Better Together: Veritas and Elastio

Ensure reliable ransomware recovery with Veritas and Elastio AI ransomware detection.

Introduction

Conventional security tools often fail to protect your data from ransomware threats effectively, as evidenced by the rise in successful attacks. When an attack occurs, organizations must ensure their recovery data is cleaned to prevent the ransomware from immediately reinfecting and corrupting data.

Elastio's AI/ML-driven engine, developed from reverse-engineering over 2,300 ransomware families, achieves 99.95% accuracy in detecting known and unknown ransomware encryptions.

Ransomware can defeat the best cyber defenses. Ransomware developers use advanced techniques to evade detection. These include encryption, polymorphic code that changes with each infection, and the use of fileless malware that operates in memory rather than leaving traces on the hard drive.

And ransomware often enters systems through phishing emails or malicious attachments, exploiting human vulnerabilities rather than technical ones. These attacks can be highly targeted and convincing, making it difficult for users to recognize the threat. Ransomsware also exploits zero-day vulnerabilities, which are security flaws unknown to the software vendor. Without prior knowledge of these vulnerabilities, detection systems cannot identify and block the ransomware.

Effective detection of ransomware requires deep inspection of data that will identify elusive indicators of a pending or active ransomware attack. This is a critical requirement for ransomware recovery, determining if data is free from ransomware.

Veritas and Elastio provide the ultimate solution for ensuring clean and reliable recovery. With Elastio, Veritas backup data can be inspected to ensure that ransomware encryptions are identified as soon as the data is backed up. Additionally, Elastio scans for malware binaries, which can prevent ransomware attacks. This provides trusted and reliable recovery so that organizations can restore critical business processes with confidence and trust.

Elastio integrates agentlessly with Netbackup, whether on-premises or in the cloud, actively monitoring all protected data for ransomware and corruption. Elastio scans new backups automatically according to predefined policies and tracks changes across backups to detect sophisticated attacks. It can also scan older or previously unscanned backups to ensure they are ransomware-free before recovery.

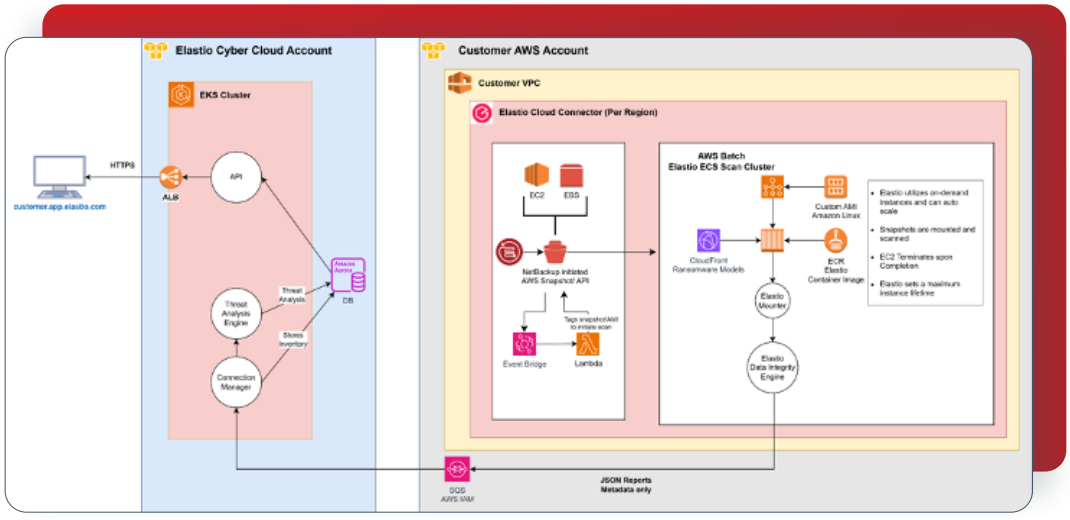

Figure 1: NetBackup Architecture for AWS workloads

Veritas

- **Tightly control platform access** with continuous service authentication and zero-trust protection.
- Use **data immutability** to ensure tamperproof backup data.
- **Achieve early detection** of ransomware threats and malicious activity.
- **Ensure reliable data recovery** by using an isolated recovery environment and limiting risk of recontamination.

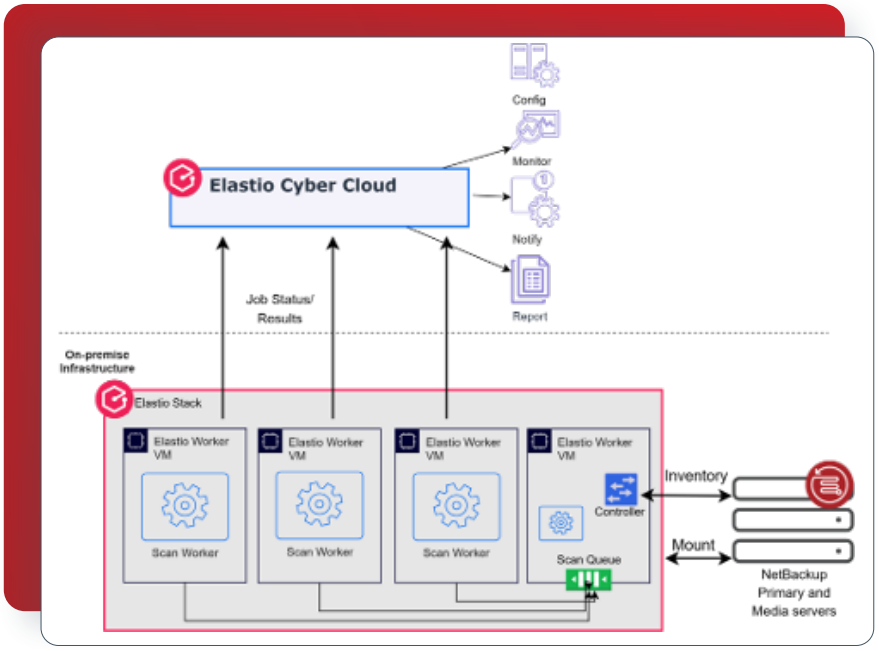

Figure 2: Netbackup Architecture for On-prem workloads

Elastio

- **Enhanced Ransomware Detection:** Elastio's AI/ML-driven deep file inspection adds an additional layer of security, detecting ransomware that traditional methods might miss.
- **Seamless Integration:** Elastio integrates agentlessly with Veritas NetBackup, ensuring continuous monitoring and scanning of backups without disrupting existing workflows.
- **Comprehensive Forensics:** Elastio provides detailed alerts and forensics, including the last known clean recovery point and specific infected file locations, aiding in quick and effective response.
- **Compliance Support:** The integration helps meet compliance requirements by ensuring that backups are regularly scanned for ransomware, aligning with standards like NYDFS, NIST CSF, and DORA.
- **Minimized False Positives:** Elastio's advanced detection model maintains a low false positive rate, enhancing the reliability of ransomware detection within NetBackup environments.

1.IBM: Cost of a Data Breach Report 2023

About Veritas

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers—including 91% 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 and 1,400+ storage targets 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 X 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

V2123 07/24