SOLUTION BRIEF

Varonis IDS Integration

Safeguard your critical data with Qumulo and Varonis

In today's data age, cyber threats are a near-daily occurrence where even a single bad actor can inflict serious reputational and financial harm on a business at any moment. More devices and users are creating, managing, and accessing data from all over the world, making data security more challenging today than ever before. Bad actors are becoming more sophisticated, faster and more efficient with their tactics, requiring immediate detection and rapid response time from IT and data security teams.

To help protect against ransomware and insider threats, Qumulo integrates seamlessly with the Varonis Data Security Platform, delivering real-time visibility and control over your critical data stored in the Qumulo file system. Varonis secures and protects data from unauthorized access and cyber threats by analyzing data activity, authentication events, and perimeter telemetry. These elements are combined to detect behavioral abnormalities that could indicate a threat and help mitigate the impact of breaches by locking down open access to data at scale. Together, Qumulo and Varonis offer a comprehensive solution that allows enterprises to easily monitor, manage, and protect data across various multi-cloud and on-premises technologies.

VARONIS

Solution Benefits

Comprehensive data security

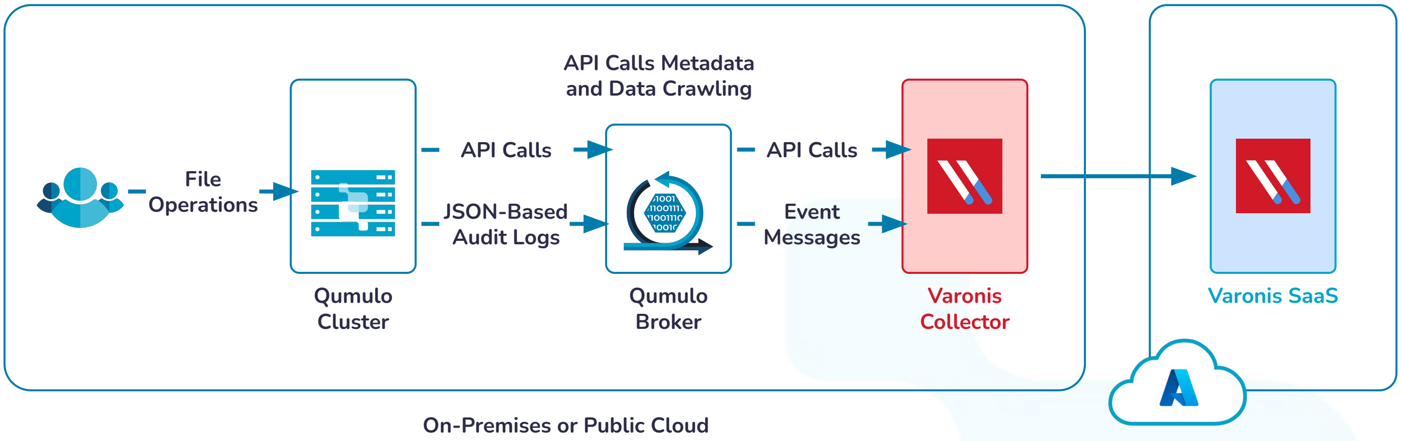
- Advanced threat detection
- Built-in replication with version control
- Data encryption at rest
- Data classification
- Granular access control
- Immutable, lockable snapshots

Visibility and control

- Real-time analytics
- Real-time alerts
- Usage tracking

Maintain a strong security posture against both internal and external threats

The Qumulo-Varonis integration forms a comprehensive security solution, providing a strong security defense against bad actors. Qumulo's own audit logs track user-driven actions such as file access and modification, data sharing through SMB shares or NFS exports, and system configuration changes. In this solution, Qumulo audit logs are sent to Varonis, where they are analyzed using proprietary machine-learning algorithms to automatically detect and alert on anomalous activity [see Fig.1 below]. The combined solution operates across three key dimensions to protect against bad actors' attempts to inject ransomware and malware: (1) prevention through least-privilege automation and continuous data monitoring, (2) detection of behavioral abnormalities across the storage and data layers, and (3) recovery of data in the event of a successful attack.



The diagram above represents how Qumulo is integrated with the Varonis at a high level. The Qumulo Broker middleware layer is responsible for preparing and dispatching events from Qumulo to Varonis.

| info@qumulo.com

Prevention

The Varonis Data Security Platform helps with ransomware prevention through continuous data monitoring and the enrichment of audit logs dispatched from the Qumulo cluster to the Varonis SaaS application. As Varonis analyzes the incoming audit logs,
the platform:

1. Automatically discovers and classifies where sensitive and regulated data lives within the Qumulo filesystems and ensures storage and usage strictly adheres to internal security policies and other regulations.

2. Automatically maps out the Qumulo file system's permission structure, allowing admins to quickly view who has access, where data is stored, and who uses it.

3. Uses the extensive metadata collected by Varonis to understand how data is accessed and used by layering in additional context like classification, geolocation information, and linking users to devices.

4. Makes intelligent decisions about who needs access to data and who doesn't – continuously reducing your blast radius without human intervention and without breaking the business.

Detection

Varonis proactively detects threats to mitigate the impact of cyberattacks and to help minimize the impact of breaches by locking down open access to data at scale. As a result, Varonis
can detect and stop advanced persistent threats, insider threats, and ransomware attacks with fewer false positives and faster incident response.

- Data activity auditing: Varonis monitors Qumulo's SMB shares without requiring native auditing. Varonis captures all the critical events against Qumulo's audit logs — such as read, move, modify, and delete — to help accelerate cross-platform security investigations across your file systems.

- Data-centric UEBA: Varonis' behavioral-based threat models detect abnormal data activity in real time — stopping threats to data before they become breaches. Our UEBA augments Qumulo's backup capabilities for comprehensive ransomware protection.

- Automatic threat response: With instant, automated responses, Varonis performs meticulous interventions to stop an attack in its tracks and limit the damage. Connect Varonis to the XSOAR tools in your tech stack via API-based integrations for automated, efficient incident recovery.

- Proactive Incident response: When you connect to the Varonis cloud, our team of cybersecurity experts can have eyes on your alerts. If we see something alarming, we'll alert you. Plus, our support team can quickly troubleshoot issues without accessing your corporate network

Recovery

Attackers may lurk for a period of time before taking action to exfiltrate data or trigger and proliferate instances of malware. It's important to have a preplanned snapshot retention strategy to ensure the right point-in-time recovery can be chosen.

Qumulo enables administrators to create snapshot policies that retain multiple copies over time. If an attacker elevates permissions and begins encrypting data, Qumulo's snapshot-locking feature can still block them from deleting or encrypting existing snapshots. This mechanism allows a storage administrator to first seal off the attack, and then revert back to the uncompromised data to continue normal operations.

Keep your data simply secure with Qumulo and Varonis

The integration of Qumulo and Varonis SaaS provides organizations a comprehensive data protection and management solution. It offers advanced threat detection, data classification, and access control features that complement Qumulo's data protection capabilities. This integration ensures that data is protected, managed efficiently, and compliant with various data
protection regulations.