Better Together: Veritas and Qualys

Manage vulnerabilities for reliable cyber recovery with Qualys.

Ransomware and other risks continue to grow. In many cases, unpatched systems, misconfigurations, and default settings allow threat actors to bypass the best security controls and thwart reliable recovery. Vulnerability management, detection, and response ensure you have what you need to effectively withstand and recover from cyber incidents.

Ransomware remains the foremost threat to cyber resiliency. As threat actors constantly evolve their strategies and tactics, you need to amplify your cybersecurity and cyber recovery controls to counter the growth and diversity of attack tools and methodologies.

Threat actors look to exploit vulnerabilities of unpatched software or improperly configured systems. Prioritizing vulnerability detection and remediation benefits security and recovery against ransomware.

According to Verizon's 2023 Data Breach Investigations Report, vulnerability exploitation is one of the top three vectors of attack. Reciprocally, implementing a robust vulnerability management process that includes continuous assessment is a top strategic defense option.

Qualys vulnerability management prevents threat actors from exploiting known weaknesses in systems and applications to gain access and launch attacks.

Combined with Veritas cyber recovery solutions, Qualys assesses the health of backups to identify vulnerabilities in data and VMs before restoring data. Qualys provides market-leading assessment, prioritization, and remediation of ransomware-causing vulnerabilities for Veritas backup storage. This helps ensure that recoveries are always free from misconfiguration or vulnerability to ransomware. In addition, you can leverage the Veritas backup data to offload scanning from production environments.

Together, Veritas and Qualys can help you reduce the risk of cyberthreats and improve outcomes.

> *Integrated with Veritas 360 Defense, Qualys Vulnerability Management, Detection, and Response accelerates cyber resiliency."*
>
> **Shailesh Athalye,** Senior Vice President, Qualys

Veritas

- Zero Trust data protection and continuous service authentication tightly controls access to platform
- Uses data immutability to support tamperproof backup data
- Threat detection provides early identification of ransomware threats and malicious activity
- Isolated recovery environment ensures reliable recovery of data by limiting risk of re-contamination

Qualys

- Understands and manage cybersecurity risk by proactively mitigating risk exposure
- Leverages database of more than 180,000 vulnerabilities from 25,000 threat sources
- Supports identification of all assets including IT, OT, and IoT
- Uses rules-based integrations with ITSM tools for orchestration and remediation

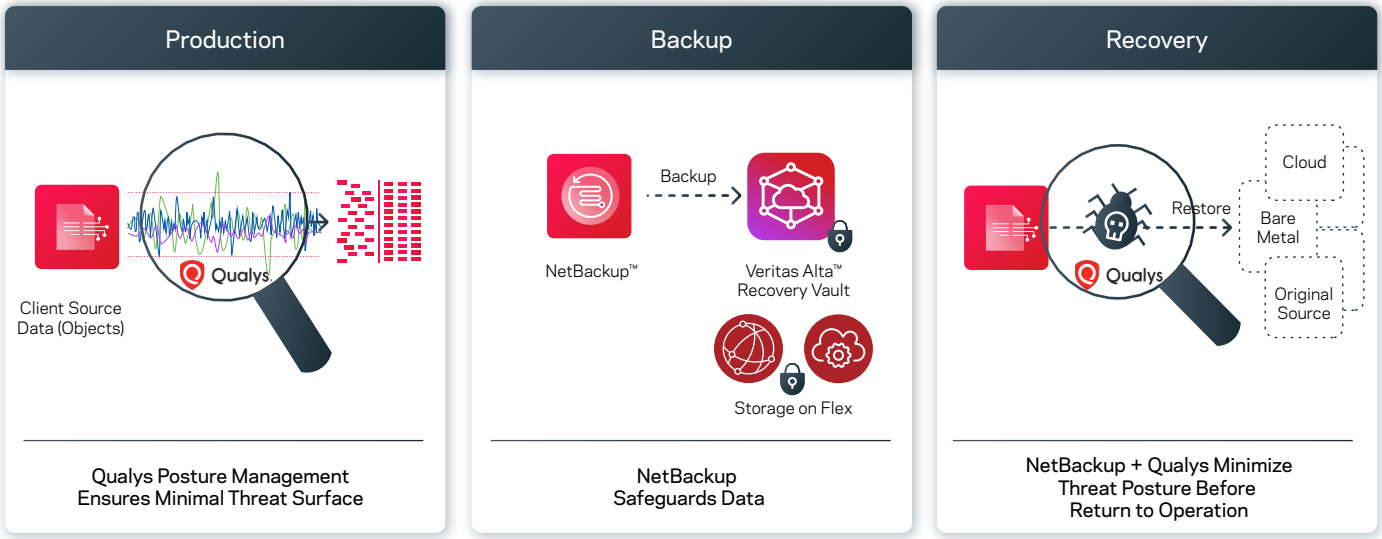

Figure 1. Veritas NetBackup and Qualys work flow

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

V2024 12/23