

ESET PROTECT Platform and Microsoft Sentinel SIEM and SOAR

Effortless integration for
enhanced threat detection
and response

Integrate and automate to maximize efficiency

Experience seamless security operations with the powerful integration of the ESET PROTECT native XDR Platform and the Microsoft Sentinel cloud-native SIEM and SOAR solution. Empower your security operations center (SOC) analysts by providing continuous threat monitoring, ensuring compliance and enabling proactive incident response. Get automated ingestion of threat data from ESET's multilayered protection engine, centralized visibility, and advanced threat analytics within Microsoft Sentinel.

Connecting ESET PROTECT and Microsoft Sentinel gives your business a comprehensive cloud-native security solution designed to protect hybrid environments. This integration significantly boosts the efficiency of your security teams by reducing manual tasks, automating data transfer, correlating endpoint data with cloud security, and streamlining incident management.

KEY BENEFITS

ENHANCED ACCURACY

By merging ESET's threat intelligence with Sentinel's SIEM, you can achieve higher detection accuracy and faster incident response times.

OPTIMIZED DATA UTILIZATION

Sentinel's analytics, automation and threat management capabilities help you transform ESET data into actionable insights, maximizing the value of your security data.

SUPERIOR INTELLIGENCE THROUGH INTEGRATION

Integrating with Azure-based security frameworks gets you a unified defense system, consolidating endpoint threat data with Sentinel's advanced capabilities.

KEY FEATURES

EFFORTLESS THREAT DATA UPDATES

Automatically retrieve the latest ESET PROTECT detection logs every five minutes with the Azure Function, ensuring your threat data is always current.

POWERFUL DATA ANALYSIS

Use custom log tables and graph queries to easily analyze ESET data alongside other security information, boosting your SOC team's analytical power.

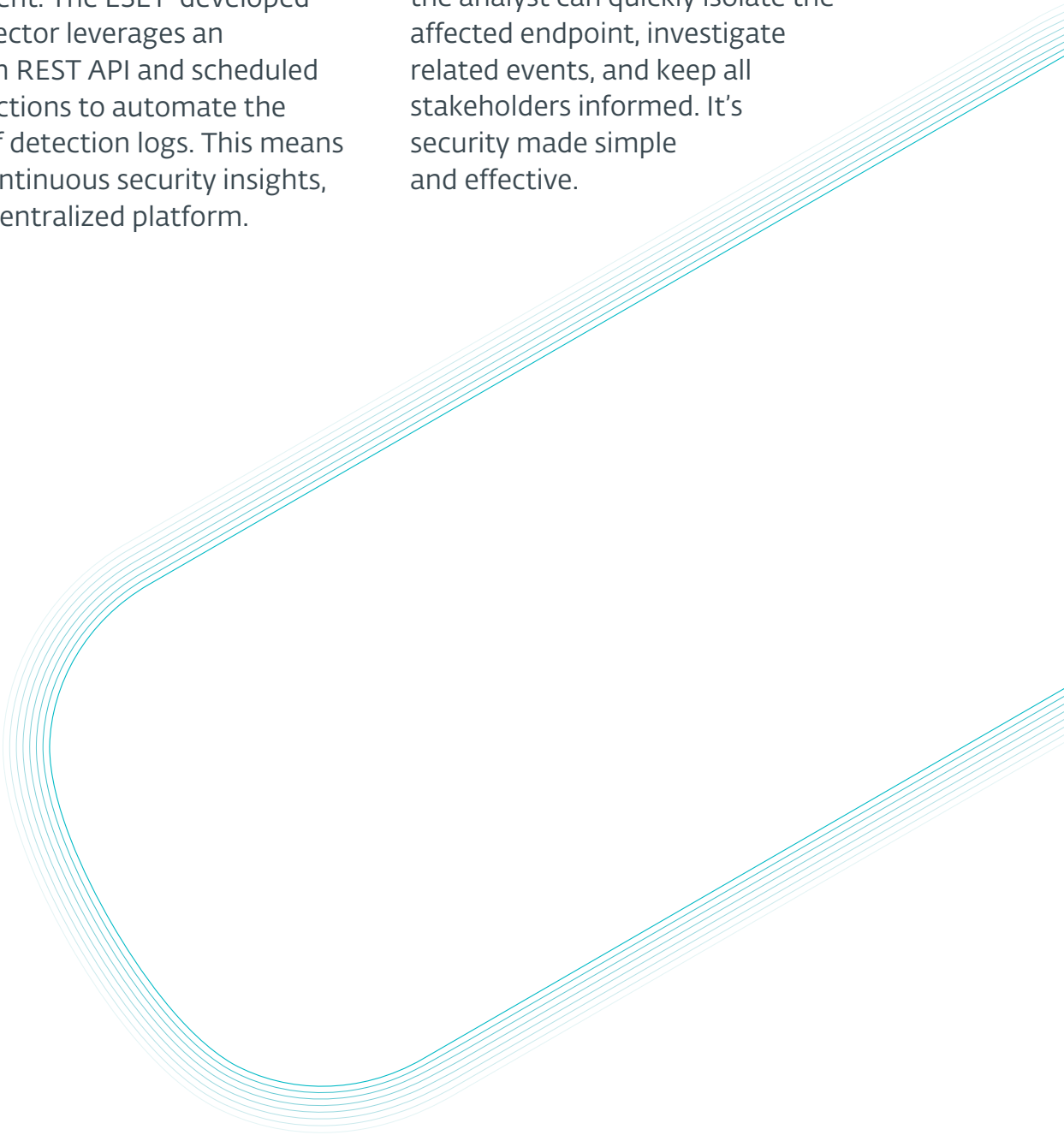
HASSLE-FREE SETUP

Deploy the data connector effortlessly with an ARM template, making configuration and data ingestion a breeze.

Enhance and simplify endpoint threat management

Simplify your endpoint threat visibility with the ESET PROTECT Platform and Microsoft Sentinel SIEM and SOAR integration. You'll also get efficient cross-platform threat correlation and management. The ESET-developed data connector leverages an Integration REST API and scheduled Azure Functions to automate the retrieval of detection logs. This means you get continuous security insights, all in one centralized platform.

How does it work in practice? Your SOC analyst would receive an alert from ESET PROTECT within Microsoft Sentinel, flagging a high-risk threat. With Sentinel's automated playbooks, the analyst can quickly isolate the affected endpoint, investigate related events, and keep all stakeholders informed. It's security made simple and effective.



About ESET

PROACTIVE DEFENSE. MINIMIZE RISKS WITH PREVENTION.

Stay one step ahead of known and emerging cyber threats with our AI-Native, prevention-first approach. We combine the power of AI and human expertise to make protection easy and effective.

Experience best-in-class protection thanks to our in-house global cyber threat intelligence, compiled and examined for over 30 years, which drives our extensive R&D network led by industry-acclaimed researchers.

ESET PROTECT, our cloud-first XDR cybersecurity platform, combines next-gen prevention, detection, and proactive threat-hunting capabilities with a wide variety of security services, including managed detection and response. ESET's highly customizable solutions include local support and have minimal impact on performance, identify and neutralize known and emerging threats before they can be executed, support business continuity, and reduce the cost of implementation and management.

ESET protects your business so you can unlock the full potential of technology.

About Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native security information and event management (SIEM) that delivers an intelligent and comprehensive solution for SIEM and security orchestration, automation, and response (SOAR). Microsoft Sentinel provides cyberthreat detection, investigation, response, and proactive hunting with a bird's-eye view across your enterprise.

Microsoft Sentinel also natively incorporates proven Azure services, like Log Analytics and Logic Apps, and enriches your investigation and detection with AI. It uses Microsoft's threat intelligence stream and also enables you to bring your own threat intelligence.

*Source: [What is Microsoft Sentinel?](#) – Microsoft Learn.