VECTRA
SECURITY THAT THINKS.®

INTEGRATED SOLUTION

Vectra for Splunk Delivers Unified Threat Visibility Across Attack Surfaces

Vectra and Splunk integration enables customers to detect, triage, investigate and respond to the most critical security alerts across their entire environment from a single dashboard. Deployed directly from Splunkbase, this integration provides analysts with AI-driven threat detection and response from a single dashboard across data centers and SaaS deployments.

Challenged by the Unknown

All too often security teams operate in the unknown. The unknown caused by ever-expanding attack surfaces, ever-evolving attacker methods and never-ending alerts that allow attackers to hide in plain sight. The unknown is what gives attackers the upper hand. By harnessing Vectra Security AI with Splunk, SOC teams can erase the unknowns and turn the tables on attackers.

Key Benefits

- Single view of priorities, across hosts, accounts and data sources.
- Seamlessly transition between Vectra and Splunk for deep investigations.
- Integrates Splunk into Vectra’s Assignments Workflow for operational metrics report.
- Vectra is deployed directly from Splunk’s marketplace, Splunkbase with a 1-click download and install.

Erase the Unknown by Integrating Vectra and Splunk

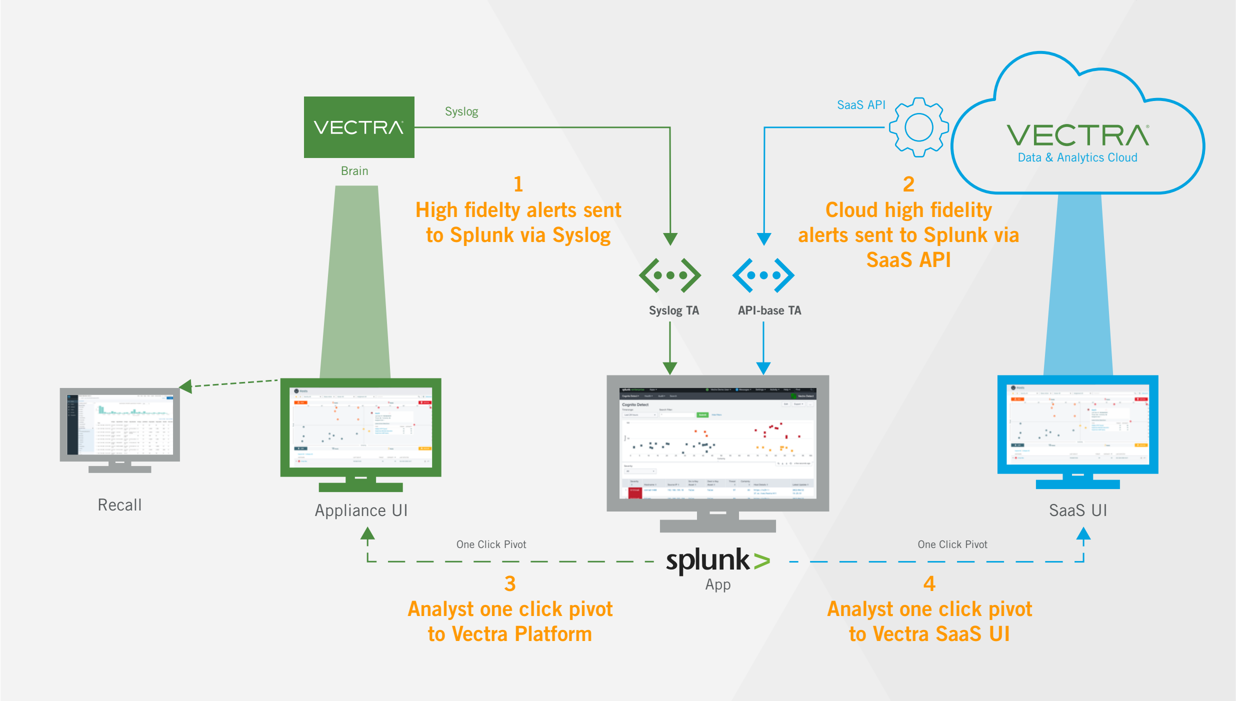
From within the Splunk dashboard, customers can leverage Vectra to gain coverage with attack visibility and context across surfaces, clarity that reduces alert noise and prioritizes critical threats and control to see and stop threats across an existing stack.

- **Coverage:** Vectra’s AI-driven detections are triaged to deliver a high-quality signal in the Splunk dashboard, providing deep context about every attack across multiple attack surfaces—public cloud, SaaS, identity, network, and endpoints.
- **Clarity:** Security teams can easily prioritize critical threats due to an 80% reduced noise rate. The integration of Vectra’s Security AI provides attack intelligence data to Splunk, so teams can address real threats faster.
- **Control:** Analysts gain an optimized process to see all threat data across existing stacks and surfaces in the Splunk dashboard and can connect to the Vectra platform for complete threat investigations.

Once the integration is deployed, analysts can investigate alerts across any current and future Vectra products. Efficient investigations can be completed without requiring deep training about the intricacies of the network or each identity and cloud provider, and without having to interpret details about where suspicious activity was spotted.

Capabilities

- Single unified view across all entities with active detections across all data sources.
- The view is organized by severity and threat score, allowing administrators to easily see the most critical threats and those that require immediate attention.
- Ability to drill down into Splunk from the entity list to see all attacker behaviors observed for a specific entity.
- Seamlessly pivot to Vectra and further investigate an incident (entity or detection).
- Integration with Vectra's Assignment Workflow enables visibility into whether an entity has previously been assigned to an analyst.
- Integrate a lockdown status view for both accounts and hosts that provides a live view of currently blocked entities as well as a 30-day historical view.


VECTRA
Brain
Syslog
1
High fidelty alerts sent to Splunk via Syslog
SaaS API
VECTRA
Data & Analytics Cloud
2
Cloud high fidelity alerts sent to Splunk via SaaS API
Syslog TA
API-base TA
Recall
Appliance UI
SaaS UI
One Click Pivot
splunk>
App
One Click Pivot
3
Analyst one click pivot to Vectra Platform
4
Analyst one click pivot to Vectra SaaS UI

About the Vectra platform

The Vectra platform is AI-driven threat detection and response for hybrid and multi-cloud environments. Harnessing patented Security AI, the Vectra Platform pinpoints attacker methods, prioritizes threats, and automates response controls leveraging your existing security stack. With the Vectra Platform, you get unified attack visibility, context across public cloud, SaaS, identity, network, and endpoints, and controls to respond immediately in the most effective way.

About Splunk

The Splunk platform removes the barriers between data and action, empowering observability, IT and security teams to ensure their organizations are secure, resilient and innovative.

Founded in 2003, Splunk is a global company — with over 7,500 employees, Splunkers have received over 1,020 patents to date and availability in 21 regions around the world — and offers an open, extensible data platform that supports shared data across any environment so that all teams in an organization can get end-to-end visibility, with context, for every interaction and business process. Build a strong data foundation with Splunk.

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai