VERITAS

REDLab

Making and Verifying Ransomware-Resilient Veritas Products

White Paper | January 2023

Executive Summary

While Veritas is innovating and investing more into ransomware resiliency, we need to validate and verify our claims in-house. This document talks about the journey of building an isolated security lab and its considerations and experiments carried out with NetBackup. It will also cover the additional steps needed for Veritas to enhance the product, since customers look at data protection as the last line of defense in the case of a ransomware attack.

Validating Ransomware Resiliency

As Veritas continues to help customers protect their data, we must evaluate and develop new ransomware protection features as critical prerequisites in our backup platform. Veritas initially used widely available research in the public domain to design our ransomware protection features, but we quickly realized that more specific research was needed to maximize the efficiency of the solution.

To conduct our own research, Veritas built an isolated lab to study ransomware and malware attacks first hand. This launched the project codenamed REDLab.

Veritas wanted to study attacks as they occurred, assess features that aid in detecting ransomware attacks, protect the backup repository, and speed recovery in case of contingency.

As an immediate step to confirm the claims in ransomware resiliency, Veritas had to perform simulated and real ransomware attacks on our products, and enable team members to acquire the skills needed to tackle these tasks.

Based on the severity and high number of ransomware attacks across large institutions, it is imperative for Veritas to keep its ransomware solutions up to date in order to quickly and efficiently introduce new capabilities to the market. Leveraging REDLab research allows Veritas to stay committed to providing industry-leading ransomware protection to all of our customers.

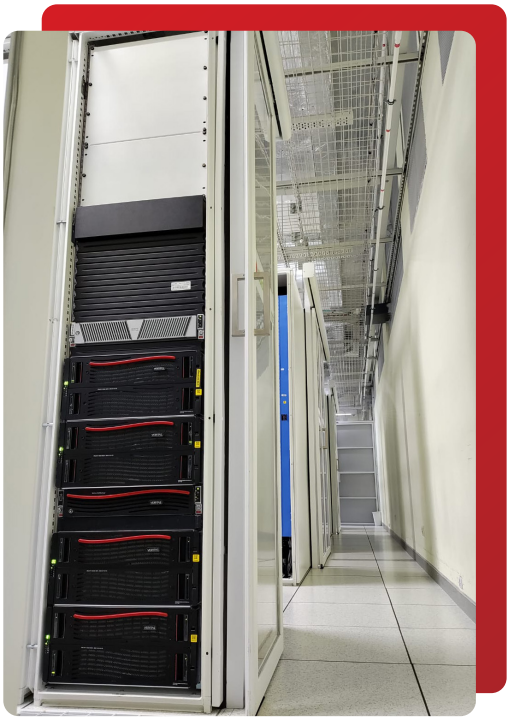
In today's dynamic environment, there is a necessity to test our products against all the possible threat vectors and confirm that the solution is resilient and stable.

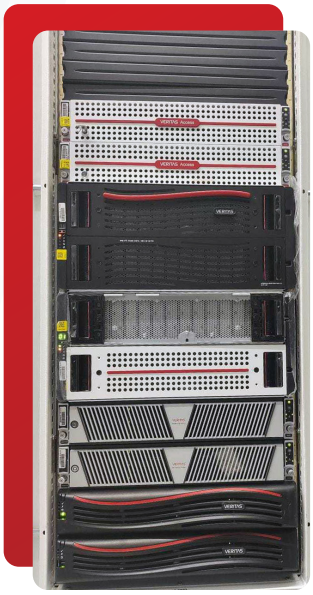
As a result, Veritas invested in recruiting full-time senior security engineers from several established security organizations, and designed an isolated testing lab. This initiative helped our team understand the requirements from infrastructure, applications, ransomware identification tools, and debugging. It also helped in defining how to maintain, clean up, rebuild systems quickly, and simulate disaster recovery scenarios.

Veritas also hired an external vendor team with more than 100 years of combined consulting experience to validate REDLab's experiments.

REDLab is completely isolated, with no outside network connectivity, and follows all security norms and stringent operating protocols.

We've also defined and outlined procedures to handle malware securely, and designed REDLab to accommodate the various solutions offered by Veritas. Implementing secure ways to bring in product binaries, writing a product-specific fuzzer, and defining standard operating procedures were some of the steps taken to build and evangelize REDLab.





The team selected several of the top 30 malwares that wreaked havoc in recent years to begin the experiments. Various production-like data sets were considered during the tests, including applications and unstructured data.

Malware injections were carried out in these environments, and detection by NetBackup malware scanning, Symantec protection, and Microsoft Defender were performed.

Veritas anomaly detection results were utilized when well-known scanners failed to detect malware. The REDLab team submitted malicious signatures to the respected vendors to improve their product detection capabilities.

These experiments showed us fascinating results and validated the Veritas claims. We also discovered some new ideas and issues during this journey, and are actively working on incorporating new features into our products.

Many experiments in REDLab were conducted to foolproof the solution, and several videos were made showcasing the outcomes.

Below are a few NetBackup features that support our claims in the cyber resilience space:

Protect

1. From the protect perspective, Veritas supports 800+ data sources, 1,400+ storage providers, and 60+ cloud providers. Our solutions include an increased level of automation through intelligent policies, air-gapped solutions to safeguard data integrity (which helps ensure backup files remain safe and untouched from malicious invaders), and immutable and indelible backup images with an internally-managed secure compliance clock.

These are the main highlights:

- ✔ **Hardened Impenetrability Flex:** The full NetBackup Appliances stack has been hardened for security, including proprietary security policies that conform with security technical information guide (STIG) guidelines, mandatory access control, and intrusion detection and protection services that maintain an audit trail of important users and system actions.
- ✔ **Modern Infrastructure Protection:** NetBackup protects multi-cloud, virtual, physical, and modern workloads from any place, all from one console.
- ✔ **Tamperproof Hardware Flex:** Appliances hosting immutable storage can move into a heightened level of security to protect data and infrastructure.
- ✔ **Zero Trust Security Posture:** Granular role-based access control (RBAC) with multifactor authentication (MFA) using a security assertion markup language (SAML) 2.0 compliant identity provider.

Detect

2. From the detect perspective, Veritas offers AI-powered anomaly and malware detection on primary and backup data. Event-triggered malware scanning provides an increased chance to act before cybercriminals do.

Features include:

- ✔ **Integrated Malware Scanning:** Veritas provides automated and on-demand scans for protected backups
- ✔ **Anomaly Detection:** NetBackup provides AI-powered anomaly detection that discovers unusual data across the entire environment and provides alerts to suspicious anomalies in near-real-time
- ✔ **IT Analytics:** NetBackup IT Analytics provides a ransomware risk assessment dashboard using predictive analytics to understand potential risks within a backup environment
- ✔ **Secured Access Controls:** Veritas offers role-based access, single sign-on, and customizable authentication

Recover

3. From the recover perspective, Veritas has built-in security solutions to ensure that ransomware-free data and environments are brought back online. It can recover an entire data center in the cloud and on demand, with the flexibility to quickly recover individual databases and files. Veritas offers servers to be recovered elsewhere, recover at scale including orchestrated bulk recovery.

- ✔ **Isolated Recovery Environment (IRE) in Bring Your Own (BYO) and Flex:** The IRE offers a secure copy of the critical backup data, providing administrators a clean set of files on demand for recovery
- ✔ **Lost Active Directory:** NetBackup provides the capability to recover a lost Active Directory
- ✔ **Recovery Post Infection:** Veritas offers a wide range of capabilities to help recover at scale, including 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, and Bare Metal Restore
- ✔ **Tiered Recovery Orchestration:** NetBackup Resiliency Platform allows users to rehearse or orchestrate recovery of one or more multi-tiered applications, using a choice of data mover technologies

In conjunction with ongoing work, Veritas integrations for third-party security information and event management (SIEM) platforms feed NetBackup audit events, and potential anomaly and malware security threats, before they trigger a business continuity event. NetBackup can also automatically pause data protection and expiration activities using built-in controls, if malware infection is confirmed on a protected system. In addition to the built-in capabilities, security orchestration, automation, and response (SOAR) platforms can be programmed to launch NetBackup APIs to automate security response.

We are also working on advanced artificial intelligence/machine learning (AI/ML) algorithms to catch zero-day attacks on NetBackup protected entities.

Veritas is proud to invest in REDLab in order to test and validate our solutions in an isolated environment to overcome live malware attacks and improve our ransomware resiliency, and we look forward to innovating further.

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 02/23