superna®

SOLUTION BRIEF

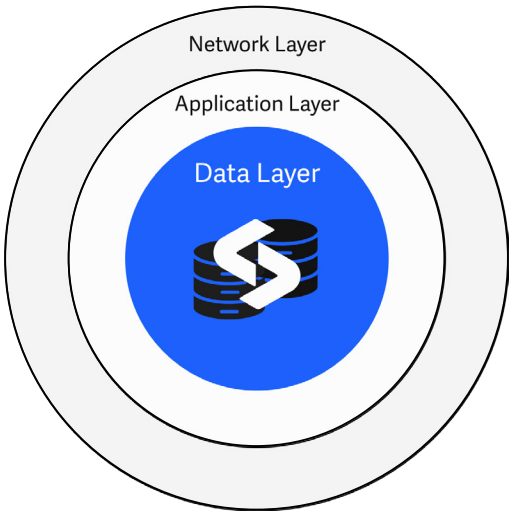
Tenable & Superna Continuous Threat Evaluation Data Vulnerability Management Solution

tenable

Business Challenge

Organizations struggle with traditional vulnerability management solutions that fail to prioritize data risks effectively, including:

- Inaccurate vulnerability scoring, ignoring user access patterns, data classification and data protection
- 50% of the attack surface missed by not considering user identities
- Reactive threat response instead of proactive risk management
- Blind spots due to lack of real-time attack surface discovery
- Inability to enforce real-time mitigation and compensating controls
- Lack of Zero Day vulnerability protection
- Missing a data-centric view of assets and risks



Solution

Superna Data Vulnerability Management uses AI-driven risk prioritization at the data layer to enhance traditional vulnerability management. Security teams can proactively identify and automate the mitigation of high-risk assets & users by analyzing data permissions, user access behavior, PII data classification, host risk scores, and user attack surface intelligence.

Value

The integration helps security teams to:

- ✓ Prioritize remediation based on actual **data risk** rather than device risk scores, **reduce time and resources** spent on remediation
- ✓ Identify high-risk hosts and users in **real-time** to gain an advantage over adversaries
- ✓ Implement automated compensating controls to block data access from vulnerable assets to **strengthen Your Data Security Posture**
- ✓ **Measure risk** with deep understanding of the classification risk within the data itself
- ✓ **Improve** mean time to detect (MTTD) and mean time to respond (MTTR) for critical vulnerabilities.
- ✓ Enable Active Defense to **protect data from zero-day vulnerabilities**
- ✓ **Gain asset visibility** to regulatory data risk and exposure.

Features

- → **Data Attack Surface Visibility**: Identifies high-risk users and hosts with privileged access to sensitive data.
- → **Data-Centric Risk-Based Prioritization**: Uses AI to score hosts and users based on data exposure risk.
  - User access behavior patterns and permissions
  - Host risk assessment based on data exposure
  - PII, PHI & Financial Data Classification of hosts and users accessing high risk data
- → **Automated Remediation**: Blocks data access from high-risk assets until vulnerabilities are mitigated.
- → **Dynamic Data Shield (DDS)**: Enforces security policies to prevent untrusted hosts from accessing data.
- → **Integration with ITSM & SIEM**: Automates security incident creation and remediation tracking

How It Works

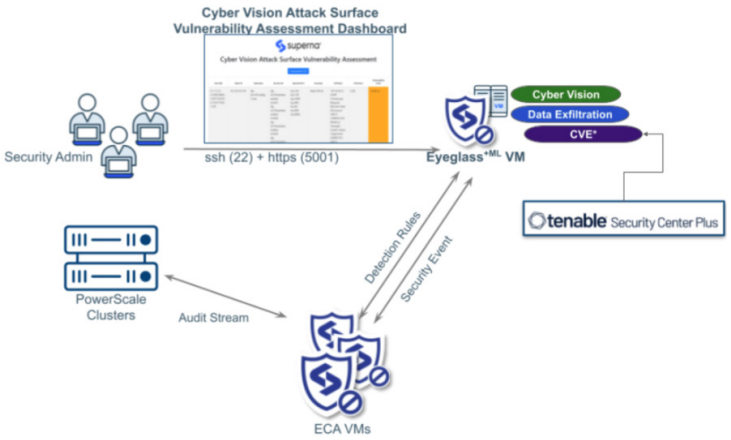
1. **Data Access Discovery:** DVM continuously monitors data access and host-user interactions.
2. **Risk Scoring:** AI-driven models analyze vulnerability data and access patterns
3. **Threat Detection & Prioritization:** High-risk users and hosts are identified in real-time and synced into a Dynamic Asset in Security Center Plus, providing a single location to view all data attack surface hosts.
4. **Tenable Security Center integration:** Creates a Dynamic Asset listing all the IP addresses of Data Attack Surface hosts identified by the DVM AI model. This asset list can be used to launch scans on a more frequent basis to ensure these hosts have the most up to date information and are used for remediation prioritization planning.
5. **Compensating Controls Activation:** *(Optional)* If a host or user is deemed high-risk, access to sensitive data is blocked until remediation is complete. This applies a real-time data blocking permission to the underlying storage that blocks access to data.
6. **Automated Remediation & Reporting:** *(Optional)* ITSM integration creates tickets regarding offense compensating controls that have been actively applied.
7. **Continuous Monitoring & Policy Enforcement:** Security teams receive updates on autonomous mitigation progress.

Technology Components

- Tenable Security Center *(version 5.4 or higher)*.
- Superna Data Vulnerability Management (DVM) & Data Security Edition.
- Endpoint protection integrations *(Optional)*
- ITSM integrations*(Optional)*

Key Capabilities

- Data Risk Profile Scoring System using AI-powered risk models applied to hosts and users.
- Real-time asset inventory of devices interacting with data.
- Zero-day threat compensating controls to enable proactive defenses.
- Enforcement policies to block high-risk data access until vulnerability remediation is complete.
- Automated solution with no daily administration, leveraging Security Center workflows.



superna®
superna.io | sales@superna.io

About Superna

Superna® is a global leader in data security and cyberstorage solutions for unstructured data. Superna's technology enables enterprises to protect critical data assets, reduce attack surfaces, and respond to threats in real-time. Learn more at superna.io

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 44,000 organizations rely on Tenable to understand and reduce cyber risk. Tenable's solutions extend vulnerability expertise to digital asset security worldwide. Learn more at tenable.com