Cisco Talos Threat Intelligence Services

Cisco Talos delivers industry-leading threat research and intelligence, proactive security services, and incident response to defend organizations against evolving cyber threats. Talos delivers unmatched and coordinated security across comprehensive platform of security products.

Contents

Threat Intelligence Services Overview

Cisco Talos is one of the most trusted threat intelligence research teams worldwide, consisting of elite researchers, analysts, incident responders, and engineers. Talos delivers comprehensive, proven intelligence that powers the entire Cisco security portfolio—protecting customers across all environments, every event, and every day.

Our mission is to safeguard Cisco customers by analyzing the evolving threat landscape supported by Artificial Intelligence and Machine Learning. These technologies allow Talos to process vast amounts of telemetry, detect threats with greater speed and accuracy, predict emerging risks, and provide actionable intelligence and rapid response.

Integrating threat intelligence into security products, across the platform, enhances real-time visibility, improves threat detection, enables proactive defense, automates response, reduces false positives, and enhances behavioral detections.

Talos empowers organizations with coordinated security services, integrated threat intelligence and incident response services. Disrupting attacks, providing unparalleled protection and empowering SOC teams with coordinated and centralized insights.

Threat Intelligence Service Catalog

Malware Defense

Service	Description
Cisco Talos Anti-Virus	Cisco Talos' Anti-Virus is built with malware detection in mind, delivering deep file analysis and pattern matching for file classification. This also includes regex or bytes for signature matching, as well as reviewing file hashes and image fuzzy hashes. It may also be automatically submitted for advanced sandboxing to Cisco Secure Malware Analytics.
Cisco Talos Malware Protection	Cisco Talos Malware Protection protects your endpoints and systems from malicious software delivered by threat actors looking to gain a foothold in your environment. Through our expert threat intelligence, a team of reverse engineers and machine-learning models, we provide a deep-layer of defense across our products both against the malicious software with file dispositions, as well as with behavioral indicators and protections that alert you when threat actors may be using living off the land binaries (lolbins), which are legitimate software tools used by attackers to carry out malicious activities.

Service	Description
	We continuously monitor all user and endpoint activity to protect against malicious behavior in real-time. It matches a stream of activity records against a set of dynamically updated attack activity patterns as threats evolve. This enables granular control and protection from the malicious use of living-off-the-land tools, which are legitimate software tools used by attackers to carry out malicious activities. Our malware protection services show up in products as behavioral indicators, behavioral protections, cloud indicators of compromise (Cloud IoCs) and classifiers.

Email Security

Service	Description
Cisco Talos Email Filtering	Cisco Talos Email Filtering provides layers of security, checking the URLs contained in email, file hashes of attachments, and multiple scanning engines to block malicious, unwanted, and inappropriate emails. This intelligence is based on sender reputation, selectable categories, and various atomic indicators. Talos looks at sender domain and IP reputations to block emails from suspicious or malicious senders, and crawls URLs within emails to ensure the security of users and compliance with acceptable use policies. Cisco Talos Email Filtering provides a robust set of intelligence and tools to protect users and ensure compliance. The industry-leading visibility and intelligence offered by Talos keeps users safe, secure, and productive.
Cisco Talos Email Threat Prevention	Going beyond email filtering, Cisco Talos Email Threat Prevention protects against various email threats, including brand impersonation. Business email compromise, and phishing. Brand impersonation involves attackers pretending to be a trusted brand to deceive recipients. Cisco Secure Email leverages Talos' intelligence to detect and prevent such attacks by analyzing anomalies, monitoring traffic trends, and using techniques like DMARC verification to ensure the authenticity of email senders. This helps protect organizations from phishing and business email compromise attacks that exploit brand trust.

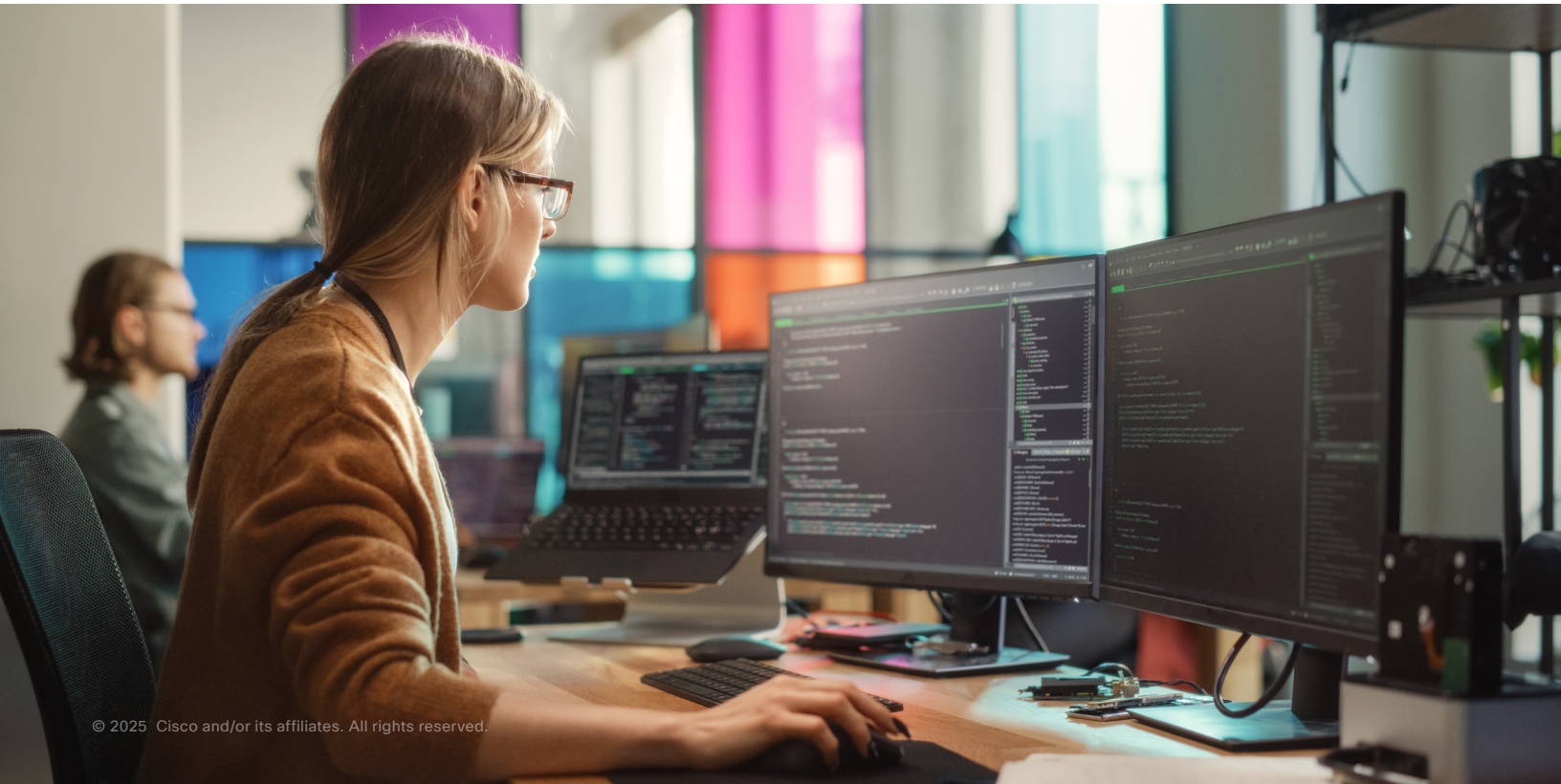
Service	Description
	Cisco Talos Business Email Compromise (BEC) Protection protects against BEC attacks focused on executives, who are considered high-value targets. It helps block these customized attacks and provides detailed logs on all attempts and actions taken. Combining global threat intelligence from Talos with local intelligence and machine learning to model trusted email behavior and detect anomalies. Cisco Talos Phishing Defense stops identity deception-based attacks such as social engineering, imposters, and BEC by combining global Cisco Talos Email Threat Prevention also utilizes machine learning techniques with daily model updates, maintaining a real-time understanding of email behavior to stop identity deception. It also includes rapid DMARC, advanced display name protection, and look-alike domain imposter detection.

Web Security

Service	Description
Cisco Talos DNS Security	Cisco Talos DNS security help organizations protect against Domain Name System (DNS)- based threats such as malware delivery, data exfiltration, phishing and command and control (C2) communications. DNS-Layer security blocks malicious domains, IPs and URLS at the DNS level before they reach the network and protects users regardless of their location. Using the NGFW as an example, additional features like deep packet inspection and DNS sinkholing drive better detection and prevention of the emerging threats.
Cisco Talos Web Filtering	Cisco Talos Web Filtering provides robust protection against online threats while ensuring compliance and visibility into web activity. This service protects users from accessing malicious or inappropriate web content through reputation and categorization across domain, IP, and URL indicators. Organizations have the ability to block harmful sties and enforce acceptable use policies. Whether through cloud-based solutions like Cisco Umbrella, Cisco Secure Access or on-premises appliances like Cisco Secure Firewall, organizations can achieve a high level of control and security for their web traffic in near real time.

Network Security

Service	Description
Cisco Talos Network Intrusion Prevention	Cisco Talos' Network Intrusion Prevention (Snort) is an advanced Intrusion Prevention System (IPS) that provides real-time traffic analysis and threat detection. This service identifies and blocks known network attacks by using machine learning delivered through SnortML and a comprehensive set of rules and signatures to detect malicious activity and zero-day attacks originating from both external and internal sources. Main Features of Cisco Talos IPS ▪ Deep Packet Inspection (DPI) ▪ Automated response to detected threats ▪ Signature-based and anomaly-based detection SnortML is a machine learning-based detection engine capable of detecting zero-day attacks by identifying payloads that match vulnerability classes, even if there are variations, allowing customers to get in front of the fight against zero-day attacks.



Threat Intelligence Service and Security Product Mapping

Please note that licenses and configurations may need to be enabled to benefit from these services. For example, Cisco Firewall integrates with Cisco Secure Endpoint and Cisco Malware Analytics.

Cisco Talos	Network Security	Web Security		Email Security		Malware Defense		
Threat Intelligence Services and Security Product Matrix	Cisco Talos Network Intrusion Prevention Service	Cisco Talos DNS Security	Cisco Talos Web Filtering	Cisco Talos Email Filtering	Cisco Talos Email Threat Prevention	Cisco Talos Malware Protection	Orbital Queries and Scripts	Cisco Talos Anti-Virus
Cisco Firewall	x	x	x			x		x
Cisco Multicloud Defense			x					x
Cisco Cybervision	x							
Cisco Secure Access			x					
Cisco Secure Connect		x						
Cisco Secure Endpoint						x	x	x
Cisco Umbrella	x	x	x					
Cisco Web Security Appliance (WSA)			x			x		x
Cisco Email Security			x	x	x	x		x
Cisco Email Threat Defense			x	x	x			x
Cisco Malware Analytics						x	x	x
Cisco Network Analytics			x					
Cisco Vulnerability Management								
Cisco XDR			x					
Cisco Security Cloud Control **(formerly Defense Orchestrator)**	x							

Cisco Talos	Network Security	Web Security		Email Security		Malware Defense		
Threat Intelligence Services and Security Product Matrix	Cisco Talos Network Intrusion Prevention Service	Cisco Talos DNS Security	Cisco Talos Web Filtering	Cisco Talos Email Filtering	Cisco Talos Email Threat Prevention	Cisco Talos Malware Protection	Orbital Queries and Scripts	Cisco Talos Anti-Virus
Cisco Meraki	x		x					
Cisco DNA Center			x					
Cisco ISR						x		x
Cisco WebEx								x
Splunk Attack Analyzer			x					
Cisco Enterprise Security			x					
Splunk SOAR			x					
Catalyst SDWAN	x		x			x		

C78-4861649-00 03/25