# Data Security Essentials

Unstructured Data Platforms - PowerStore/PowerEdge/Windows

Protect your data at its source

Cyber attacks continue and are accelerating, with attackers targeting enterprise data.

- 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.

- In 2024, the average cost of a ransomware attack was $4.54M (IBM).

Application Layer / Endpoint Layer / Network Layer / Storage Layer
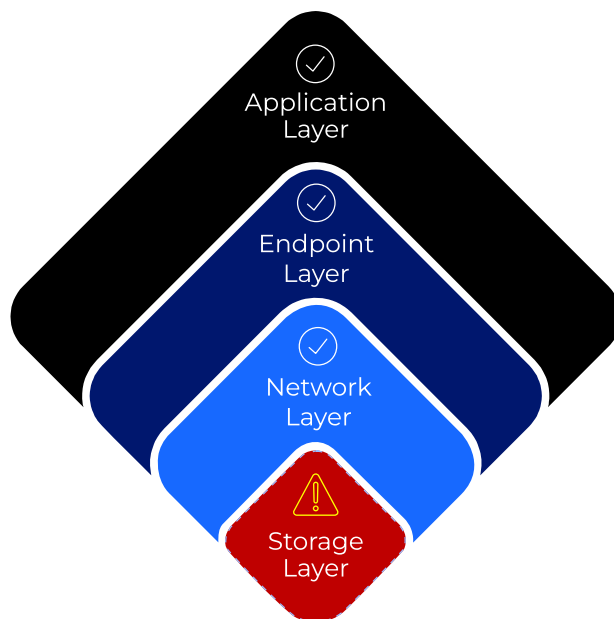
The Solution

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.

Cyber threats evolve faster than traditional defenses. **Superna Data Security Essentials**, integrated with **your unstructured data platform**, provides **automated, real-time threat detection and response** at the data layer. This lightweight, fast-to-deploy solution protects your most valuable data from ransomware and insider threats—without adding complexity.

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 Essentials Highlights

→ **Prevention is the new recovery**: Stop threats before they impact business operations.

→ **Cyberstorage security at the data layer**: Protect your data where traditional security fails.

→ **Security Integrations**: Into SIEM and SOAR infrastructures.

→ **Instant protection, no complexity**: Lightweight install, no new infrastructure required.
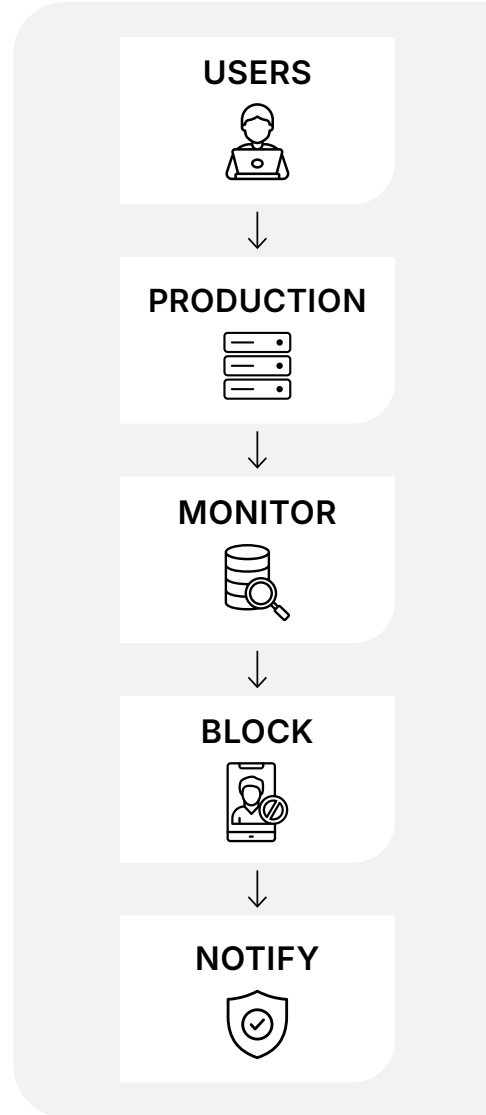
Detect and Respond

Prevention

- Watch for suspicious behavior in real time.
- Spot known ransomware extensions and abnormal patterns fast.
- Stop mass deletions with policy-based protection.
- Set custom rules to catch threats early.
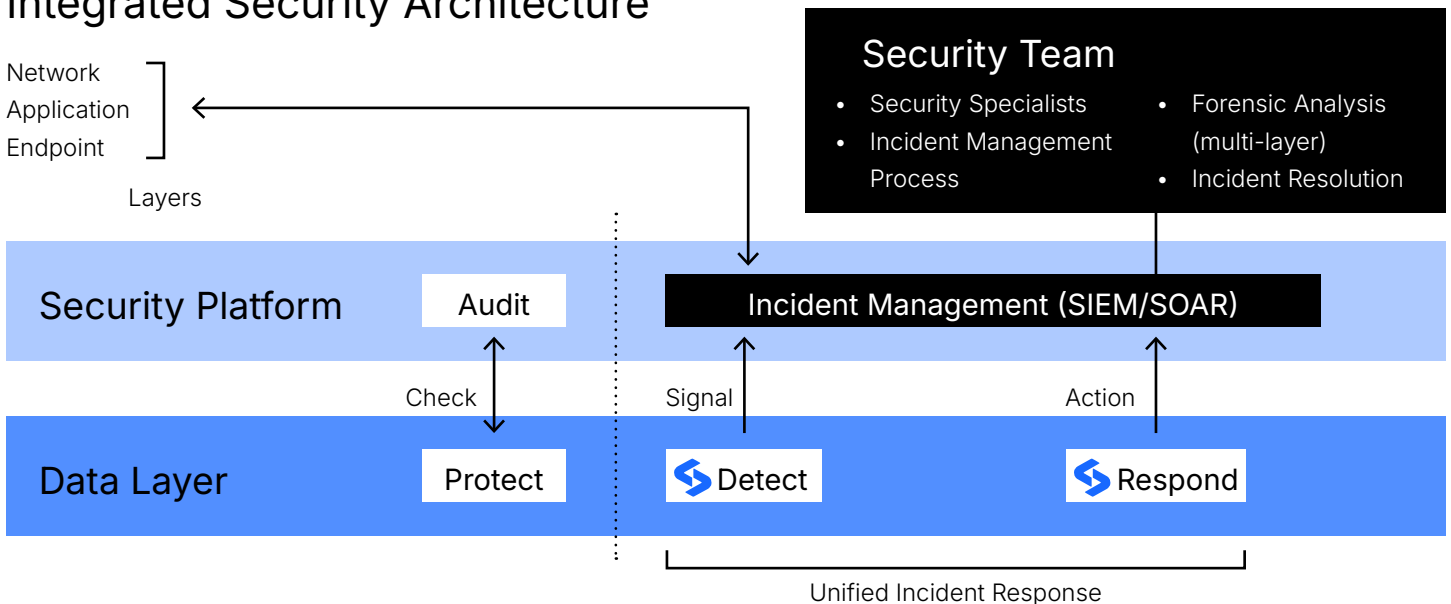- Protect your shares and/or application servers

Response

- **Auto Lockout Block**: Access to shares, disable AD accounts, log off the user.
- **Block Dangerous Files**: Stop creation or access of unwanted file types. Delete or quarantine by extension.
- **Stay Alert**: Send real-time alerts. Feed security data into your SIEM and IT ops tools.
- **Investigate Quickly**: Track user behavior over time. Pinpoint what was hit and when. Speed up incident response.
- **Find Misplaced Data**: Follow the trail when files get moved. Help users recover what they lost.
- **Clean Up After Incidents**: Hunt down files with ransomware extensions. Quarantine or delete as needed.

Manage Storage Smarter

- **Aged Data Deletion**: Clear out files past retention timelines.
- **Temporary File Cleanup**: Remove orphaned temp files left behind by crashed apps.
- **Quota Controls**: Set limits per share or directory. Keep storage use and cost in check.

USERS

↓

PRODUCTION

↓

MONITOR

↓

BLOCK

↓

NOTIFY

Integrated Security Architecture

Network
Application
Endpoint
]
Layers

Security Team
- Security Specialists
- Incident Management Process
- Forensic Analysis (multi-layer)
- Incident Resolution

Security Platform   Audit   Incident Management (SIEM/SOAR)

Check   Signal   Action

Data Layer   Protect   Detect   Respond

Unified Incident Response

Technical Highlights

- Built-in support for the CEE framework on Dell PowerStore and Unity

- Native integration with the Windows file system

- End-to-end protection for Windows OS hosts, PowerStore, and Unity

- Supports Windows-based PowerEdge servers.

- Lightweight, agent-based architecture with centralized control

- Installs in minutes on any Windows OS

- No extra hardware—runs inside your existing setup

- Adds a low-impact security layer that works seamlessly with your storage

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.

Get Started with Superna
📅 **Schedule a Demo** | 📞 **Speak with an Expert**