Cisco Talos Threat Hunting Program Ordering Guide

Contents

Introduction

This ordering guide is designed to help Cisco sales teams, partners, and distributors qualify, quote, and prepare orders for the Cisco Talos Threat Hunting program as an offer within the Cisco Security Cloud Control product suite. This guide will help you:

- Understand the program-level offer and its telemetry-domain entitlements.
- Determine the required Cisco base products, Security Cloud Control access, telemetry prerequisites, and threat-hunting entitlement for the requested domain.
- Avoid quoting phased, unsupported, or proposal-stage capabilities and commercial constructs.
- Validate the bill of materials and prepare the customer for activation, onboarding, and telemetry verification.

This guide is intended for authorized Cisco and channel personnel. Current Cisco Commerce (CCW), Global Price List, contractual, legal, tax, support, and approved offer guidance remain authoritative whenever they differ from this guide.

Product overview

Cisco Talos Threat Hunting is a continuous, intelligence-led threat hunting service that proactively searches for attacker behavior across eligible Cisco security telemetry. Cisco Talos develops and maintains standardized hunt hypotheses; an autonomous hunting engine runs continuously, and Talos analysts validate meaningful findings before customers are notified.

The offer is one Talos-led service program with modular telemetry coverage. Secure Firewall telemetry through Security Analytics and Logging (SAL) is the phase-one network path; it should not be positioned as a separate firewall-only service or as the identity of the entire program. Endpoint and Identity are additional telemetry domains with different entitlements and delivery behavior.

Service model: Cisco Talos identifies, validates, and communicates findings. The customer retains ownership of investigation decisions, containment, remediation, and operational response.

Coverage model: The autonomous hunting engine runs 24 hours a day, 7 days a week. Current-release human analyst validation and customer notification occur during U.S. business hours, Monday through Friday, spanning Eastern through Pacific Time. Do not describe the offer as 24x7 human analyst coverage.

Customer deliverables

- Enriched threat notifications with an executive summary, technical evidence, indicators of compromise, timestamps, Talos analyst commentary, MITRE ATT&CK mapping, recommended next steps, and relevant intelligence links.
- Monthly Threat Hunting Reports summarizing hunts performed, validated findings, notifications, telemetry-query metrics, and inquiry status, including months in which no validated findings occur.
- A quarterly Global Threat Landscape Brief for program customers.
- Searchable history, detailed reports, hunt metrics, MITRE coverage metrics, and customer inquiry workflows in the Security Cloud Control Threat Hunting Portal where supported by the telemetry path.

Scope

This guide addresses qualification, entitlement selection, bill-of-material preparation, CCW validation, and post-order activation for Cisco Talos Threat Hunting. It covers supported Cisco telemetry domains and the current U.S.-only release boundary.

The following are outside the current service and must not be represented as included:

- Incident response, containment, cleanup, or remediation; Cisco Talos Incident Response is a separate engagement.
- Device management, product tuning, or configuration services for Secure Firewall or other security products.
- Cisco Adaptive Security Appliance (ASA) telemetry.
- Third-party telemetry, vendor-neutral hunting, or non-Cisco infrastructure telemetry.
- Customer-specific hunting logic or custom playbook development.
- A replacement for the customer's SOC, SIEM, XDR, MDR, or incident-response function.
- 24x7 human analyst coverage or a guaranteed real-time inquiry-response SLA in the current release.

Product licensing and entitlement overview

Talos Threat Hunting is organized by telemetry domain. For every requested domain, the customer must hold the qualifying Cisco base-product entitlement and the applicable threat-hunting entitlement. The table below provides the supported entitlement model; validate current orderability in CCW.

Telemetry domain	Required base entitlement	Threat-hunting entitlement	Delivery and current-state note
Network/Secure Firewall	Supported Cisco Secure Firewall Threat Defense subscription; SCC access; SAL telemetry	Firewall Threat Hunting add-on (TTH-SEC-SUB)	Threat Hunting Portal and email. This guide covers U.S.-only availability. ASA is not supported.
Endpoint	Cisco Secure Endpoint Premier	Included with Premier entitlement	Endpoint-only findings currently remain in Cisco Secure Endpoint; SCC portal delivery is planned for a future phase.
Identity	Duo or Cisco Identity Intelligence	Identity hunting add-on when orderable	Phased rollout. Do not quote until the offer is active in approved guidance and CCW.

One program, modular coverage. Customers with multiple eligible domain entitlements may receive correlated findings across available domains. Correlation depth and delivery path depend on current entitlement and portal support; do not promise identical behavior for every domain. The Security Cloud Control Threat Hunting Portal is visible only to customers that purchase and activate the Firewall Threat Hunting add-on SKU. Customers with other entitled telemetry may still be hunted, but that entitlement alone does not grant Portal access.

Firewall offer prerequisites

- Supported physical, virtual, or container Cisco Secure Firewall Threat Defense (FTD) environment.
- A qualifying Secure Firewall subscription as defined in current approved offer rules.

- A Security Cloud Control tenant and the required SCC/cdFMC access path.
- Security Analytics and Logging (SAL) enabled for the selected Firewall telemetry path.
- The approved Firewall Threat Hunting add-on and its defined order metric.
- Customer willingness and ability to enable the required data-sharing or log-export configuration and identify the selected firewall IDs for onboarding.

Service and support model

The service includes Talos-led onboarding, analyst validation, validated finding delivery, recurring reporting, and inquiry support. The current offer configuration uses no separate Talos support PID. Support is provided through the underlying SAL offer, with one required "BU Support (SAL support)" selection (MIN 1 / MAX 1). James Boyd from Talos owns the in-house support path.

Service activity	Cisco Talos responsibility	Customer responsibility
Onboarding	Lead kickoff, checklist/RFI, back-end enablement, and go-live confirmation	Provide contacts, context, documentation, and customer-side configuration
Telemetry configuration	Provide requirements and resolve Talos/back-end ingestion issues	Enable and maintain customer-side connectors, data sharing, and log flow
Hunting and validation	Run autonomous hunts and validate signals before notification	No operational action required until findings are received
Finding response	Deliver evidence, analyst context, and recommended next steps	Investigate, contain, remediate, and own response decisions
Finding inquiries	Respond through portal messaging; same-day U.S.-business-hours response is a best-effort target, not an SLA	Initiate inquiry and provide follow-up context
Active incident response	Not included; Talos Incident Response may be engaged separately	Procure and coordinate any separate incident-response engagement

Ordering process

Quoting guidelines

Quote control. Use only current CCW and approved offer/pricing guidance. Earlier planning materials include percentage-of-firewall-list-price pricing, minimums, Core/Enterprise tiers, SAL bundling options, average three-year terms, and a proposed two-PID motion. Those constructs are not established as final orderable terms in the available source set and must not be quoted from this guide.

- This guide covers U.S. customers only. Do not use it for federal or non-U.S. customers unless newer approved guidance expands eligibility.
- Select entitlement by telemetry domain. Never treat one domain's prerequisite or delivery path as universal across the program.
- For Firewall, SAL is required for the supported telemetry path. Do not generalize SAL as a prerequisite for every current or future domain.
- For Endpoint, Secure Endpoint Premier includes Endpoint Threat Hunting. Avoid adding a duplicate entitlement unless current CCW explicitly requires one for the requested cross-domain motion.

- For Identity, treat the offer as phased and non-quotable until current approved guidance and CCW confirm availability.
- Do not promise third-party telemetry, ASA support, custom hunts, remediation, 24x7 human staffing, or a guaranteed inquiry SLA.

Step 1: Qualify the customer and select telemetry domains

Before constructing the bill of materials, confirm:

- **Telemetry scope.** Firewall, Endpoint, Identity, or an eligible combination.
- **Base products.** The customer owns or is purchasing the qualifying Cisco base entitlement for every requested domain.
- **Geography.** The customer is eligible under the current U.S.-only release rules.
- **Operating model.** The customer understands Detect and Notify and has a process to investigate and remediate validated findings.
- **Technical readiness.** The customer can complete the configuration checklist, RFI, telemetry setup, and environmental-context requirements.
- **Expectation fit.** The customer is not seeking MDR, incident response, device management, ASA coverage, third-party telemetry, or custom hunt development as part of this offer.

Step 2: Build the domain-specific bill of materials

Scenario	Include in the order or validate as needed	Do not assume
New Firewall hunting customer	Supported Secure Firewall entitlement, SCC access, SAL, and approved Firewall Threat Hunting add-on	Any PID, pricing, quantity rule, or automatic SAL behavior not exposed by current CCW
Existing Secure Endpoint Premier customer adding Firewall	Existing Premier entitlement plus the required Firewall, SCC, SAL, and Firewall hunting components not already owned	That Endpoint entitlement automatically covers Firewall hunting
Existing SAL Premier or SAL Unlimited customer	Existing SAL entitlement and compatibility with the current Firewall hunting configuration	That SAL will auto-add, auto-deselect, migrate, or co-term in the proposed manner
Endpoint-only customer	Cisco Secure Endpoint Premier	SCC portal delivery for Endpoint-only findings in the current phase
Identity customer	Duo or Cisco Identity Intelligence plus the approved Identity hunting add-on when released	Current orderability before approved phased-rollout guidance
Enterprise Agreement customer	Current EA coverage plus any separately orderable hunting add-on defined by approved rules	That Talos Threat Hunting is included in the EA; planning artifacts state EA treatment was under analysis

Step 3: Configure the offer in Cisco Commerce

Configure the Firewall offer in CCW using TTH-SEC-SUB and the current approved option structure. CCW and the Global Price List remain authoritative.

1. Search for and add TTH-SEC-SUB — Cisco Talos Threat Hunting for Firewalls Subscription.

2. Select the Firewall telemetry option and the applicable supported device billing PID from Appendix A. Endpoint Threat Hunting is included with Secure Endpoint Premier; Identity is not quotable until released.
3. Enter the covered-device quantity using UOM Device. Use current CCW and Global Price List pricing; do not calculate price from another offer or an unapproved percentage.
4. Confirm SCC access, SAL telemetry, and one required “BU Support (SAL support)” selection (MIN 1 / MAX 1).
5. No separate Talos support PID is required. Support is provided through the underlying SAL offer; James Boyd from Talos owns the in-house support path.

CCW validation control. Interface labels may change. Validate the offer identity, device option, quantity, term and billing, included SAL behavior, and order summary directly in CCW before saving the order.

Step 4: Confirm term and billing details

- Select an allowed term of 1–60 months; the configuration workbook specifies a 36-month default.
- Select prepaid or annual billing, a Requested Start Date within 90 days, standard CCW co-term behavior, and the current renewal setting exposed by CCW.
- The configuration workbook specifies 12-month auto-renew by default with user opt-out. Confirm the live configuration before submitting the order.
- For existing SAL and EA customers, validate transition, credit, replacement, and co-term handling in current CCW and the customer’s governing agreement.

Step 5: Validate and save the order

- **Offer identity.** The order uses the approved Talos Threat Hunting PID/SKU and the intended telemetry-domain options.
- **Entitlements.** Every domain has its qualifying base product and hunting entitlement, with no unintended duplication.
- **Firewall prerequisites.** SCC access, SAL, supported FTD environment, and selected firewall coverage are represented or validated.
- **Eligibility.** Geography and customer-type restrictions are satisfied.
- **Commercial terms.** Price meter, quantity, term, support, billing, renewal, and EA treatment match approved guidance.
- **Provisioning contacts.** Customer administrator, operational contacts, and onboarding contact details are complete.
- **Validation.** Run the CCW validation action, resolve all messages, and save the validated configuration.

Provisioning information

After the offer is activated, Cisco Talos conducts remote onboarding. The kickoff call is targeted within two weeks of service activation, but overall onboarding duration depends on customer completion of required configuration and information requests and is not a guaranteed service level.

1. Kickoff call: confirm customer points of contact, explain the Detect and Notify service model, review communication paths, and align on onboarding responsibilities.
2. Configuration checklist and RFI: provide the technical telemetry requirements and request environmental context, including network documentation, critical assets, known exclusions, and notification contacts.
3. Telemetry setup: for Firewall, identify the selected firewall IDs and enable the required SCC/SAL data-sharing or log-export configuration. Customer-side connector and configuration work remains the customer's responsibility.
4. Telemetry verification: Cisco Talos and the customer confirm that the required supported telemetry is flowing. Cisco Talos owns backend ingestion remediation; the customer owns customer-side remediation.
5. Go-live confirmation: Cisco Talos confirms when hunting is active and notifies the customer by email and through the Threat Hunting Portal where supported.

Customer access and notification routing

Finding scenario	Primary delivery path	Ordering/onboarding implication
Firewall finding	SCC Threat Hunting Portal and email	SCC access, portal users, notification contacts, and SAL telemetry must be validated
Identity finding	SCC Threat Hunting Portal and email	Use only when the Identity domain is orderable and activated
Correlated cross-domain finding	SCC Threat Hunting Portal and email	Customer must hold eligible entitlements for the contributing domains
Endpoint-only finding	Cisco Secure Endpoint	Cisco Secure Endpoint Do not promise SCC portal delivery until approved for that path

In Cisco Security Cloud Control, navigate to Security > Talos Threat Intel Center > Threat Hunting Portal. It provides searchable notifications, detailed reports, hunt metrics, MITRE coverage metrics, report export where available, and a messages/ticketing path for questions about specific findings.

Subscription renewals, changes, and cancellations

Policy control. The source set does not establish final Talos-specific renewal, change, cancellation, credit, co-term, or auto-renew rules. Use the current CCW configuration, approved offer documentation, applicable agreement, and published Cisco Commerce guidance. Do not copy those rules from another SCC product.

Subscription or entitlement changes

When a customer adds a telemetry domain, changes coverage, modifies quantity, or transitions an existing SAL or EA position, use the approved Talos change motion and migration playbook. Validate that the change preserves the required base entitlements, avoids duplicate hunting coverage, and maintains the intended SCC/SAL delivery path.

Renewal and cancellation

Use the customer's approved order, governing agreement, and current Cisco Commerce policy for renewal timing, notice, auto-renew, cancellation, credit, and midterm restrictions. This guide does not create Talos-specific commercial terms.

Order-validation checklist

- **Customer eligibility.** U.S. geography and current customer-type restrictions confirmed.
- **Requested domains.** Firewall, Endpoint, Identity, or approved combination clearly identified.
- **Base entitlements.** Qualifying Secure Firewall, Secure Endpoint Premier, Duo, or Cisco Identity Intelligence entitlement confirmed for each domain.
- **Hunting entitlements.** Applicable add-on or included entitlement confirmed in current CCW.
- **Firewall data path.** SCC tenant, SAL, supported FTD deployment, selected firewall IDs, and data-sharing/log-export readiness confirmed.
- **Delivery path.** Portal/email versus Secure Endpoint behavior explained accurately.
- **Service boundary.** Detect and Notify, customer-owned remediation, U.S.-business-hours human validation, and inquiry-response limits acknowledged.
- **Exclusions.** No ASA, third-party telemetry, custom hunts, device management, MDR/SOC operation, or incident response included.
- **Commercial accuracy.** PID/SKU, offer classification, price meter, quantity, term, support, EA, renewal, change, and cancellation rules sourced from approved guidance.
- **CCW validation.** All configuration messages resolved and validated summary saved.
- **Onboarding readiness.** Customer administrator, security contacts, environmental documentation, critical assets, exclusions, and telemetry owner identified.

Authoritative-source control

CCW, the Global Price List, approved offer documentation, support guidance, and governing agreements are authoritative. Validate the order against those sources before submission.

Glossary

CII: Cisco Identity Intelligence.

Detect and Notify: Service model in which Cisco identifies, validates, and communicates findings while the customer owns investigation and response.

FTD: Cisco Secure Firewall Threat Defense.

SAL: Security Analytics and Logging; required for the current Secure Firewall telemetry path.

SCC: Cisco Security Cloud Control, including the Threat Hunting Portal under the Talos Threat Intel Center.

Telemetry domain: A supported Cisco data source and its entitlement/delivery path, such as Firewall, Endpoint, or Identity.

Source and approval boundary

Source basis: the TTH-SEC-SUB PID and PDT Rules workbook reviewed August 13, 2026; the June 18, 2026 Talos Threat Hunting Field FAQ; the BU/legal-review Product Description; and current program guidance. Current CCW, the Global Price List, approved Offer Description and Disclosure, support mapping, provisioning runbook, and governing agreements are authoritative.

Appendix A — Firewall SKU Reference

Use this appendix to identify the Firewall offer and current billing PID family. Validate availability and current pricing in CCW before quoting.

Top-level ATO: TTH-SEC-SUB — Cisco Talos Threat Hunting for Firewalls Subscription.

Billing PIDs (UOM: Device): TTH-CSF220; TTH-FPR1010; TTH-FPR1120; TTH-FPR1140; TTH-FPR1150; TTH-CSF1210CE; TTH-CSF1210CP; TTH-CSF1220CX; TTH-CSF1230; TTH-CSF1240; TTH-CSF1250; TTH-FPR3105; TTH-FPR3110; TTH-FPR3120; TTH-FPR3130; TTH-FPR3140; TTH-FPR4215; TTH-FPR4225; TTH-FPR4245; TTH-CSF6160-A; TTH-CSF6170-A.

SKU controls: hardware-EOL PIDs and the unreconciled 9K and FTDv entries are excluded from this reference. Do not quote TTH-FPR9K or TTH-FPRTD-V. Endpoint Threat Hunting is included with Secure Endpoint Premier; no Endpoint PID is defined in this Firewall ATO workbook.

Legal information