

# Ransomware Defender for Qumulo

Protecting against cyberthreats at the data layer

## OVERVIEW

More than 90% of the world's digital data is unstructured, and it's growing daily. Managing all this data – often containing sensitive information, intellectual property, and corporate assets – poses a significant challenge. Superna helps to close the data security gap, offering cyberdefense at the data layer.

IT Security Company NCC Group's **Monthly Threat Pulse** of March 2023 reported a 91% increase (459 incidents) in ransomware attacks in March 2023 compared to February 2023, and a rise of 62% compared to March 2022. And unstructured data sits squarely in the crosshairs. The need to protect data at the storage layer has never been more pressing, as cybercriminals continue to exploit vulnerabilities in organizational structures and are now targeting data storage.

## DESIGNED TO FORTIFY YOUR STORAGE ECOSYSTEM

Superna Ransomware Defender provides real-time detection of suspicious behavior at the data layer. When a malicious file is dropped, Superna detects behavior consistent with ransomware access patterns and allows you to prevent replication of ransomware across your storage and network.

## KEY FEATURES

- Automates malicious behavior detection, real-time behavior detection, manual and automated false-positive detection, exfiltration events consistent with ransomware access patterns.
- Alerts administrators and other users involved in the incident response providing them with enough information to prioritize the incident.
- Supports restricting access strictly to already known and trusted sources, paths or users (whitelisting), while effectively blocking all the untrusted ones.
- Tracks and reports previous file access history, prior to the attack for a more effective incident analysis and more accurate incident response.

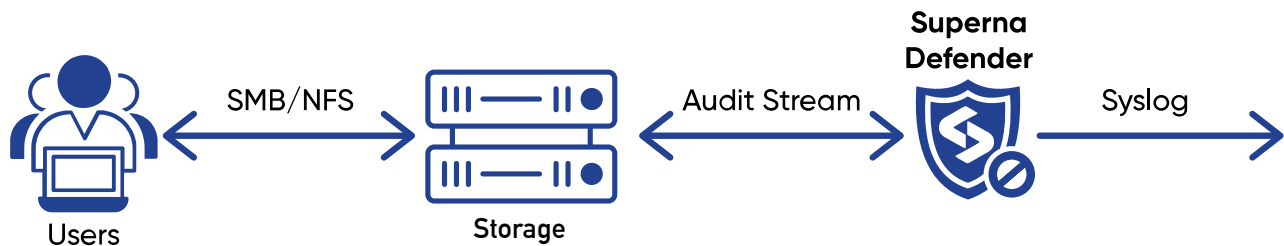


## HIGHLIGHTS

- Superna® Ransomware Defender™ provides universal file and object threat mitigation for object storage environments
- Provides real time threat detection and alerting, with infected files logged for recovery
- Defends against untrusted or malicious data behaviors, including ransomware, exfiltration, mass delete, and untrusted network access in object storage
- Provides post-breach analysis for compliance and forensics
- Based on best practices established by the National Institute of Standards and Technology (NIST)

## USE CASE

In situations where an employee unknowingly opens a malicious attachment or clicks on a malicious link, the ransomware payload begins to infiltrate the organization's network by encrypting files on the company's servers, rendering them inaccessible to users. Superna Ransomware Defender is designed to identify suspicious behaviors, classifying the activity into one of three categories based on severity: warning, major or critical. Initially, it categorizes the incident as a warning. However, if suspicious behavior persists, the severity level escalates, triggering additional notifications to the administrator. They can then review the events and operations that triggered the warning and take appropriate action.



## UPCOMING FEATURES

- Preventing your data from being compromised by initiating automated lockout action against SMB shares and NFS exports with per-user/per-host granularity limiting potential damage and data loss. Allows admins to configure user and critical path snapshots.
- Simplifying recovery by tracking compromised user accounts and infected files which allows administrators to react quickly minimizing disruption and maintaining business continuity.
- Running an automated compliance self-test to ensure the organization is fully protected from the ransomware attack.

## SUMMARY

Unstructured data on large file systems presents a security and audit challenge, with millions to billions of files and thousands of users requiring data access. Superna's subscription license model and a host of easy-to-use features allow you to extract business value from your data repositories.

## WANT TO LEARN MORE?

Interested in learning more about how Superna allows you to secure and protect your structured and unstructured data regardless of where it resides: on-prem, in the cloud, or in a hybrid environment? Contact [letschat@superna.io](mailto:letschat@superna.io) to speak to one of our data protection experts or to schedule a personalized demo.

---

For more on how Superna® can help solve your organization's unstructured data security challenges, visit [superna.io](https://superna.io).