superna®

DATASHEET

Superna Threat Hunting Module

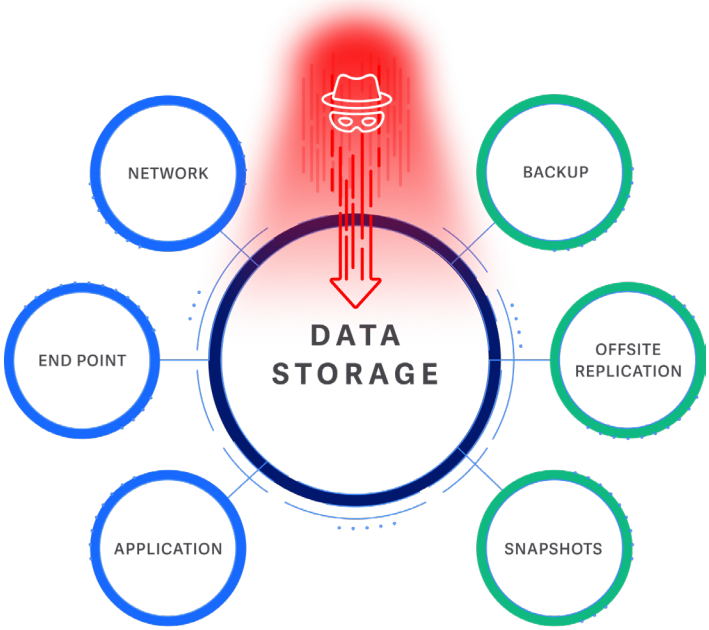
AI-powered anomaly detection for unstructured data

The Challenge

Ransomware and insider threats are advancing rapidly, often bypassing traditional perimeter defenses. While firewalls, endpoint tools, and monitoring systems provide essential coverage, they rarely extend to unstructured data activity inside the environment. This creates a dangerous blind spot where attackers can:

- Scan file shares and map directory structures undetected
- Identify and target high-value data for encryption or exfiltration
- Operate silently during the reconnaissance phase, leaving no trace until it's too late

Storage administrators are not equipped to review and interpret every file access alert, and security teams often lack file-level visibility. The result is delayed detection, alert fatigue, and missed early warning signs that could stop an attack before it escalates.



The Solution

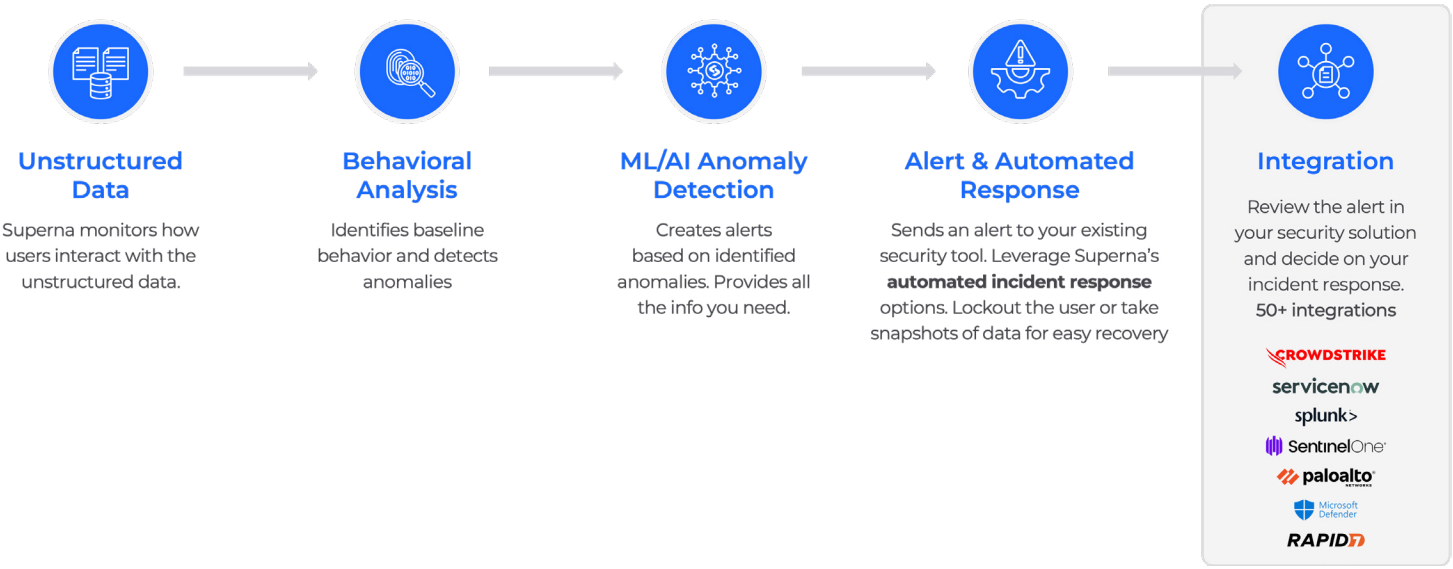
Superna's Threat Hunting Module uses AI-driven anomaly detection to close this visibility gap. Superna Threat Hunting identifies cyber threats that have infiltrated the network, but have not yet triggered alerts or been discovered by automated tools. By continuously monitoring user file activity, the system learns normal behavior patterns and flags unusual deviations that may indicate early-stage reconnaissance or malicious activity.

How it Works

- Confidence scoring for anomalies to focus on high-risk events and reduce noise
- On-premises data processing to ensure privacy and sovereignty
- Seamless integrations with your SIEM/SOAR platforms *(e.g., Splunk, Crowdstrike, ServiceNow, MS Defender, SentinelOne)*
- Automated workflows that deliver file access context directly into existing security processes

This approach shifts the burden away from storage admins and empowers security teams with actionable, contextual data. This enables faster, smarter incident response.

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. **Gartner's Cyberstorage Report** shows how organizations are leveraging this breakthrough technology to stay ahead of evolving threats.



Review the alert in your security solution and decide on your incident response

- ✓ Detect ransomware reconnaissance and insider threats before encryption or data theft
- ✓ Reduce "dwell time" by attackers, limiting time to access, collect, exfil data
- ✓ Reduce Mean Time to Detect (MTTD)
- ✓ Reduce alert fatigue with prioritized, high-confidence alerts
- ✓ Fully integrated with 50+ security tools, enabling security teams to correlate file anomalies with broader intelligence
- ✓ Provide full visibility into who accessed what, when, and how

With Superna Threat Hunting, your team can detect early, respond faster, and stay ahead of evolving threats, without compromising data privacy or sovereignty.

Protect Your Data. Eliminate Downtime. Get Started Today.

📞 **Speak with an Expert**