Ransomware Resiliency

Three steps to building an effective strategy.

VERITAS

OVERVIEW

Today, an organization is hit with a ransomware attack every 11 seconds. In the time required to reach the closing sentence of this brief, a predicted 30+ additional organizations will have potentially fallen victim to this data-damaging malware phenomenon. And the bad actors behind these threats are only getting smarter. Fortunately, so is Veritas, and we're committed to sharing our knowledge to improve customers' confidence in operational resiliency in the face of an attack.

Building a resiliency strategy is no longer a measure taken only by organizations bound by stringent compliance and security standards—it's a necessity for all those seeking to ensure the livelihood of their organization. Preparing for a ransomware attack is an essential part of this strategic groundwork.

Data protection experts across Veritas collaborated in drafting this three-part solution guide to improving ransomware readiness, including steps to help your IT team develop a framework to support data integrity in your organization.

Reduce IT attack surface

In an ideal world, an organization's frontline cybersecurity solution would provide an impenetrable layer of protection to IT systems. However, given the evolving state of malware coupled with increasing IT complexity, a single layer, no matter how robust, may potentially be breached. At Veritas, we advise customers take a multilayered approach to protection, so if one defense measure fails there are others to secure the system.

Today, any data that can be accessed can be potentially compromised and encrypted by ransomware, including network-accessible backup files. Recent strings of ransomware have been designed to seek and infect backup files, dramatically delaying or inhibiting an organization's ability to recover. With backups representing an organization's key to recovery, it's critical they remain intact and unaltered in a ransomware attack. Implementing hardening measures and a security framework is essential. Steps such as having multiple copies of data, including storing copies on air-gapped and immutable storage, provide assurance backups will function as intended if and when they're needed.

Maintain data integrity with:

- Veritas NetBackup™ and Veritas Backup Exec™ software supporting encryption at-rest, role-based access control and secure communications to protect backup data and configuration.
- Veritas Appliances for a hardened platform and immutable storage.
- Veritas Access Appliances for secure, long-term retention.
- Built-in replication features with NetBackup Auto Image Replication (AIR) that can facilitate securing data in other locations, including air-gapped storage.

Detect anomalous activity and behaviors

An important line of defense against ransomware is awareness—knowing what data you have, where it resides and who can access it. Although today's complex IT deployments can make end-to-end visibility a challenge, we can now gain clarity using tools to present cross-system data and infrastructure information, including audit logs, file types, access permissions and reads and writes—all in

customizable, intuitive user interfaces. You can then use these powerful tools to refine role-based permissions, ensuring data is accessed and managed only by trusted parties in your organization.

Once clarity on user access and data management permissions is in place, IT teams will benefit from tools capable of automatically detecting and reporting changes in data access and baseline data activity. Establishing a standard of awareness of interaction with the organization's data and infrastructure supports swift detection of anomalous activity and the ability to respond purposefully, including orchestrating blocking access to suspicious users and compromised accounts as well as targeting known ransomware files.

Monitor and report with:

- APTARE™ IT Analytics, presenting infrastructure in a single view to identify protection and security gaps.
- Veritas Data Insight, scanning data across different data sources, with the ability to detect and report anomalous behavior and deviations in usage patterns as well as identify potential ransomware files based on known ransomware file extensions.

At-scale, strategic recovery

A ransomware attack rarely impacts a single system; what can start as one corrupted device can quickly spiral and endanger the entire data center. Today, many IT teams are building and maintaining hybrid and multicloud infrastructures to satisfy the multifaceted needs of the modern enterprise—and that complexity compounds recovery.

When ransomware strikes, maintain control of your business with an automated, orchestrated recovery process that cuts through the complexity and works across any and every infrastructure. And complement those recovery capabilities with frequent and comprehensive nondisruptive testing.

Orchestrate recovery with:

- NetBackup and Backup Exec, offering easy, reliable data recovery—even at scale.
- Veritas Resiliency Platform with NetBackup, supporting automated, orchestrated recovery with testing capabilities to ensure plan functionality and malware-free recovery.

Answering "What if?" with peace of mind in resilience

Although rumination over ransomware can take a toll, it's not for naught. Guided by our three steps to improve ransomware readiness, you can develop and test a resiliency strategy to reinforce your organization's data and infrastructure against modern malicious threats and take on ransomware with confidence.

Today, Veritas helps to instill this confidence with the Enterprise Data Services Platform—a comprehensive set of technologies built to protect IT systems, detect potential risk and ensure strategic recovery. Even though we can't account for every variable the future holds, we can help you gain peace of mind and defy uncertainty, knowing your organization can recover regardless of the scenario.

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 99 of the Fortune 100—rely on us to abstract IT complexity and simplify data management. Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas supports more than 500 data sources and over 150 storage targets, including 60 clouds. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

VERITAS

V1041 07/20