Cisco Secure Malware Analytics Cloud Subscription + Cisco Secure Email

Cisco Secure Email with Secure Malware Analytics

Product Description

Email is a leading threat vector for cyberattacks, according to Cisco's Annual Security Report. Keep your critical business email safe from spam, malware, and other threats. Our industry-leading solution gives you faster, more complete email protection to stop email-based threats and provide continuous protection before, during, and after an attack.

CISCO

The bridge to possible

Use Cases

Before an attack, Cisco Secure Email is powered by the Cisco Talos Security Intelligence and Research Group. The Talos threat intelligence detects, analyzes, and protects against both known and emerging threats.

During an attack, Cisco Secure Email provides the industry's first proven zero-hour antivirus solution. It offers a best-in-class capability to control and encrypt sensitive outbound email. At the same time, its layered defense, built into a single appliance, quickly blocks incoming attacks.

After an attack, with Cisco Secure Malware Analytics, Cisco Secure Email features file reputation scoring and blocking, static and dynamic file analysis, and file retrospection allows for the continuous analysis of threats, even after they have traversed the email gateway. Users block more attacks, track suspicious files, mitigate the outbreak, and quickly remediate.

Cisco Secure Malware Analytics embeds class leading dynamic malware analysis directly into Secure Email to protect against unknown files. The option of a Cisco Secure Malware Analytics Appliance offers a on-premises solution for organizations that have compliance or policy restrictions on submitting malware samples to the cloud.

Cisco Secure Email with Secure Malware Analytics
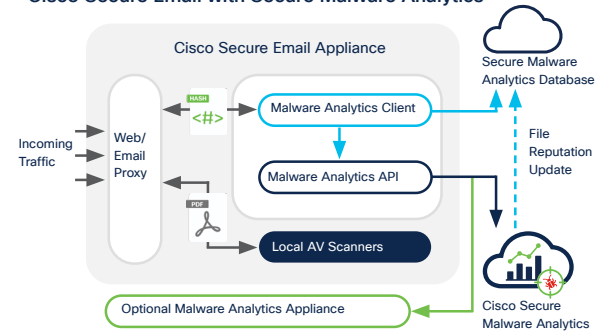
Secure Malware Analytics Cloud Subscription

Product Description

A full subscription to Cisco Secure Malware Analytics, formerly Cisco Threat Grid, provides class-leading advanced sandboxing and analysis of advanced malware. It is a unified malware analysis and threat intelligence solution that goes well beyond simple malware detection, providing a global view of malware samples, behaviors, and their associated families.

Use Cases

High Privacy Requirements: Secure Malware Analytics appliances provide on premises malware analysis, ensuring customers adhere to corporate and compliance mandates.

Security Operations: Secure Malware Analytics provides an intuitive web portal for junior analysts to quickly understand the scope of a threat and respond to incidents—all driven by high fidelity analyzed content. The portal also provides a detailed analysis and threat score for rapid prioritization of threats, as well as user interaction with the malware using Glovebox.

Threat Intelligence: With access to a robust API to integrate sample submission, Secure Malware Analytics enriches security event and threat content, allowing customers to automate and enhance the capabilities of their existing IT security infrastructure and procedures.

Data enrichment: Secure Malware Analytics leverages a robust data store of analyzed malware content that is rich in historical context and fully correlated, enabling the quick development of actionable defense and IR remediation plans.

Drill Down: Secure Malware Analytics's depth of malware analysis and data pivoting capabilities provide reverse engineers and incident responders the context, depth of data, and malware analysis they require to be effective.

The Secure Malware Analytics Cloud subscription provides threat intelligence feeds, with the option to create customized feeds for a customers unique security needs, industry, and threat environment.

CISCO SECURE

Feature / Capability	Secure Email with Secure Malware Analytics	Secure Malware Analytics Cloud Subscription
SPAM Blocking	X	
Graymail Detection	X	
Sender Base Reputation Filter	X	
URL Threat Protection	X	
Phishing Protection	X	
Email Encryption	X	
Web Interaction Tracking	X	
Outbreak Filters	X	
Data Loss Prevention	X	
Simple search of name and SHA256	X	X
Cloud or On Premises Deployment	X	X
Network, Process, Artifact, and File Activity reports	X	X
Behavioral Indicators	X	X
Threat Score	X	X
Global and historical context & correlation (pivot in reports with hyperlinks)		X
Download sample PCAP, and report JSON		X
Download Sample, Artifacts, Video		X

Feature / Capability	Secure Email with Secure Malware Analytics	Secure Malware Analytics Cloud Subscription
Interact with malware samples in Glovebox		X
Process Graph and Process Timeline JSON		X
Advanced search (samples, artifacts, IPs, registry, URLs, etc)		X
API integration for automation of sample uploads		X
API integration of threat intel into SIEM, visualization tools, etc.		X
Premium Threat Intelligence Feeds		X
Default Sample Submissions per Day	200*	Scalable*

*Scale sample limits as needed with the purchase of additional Advanced File Analysis packs

Cisco Secure Malware Analytics benefits security functions across

- SOC Team
- IR Team
- Threat Intelligence Team
- Security Infrastructure Engineering Team
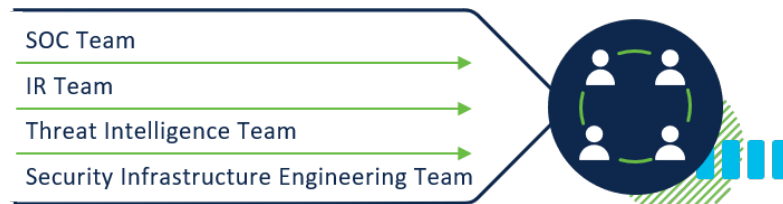
Learn more:

To find out more about Secure Malware Analytics visit:
http://www.cisco.com/go/amptg