superna® SOLUTION BRIEF

Superna Data Security and Disaster Recovery Solutions for VAST

Bringing cyberstorage capabilities to the VAST Data Platform

MANAGING RISK IN THE AGE OF RANSOMWARE

Many sectors — especially financial services, healthcare, media, infrastructure, and government — have been the target of persistent ransomware attacks. Some make headline news, others are quietly covered up, but up to $265 billion in ransomware damages have been projected. You can't afford to be in a position to permanently lose data, pay extortionate bribes, suffer outages, or face productivity impacts. Unfortunately, traditional approaches to network security, disaster recovery, backups and snapshot archives don't always prevent (or even detect) these types of activities, leaving you wide open to bad actors.

You need sophisticated ransomware protection — embedded at the storage layer — along with robust mechanisms for meeting business continuity and disaster recovery efforts after an attack. You need a unified solution that provides better protection with less effort, so you can restore operations quickly and confidently. Consider this: 33 billion records lost in 2023; $456 million in ransomware payments in 2022; $243 billion in banking non-compliance fines since 2008; and a 50% increase in cyber insurance premiums in 2023. Investing now in cyberstorage protection not only makes good business sense, it's essential!

THE CHALLENGE

Traditional approaches to data protection and cybersecurity have already proven inadequate to detecting and stopping ransomware attacks. More importantly, they're focused on the network and application layers, not storage. Even organizations with extensive security and data management approaches in place have suffered permanent data loss and costly business disruption, resulting in severely damaged reputations.

HIGHLIGHTS

Data Security

- Two-way security integrations into native SIEM and SOAR infrastructures

Data Resiliency

- Surgical recovery of last-known-good version of files
- RTO of seconds or minutes... not days, weeks... or never

Based on best practices established by the National Institute of Standards and Technology (NIST).

WHY CYBERSTORAGE?

Gartner's 2023 Hype Cycle for Storage and Data Protection Technologies recommends that you "prioritize active protection and security of unstructured and structured data storage systems because limiting or blocking an attack is more effective than recovering from one."

HOW SUPERNA COMPLEMENTS THE VAST DATA PLATFORM

Seamless integration with VAST products. Superna and VAST engineers have worked together to provide a native experience for customers to expand the capabilities of the VAST Data Platform.

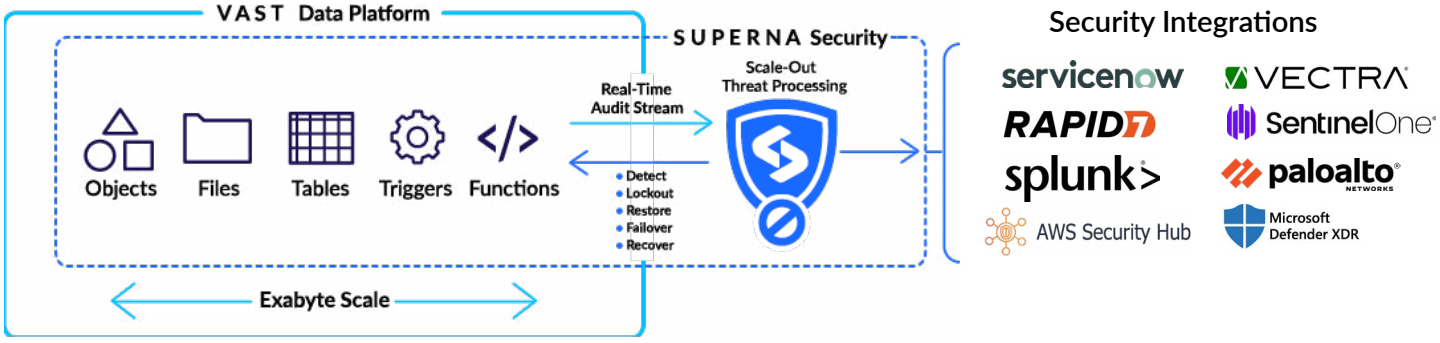
Improved business continuity. By capturing snapshots for rapid recovery, **Superna Disaster Recovery Edition** mitigates the impact of attacks, facilitating uninterrupted business operations.

Preferred protection levels. Whether focusing on recovery options or adopting a more defensive approach by restricting user access. Choose the solution that aligns with your company's processes, and specific needs.

Comprehensive security. The **Superna Data Security Edition** offers a multi-layered defense, including behavioral data, providing protection against both known and emerging ransomware threats.

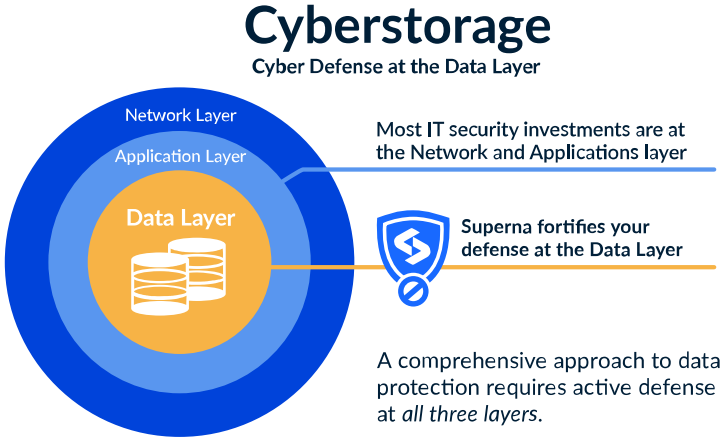
Ease of integration with security tooling. Integrate the **Superna Data Security Edition** into your existing cyber-security infrastructure, enhancing your defense without disrupting your workflow and your process.

Heterogeneous environments. As many people undertake initiatives like move to cloud, repatriation, and diversification of storage (intentional or not), the ability to provide a consistent approach everywhere is essential.



RANSOMWARE DEFENSE

- **Ransomware detection.** You can detect suspicious user behavior patterns, file extensions, and honeypot activity. You can see active and historical alerts based on both learned and configurable sensitivity thresholds. You can custom define specific paths, users, sources, files, and extensions to be either ignored or closely monitored, as appropriate. Ransomware detection is self-testing to make sure it's operating correctly at all times.
- **Ransomware lockout.** Suspicious activity thresholds can trigger automatic user lockout for immediate protection. Or you can instead notify storage administrators or security ops teams to manually review and avoid interruption of business from possible false positives.
- **Ransomware recovery.** When suspicious activity is detected, instantaneous snapshots are taken using NFS exports and SMB shares. You can designate critical paths and quotas to balance protection versus growth of storage necessary. Using the recovery manager, you can review affected files and prioritize which are restored first.



- **Security tooling integration.** You can set up Webhooks, a Zero Trust API, and integrations with popular IT security and operations platforms like ServiceNow, Splunk, and Palo Alto Networks. These will feed Superna data into the central dashboards and alerting mechanisms for seamless monitoring.

DISASTER RECOVERY AND BUSINESS CONTINUITY

- **Planned failover/fail back.** With **Superna Disaster Recovery Edition**, you can greatly simplify and orchestrate the process of switching operating environments with an automatic inventory of services and storage to help you configure smart alerts and jobs. Designs can include hot/hot (active) or hot/cold (standby) clusters and storage. This can be very helpful when normal maintenance and administration would otherwise interfere with access to data and services. You won't need to maintain complex, error-prone scripts nor manually redirect clients to the new location.

> "Before we implemented [Superna], we had been compromised and hit by ransomware several times... [Superna] has alleviated the burden on the helpdesk and the IT department because we're not policing Windows machines that are hosting files anymore. This is a purpose-built, wholly integrated solution for us, so we don't feel like we're the low hanging fruit anymore."
>
> — Christopher Stratis,
> *Director of Information Technology*, MRCE

- **Unplanned failover.** When an event or disaster is detected that impacts access to data, you can orchestrate failover (automatically or manually, depending on preference) to another facility to minimize interruption of services. Simulated failovers demonstrate how effective the system would be in a real event.
- **Daily sync.** You can maintain disaster recovery readiness with daily sync of storage, monitoring and reporting to stay confident the solution is operating as expected. Shares and exports are automatically kept up to date.

About Superna

For more than a decade, Superna has provided innovation and leadership in data security and cyberstorage solutions for unstructured data, both on-premise and in the hybrid cloud. Its solutions are in use in thousands of organizations around the globe, helping them to close the data security gap by providing automated, next-generation cyber defense at the data layer. Superna is recognized by Gartner as a solution provider in the cyberstorage category. For more information, visit www.superna.io.

Ready to get started? Contact your VAST and Superna teams today!