Cisco Threat Response Data Sheet

Contents

Solution overview

Security attacks wait for no one, making threat investigations increasingly complex, all the while with understaffed security operations teams. Security analysts need to stay ahead of current threats and minimize impact in the event of an attack, but they're often pivoting between multiple, disparate cybersecurity tools and spending valuable time and resources in the process.

Cisco® Threat Response is a security investigation and incident response application. It simplifies threat hunting and incident response by accelerating detection, investigation, and remediation of threats. Threat Response provides your security investigations with context and enrichment by connecting your Cisco security solutions (across endpoint, network, and cloud) and integrating with third-party tools, all in a single console. Threat Response is included at no additional cost with the following Cisco security licenses:

Endpoint	Cisco Advanced Malware Protection (AMP) for Endpoints Email Security Web Security
Network	Cisco Firepower® Cisco Stealthwatch® Enterprise
Cloud	Cisco Umbrella™
Intelligence	Cisco Threat Grid

To understand whether a threat has been seen in your environment as well as its impact, Threat Response aggregates contextual awareness from Cisco security product data sources along with global threat intelligence from Talos® and third-party sources via APIs. Threat Response identifies whether observables such as file hashes, IP addresses, domains, and email addresses are suspicious or malicious, and whether you have been affected by them. It also provides the ability to remediate directly from the interface and block suspicious files, domains, isolate hosts, and more without pivoting to another product first.

With Threat Response you will:

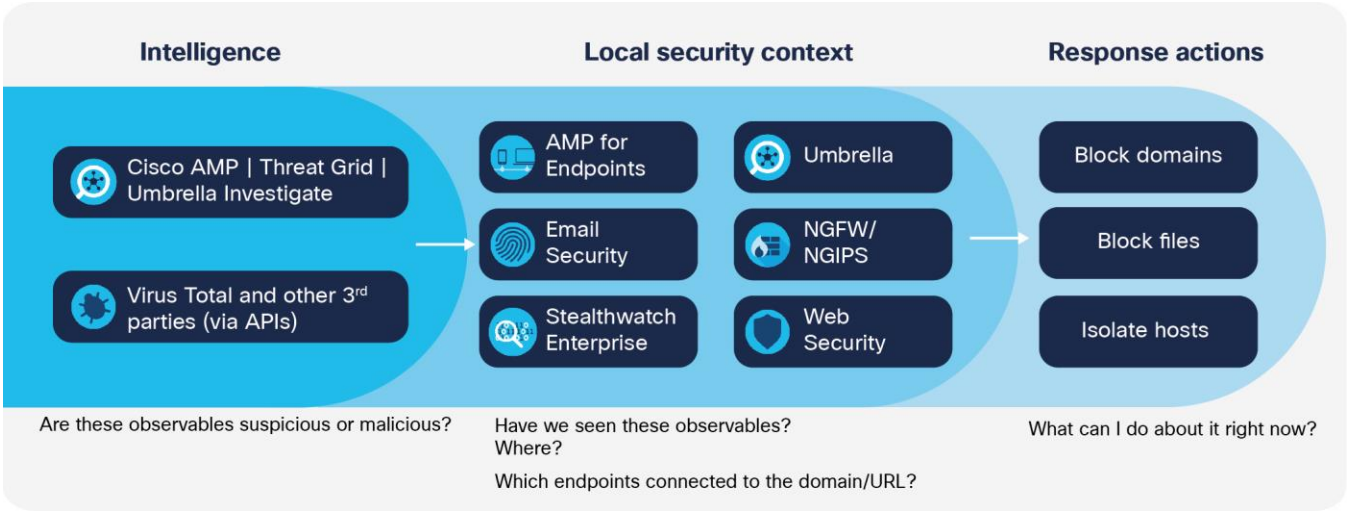
- Simplify threat investigations
- Get rapid, coordinated incident response
- Lower Mean Time To Respond (MTTR) and dwell time

Primary use cases

- Incident response: Leverage multiple security technologies in a single console to address and manage the aftermath of an attack in your environment by aggregating multiple security technologies for a holistic investigation and remediating in a single console.
- Threat hunting: Proactively search for active threats in your environment with a holistic, integrated approach by aggregating multiple security technologies in a single console.

How Threat Response works

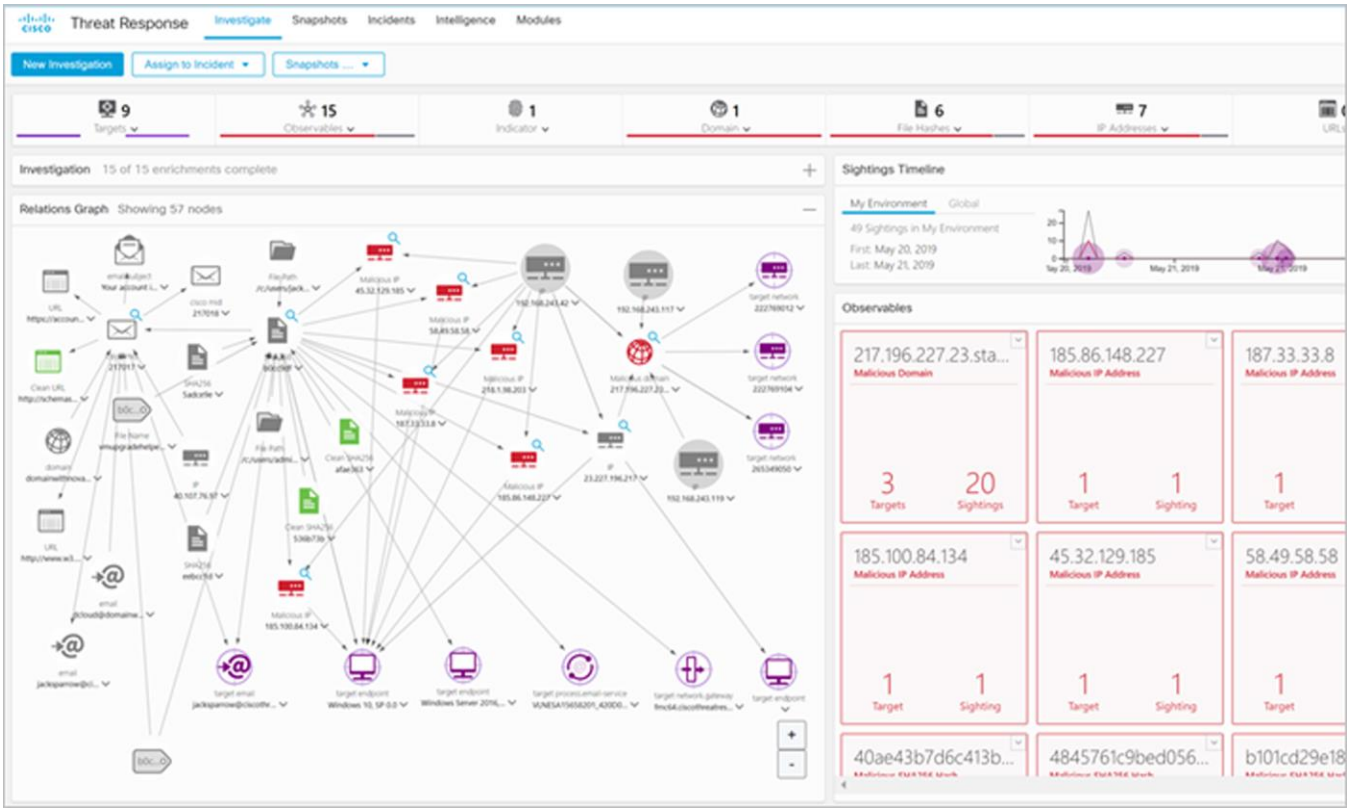
Threat Response aggregates intelligence from both Cisco security product data sources and third-party sources via APIs to identify whether observables such as file hashes, IP addresses, domains, and email addresses are suspicious. The left-hand side of the diagram below shows the intelligence sources that are used to generate verdicts on the Indicators of Compromise (IOCs). When you paste the observables to the Investigate interface of Threat Response and start an investigation, the product adds context from integrated Cisco security products automatically, so you know instantly which of your systems was targeted and how. It brings that knowledge back from intel sources and security products, displaying results in seconds. From there, security operations teams can take action immediately or continue their investigation with the tools provided.



Main features and capabilities

Feature	Description	Benefit	Requirements
Casebook	Tool for saving, sharing, and enriching threat analysis that allows to document all the analysis in a cloud casebook and to save snapshots from all integrated or web-accessible tools.	Get a correct verdict on dispositions on observables quickly and intuitively and pivot to individual data sources for more information, working across multiple integrations in the Cisco security portfolio.	Available via: • Cisco Threat Response Investigate UI • Other integrated Cisco products and tools • Any webpage via browser plug-in, including other Cisco products, integrated or external threat intel sources, and existing third-party tools.

Feature	Description	Benefit	Requirements
Incident Manager	Automated triage and prioritization of alerts from Cisco Firepower and Cisco Stealthwatch Enterprise. Allows for investigating and enriching events with context from integrations across security products as well as responding to high-urgency incidents.	• Convenience of common UI for all Cisco-detected security incidents • First-level triage, promoting raw security events to Incidents • Customizable auto-promotion rules	Required integrations: • Cisco Firepower integration • Cisco Stealthwatch Enterprise integration
Response	Remediation actions: • Isolate hosts • Block files • Block domains	Respond to threats immediately through the convenient interface of one console.	Required integrations: • AMP for Endpoints integration to isolate hosts and block files • Umbrella Enforcement APIs to block domains
Browser plug-in	Browser extension that allows for pulling IP addresses or domains from anywhere an observable is seen, for an investigation.	Quickly and easily pull in indicators of compromise from any webpage or browser-based console, Cisco or otherwise, and start an investigation.	Installed plug-ins for Google Chrome or Firefox
Relations graph	Part of the Threat Response interface that shows all the observables found during the investigation and indicates relationships between them. Intuitive color and shape coding helps determine the nature of the events and the relationships.	Visually intuitive guide to enrichment results, which allows for an at-a-glance verdict for the observables you are investigating (malicious, benign, and unknown) and helps you immediately tell if these observables are seen locally in your network.	Available via: • Cisco Threat Response Investigate UI
Open-source integrations	Custom integrations of any security operations tools and workflows available through open and well-documented APIs.	Leverage your full security stack by integrating all tools into one console, enhancing your existing Security Information and Event Management (SIEM) and Security Orchestration, Automation, Response (SOAR) technologies.	Available via open APIs



Product specifications

Cisco Threat Response is a cloud-based product available in three regional clouds:

- U.S. cloud
- EU cloud
- Asia Pacific cloud

Browser requirements: current and preceding versions of Chrome, Edge, Firefox, and Safari

Cisco security integrations

The product can integrate with selected cloud and on-premises solutions. Cloud services are typically integrated using API keys, available under the settings menu of the cloud service itself. For on-premises devices to be integrated with Threat Response, it must first be added and then registered in Security Services Exchange. Security Services Exchange (SSE) is a Cisco cloud platform that handles cloud-to-cloud and premise-to-cloud identification, authentication, and data storage for use in Cisco cloud security products. The connected devices can write to the storage in SSE and then from there to Threat Response.

Value of the individual product integrations

Cisco Threat Response and Umbrella: Umbrella automatically uncovers attacker infrastructure staged for current and emerging threats and proactively blocks malicious requests before they reach a customer's network or endpoints. With Cisco Umbrella enrichment for Threat Response, customers can stop phishing and malware infections earlier, identify already-infected devices faster, and prevent data exfiltration. The integration provides complete visibility into Internet activity across all locations and users and allows you to take action with a two-click response to quickly block domains.

Cisco Threat Response and Email Security: Integration with Email Security allows you to understand email as a threat vector by visualizing message, sender, and target relationships in the context of a threat. You can search for multiple email addresses, subject lines, and attachments at once to understand how a threat has spread.

Cisco Threat Response and Firepower: Integration with Cisco Firepower provides the capability to investigate, identify, and enrich Cisco Firepower intrusion events with context from integrations across security products. It also offers an automated triage and prioritization of intrusion events through the built-in Incident Manager.

Cisco Threat Response and AMP for Endpoints: Integration with AMP for Endpoints allows you to investigate and identify multiple files with context from integrations across security products. It provides detailed information on affected endpoints and devices, including IP addresses, OS, and AMP GUID. Additionally, it allows you to block files at endpoints and AMP-capable edge devices and immediately quarantine affected endpoints with the AMP Host Isolation response feature.

Cisco Threat Response and Threat Grid: Integration with Threat Grid allows you to get detailed intelligence about malware, associated paths, and more.

Cisco Threat Response and Stealthwatch Enterprise: Stealthwatch network-based visibility and security analytics will enrich threat detection and response in the Threat Response console with agentless behavioral and anomaly detection capabilities. Threat Response integrations with other sources of global threat intelligence and internal visibility will affirm and enrich Stealthwatch findings with confirmed threat intel and local sightings. Integrations with Cisco control devices provide two-click mitigation and resolution.

Cisco Threat Response and Web Security: The Web Security Appliance (WSA) leverages multiple technologies to protect your network against the most common threat vector and provides Threat Response users with visibility into connections with unsafe or suspicious websites. Threat Response integrations with other sources of global threat intelligence and internal visibility will affirm and enrich WSA findings with confirmed threat intel and local sightings.

Integrated product software compatibility

Product	Requirement
AMP for Endpoints	Cloud only
Threat Grid	Cloud only
Email Security	• (With Security Management Appliance (SMA)): AsyncOS12.5 on both the Email Security Appliance (ESA) and the SMA • (Standalone): AsyncOS13.0
Umbrella	Cloud product, N/A
Web Security	(SMA or standalone): AsyncOS 12.0
Stealthwatch Enterprise	V7.1.2+
Firepower	v. 6.3+

Integrating your Cisco security products with Cisco Threat Response

- Quick-start guides for integrated products:
  - Umbrella
  - E-mail Security
  - Firepower Next-Generation Firewalls (NGFW)
- Configuration tutorials on YouTube
  - AMP for Endpoints
  - Umbrella
  - Firepower NGFW

APIs/third-party integrations

Threat Response is developed using an API-first approach, which means that all features are built into the API, and then the user interface is updated to call that API function. Functionally, this means that any action you can perform in the UI, you can also perform via the API. The API documentation is robust and even includes prototyping tools that you can use to help develop your own integrations and middleware.

Use cases for the API include, but are certainly not limited to:

- Adding your own threat intelligence, regardless of source or collection method, to Threat Response for future investigations
- Performing automated investigations on observable feeds, checking for local sightings
- Promoting alerts and events from third-party tools into Threat Response's Incident Manager

To get started learning how to use this powerful, versatile tool, see the Cisco Learning Lab on the Threat Response API at https://cs.co/CTR-API-labs.

API aggregation

Threat Response can be thought of as an API aggregator—we use the APIs of the integrated products so that you don't have to. Threat Response uses those APIs to retrieve information and relay response actions to the products that offer them. For example:

- Using the SMA API to ask if the SMA has any record of interactions with an IP address
- Using the AMP file database API to get a reputation lookup on a file hash
- Using the AMP for Endpoints API to request host isolation on an endpoint

Each of these integrated tools adds their own capabilities to the toolset.

Threat Response is not a SIEM, or a SOAR—although it provides some functionality commonly associated with each. Like a SIEM, Threat Response gives you one place where you can check logs from multiple products—not by aggregating the logs themselves, as in a traditional SIEM (adding storage cost and maintenance), but by aggregating the lookups against those existing information stores. Similar to a SOAR, Threat Response gives you quick response capabilities across multiple control planes in a single interface. However, Threat Response is a free application, and it can very well coexist with SIEM and SOAR tools and empowers them to integrate with Cisco products more easily—in fact, we already have supported integration tools for Splunk, LogRhythm, and others soon to come.

Support

If you require technical assistance with Threat Response, you can open a case in Support Case Manager. The Cisco security product(s) through which you have access to Threat Response entitle you to a number of technical services. You would need your product serial number or product service contract to create a support case. Alternatively, you can either manually select “Threat Response” in the technology window and bypass the entitlement or contact Cisco Support at 1 800 553 2447.

Resources

For more information about Cisco Threat Response, visit cs.co/threat_response or contact your Cisco security account representative to learn how your organization can get more value out of your existing security investment by leveraging Cisco Threat Response at no additional cost.

Other helpful resources:

- Threat Response community page
- Threat Response YouTube videos
- Threat Response at-a-glance
- Threat Response FAQs

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-743307-00 01/20