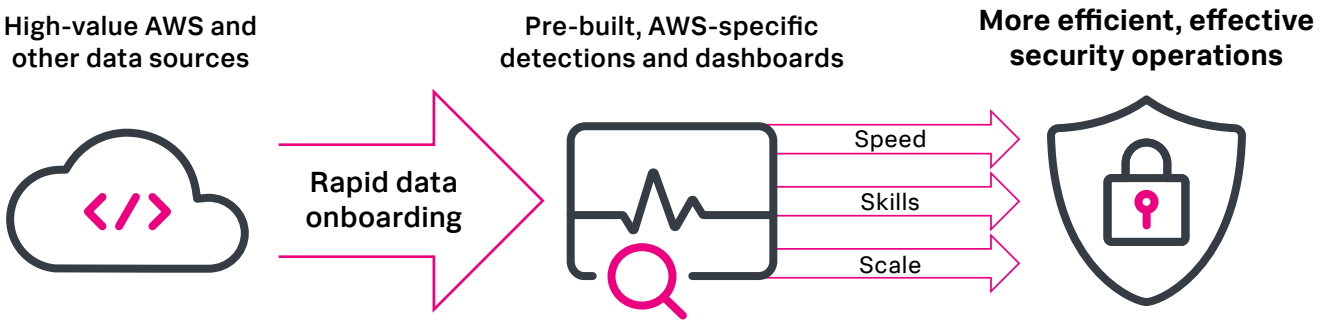
PRODUCT BRIEF

Splunk Security Analytics for AWS

Quickly detect, triage and automate security incidents in your AWS environment

- **Insights within hours of subscribing,** instead of weeks or more.
- **Pre-built, AWS-specific dashboards and detections** for IAM, network and other security data.
- **Dynamic investigative capabilities** with tools and guides created by Splunk's Threat Research team.



Lean security teams need an efficient way to detect and investigate threats

Security teams face several persistent challenges. Teams struggle to detect threats quickly, as evidenced by a global median dwell time of almost one month. This is due in part to the ongoing cybersecurity skills shortage. When considering the shortage alongside the proliferation of both security tools and new cloud applications and services that security teams have to manage, it's easy to understand how security teams' resources are often strained.

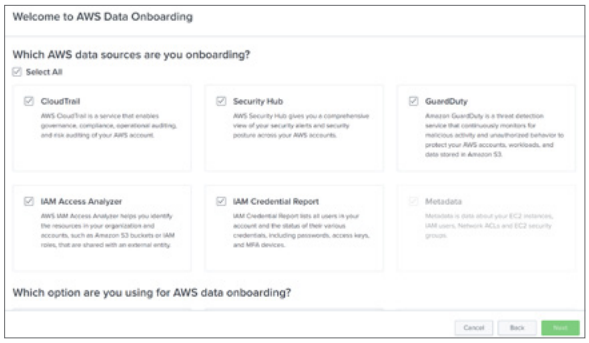
These challenges affect lean security teams more acutely than they do larger teams. Mature IT and security groups have security tool and domain experts. They can afford the price tag and opportunity cost — for e.g. extensive project scoping, requirements gathering, solution architecture and formalized bidding/procurement cycles — that comes with traditional enterprise software. Lean teams don't have those luxuries. Everyone on a lean team needs a broad understanding of security and how to use their team's tools. For lean teams, the traditional enterprise software sales, onboarding, and learning processes take too much time and focus away from actually doing security.

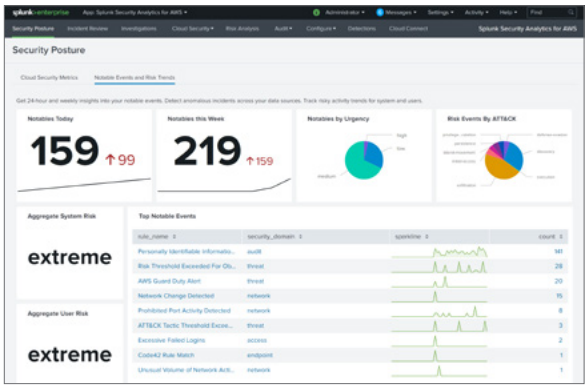
Splunk Security Analytics for AWS

Splunk Security Analytics for AWS is a security analytics solution designed for security teams with a smaller staff. Available exclusively in AWS Marketplace, the offering's accelerated data onboarding process takes users from signup to insights within hours, not weeks or longer as is common with traditional enterprise software. With Splunk's data-to-everything platform as its foundation, the offering brings award-winning security capabilities to lean security teams in an easy-to-buy, easy-to-use offering.

Speed through onboarding and configuration

Splunk Security Analytics for AWS rapidly onboards data from your security-relevant AWS services such as AWS CloudTrail, Amazon GuardDuty, and AWS Security Hub, and other data sources — like Microsoft 365 — with minimal time and human input required. This in contrast to the weeks or more of onboarding and configuration time often required by traditional security software.



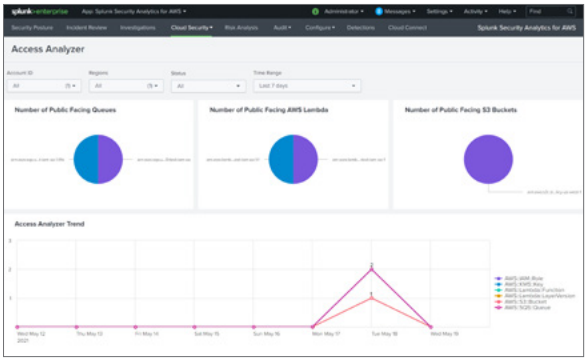


Visualize your AWS environment in one place

Onboarded data immediately starts populating pre-built dashboards to get you detecting threats quickly. Additionally, AWS-specific detections built by Splunk's Threat Research team identify threats and risks out-of-the-box. Splunk's Threat Research team provides new and updated detections and security guides to you to help you stay ahead of threats.

Get to the root cause quickly

Swiftly investigate incidents using Splunk's powerful search capabilities and Investigation Workbench, which allows you to build, collaborate on, and manage investigations from one interface. Dive deep into user and system behavior across your environment, construct incident timelines, and much more. Built-in MITRE ATT&CK® mapping and risk scoring allow you spot suspicious behavior earlier and conduct more targeted investigations.



Subscribe through AWS Marketplace: Splunk Security Analytics for AWS is available exclusively in AWS Marketplace. Avoid lock-in with monthly pay-as-you-go pricing at a flat rate. The offering comes with standard Splunk support and is priced to include 50 GB/day of data ingestion. Learn more here or check it out now in AWS Marketplace.

splunk> | aws

www.splunk.com

21-18921-Splunk-Splunk Security Analytics for AWS-PB-106