ESET PROTECT and Splunk

Redefining threat management

Digital Security
Progress. Protected.

SOLUTION BRIEF

Cutting-edge endpoint protection meets advanced analytics

In the current cybersecurity landscape, organizations face increasingly complex threats that require powerful, integrated solutions. Security Analysts and IT Administrators are often overwhelmed by fragmented security data, leading to incomplete visibility and delayed responses. These challenges are especially pressing for Security Operations Managers (SOC Managers) and CISOs/CIOs, who need centralized, automated solutions to manage their security effectively.

ESET PROTECT integrates seamlessly with **Splunk** to consolidate security alerts and telemetry into a single interface. The integration empowers your organization to swiftly investigate threats, automate workflows, and manage security.

ESET PROTECT leverages award-winning multilayered technology to detect and neutralize the most sophisticated cyber threats. When combined with Splunk's robust data analytics and security insights, this integration delivers a comprehensive solution to enhance visibility, accelerate response times, and simplify security management.

Key benefits

ADVANCED THREAT DETECTION

Harness the power of ESET's multilayered technology to identify and mitigate complex cyber threats.

REAL-TIME RESPONSE

Benefit from immediate alerts and automated responses to potential security incidents—ensuring speedy containment and resolution.

CENTRALIZED MANAGEMENT

Enjoy the convenience of a single console for monitoring and managing all security.

SCALABILITY

Adapt to growing business needs with flexible solutions designed to scale effortlessly.

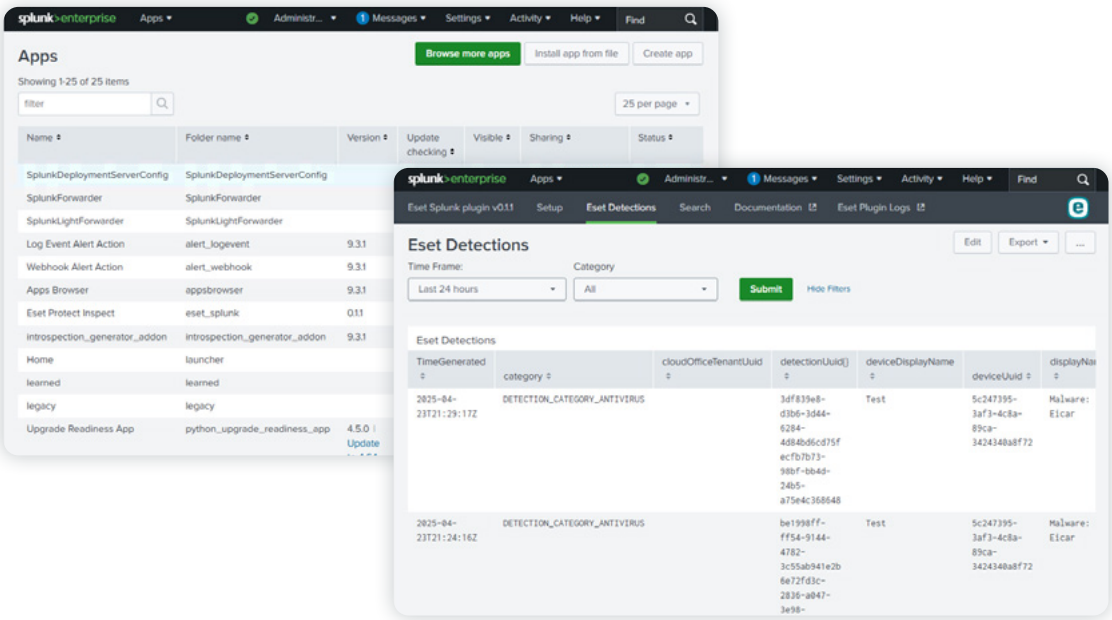
COMPLIANCE

Satisfy regulatory compliance with comprehensive data protection measures.

How it works

ESET PROTECT integrates with Splunk using Syslog and API-based methods. Syslog integration allows ESET PROTECT to push logs to Splunk in real time, while API integration allows Splunk to query ESET PROTECT for threat logs, events, and detections. This integration ensures that your security team can aggregate ESET detection events with Splunk's broader security telemetry, providing holistic insight and reducing manual overhead.

- Syslog-based integration: Seamlessly export Syslog-format events from ESET PROTECT to Splunk for real-time event streaming and correlation.
- API-based Integration: Utilize ESET's REST APIs to allow Splunk to query and pull relevant security events and telemetry directly, enhancing data-driven decision-making.



Next-level threat management in action

EXAMPLE SCENARIO

ESET's endpoint sensors identify a malicious IP as a command-and-control (C2) server communicating with multiple endpoints.

WORKFLOW

1. DETECTION: ESET PROTECT flags suspicious traffic from an endpoint to a C2 IP.

2. EVENT FORWARDING: ESET sends the detection event (via Syslog or REST API) to Splunk in real time.

3. CORRELATION: Splunk automatically correlates this IP with other network logs, identifying multiple endpoints communicating with the same malicious address.

4. AUTOMATED RESPONSE: An automated Splunk alert triggers a REST API call back to the ESET PROTECT console or gateway firewall solution, instructing it to block the malicious IP across the network.

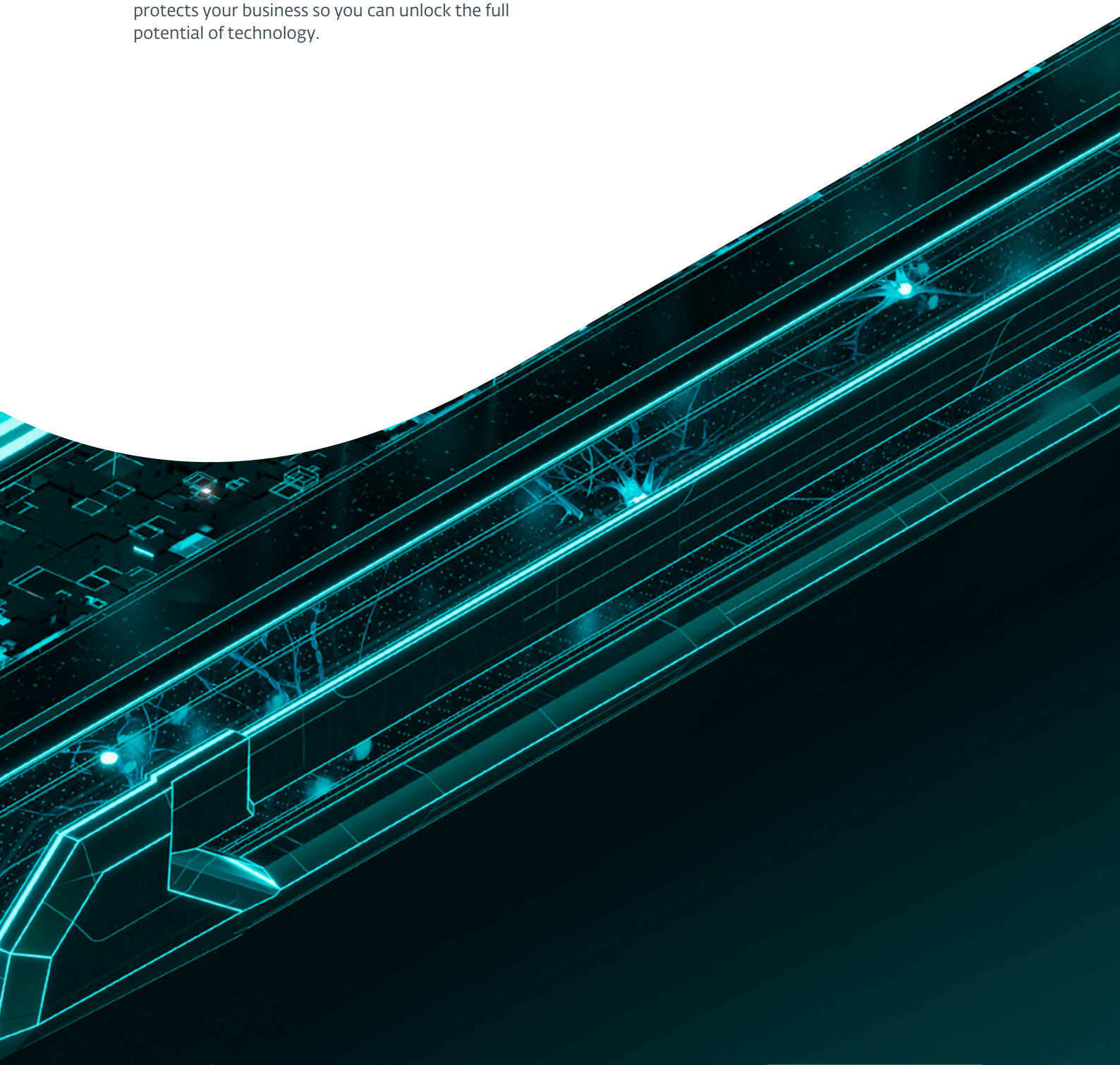
5. CONFIRMATION: The block is confirmed and reported in Splunk, providing end-to-end visibility for the security team.

About ESET

PROACTIVE DEFENSE.
MINIMIZE RISKS WITH PREVENTION.
Experience best-in-class protection thanks to ESET's in-house global cyber threat intelligence, compiled and examined for over 30 years, which drives our extensive R&D network led by industryacclaimed researchers. ESET PROTECT, our cloudfirst XDR cybersecurity platform, combines next-gen prevention, detection, and proactive threat-hunting capabilities. ESET protects your business so you can unlock the full potential of technology.

About Splunk

Splunk is a leading provider of data analytics and security solutions. Splunk's platform enables organizations to gain real-time insights from their data, enhancing their ability to detect, investigate, and respond to security threats. By integrating with ESET, Splunk offers a powerful combination of endpoint protection and comprehensive security analytics.



eset® Digital Security
Progress. Protected.

SOLUTION BRIEF