Cohesity DataProtect to work for disaster recovery, using it as part of a hybrid cloud. If a customer's production environment goes down, Emerge can spin up their VMs right on its private cloud or in Azure.

Highlights of the ransomware attack recovery for Emerge's manufacturing customer:

- **3 days to restore 80% of operational data encrypted in attack**
- **11 to 18 days faster recovery than typical for this type of attack**
- **Approximately $12M saved in downtime costs**
- **No ransom paid**

LEARN MORE

Visit https://www.cohesity.com/solutions/ransomware to learn more about mitigating ransomware risk, and take the ESG Ransomware Preparedness Assessment. You can also download Protect, recover, and get more from your data: A guide to selecting an AI-powered data security and management platform.

COHESITY