Cisco Talos Threat Hunting

Identify emerging threats before they become everyone else's alerts

Experts proactively search your Cisco endpoint, firewall, and identity* telemetry for stealthy attacker behavior that evades automated detection, delivering high-confidence notifications directly to you

Increase confidence in your defense as frontier AI models shorten time-to-exploit windows

Threat actors don't announce themselves. They move slowly, blend into legitimate traffic, abuse trusted identities, and exploit the gaps between your tools. By the time a detection fires (if it fires at all) the attacker may have been in your environment for days or weeks.

Adversaries are now leveraging frontier AI models to move faster, craft more convincing lures, and automate the reconnaissance that used to take them weeks. The gap between when an attacker enters your environment and when they cause damage is shrinking, so reacting to alerts is no longer enough.

Talos Threat Hunting goes looking before alerts exists. Hunt hypotheses are developed by the same Talos team that tracks nation-state actors, ransomware groups, and zero-day vulnerabilities globally. The intelligence that protects millions of endpoints, networks, and inboxes worldwide is also working for you.

These experts use AI to distill millions of signals to answer questions like: What traces would this living-off-the-land technique leave in firewall telemetry? If Talos research has uncovered a new endpoint attack technique, what evidence should we expect to see in the network?

From there, Talos threat hunters investigate every potential finding and apply those findings to your specific environment and telemetry context.

Once a threat specific to your telemetry is validated, you receive a high-confidence threat notification in Cisco Cloud Control, with detailed documentation of their findings and recommended next steps.

You'll get confidence that the same experts who have a pulse on the global attack surface are watching for threats across your telemetry.

© 2026 Cisco and/or its affiliates. All rights reserved.

Early defense for AI-driven threats

Cisco Talos Threat Hunting delivered across endpoint, firewall, and identity* telemetry

Why Cisco Talos Threat Hunting?	How it makes a difference for you
Global intelligence refined for your environment	Talos threat hunters use novel threat research, incident response evidence, and nearly 50M sensors.
AI-powered scale, human-validated accuracy	Automation hunts at machine speed while Talos analysts validate every finding.
Cross-domain correlation	Talos correlates endpoint, network, and identity activity instead of focusing on one product.
Designed to work below the alert threshold	Talos hunts below the alert threshold of SIEM, EDR, or firewall.
Direct access to threat hunting experts	Dashboard allows users to directly message the Talos experts who built and validated the hunt.
Seamless incident response (IR) handoff	If Talos IR is needed, the hunter joins the response team with full context.

Monthly threat hunting report
A recurring record of service activity is delivered every month, even months without threat notifications. The report covers hunts performed, findings summary, outbreak hunting results, and an "all-clear" log that shows which potential risks were ruled out. This is documentation your security team, leadership, and auditors can actually use.

Global threat landscape brief
An exclusive, private briefing from Cisco Talos on the most significant threat trends observed globally during the quarter. This is non-public intelligence delivered directly to Cisco Talos Threat Hunting customers.

One view for findings and metrics
The threat hunting portal in the Security view of Cloud Control is your centralized command center for the service. Real-time dashboards show all findings, hunting metrics, MITRE ATT&CK coverage visualization, telemetry status, and a full archive of metrics and notifications.

*This feature is in development and offered on a when-and-if-available basis. Cisco reserves the right to change delivery timelines and will have no liability for any delays or failures to deliver.

© 2026 Cisco and/or its affiliates. All rights reserved.