# Data Security Essentials

Unified protection against ransomware and other cyberthreats

## SUPERNA DATA SECURITY ESSENTIALS

Traditional approaches to data protection and cybersecurity have proven to be inadequate for detecting and stopping ransomware at-tacks, because they're focused on the *network* and *application* layers, not *data*. Even organizations with extensive security and data management approaches already in place continue to suffer permanent data loss and costly business disruption, resulting in both lost business and reputation-al damage.

**Superna Data Security Essentials** is a unified data protection solution that detects ransomware-associated file extensions and suspicious user behavior. It allows you to intervene immediately to stop suspicious user activity, and conduct thorough incident investigations and forensic reporting. It provides security *at the data layer* to protect against ran-somware and other cyberthreats. It reduces risk, minimizes operational disruption and helps ensure data integrity.

## HOW IT WORKS

Powered by a comprehensive database of known ransomware threats (updated regularly), it employs write-blocking technology, allowing fo-rensic investigators to access and examine digital storage media without altering or compromising the integrity of the data.

**Superna Data Security Essentials** allows you to easily define policies and directories you want protected against ransomware. Upon detection of known ransomware extensions or suspicious activity, that user will be blocked in a manner you specify: They can be denied access to the share; they can be disabled in Active Directory; even logged-off of their work-station. It also triggers an alert enabling further investigation for detemi-ning additional actions to be taken.

### HIGHLIGHTS

**Data Protection**
- Protects your data from suspicious user activity.

**Control over Quotas**
- Enhances user-to-business report-ing and notifications.

**Blocks Unwanted File Types**
- Manages lists of unwanted file types and prevents their storage on corporate file shares.
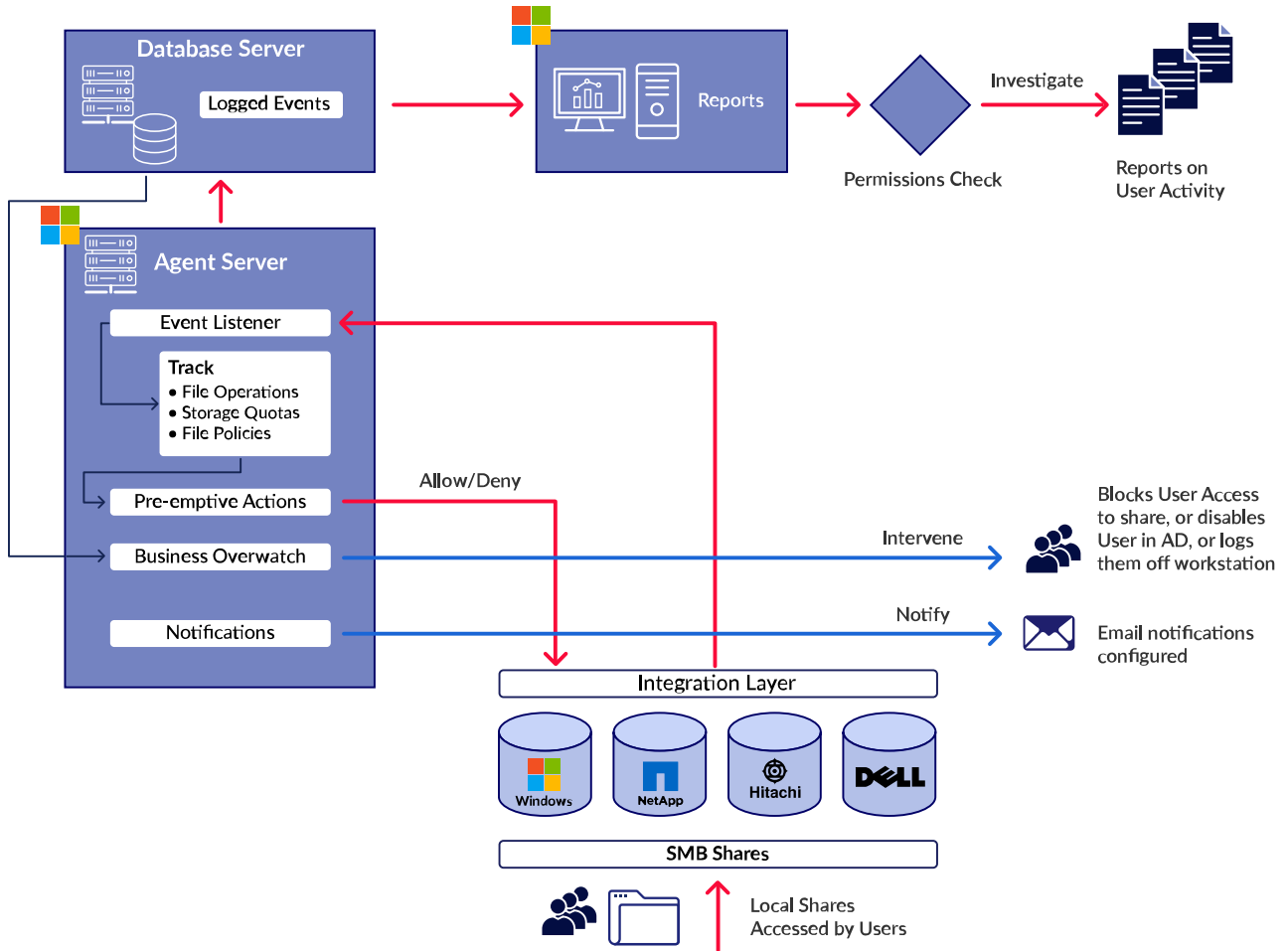
**Data forensics and investigation**
- Tracks real-time user activity for fast, accurate incident investiga-tion.

**Notifications and Reporting**
- Provides quick insight into data access patterns including users, folders, and access summaries.

superna®

Superna Data Security Essentials includes a range of features: quotas to optimize resource allocation; the blocking of dangerous and unwanted file types; comprehensive auditing capabilities for full audit trails; and automated file management policies in support of data governance. Powered by a comprehensive – and continually updated – database of identified ransomware threats and advanced write-blocking technology, Superna Data Security Essentials provides strong, continuous protection against cyberattacks.

## Superna Data Security Essentials



Database Server
Logged Events

Reports

Investigate

Permissions Check

Reports on User Activity

Agent Server

Event Listener

Track
• File Operations
• Storage Quotas
• File Policies

Pre-emptive Actions — Allow/Deny

Business Overwatch — Intervene — Blocks User Access to share, or disables User in AD, or logs them off workstation

Notifications — Notify — Email notifications configured

Integration Layer

Windows   NetApp   Hitachi   DELL

SMB Shares

Local Shares Accessed by Users

## ▤ TECHNICAL HIGHLIGHTS

- Full integration with NetApp's FPolicy engine
- Native integration with the Windows file system
- End-to-end security for NetApp NAS and connected Windows OS hosts
- Flexible centralized management and distributed agent-based architecture
- Quick and easy installation on any Windows OS in minutes

**Supports popular storage solutions**
- Dell PowerEdge
- Dell PowerStore
- Dell Unity XT
- Hitachi HNAS
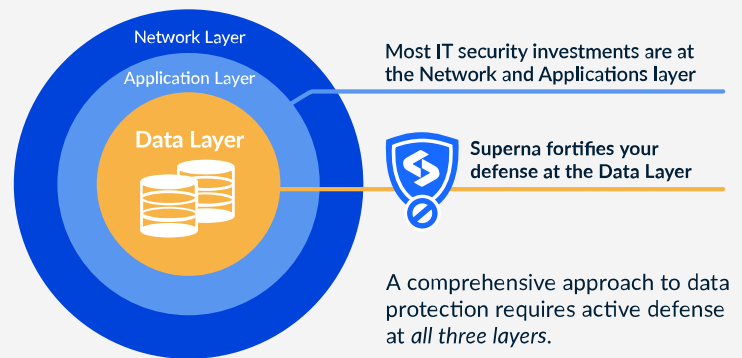- NetApp OnTap
- Windows Server
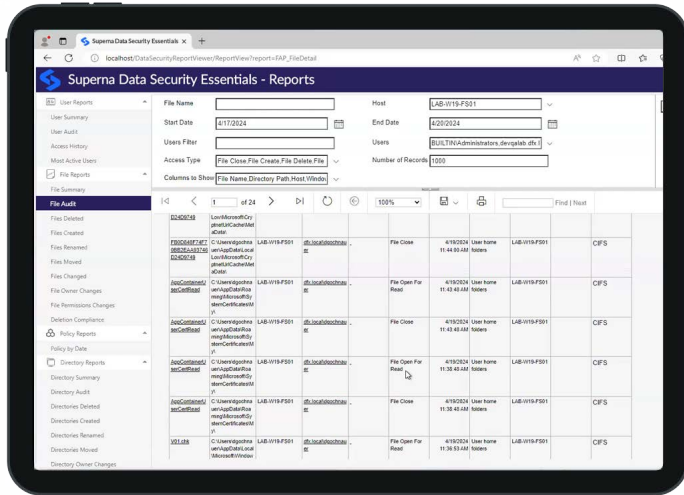
**Detects both bad actors and insider threats**

Superna Data Security Essentials allows you to protect sensitive data from suspicious activity indicative of malicious behaviors and even insider threats.

## 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."

# Cyberstorage
**Cyber Defense at the Data Layer**



Most IT security investments are at the Network and Applications layer

Superna fortifies your defense at the Data Layer

A comprehensive approach to data protection requires active defense at *all three layers.*

# 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.](http://www.superna.io)

## Ready to get started? Contact your [Superna](#) team today!

**Prevention is the new recovery**

superna.io  |  sales@superna.io

20240530