Document type Confidentiality

Qumulo NeuralProtect with Cisco N9300 Series Smart Switches, Cisco Hypershield, and Splunk

Stop Ransomware in Real Time and Recover in Seconds

Detect threats as files are written, isolate compromised data and hosts automatically, and preserve a known-good recovery point – all through a coordinated defense spanning storage, the network, and security analytics.

Overview

Ransomware and malware can bypass traditional defenses, disrupt operations for weeks or months, and make recovery slow and uncertain. Backups alone do not stop an active attack, and disconnected tools can leave security teams trying to correlate events after damage has spread.

Qumulo NeuralProtect works with Cisco N9300 Series Smart Switches, Cisco Hypershield, and Splunk to create a real-time, multilayer defense. NeuralProtect inspects file content at the point of write, detects known and zero-day malware, creates defensive snapshots, and quarantines compromised files. It then notifies Cisco Hypershield so L4 microsegmentation policies can isolate affected hosts through the N9300 switching fabric. High-fidelity telemetry flows to Splunk for correlation, incident reconstruction, and future automated response. The result is coordinated detection, containment, investigation, and recovery designed to strengthen data and business resilience.

Use the supplied solution architecture diagram showing the integration among Qumulo NeuralProtect, Cisco N9300 Series Smart Switches, Cisco Hypershield, Splunk, and the Cisco Nexus Dashboard.

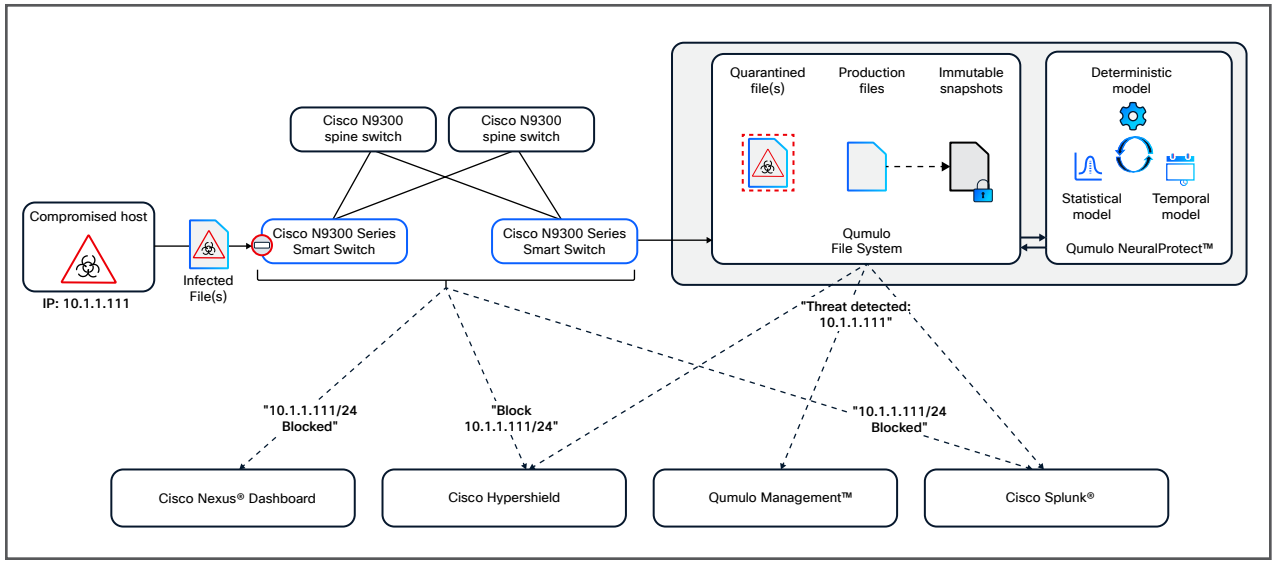

Figure 1. Qumulo NeuralProtect coordinates file inspection, snapshots, quarantine, network containment, telemetry, and incident analysis across the integrated architecture

Benefits

- Detect known and zero-day ransomware in real time with content-based deep file inspection and deterministic, statistical, temporal, and Bitdefender detection engines
- Contain damage immediately by quarantining compromised files and notifying Cisco Hypershield to update L4 microsegmentation policies across Cisco N9300 Series Smart Switches
- Recover faster with defensive, immutable snapshots that preserve the most recently known good-data state when a threat is identified
- Reconstruct incidents with high-fidelity telemetry streamed to Splunk for correlation, analysis, and future automated response
- Reduce operational disruption with a coordinated workflow that links storage protection, network isolation, and security analytics

Ransomware demands coordinated, real-time defense

Ransomware and malware attacks can cause major financial losses and operational disruption that lasts for months. The source document cites an average financial impact of $5 million per incident. Recovery from conventional backups may still take weeks to months, while attackers can bypass standard security controls and continue moving through the environment.

The core challenge is not simply detecting a suspicious file. Organizations must identify known and previously unseen threats as data is written, contain both the compromised data and the affected host, preserve a clean recovery point, and give security teams enough telemetry to understand what happened. When storage, network security, and analytics operate separately, each handoff adds time and uncertainty.

An integrated architecture addresses that gap. Qumulo NeuralProtect provides file-level inspection and isolation, Cisco Hypershield and Cisco N9300 Series Smart Switches extend containment to the network, and Splunk correlates telemetry for investigation and response. Together, these capabilities help you move from delayed recovery to proactive detection, coordinated containment, and rapid restoration.

How it works

A lifecycle of protection

The solution coordinates four stages: detection, containment, recovery, and remediation. Qumulo NeuralProtect monitors file access in real time. When it detects malware, it snapshots the file system and quarantines affected files. It also sends notifications to Cisco Hypershield and telemetry to Splunk, enabling network isolation and incident reconstruction without waiting for a manual handoff.

Deep file inspection in real time

Instead of inferring threats only from entropy or file-pattern changes, Qumulo NeuralProtect opens and inspects every file at the point of write. Its mixture-of-models detection engine combines complementary methods:

- **Deterministic model:** identifies known ransomware families and signature-based threats
- **Statistical model:** detects zero-day ransomware variants that do not have known signatures
- **Temporal model:** analyzes changes over time to identify sophisticated slow-burn attacks
- **Bitdefender security engine:** adds multilayer security technology for real-time blocking and removal of known malware

Instant response and data isolation

When a threat is identified, Qumulo NeuralProtect creates a defensive, immutable snapshot so the latest known good- data state is available for recovery. It moves infected files to a protected quarantine folder and produces an explicit list for forensic analysis. These actions contain contaminated data while preserving evidence and a rapid restoration point.

Coordinated network containment

Qumulo NeuralProtect extends the security perimeter beyond storage by notifying Cisco Hypershield. Hypershield updates L4 microsegmentation policies across Cisco N9300 Series Smart Switches, which automatically quarantine affected hosts. This coordinated action helps prevent a compromised endpoint from continuing to reach protected resources.

Telemetry, investigation, and response

Qumulo NeuralProtect streams high-fidelity telemetry to Splunk. Splunk analyzes and correlates those events with other available signals to reconstruct the incident, guide remediation, and support future automated response. The same workflow helps teams understand the sequence of an attack rather than treating each alert in isolation.

Operational resilience and accuracy

The source document reports a false-positive rate below 0.01 percent, 100 percent detection for known variants, and more than 95 percent detection for zero-day attacks. It also states that rapid containment and instant restoration from defensive snapshots can reduce recovery time from days to seconds.

Practical applications

Environment	Use case
File-based workloads	Inspect files at the point of write, quarantine compromised items, and preserve a known-good snapshot for rapid recovery
Security operations	Stream high-fidelity telemetry to Splunk to correlate events, reconstruct incidents, and guide remediation or automated response
Integrated data centers	Notify Cisco Hypershield to update L4 microsegmentation policies across Cisco N9300 Series Smart Switches and isolate affected hosts

“Detect threats as files are written, isolate compromised data and hosts automatically, and preserve a known-good recovery point.”

“Move from delayed recovery to proactive detection, coordinated containment, and rapid restoration across storage, network security, and analytics.”

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there’s just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

The Cisco Advantage

Cisco extends Qumulo NeuralProtect containment beyond the storage layer. Cisco Hypershield can translate threat notifications into updated L4 microsegmentation policies, while Cisco N9300 Series Smart Switches enforce isolation across the switching fabric. Combined with Splunk telemetry and Qumulo file-level protection, this creates a coordinated architecture for detecting, containing, investigating, and recovering from ransomware.

Learn more

Plan your coordinated ransomware defense

Contact your Cisco or Qumulo representative to review how Qumulo NeuralProtect, Cisco Hypershield, Cisco N9300 Series Smart Switches, and Splunk can fit your environment. Approved public resource URL: N/A – not provided in the source document.

C22-6661301-00 09/26