Splunk Security Essentials

Strengthen your security program and amplify the power of your Splunk Security technologies

Product Benefits

Get faster time to value for security use cases

Establish a proactive, data-driven security maturity strategy

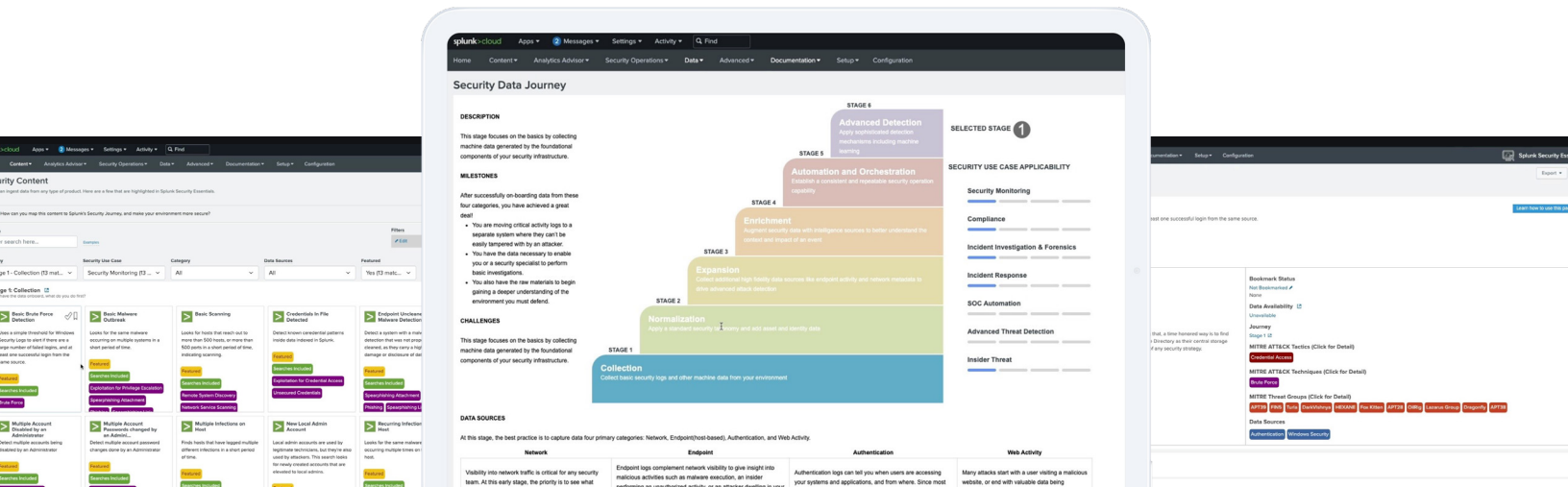
Stay ahead of existing and emerging threats

Today, it's clear that cybersecurity is important for organizations of all sizes, in all industries. While some organizations have been investing in their security program for years, others are just getting started. Regardless of where they are in their security maturity journey, it can be hard for organizations to take their security operations to the next level. Common challenges include:

- A lack of resources — whether that's time, money, or both
- Security teams don't have a holistic view of the security content and data sources already active in their environment
- Security teams are unsure how to advance their security program and take the next logical step

Splunk Security Essentials is an app that can amplify the power of existing security technology investments to strengthen an organization's security program — no matter their current level of maturity. The app provides an extensive library of pre-built security content that aligns with the MITRE ATT&CK framework and Cyber Kill Chain, making it easy to visualize your current security coverage and find and implement new content that addresses your organization's needs — without having to create it from scratch. It also offers a prescriptive security maturity framework that helps you determine your current level of maturity and provides recommendations on additional data sources and security content to implement to reach the next level of maturity.

While security teams can deploy the app on-premises or in the cloud as part of their existing Splunk Enterprise or Splunk Cloud Platform deployments, the app is especially powerful when deployed and used from within Splunk Enterprise Security. With Splunk Security Essentials, organizations are able to speed up their security program's time to value, stay ahead of threats, and establish a data-driven security maturity strategy.



Get faster time to value for security use cases

Implement security use cases faster by using pre-built content that can be activated with a few clicks. Splunk's extensive library of pre-built security content features prescriptive detections and analytic stories ready to deploy in your Splunk environment. All content (including custom detections, threat group lists, and threat technique lists) is stored in a central repository so it's easier to manage. Filter content by security maturity journey stage, data sources, risk or threat object type to easily find the content most relevant to your security needs.

Get your data in order

Automatically detect 150+ popular security data sources, categorize them by product type, pull in metadata, and add them to data source categories that align with Splunk's Common Information Model. To further standardize and support data onboarding, onboarding guides show you how to configure the products in your environment to send the logs required to activate security detections. Use the Data Inventory Dashboard to easily see what security content can be activated with your current data.

Establish a proactive security maturity strategy

Leverage pre-defined frameworks to clearly define your current level of security maturity and build an actionable roadmap to strengthen your security posture. You can identify gaps in your security posture in alignment with the MITRE ATT&CK and Cyber Kill Chain frameworks. You can leverage the Splunk Security Maturity Journey prescriptive framework to determine your current maturity status, and get recommendations on data sources to ingest and milestones to target to reach your next level of maturity.

Stay ahead of existing and emerging threats

Leverage a regular cadence of new content created by Splunk's industry-recognized experts to address the latest threats. Splunk's Security Content Library automatically updates every 24 hours to pull in the latest security content from the Splunk Threat Research Team. The Analytic Stories functionality groups detections against a specific attack or threat group to provide actionable guidance for detecting, analyzing, and addressing security threats. All of this functionality allows for rapid identification of potentially malicious activity.

Learn More >

Get Started >

Get the App >

splunk>

Contact us: www.splunk.com/asksales

www.splunk.com

24-493145-Splunk-Splunk Security Essentials-PB-103