Cisco Security Analytics and Logging

Aggregate and analyze logs at scale

The network is constantly evolving and becoming increasingly complex. As a result, organizations need to continuously adapt policies to strengthen their defenses and improve security posture. This increased complexity continues to put more demand on your network operations team and leaves security operations grappling with a barrage of security alerts.

To detect tomorrow's attacks, you need to be one step ahead. A new paradigm is required that can not only scale with your growing network, but also help you seamlessly manage polices across your environment powered by analytics.

Scalable firewall log management is an important part of protecting your business as firewalls typically generate large amounts of log information. But the critical piece is the log analysis that provides administrators real-time information on breach attempts to quickly review, respond, and remediate against an attack. And continuous log analysis is key to protecting your network from future attacks by helping you refine your security posture to ensure a preventative solution has been put in place.

Cisco Network Policy simplifies policy management across your firewalls. The event viewer is an intuitive dashboard that allows users to see what is happening on their firewalls, manage policy, and enable quick corrective actions. Cisco Secure Network Analytics SaaS brings behavior-based machine learning to your private network and public cloud environments to generate high-fidelity threat detections. Cisco Security Analytics and Logging ties these two solutions together without requiring separate licenses.
It provides simple event viewing and policy management and aggregates static events at the perimeter, private network, and even public cloud for further analysis and threat detections.

Cisco Security Analytics and Logging capabilities

Store logs securely in the cloud—accessible and searchable within Cisco Network Policy.
Cisco Security Analytics and Logging is available for all Cisco Secure Firewalls, both Firepower Threat Defense (FTD) and Adaptive Security Appliance (ASA) models and all management configurations. Access search filters, download features and gain an intuitive firewall-logging experience.

Achieve end-to-end visibility by aggregating perimeter, internal, and even public cloud logs.
Cisco Security Analytics and Logging correlates static events at the perimeter with the behavior-based threat detections of Secure Network Analytics SaaS, generating high-fidelity alerts solely based on firewall activity. Cisco Security Analytics and Logging's three unique licenses allow users to broaden their usage with added private network log storage, analysis, and high-fidelity alerts. The 3rd tier license provides users the ability to add these features on to their public cloud environment through Secure Cloud Analytics, allowing for comprehensive visibility and protection at all ends of the network. Network telemetry is correlated with Cisco Talos threat intelligence, the largest non-governmental global threat intelligence organization in the world, to ensure that potential threats don't go unnoticed.

Enable corrective policy actions and automate threat detections for quicker investigations.
Cisco Security Analytics and Logging enables quick corrective actions and visibility into firewall events. Network operations managers can control internal and external policies and ensure that these are being adhered to. This solution brings automated threat detection and simple firewall management together.

Benefits

Simplify security management. Greatly reduce false positives with high-fidelity alerts and simplified policy orchestration.

Provide better intelligence to harmonize policy management. Monitor your networks and deploy behavioral-based analytics on firewall logs and network telemetry.

Enhance threat detection across the organization. Detect internal and external threats or suspicious activity by proactively monitoring network behavior. Using advanced analytics powered by Secure Network Analytics SaaS, detect threats such as C&C attacks, ransomware, DDoS attacks, illicit cryptomining, known malware, and insider threats.

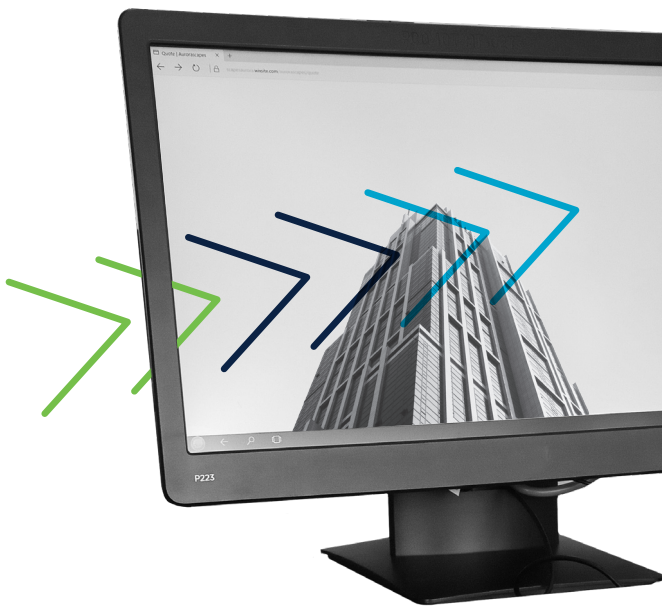
Meet compliance mandates. Enable logging and analytics capabilities to easily monitor your organization for compliance with industry regulations such as PCI, HIPAA, FISMA, and more.

Three unique license tiers

Logging and troubleshooting
The first tier offers log viewing for both FTD and ASA models. This live event viewer includes download capabilities and a base storage period of 3 months, which can be upgraded to 1, 2, or 3 years.

Logging analytics and detection
The second tier correlates firewall log data with the behavior-based threat detections of Secure Network Analytics SaaS. Users can access alerts based solely on firewall log data like malware event observation, IDS notice spike, potentially harmful hidden file extension, and many more.

Total network analytics and detection
The third and final tier offers consolidated analysis on the combined dataset of firewall, internal, and even public cloud logs for comprehensive threat detection. This unlocks its full potential. With this license, get more effective threat detections and protection at the perimeter, inside your network, and in the public cloud.



Learn more

Visit our webpage and sign up for a free trial today.