WHITE PAPER

superna

A PROACTIVE APPROACH

# Evolving from Data Protection to Data Security

VECTRA

DELL Technologies

Dale O'Grady, Vectra
Andrew MacKay, Superna

## OVERVIEW

When a physical threat presents itself, most people will implement protection mechanisms. When warned of an impending hurricane, people will naturally board-up their property and take cover. This behavior is conditioned, but why doesn't that conditioning extend to enterprise security programs?

Protecting your data requires several controls that together will improve your defense against a cyberattack. Providing detection or response functionality on its own is not sufficient. Individual solutions may allow you to minimize damage, but proactively protecting your data in advance of damage is what security professionals truly aspire to, and that is what this blog will cover.

## UNDERSTANDING THE PROBLEM STATEMENT

Many organizations implement controls to identify when data is compromised and how best to recover from the challenge. This approach is common because 100% prevention is not possible. As we are aware, threat actors are very clever and innovative in the methods that they use to compromise organizations. With this approach, endpoint protection seems to be "the tool" most organizations want to have in place. It is ubiquitous but can be insufficient as attackers have been able to bypass these protections by compromising identity and access credentials.

Endpoint protection approaches can be challenging implementations, requiring a combination of techniques for actual effectiveness and usability requirements. They may also create interoperability issues, require extensive, skilled operators, or result in high false positives that quickly exhaust resources. The typical enterprise can protect approximately 40% of its environment with endpoint protection, leaving the remainder exposed. Threat actors have proven their ability to bypass endpoint protection with novel exploits and vulnerabilities. Furthermore, with valid credentials, threat actors can gain access and initiate a campaign that is difficult to stop using reactive endpoint protection approaches. With this being the case, other solutions are required to detect when data access is abused.

## HIGHLIGHTS

- Traditional protection and response functionality is no longer sufficient defense against cyber-threats.
- Inceased sophistication of cyber-criminals means 100% prevention is no longer an achievable goal.
- While individual solutions might minimize damage, a proactive approach helps ensure resiliency and recoverability.
- *Superna for Dell* in conjunction with *Vectra* use real-time analytics and advanced AI to allow you to get ahead of threats by identifying and prioritizing suspicious activity, proactively securing your data environment.
- Protects against ransomware, data leakage, mass deletes, untrusted user access, and internal bad actors.

## GETTING AHEAD OF THE THREAT

It is possible to get ahead of threats and proactively protect data by removing the security control silos and striving to adopt a holistic security approach. The concept of holistic security is not new. The NIST (National Institute of Standards and Technology) Cybersecurity Framework does an excellent job of laying out the critical elements of holistic security, as well as their relationships. These components are centered on capabilities that *Identify, Protect, Detect, Respond and Recover*. By design, security vendors traditionally focus on such controls individually simply due to the vast scope of cyber threats and the complexity involved in addressing them. Since security vendor use cases are traditionally isolated to specific controls, this places an enormous burden on the operator to manually define proactive security control relationships across an increasingly complex threat landscape.

## VENDOR-ASSISTED PROACTIVE DATA PROTECTION

**Superna for Dell**, a global leader in unstructured data security and **Vectra**, a global leader in threat detection and response have collaborated on this problem statement to assist customers in automatically implementing proactive data protection controls. In doing so, Superna and Vectra are helping customers evolve traditional data protection into advanced data security.

Vectra uses advanced artificial intelligence to identify and prioritize suspicious activity early in the attack progression — before any damage is inflicted. When individual threats or attack profiles target data, Vectra notifies Superna so that critical data can be immediately placed into a protective, immutable state without impacting production data access. Thus, securing the data and preventing the need for costly recovery.

Additionally, Superna delivers its real-time analytics and historical forensics at the data layer itself, understanding when a nefarious activity poses a direct threat to critical data, even if a traditional security tripwire has not been triggered. This advanced, real-time auditing and historical view of data activity helps secure customers from the activities of bad internal actors and Ransomware, data leakage, mass deletes and untrusted user access. The Superna data-first strategy paper is available here.

## A UNIQUE APPROACH

Ransomware is likely the most common data destruction/disruption technique encountered today. While several solutions can detect known ransomware variants or the active process of encrypting traffic, that is still more reactive than proactive. Furthermore, taking precautionary measures based on individual threats unnecessarily disrupts the business. This will occur if the threat signal is not high quality and prioritized appropriately.

— POWERED BY —
DELL Technologies

Vectra and Superna offer a unique approach to addressing these problems. Vectra is uniquely positioned by harnessing patented Security-AI driven Attack Signal Intelligence™ to automatically detect, triage and prioritize known and unknown threats in real time. The AI-driven security approach identifies attacks as early as possible in their progression. One such application of this in practice is discussed in the paper, “Stop a RansomOp Before Ransomware.” The unique ability to identify the early signs of ransomware prior to any data exfiltration or encryption, along with the ability to surface with urgency is paramount to enabling proactive data protection.

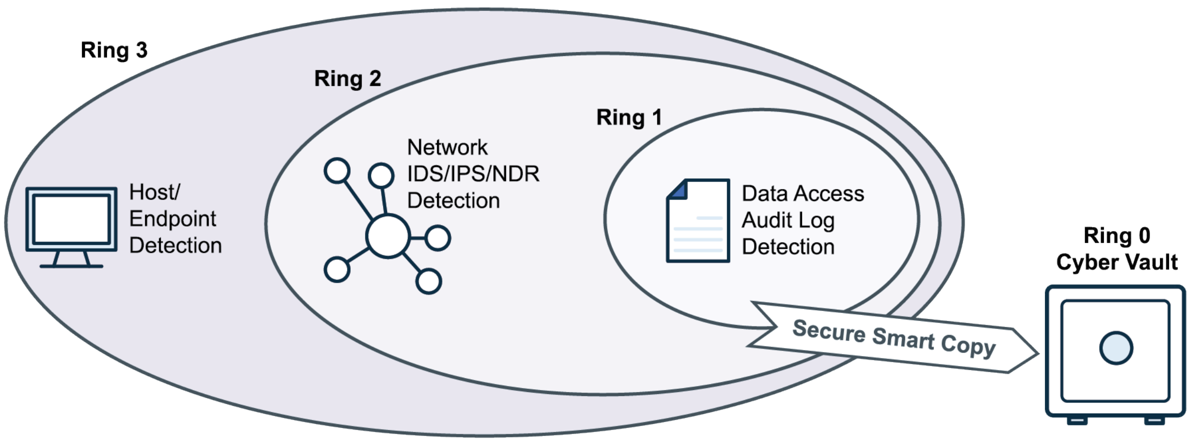
Superna has full visibility into the unstructured data footprint and has the unique ability to snapshot the appropriate file systems or object stores and place them in a protective immutable state to prevent disruption or costly recoveries without impacting production data. Clean copies of production data can be stored in an air-gapped cyber vault which is critical for industries like finance and healthcare.

## DATA-FIRST SECURITY ARCHITECTURE

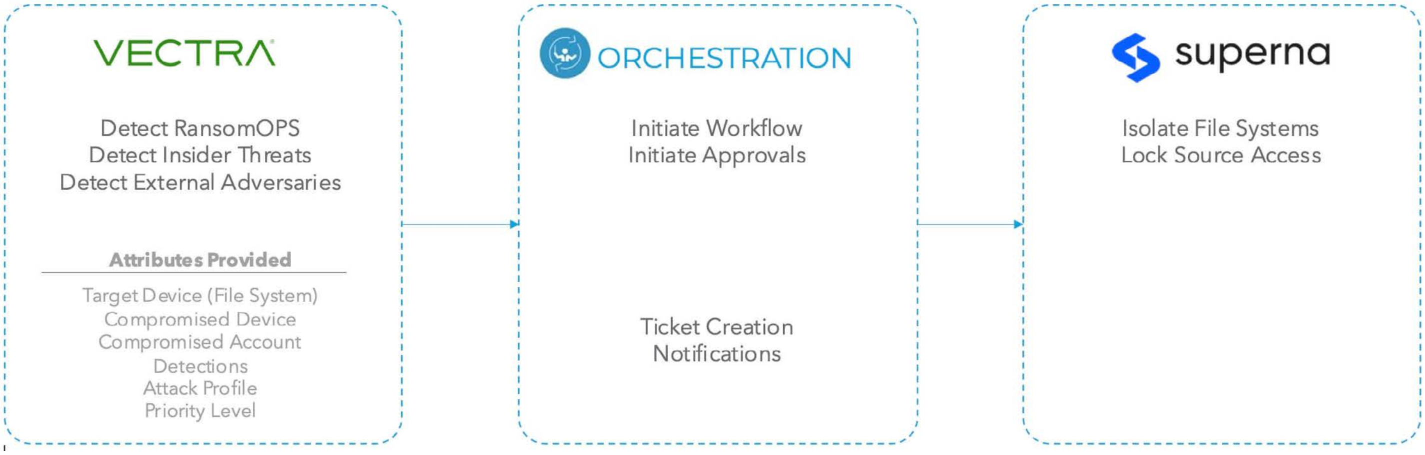
A data first security architecture begins with protecting your data in rings that surround your data and work outwards toward the least significant detection domain. An example of this would be a domain with the highest percentage of false positives or where only partial monitoring coverage is available like endpoints. The image below illustrates how **Data First Security Architecture** might appear in your environment.

### Data-First Security Architecture

Priority should be placed on detections originating from Ring 1, then Ring 2, then Ring 3.



### Workflow Implementation Overview



VECTRA

Detect RansomOPS
Detect Insider Threats
Detect External Adversaries

**Attributes Provided**

Target Device (File System)
Compromised Device
Compromised Account
Detections
Attack Profile
Priority Level

ORCHESTRATION

Initiate Workflow
Initiate Approvals

Ticket Creation
Notifications

superna

Isolate File Systems
Lock Source Access

To learn more, please visit Vectra Attack Signal Intelligence™ and Superna for Dell.

For more insight into how Superna® can help solve your organization's unstructured data security challenges, visit us at superna.io.

superna

Securing unstructured data,
wherever it resides

superna.io
marketing@superna.io