Splunk Security Cloud
Modernize your security operations

Advanced security analytics | Automated response | Best-in-class platform

Organizations adopt cloud services to accelerate digital transformations. Eliminating hardware procurement and maintenance costs, unlimited scalability, and faster time-to-value are a few reasons organizations are prioritizing cloud investments.

Security teams don't want siloed products and complicated pricing when they move to the cloud. Solutions that are easy to procure and consume are part of cloud's promise and are a requirement for organizations looking to modernize legacy systems.

Splunk Security Cloud delivers on the promise of security as-a-cloud-service. Offering market-leading capabilities with simplified pricing and packaging, Splunk Security Cloud is designed to make your experience of buying and using Splunk seamless.

Introducing protected-device pricing

Splunk Security Cloud is priced using our new protected-device pricing model. Put simply, the offering is priced based on the number of devices you protect with Security Cloud.

Splunk Security Cloud capability matrix

Splunk Security Cloud is available in two editions, Standard and Plus:	Splunk Security Cloud Standard Protected-Device Pricing Centralize your security data and analysis, integrating data in real time from any source	Splunk Security Cloud Plus Protected-Device Pricing Detect complex threats with pre-built frameworks, workflows and dashboards
Correlate data across your security tools for increased visibility	✔	✔
Apply prescriptive detections and guidance to detect threats faster	✔	✔
Easily align your detections to industry-standard frameworks, like MITRE ATT&CK®	✔	✔
Integrate threat intelligence into your operations for more effective threat hunting		✔
Determine root cause quickly with pre-built frameworks and risk scoring		✔
Automate an unlimited number of actions to force multiply your security operations	Add SOAR	Add SOAR

Splunk Security Cloud Capabilities

- **Security Cloud Plus:** Security Cloud Plus provides market-leading SIEM and security analytics capabilities with pricing based on the number of devices protected with Splunk. Gain deep visibility into your environment, pre-built detections for cloud environments, high fidelity alerts mapped to industry standard frameworks, seamless integration of threat intelligence, and more.

- **Security Cloud Standard:** Security Cloud Standard allows you to ingest data in real time from any source, and it includes prescriptive guidance on how to achieve specific security outcomes. We've mapped data sources to Splunk searches and Splunk searches to security use cases. You can integrate the necessary data sources and deploy those pre-built searches in just a few clicks.

- **SOAR:** SOAR capabilities empower you to work smarter by automating repetitive tasks, respond to security incidents in seconds, and increase analyst productivity and accuracy to better protect your business. Customers can add SOAR capabilities to either edition of Splunk Security Cloud and pay per-protected-device.

Straightforward, predictable pricing

Faster time-to-value

Market-leading capabilities

Key Benefits

- **Straightforward, predictable pricing:** Our new pricing model—protected-device pricing—for Splunk Security Cloud prices our capabilities based on the number of devices protected with Splunk. The model makes it simple to determine your costs. We are also happy to help you determine the number of devices in your environment.

  Protected-device pricing decouples price and data ingest. Our customers often want to bring more data into Splunk to attain increasingly valuable security insights, but with ingest pricing those additional insights come at a cost. With protected-device pricing, you can focus on achieving your security goals by bringing the necessary data into Splunk.

- **Faster time-to-value:** We designed the editions of Splunk Security Cloud to provide customers security capabilities aligned to common needs across customer sizes and industries. Security Cloud Standard meets our customers' basic security needs while accelerating their development as security organizations. Security Cloud Plus includes all the features of Standard, but also brings you advanced security analytics capabilities. Additionally, Splunk Security Cloud accelerates your time-to-value via tailored professional services packages.

- **Market-leading capabilities:** Don't take our word for it that we're market leaders in security operations—listen to industry experts and other security practitioners. In 2020, Gartner named Splunk a Leader in its Magic Quadrant for SIEM for the seventh consecutive time. Forrester named Splunk a Leader in Forrester's Security Analytics Wave in 2020, and IDC identified Splunk as having the No. 1 market share in the SIEM market in 2020. We are also thrilled that in 2020 Gartner named us a Peer Insights Customers' Choice for SIEM for the fourth consecutive year.

Want to learn more about Splunk Security Cloud? Learn more at Splunk.com.