VERITAS

VERITAS REDLab

Developing and Validating Malware Defense

Researching and testing Veritas resiliency solutions.

Solution Overview | September 2023

Executive Summary

Malware and ransomware show no signs of slowing. Their persistent evolution presents a formidable challenge for cybersecurity and data protection professionals.

Malicious actors can exploit the very tools and resources employed to thwart these threats. When successful, they can breach, threaten, and extort organizations. It is imperative to take a dynamic, proactive approach to data security to stay ahead of the tactics of cybercriminals.

To better protect your data, we built Veritas REDLab, a proprietary lab. REDLab tests and validates our solutions to ensure we provide the highest levels of data protection. We use this information to continually evaluate and develop new data protection features within our portfolio.

Our testing helps us identify enhancements to help keep your data—and your business—safe.

Cybersecurity Ventures predicts global ransomware damage costs to exceed

$265 billion

by 2031[1]

Validating Resiliency

Data protection is the last line of defense in ransomware attacks. We focus on ransomware protection features as critical elements of our portfolio. We initially used publicly available research in our design process, but we quickly realized that we needed more specific information to maximize the efficiency of our solutions.

In particular, we want to conduct our own research to study attacks as they occurred so we can:

- Assess features to aid in detecting ransomware attacks
- Improve protection of backup repositories
- Provide faster recovery when needed

Staffed by senior security engineers from several established security organizations, REDLab is completely secure. We hired an external consulting team with more than 100 years of combined experience to validate our initial REDLab tests.

Our first task was to verify our claims in ransomware resiliency. The REDLab team performed simulated and real ransomware attacks on Veritas products, including Veritas Alta™ Data Protection, NetBackup™, and NetBackup Appliances. These tests also provided us with a new perspective into the inner workings of ransomware itself.

Cybercrime is a dynamic, evolving environment. It is critical that we test against all possible threat vectors to confirm product resilience and stability. Doing so allows us to keep our solutions up to date, while efficiently introducing new capabilities. REDLab research enables us to consistently provide industry-leading ransomware protection.

The REDLab initiative has improved our understanding of the requirements for infrastructure, applications, ransomware identification, and debugging. It also helped define how to simulate disaster recovery scenarios, as well as maintain, clean up, and quickly rebuild systems.

The REDLab team defined and outlined procedures for secure handling of malware with Veritas solutions. This effort included:

- Implementing secure ways to bring in product binaries
- Writing a product-specific fuzzer program to expose vulnerabilities
- Defining standard operating procedures

83%

of organizations studied have had more than one data breach.[2]

Ensuring Security

Our development teams focus on detecting malware, protecting against threats, improving detection, and new ways to enhance protection. To begin testing, the REDLab team selected several of the top 30 malwares that have wreaked havoc in recent years.

The team used multiple production-like datasets during the tests, including applications and unstructured data. After injecting malware into the environments, they performed detection with Veritas Alta Data Protection and NetBackup malware scanning, Symantec protection, and Microsoft Defender. When well-known scanners failed to detect the malware, the team relied on Veritas anomaly detection results. The REDLab team shared malicious signatures with the respective vendors to help them improve their own detection capabilities.

The tests validated the Veritas product claims.

The testing also uncovered new ideas and identified issues that we've actively worked to address with new product features. We use further tests to foolproof the solutions as part of the development process.

 Protect	Veritas protects more than 800 data sources and more than 1,400 storage providers. Veritas solutions include increased levels of automation through intelligent policies. Air-gapped solutions safeguard data integrity, helping to ensure that backup files remain safe and untouched from malicious invaders. Immutable and indelible backup images use an internally managed, secure compliance clock.	**Impenetrability:** Hardened for security, the full NetBackup Appliance stack includes proprietary policies that conform with Security Technical Implementation Guide (STIG) standards. Mandatory access control, intrusion detection, and protection services maintain an audit trail of important users and system actions.
		Infrastructure Protection: Veritas Alta Data Protection and NetBackup use a single console to protect multi-cloud, virtual, physical, and modern workloads from any place.
		Tamperproof Hardware: Appliances hosting immutable storage can move into a heightened security level to protect data and infrastructure.
		Zero Trust Security Posture: Granular role-based access control (RBAC) with multi-factor authentication (MFA) uses a security assertion markup language (SAML) 2.0-compliant identity provider.

 Detect	Veritas offers AI-powered anomaly and malware detection on primary and backup data. Event-triggered malware scanning increases your opportunity to act before cybercriminals do.	**Integrated Malware Scanning:** Veritas Alta Data Protection and NetBackup provide automated and on-demand scans for protected backups.
		Anomaly Detection: Veritas Alta Data Protection and NetBackup identify unusual data across your entire environment and provide alerts to suspicious anomalies in near-real-time.
		IT Analytics: Veritas Alta™ View and IT Analytics provide a ransomware risk assessment dashboard with predictive analytics to identify potential risks within backup environments.
		Secured Access Controls: Veritas Alta Data Protection and NetBackup offer role-based access, single sign-on, and customizable authentication.
 Recover	Built-in security solutions ensure that recovery procedures bring ransomware-free data and environments back online. Veritas can recover an entire data center in the cloud and on demand, with the flexibility to quickly recover individual databases and files. Additionally, Veritas offers the ability to recover servers elsewhere, andplus perform rapid recovery at scale, including orchestrated bulk recovery.	**Isolated Recovery Environment (IRE):** The IRE offers a secure copy of critical backup data, providing administrators with a clean set of files on demand for recovery.
		Active Directory: Veritas provides the capability to recover a lost Active Directory.
		Recovery Post Infection: Leverage a range of capabilities to recover at scale, including: ▪ Veritas Alta Data Protection and NetBackup instant rollback for VMware ▪ VM recovery ▪ Instant access for MSSQL and VMware ▪ NetBackup Snapshot Manager ▪ Universal share and protection points ▪ Long-term retention archive ▪ Bare metal restore
		Tiered Recovery Orchestration: The NetBackup Resiliency Platform allows users a choice of data-mover technologies to rehearse or orchestrate recovery of one or more multi-tiered applications.

Staying Ahead of the Curve

Veritas integrations for third-party security information and event management (SIEM) platforms feed our solutions audit events, as well as potential anomaly and malware security threats, before they trigger a business continuity event. If a malware infection is confirmed on a protected system, Veritas Alta Data Protection and NetBackup can use built-in controls to automatically pause data protection and expiration activities. In addition to the built-in capabilities, IT teams can program security orchestration, automation, and response (SOAR) platforms to launch Veritas Alta Data Protection and NetBackup APIs to automate security responses.

We are also working on advanced AI and machine learning algorithms to catch zero-day attacks on entities protected by Veritas Alta Data Protection and NetBackup.

To ensure that our customers have the best data protection and fastest recovery possible, Veritas considers it a necessity to invest in REDLab to test and validate our solutions in a secure environment..

Keep up-to-date with Veritas REDLab.

1. 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics, Cybersecurity Ventures, May 2023
2. Cost of a Data Breach Report 2022, IBM, 2022

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. 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

V1806 09/23