superna®

DATA SHEET

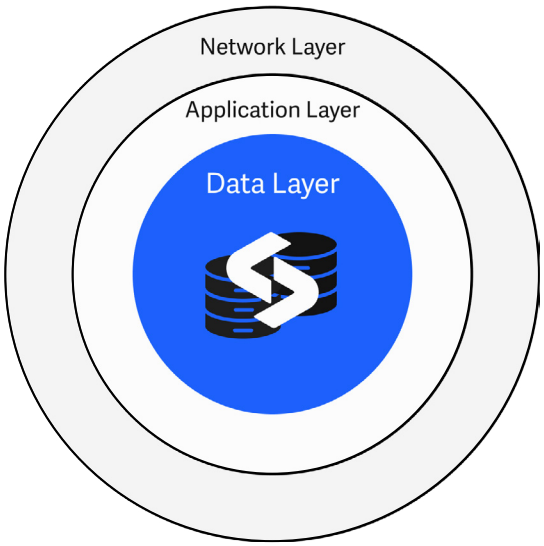
Data Security for DELL

Unstructured Data Platforms - PowerScale and ECS

Protect Your Data at Its Source

Cyber attacks continue and are accelerating. **The attackers are after your data, backups included.**

- Traditional approaches to data protection and cybersecurity have proven inadequate in detecting or stopping ransomware attacks. These solutions typically focus on the network and application layers, but not the data layer.
- Even organizations with extensive security and data management approaches in place have suffered permanent data loss and costly disruption, often resulting in severely damaged reputations.
- For organizations working on developing AI models, data must remain unaltered and accurate throughout its lifecycle - altered models or exfiltration could prove catastrophic.
- In 2024, the average cost of a ransomware attack was $4.54M (IBM).



The Solution

Securing the perimeter is no longer enough. Your data needs to be **protected at its source**.

Coined **Cyberstorage** by Gartner, Cyberstorage protection not only makes good business sense, but is essential for a robust cyber resilience strategy.

Close this security gap with **Superna Data Security Edition** – sophisticated ransomware protection, embedded at the data layer.

Why Cyberstorage?

Gartner Innovation Insight Report: Cyberstorage

"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."

Data Security Highlights

→ **Multi-layered defense**: Behavioral analytics, providing protection against both known and emerging threats.

→ **Proactive, Automated Responses Stopping Threats**: Data snapshots and user lockout on your production cluster to stop attacks and minimize the data loss.

→ **Precision Recovery**: Instantly evaluate the impact and restore the last-known good version of files in just minutes.

→ **Two-way Security Integrations**: Into native SIEM and SOAR infrastructures.

→ **NIST Aligned**: Incorporates best practices established by the National Institute of Standards and Technology (NIST).

→ **DORA and NIS2 Compliant**: Aligns with the Digital Operational Resilience Act (DORA) and the NIS2 Directive for enhanced security and compliance.

Gartner Innovation Insight Report: Cyberstorage Traditional security layers alone aren't enough to combat modern cyberattacks. Cyberstorage adds a crucial storage-level defense to mitigate ransomware and minimize data loss. Download the Gartner Cyberstorage Report to discover how organizations are leveraging this breakthrough technology to stay ahead of evolving threats.

Detect, Respond, Recover

Detection and Prevention

- **Attack detection** - Leverage dynamic learning to identify and detect suspicious user behavior patterns, file extensions, and honeypot activity in real-time, enhancing security and minimizing risks.
- **Custom Auditing** - Prevent mass deletions, data loss, and detect custom activity patterns, all with active auditing for PowerScale.
- **Simulated Attack** - Proactively simulate attacks to ensure your system is fully ready to detect suspicious behavior and trigger timely alerts.

Threat Detection Proven By Independent Testing

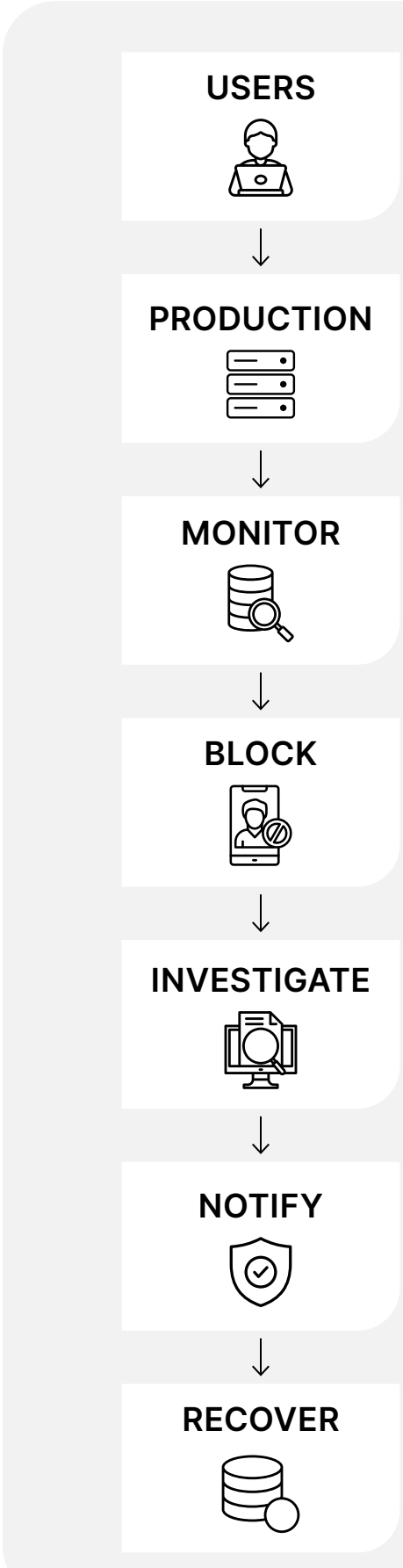
AV-Comparatives tested our solution against different ransomware strains. If you want to see real ransomware defense independent test results for yourself, don't take our word for it, **download the detailed reports**.

Response

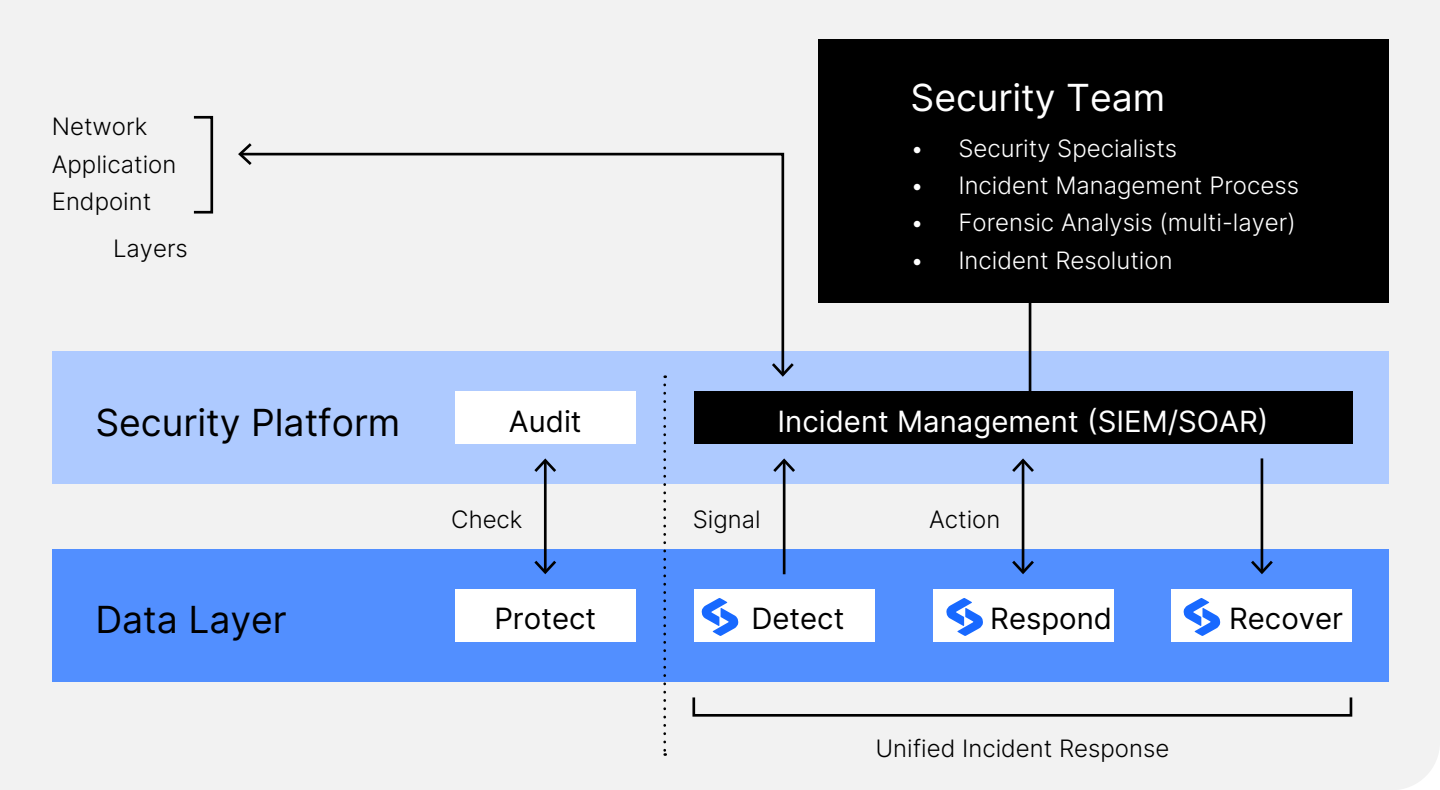
- **Proactive Defensive Snapshots** - Automated snapshot taking ensures that data is protected and can be quickly restored in the event of an incident, reducing the risk of data loss.
- **User Lockout** - Automated lockout of the user (delayed or immediate) helps to minimize the potential data loss.
- **Automated Incident Response** - Seamlessly orchestrate a unified response across hosts, endpoints, and unstructured data through our advanced bidirectional integration with leading XDR, SIEM, and SOAR tools. Elevate your security operations to the next level.
- **Data Forensics & Incident Investigation** - Our application tracks real-time user activity and historical behavior for faster and more accurate incident investigation. Review the organization's inventory to identify critical shares and data that were affected (for PowerScale).
- **WireTap** - Allows administrators to browse the file system to instantly track all user and path file activity (for PowerScale).

Resilience & Recovery

- **Data Recovery** - Impacted files can be quickly restored with one-click recovery, eliminating the need for traditional backups and accelerating RTO to minutes.
- **Quarantine & Review** - Corrupted files are automatically quarantined for thorough review by infosec teams, ensuring better control and security.
- **Where Did My Folder Go?** - Folders or files that have been moved or deleted by the end users can be easily located (for PowerScale).



Integrated Security Architecture



A full list of supported integrations is available on our website.

How Superna Complements the PowerScale Platform

- Tight integration with the DELL API and audit records of storage operations.
- Superna's user lockout mechanisms are adapted to also natively leverage DELL functionality by denying access to the SMB shares or block write access to NFS exports. The nefarious activity is immediately terminated via the API, rather than waiting for the AD session to expire and block access.
- One-click recovery from unaffected snapshots is available using DELL functions.

superna.io | sales@superna.io

©2025 Superna LLC, all rights reserved. Superna, along with Superna and logo are trademarks or registered trademarks of Superna LLC. All other third party brands, product names, and trademarks are the property of and used to identify the products or services of their respective owners. All specifications are subject to change without notice.