VERITAS

Creating Ransomware Resiliency: The Role of AI, ML, and Automation

Ransomware threatens modern organizations of all sizes and industries. Through the first half of 2021, global ransomware volume reached 304.7 million, surpassing 2020's full-year total (304.6 million)—a 151 percent year-to-date increase. The U.S. was hit with a startling 185 percent increase for the same period[1]. And yet, 64 percent of senior IT executives say that security measures haven't kept up with IT complexity[2].

To protect themselves from ransomware, enterprises need to:

1. PREVENT attacks with a layered plan that makes their data and environment more resistant to destruction, encryption, or exposure.

2. DETECT and mitigate the impact of vulnerabilities and potential threats with improved visibility and control of data, infrastructure, and user activity.

3. RECOVER to ensure one-click, orchestrated, and automated recovery, so you are up and running quickly with minimal impact to your business.

Technologies, such as advanced automation and orchestration, artificial intelligence (AI), and machine learning (ML), can help organizations prevent attacks, quickly supply alerts if attempts are made, and recover rapidly in the case of an attack.

Complex Environments, Steep Challenges

Ransomware challenges enterprises for several reasons.

A savvier enemy. Attacks are no longer perpetrated by one or two bad actors. They have become far more organized. In addition, the barrier of entry is lower due to ransomware-as-a-service which puts malware in anyone's hands. Attacks are also getting bigger and bolder. New stories come out every week of attacks on organizations ranging from local and state governments to national fuel distribution companies. Stay up to date with the latest information from the United States Government.

Accelerating change. During the COVID-19 pandemic, companies accelerated plans to modernize their infrastructure to accommodate the shift to remote work and meet new supply and demand challenges. Many of these quick and reactive shifts left security vulnerabilities that bad actors were able to take advantage of.

Complex infrastructure. As organizations modernize, they've adopted hybrid and multi-cloud infrastructures, plus containerized application and data environments. This type of architecture offers greater flexibility and scalability while also accommodating legacy infrastructure. But it has made visibility more difficult, increasing the chance of unrecognized threats.

Interconnectivity. Modern, highly integrated IT systems are more flexible and scalable, but they also make ransomware particularly destructive. Such environments provide criminals access to an organization's data—including backups—through a single point of entry. An important best practice is to develop a segmented environment and adoption of the 3-2-1 Backup Strategy.

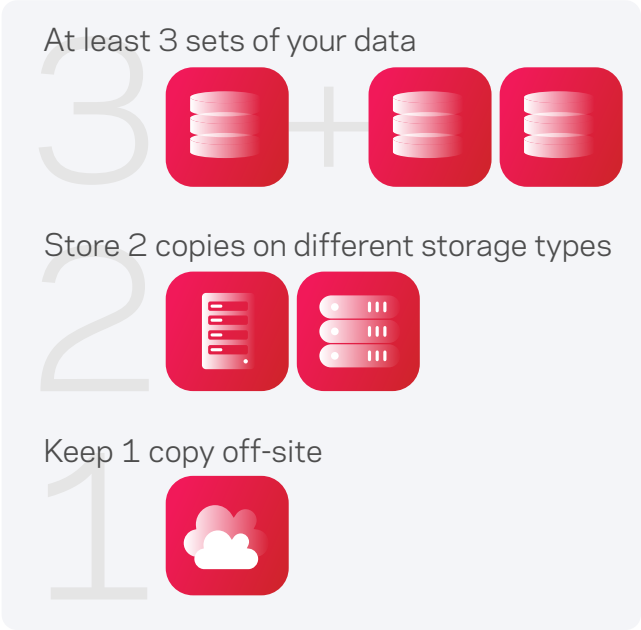

Figure 1: 3-2-1 Backup Strategy.

A false sense of security. IT organizations may think that because their data is in the cloud, it's safe. That assumption is untrue, and it has potentially dangerous consequences. Although cloud service providers (CPSs) implement the best security standards and industry certifications, storing data and important files on external service providers always creates new risks. What's more, you are responsible for data protection in the cloud—not your CSP.

Siloed security tools. As infrastructure becomes more complex and interconnected, administration is often siloed by business unit or function. Individual tools meant to discover and administer workloads are typically limited in scope, leaving undetected gaps.

Insecure backups. Any data that can be accessed and changed can be accessed and changed by ransomware. This includes backup files and peripheral aspects of backups, such as metadata tables and processes. With backups offering an organization's key to recovery, applying system-hardening and immutability best practices is essential.

64%

of senior IT executives say that security measures haven't kept up with IT complexity.

Automated Solutions to Protect, Detect, and Recover

Protecting your organization's data from malicious encryption involves automating three primary lines of defense: enabling security measures on all assets across the entire environment to prevent incursion, detecting anomalous behavior that could indicate possible breaches and malware, and orchestrating complex recovery operations.

Automated policy enforcement ensures that no workloads are overlooked—even in a containerized environment where servers regularly spin up and down. Staying ahead of ephemeral VMs with manual processes risks leaving some unprotected, and it's too time-consuming to be effective. Intelligent queries can automatically protect assets as they're created without human intervention, greatly reducing the risk of exposure.

Intelligent detection leverages AI and ML to detect anomalous activity that could indicate the presence of malware. This detection continually improves its understanding of healthy operation parameters to detect unexpected activity, such as network activity spikes, the time it takes to perform a periodic backup, or a change in deduplication ratio. Those are minor shifts, but they can also be telltale markers of malicious activity: intruders often lurk under the radar to gather information about the environment before they attack. The system also uses feedback from administrators to reduce false positive reports so IT can spend less time responding to false alarms.

Orchestrated recovery including complex, multi-step processes, such as restoring multi-tiered business services and networks with a single click. Recovery should be automated, seamless, and disruption-free.

Modern data security requires a flexible platform-based solution that protects data regardless of where it lives in your environment – physical servers, virtual machines, cloud infrastructure, and Kubernetes environments. Your solution should automate complex operations, such as shifting to an alternate network or going to cloud from an on-premises environment. To ensure recoverability, it should also automate regular health checks capable of flagging active ransomware without impacting production environments.

Veritas NetBackup offers unified data protection across all environments, giving enterprise IT a simple, powerful way to ensure the integrity and availability of their data with advanced automation and intelligent technologies.

To learn more about how Veritas NetBackup can help your IT and security teams safeguard your systems against ransomware, visit veritas.com/protection/netbackup.

1. https://www.sonicwall.com/news/sonicwall-record-304-7-million-ransomware-attacks-eclipse-2020-global-total-in-just-6-months/

2. https://www.veritas.com/content/dam/Veritas/docs/ebook/V1117_GA_EB_2020-ransomware-resiliency-report_EN.pdf

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The 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 Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

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

For global contact information visit:
veritas.com/company/contact

V1365 09/21