Cisco Security Platforms

8.7.1

Introduction

It's natural for a networking company like Cisco to think about risks within the network and risks related to traffic running on a network. If you think about how much information a system needs to ingest in order to monitor and watch for problems, you soon realize that one person alone, or even a security team full of capable people, cannot use manual processes all the time to secure a network or secure an application. You need automated ways to identify threats and mitigate risks, as well as ways to configure systems with security in mind.

Scripts can ingest data faster than a human. Scripts can look for problems and identify them much faster than a person. Plus, scripts for configuration are repeatable and do not lead to breaches due to mis-typing within configuration files.

Cisco provides a large portfolio of security technologies and product families which are configurable and manageable via APIs. This topic will focus on:

- Advanced Malware Protection (AMP) for Endpoints
- Cisco Firepower Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Cisco Identity Services Engine (ISE)
- Cisco Threat Grid
- Cisco Umbrella

8.7.2

Cisco Advanced Malware Protection (AMP)

Cisco Advanced Malware Protection (AMP) for Endpoints provides API access to automate security workflows and includes advanced sandboxing capabilities to inspect any file that looks like malware in a

safe and isolated way. AMP works with Windows, Mac, Linux, Android, and iOS devices through public or private cloud deployments.

Benefits and purpose

With AMP for Endpoints you can get information about endpoints and pull specific event information, or move endpoints to new groups using REST APIs. The AMP product continuously analyzes file activity across the extended network. With the information provided by the AMP API, you can detect, contain, and remove advanced malware.

Architecture

Advanced Malware Protection has a collection of subscription-based products. You manage them with a centralized web-based console, and you deploy AMP on devices including mobile phones, on email servers, or on web servers. With AMP for Endpoints, you install an AMP Connector on each device.

Integrations

AMP integrates across the Cisco security portfolio with multiple deployment options. Two examples of products with AMP integration are Cisco Umbrella and Meraki MX.

Environment and scale

AMP for Endpoints can be used in a university campus setting, within healthcare organizations, for government entities, or industrial and manufacturing environments.

Capabilities

AMP prevents breaches and blocks malware at the point of entry, then detects, contains, and remediates advanced threats that can evade front-line defenses and get to your network.

There are three main categories of capabilities that AMP offers:

- Prevention
- Detection
- Responses and automation

Prevention

AMP protects against identified threats in malware files by preventing breaches. You can use the API to create isolation sessions, preventing network connection of a device for a set duration so you have time to prevent further problems.

AMP uses global threat intelligence and can block file-based or non-file-based malware, IP addresses from a list, or block applications.

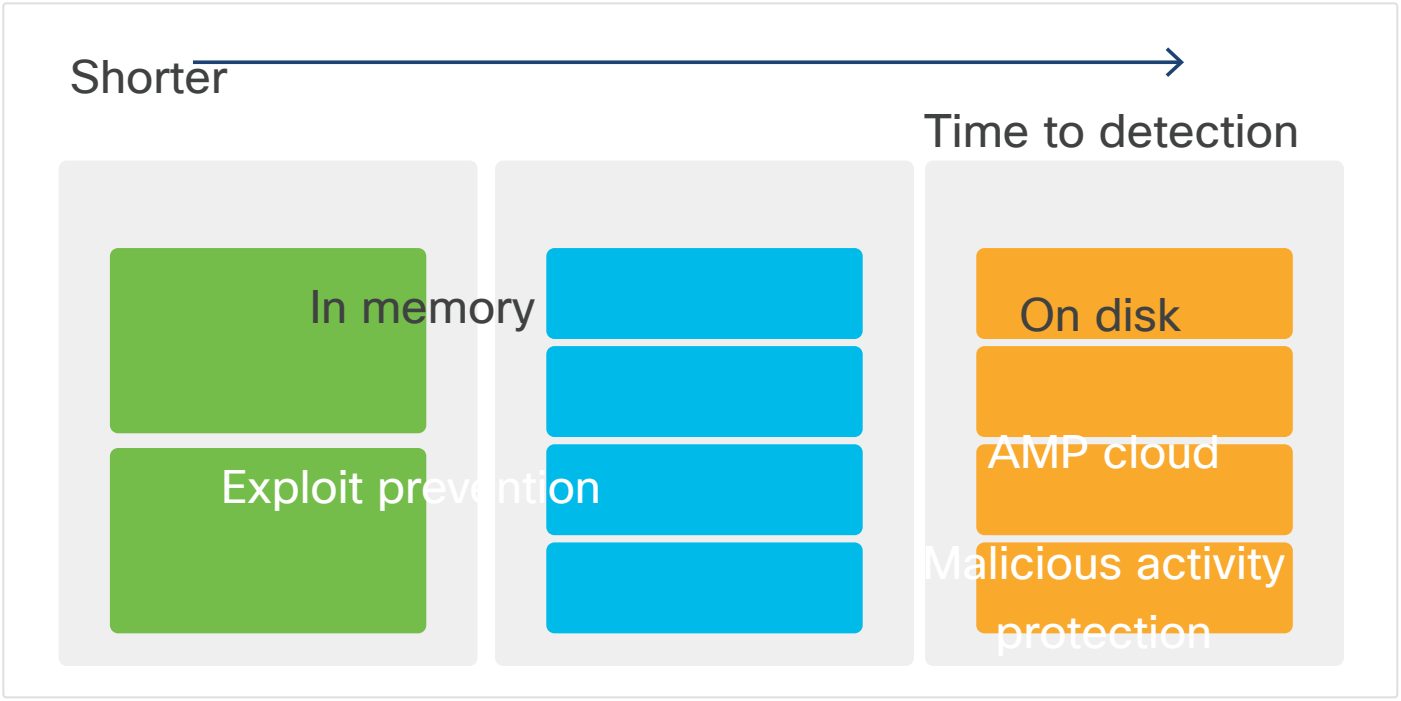
Detection

AMP continuously monitors and records all file activity to detect malware. It ensures visibility into endpoint file activity and incoming threats, as well as reporting which endpoints have been compromised.

AMP Cloud offers lookups, a signature engine, and a machine learning engine for a constantly updated intelligence database so that detection can happen on-disk. The AMP Cloud is the service you query with the AMP API.

TETRA is an antivirus engine delivered as part of the AMP Connector for Windows, and ClamAV is a similar engine for macOS and Linux.

Cisco AMP Detection



Using the AMP API, you can look for computers or devices that have associations with a particular event or activity using query parameters. For example, if you know of malware with a particular URL or `.exe` file, you can see which computers have come into contact with it.

The events resources in the AMP API v1 provide 95 different types of events, from scans to installations to specific application actions, that you can use to filter results from events happening in your monitored environment.

Responses and automation

Accelerate investigations and automatically remediate malware across PCs, Macs, Linux, servers, and mobile devices (Android and iOS). Provides advanced sandboxing so you can inspect malware. In this context, sandboxing lets you activate unknown files in a safe, isolated environment. The sandbox then records the actions and reports them. These activities are also stored for later reference.

The AMP API enables you to request isolation of an identified computer or device. Isolating a computer or device blocks all network traffic except for communication to the AMP Cloud and any other IP addresses

configured in your IP isolation allow list. An unlock code that you can provide with the API call enables management of the isolation session.

Read the documentation to learn all the details of the API.

API authentication

You can either use an API client ID with an API key for authentication, or use Basic HTTP authentication with a Base 64-encoded string that combines your API client ID with the API key.

API rate limits

Three `X-` headers provide information about rate limiting with the AMP for Endpoints API:

- `X-Rate-Limit-Limit` - Number of total allowed requests in the current period.
- `X-Rate-Limit-Remaining` - Number of requests left before reaching the limit.
- `X-Rate-Limit-Reset` - Number of seconds before the limit is reset.

As an example response, you would see:

```
x-ratelimit-limit: 3000
x-ratelimit-reset: 3588
x-ratelimit-remaining: 2980
```

API pagination

The AMP API uses Links to get to locations within the response, such as self, next, and last. You can also use an `offset` parameter to get the next number of results based on the offset value. As an example:

```
{
  "offset": 250
}
```

Sending the `offset` value in the body of the request provides the next set of 250 values.

8.7.3

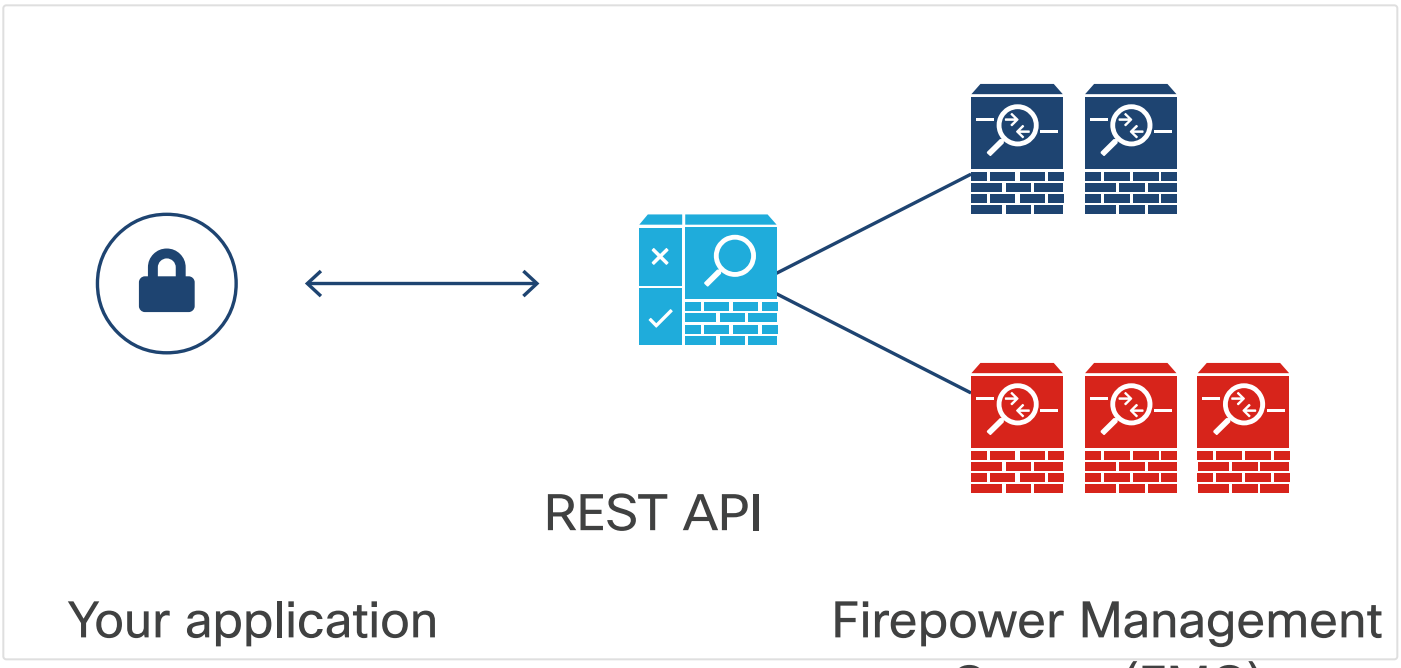
Cisco Firepower Products

Firepower Management Center (FMC) is a central management console for the Firepower Threat Defense (FTD) Next-Generation Firewall. This console can configure all aspects of your FTD including key features like access control rules (traffic filtering) and policy object configuration, such as network objects. FMC

provides a central configuration database enabling efficient sharing of objects and policies between devices. It provides a REST API to configure a subset of its functionality.

With Firepower Management Center, you manage devices on your network so that your network traffic is filtered and controlled based on various characteristics. You can also perform access control on network devices, using the network appliance with a central console and database.

Cisco Firepower Management Center (FMC) and Firepower Threat Defense (FTD)



Another management option is to directly configure the Firepower Threat Defense device through its on-device REST API, which provides for similar API capabilities to the FMC API. The FMC API and FTD APIs cannot directly co-exist. You must choose one of the following management options:

- **Firepower Device Manager(FDM)/FTD-API/CDO** – These three options can co-exist.
- **Firepower Management Center (FMC)** – For advanced scenarios, FMC provides for the most product functionality through its graphical user interface. API capabilities between the two are similar.

Benefits and purpose

These products help programmatically manage firewalls, which provide rules to stop network traffic, redirect it, or choose which traffic can go through, enabling you to comply with security policies and protect your network.

Firepower takes the following actions for traffic control:

- Inspect, log, and take action on network traffic.
- Use security intelligence data to filter traffic. You can create lists of blocked and allowed IP addresses or address blocks, domain names, or URLs.
- Control which websites are available to users on your network.
- Block or filter certain files based on lists containing data about the files.

- Rate limit network traffic based on access control.
- Create protective measures to redirect traffic to a "sinkhole server", where the firewall can fake a DNS query response for a known malicious domain. For example, when a user tries to access a known bad site, the sinkhole configuration resolves to an IP address that you define. You can display information to the end-user trying to access the bad domain.

Protection

Firepower Threat Defense configuration with Firepower Device Manager also provides protective services listed here:

- Track, backup, and protect CA Certificates.
- Manage, backup, encrypt, and protect private keys.
- Internet Key Exchange (IKE) key management, which helps with site-to-site IPsec VPN.
- Provide Access Control Lists to select traffic for services. You can configure two types of ACL:
  - **Extended** - (IPv4 and IPv6) Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses, which you can mix in a given rule.
  - **Standard** - (IPv4 only) Identifies traffic based on destination address only.

Architecture

Firepower Management Center can run on VMware vSphere or Amazon Web Services (AWS). It can also run on a range of physical devices, including the Cisco FMC 1000, 1600, 2000, 2500, 2600, 4000, 4500, and 4600.

These management tools are purpose-built for customers to manage and configure their Firepower Threat Defense devices. Firepower management tools run on VMware vSphere or Amazon Web Services (AWS) and include:

- **Firepower Management Center (FMC)** – This is a multi-device manager for large Enterprise deployments with the need for deep correlation and analytics capabilities.
- **Firepower Device Manager (FDM)** - This is a "single" device manager for small and medium customers with small number of devices with simple dashboards and easy to use configuration wizards. It contains the FDM and Next Generation Firewall APIs.

These can be used to manage appliances and devices including those in the Cisco Firepower 1000, 2100, 4100, and 9300 series (which run Cisco Firepower Threat Defense and can alternatively support Cisco Adaptive Security) and the Cisco ASA 5500-FTD-X series appliances for SOHO and edge-network defense.

Integrations

Firepower Management Center (and Device Manager, though currently with a limited feature set) can integrate with Cisco Identity Services Engine (ISE). The integration of ISE with FMC lets you move particular users in or out of quarantine after they start a VPN session, blocking access to a particular IP as needed.

Other products, such as Threat Grid and Umbrella, can integrate with Firepower Threat Defense devices. For example, Umbrella can identify malicious domains and use Firepower Threat Defense to block those

domains (or mark them as safe).

Environment and scale

FMC is intended for larger environments where automatic deployment and automated actions are crucial for efficiency gains and configuration accuracy.

Within Firepower Threat Defense, the Firepower Device Manager (FDM) and Next Generation Firewall APIs help small and medium-sized businesses so that they do not have to hire security experts.

You can try the Firepower Management Center REST API explorer on the device itself, at the following URL: `https://<management_center_IP_or_name>:<https_port>/api/api-explorer`. The Firepower Threat Defense REST API also has an API "Try it out" capability hosted on the FTD device. You can use the DevNet Sandbox if you want to try the API Explorer on FMC or FTD.

Capabilities

The APIs include Firepower Management Center REST API and Firepower Threat Defense REST API.

- **Firepower Management Center API** - Gives access to network and endpoint security event data and host information.
- **Firepower Threat Defense API** - Used to update configuration settings on the device. You deploy those changed configuration settings using a POST call. Refer to the documentation for details about deployment using the REST API.

API authentication

For the Firepower Management Center API, you use an access token to authenticate to the REST API. The token lasts for 30 minutes before the client must refresh it. To make the call, you use the header `X-auth-access-token:<authentication token value>`. To refresh the token, request another token from the API and then send both the token value X-header and `X-auth-refresh-token:<refresh token value>` with the next call.

For the Firepower Threat Defense REST API, OAuth 2.0 workflows authenticate calls from API clients. OAuth is an access token-based method, and you can read about the framework in RFC7519. JSON web tokens (JWT), from RFC7519, are used for the schema. You provide a username and password, then receive a normal token. Then, you can define additional custom tokens (sensibly named to facilitate management). The token goes in the Authorization: Bearer header of requests. Tokens can also be revoked using the API.

API limits

To limit network load, the FMC API accepts a maximum of 120 messages per minute from an individual IP address. In addition to this rate limiting, there is payload limiting where the API cannot accept a payload larger than 20480 bytes.

With the Firepower Threat Defense API, you can send a limit value as a parameter for your request to bring back a limited number of responses. By default, the API's upper limit value is 1000.

8.7.4

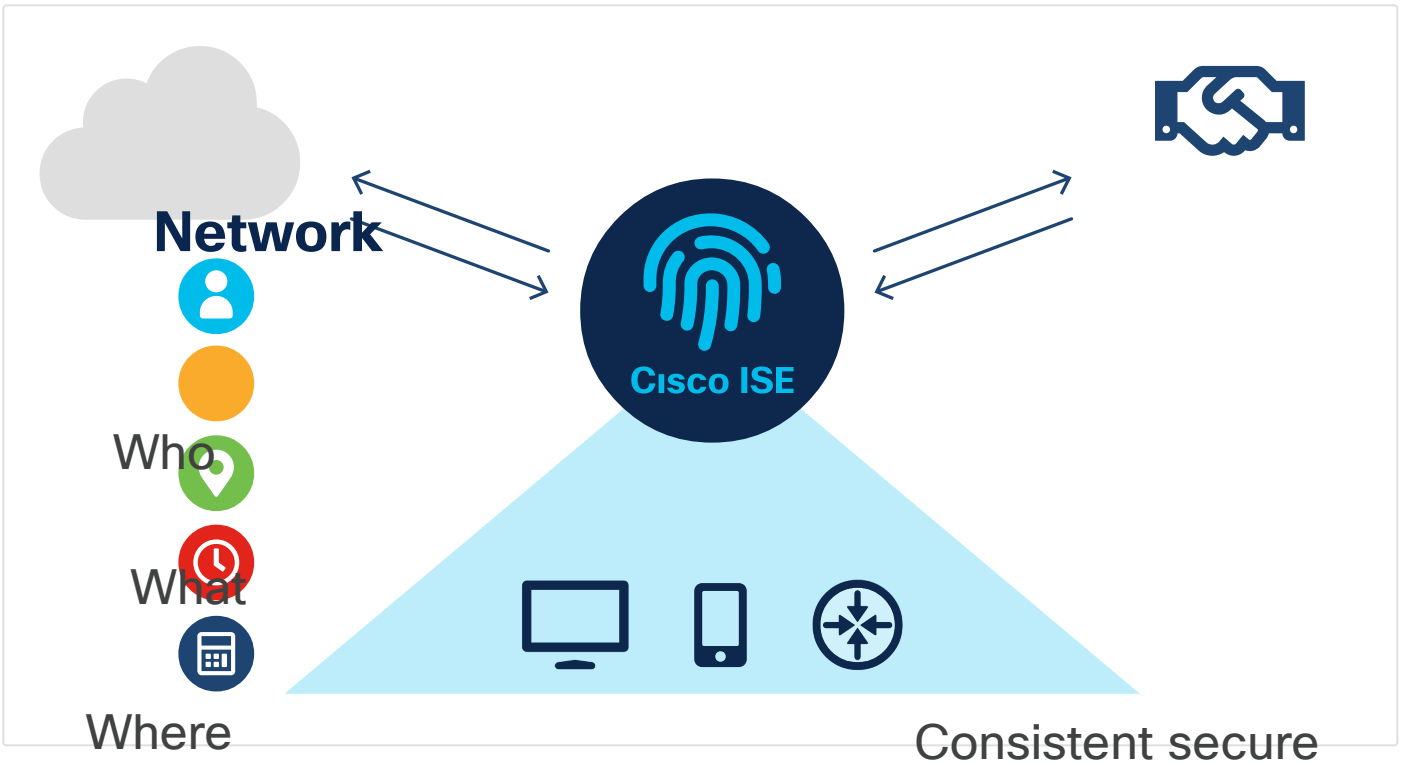
Cisco Identity Services Engine (ISE)

The Cisco Identity Services Engine, or ISE, can be pronounced as "ice" and is an integral part of the Cisco security portfolio.

Benefits and purpose

ISE provides a rule-based engine for enabling policy-based network access to users and devices. It enables you to enforce compliance and streamline user network access operations. With the ISE APIs, you can automate threat containment when a threat is detected. It integrates with existing identity deployments.

Cisco ISE Overview



Architecture

Cisco ISE architecture consists of nodes with defined node types. A node is an individual physical, or virtual, Cisco ISE appliance. These Cisco ISE nodes can assume any of the following node types: Administration, Policy Service, Monitoring, or pxGrid:

- **Administration node -** In this node you perform all administrative operations on Cisco ISE. It handles all system-related configurations such as authentication, authorization, and accounting.

- **Policy Service node -** A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. The policy information point represents the point at which external information is communicated to the Policy Service persona. For example, external information could be a Lightweight Directory Access Protocol (LDAP) attribute.
- **Monitoring node -** A Cisco ISE node with the Monitoring persona is the log collector. It stores log messages from all the Administration and Policy Service nodes in a network.
- **pxGrid node -** The pxGrid framework integration enables the system to exchange policy and configuration data between nodes. This is how the system can share tags and policy objects between Cisco ISE and third party vendors.

The remaining pieces of the ISE architecture are the network resources and endpoints, or devices connecting to the network.

You can configure node deployments for high availability, load balancing, and automatic failover, depending on the size of the deployment.

There is also the option to have a standalone deployment. In this architecture, one ISE node runs the Administration, Policy Service, and Monitoring personas.

Integrations

In order to get the most out of the platform, there are multiple integrations available for Cisco ISE. Some are for information and data sharing, remediation, and certificate revocation. It also integrates with identity systems for identity management including role-based access control (RBAC), Okta/SAML Single-Sign On (SSO), Lightweight Directory Access Protocol (LDAP), Active Directory (AD).

Environment and scale

Cisco ISE is used in various sized environments, from small to medium and large businesses. At the largest scale, it provides support for 250,000 active, concurrent endpoints, and up to 1,000,000 registered devices.

Capabilities and use cases

You can read about more than twenty use cases on the Cisco Case Studies page for ISE. ISE's capabilities can be summarized as follows:

- **Asset visibility -** Bring your own devices with both guest and secure wireless access for employees. Use the ISE posture assessment functionality to allow personal mobile devices onto the network, such as at a hospital or retail location.
- **Policy compliance -** ISE and enforced consistent security policy integrate with Cisco TrustSec for software-defined segmentation across the network.
- **Secure wired access -** Cisco ISE identifies every single device and user accessing the network, whether wired, wirelessly, or remotely. After they are identified, the connecting device and user are then automatically and securely placed into the right part of the network. This segmentation offers efficiency gains as you can use one network for two separate organizations. It enables secure wired access while also giving asset visibility.

- **Segmentation -** For example, at a large sports event you need to enable attendee device networks as well as media output for high-definition video being broadcast to the world. The integrated system automatically segments traffic away from the rest of the network using Cisco ISE.

8.7.5

Cisco Threat Grid

Threat Grid is a malware analysis platform that combines static and dynamic malware analysis with threat intelligence from global sources. You can add a Threat Grid appliance to your network, or use the Threat Grid service in the cloud. It can also be integrated into other security technologies such as Advanced Malware Protection (AMP).

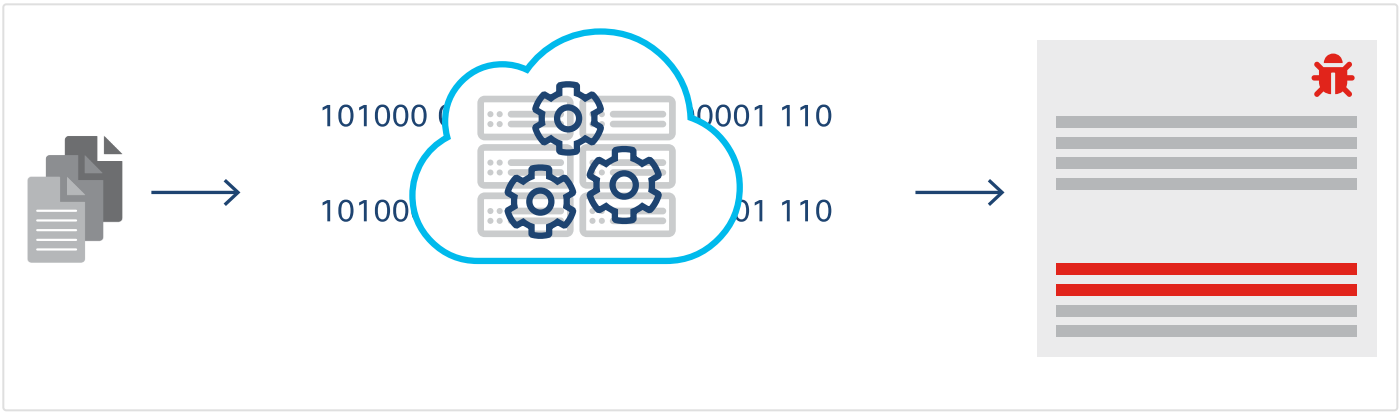
Benefits and purpose

With Threat Grid you can review and analyze potential threats or behavior indicators of malware activity.

A Threat Grid appliance delivers on-premises malware analysis with threat analytics and content. Organizations with compliance and policy restrictions can analyze malware locally by submitting samples to the appliance.

The user interface and API workflows are designed for Security Operations Center (SOC) analysts, malware analysts, security specialists, and forensic investigators.

Cisco Threat Grid Overview



Integrations

Threat Grid is also available through integrations with other Cisco Security products, such as Advanced Malware Protection, next-generation firewalls, and Cisco ASA with FirePOWER Services. You can integrate Threat Grid with Threat Response for no additional cost as a threat hunting tool.

Environment and scale

The content subscription license has the capacity to sample and analyze between 500 and 10,000 samples per day.

Capabilities

Threat Grid offers malware analysis capabilities, both static and dynamic.

- Static analysis provides identifying information about the file, file headers, and its contents.
- Dynamic analysis actually executes the malware in a safe, specialized virtual environment called a "glovebox". This enables you to interact with the malware without harming your production system, and helps you discover file modifications, process calls, network activity or connections.

You can use the Threat Grid intelligence feed to build actions based on the analyses.

When you submit intelligence samples to Threat Grid, you can extract relevant data for use with other platforms like Firepower or AMP endpoints.

Organizations can use the Threat Grid API to build their own front ends, dashboards, or workflows.

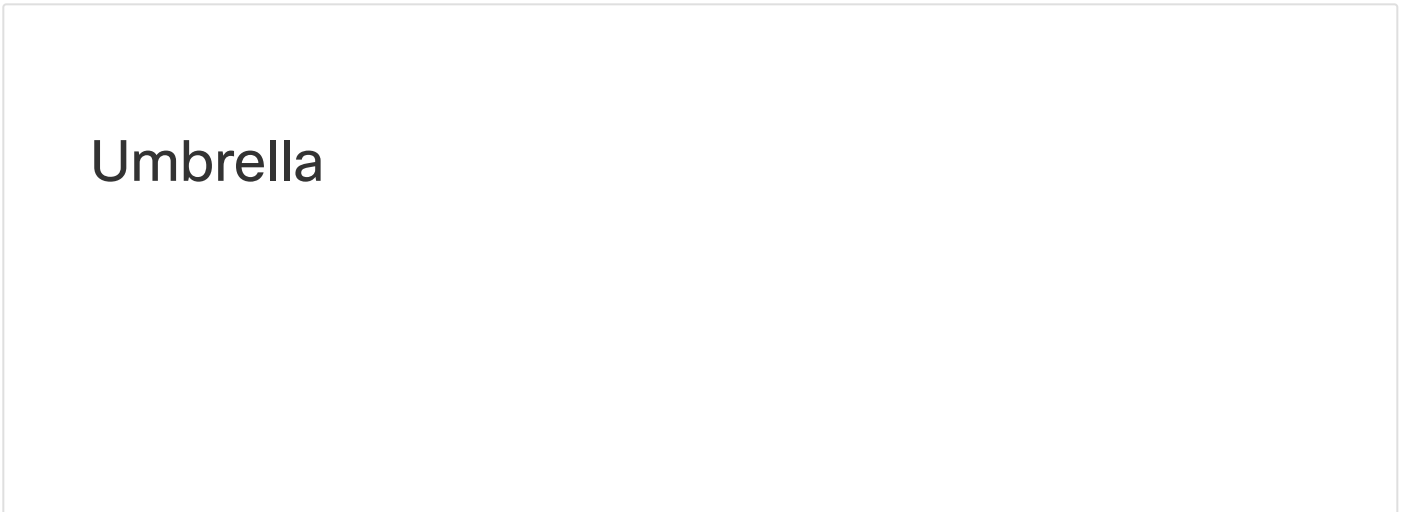
Read more details in the Threat Grid online API documentation, which you can access with a Cisco Security account.

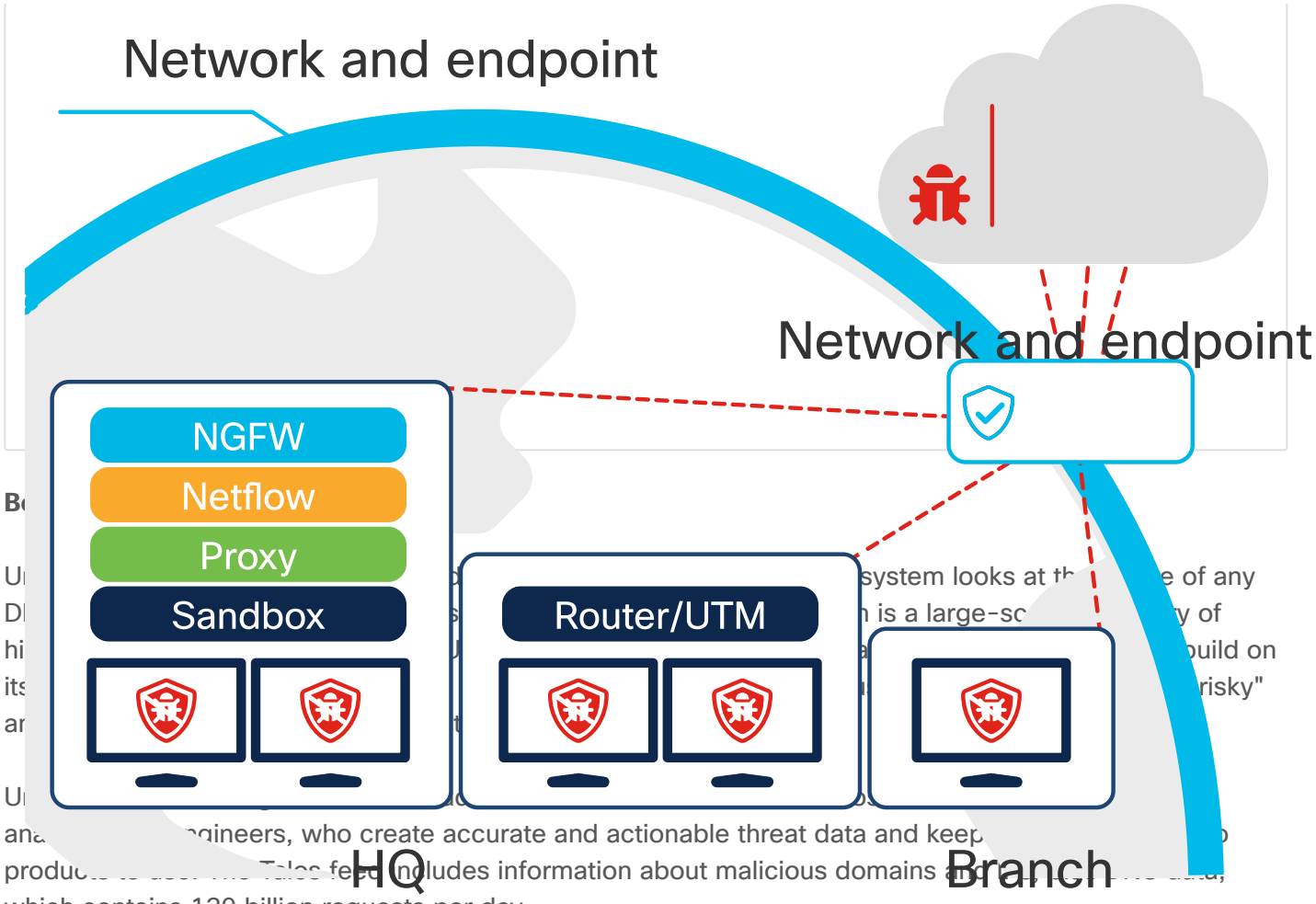
8.7.6

Cisco Umbrella

Umbrella uses Domain Name Servers (DNS) to enforce security on the network. You configure your DNS to direct traffic to Umbrella, and Umbrella applies security settings on their global domain name list based on your organization's policies.

Cisco Umbrella Overview





Be

Ur system looks at th e of any
Dl is a large-sc y of
hi uild on
its risky"
ar

Ur
ana gineers, who create accurate and actionable threat data and keep
produc Talos fee includes information about malicious domains a
which contains 120 billion requests per day.

Architecture

- The **Enforcement API** integrates security events with Umbrella.
- The **Network Devices API** integrates hardware devices with Umbrella.
- The **Investigate API** gives you data to find more about security incidents.
- The **Reporting API** enables organizations to run several reports.

To learn more about each API, refer to https://docs.umbrella.com/developer.

Integrations

To use Umbrella, you will add hardware devices for management by Umbrella security. There are also API integration points with threat protection and enforcement use cases. You can integrate Meraki MR and Umbrella for wireless protection use cases.

Developers and security experts use the Umbrella Enforcement API to take actions on a domain request, or use the Umbrella Investigate API to pull threat intelligence data programmatically. The Enforcement API and its scoring is described in more detail in the Capabilities section.

Environment and scale

Umbrella is used in larger retailers, large hospital settings, and university campuses. Umbrella can protect hundreds, thousands, or tens of thousands of endpoints.

Capabilities

Umbrella's protection capabilities include:

- Wi-Fi protection when guests are on your network
- Selected application blocking
- Endpoint security for off-network (not on VPN) devices
- Web filtering

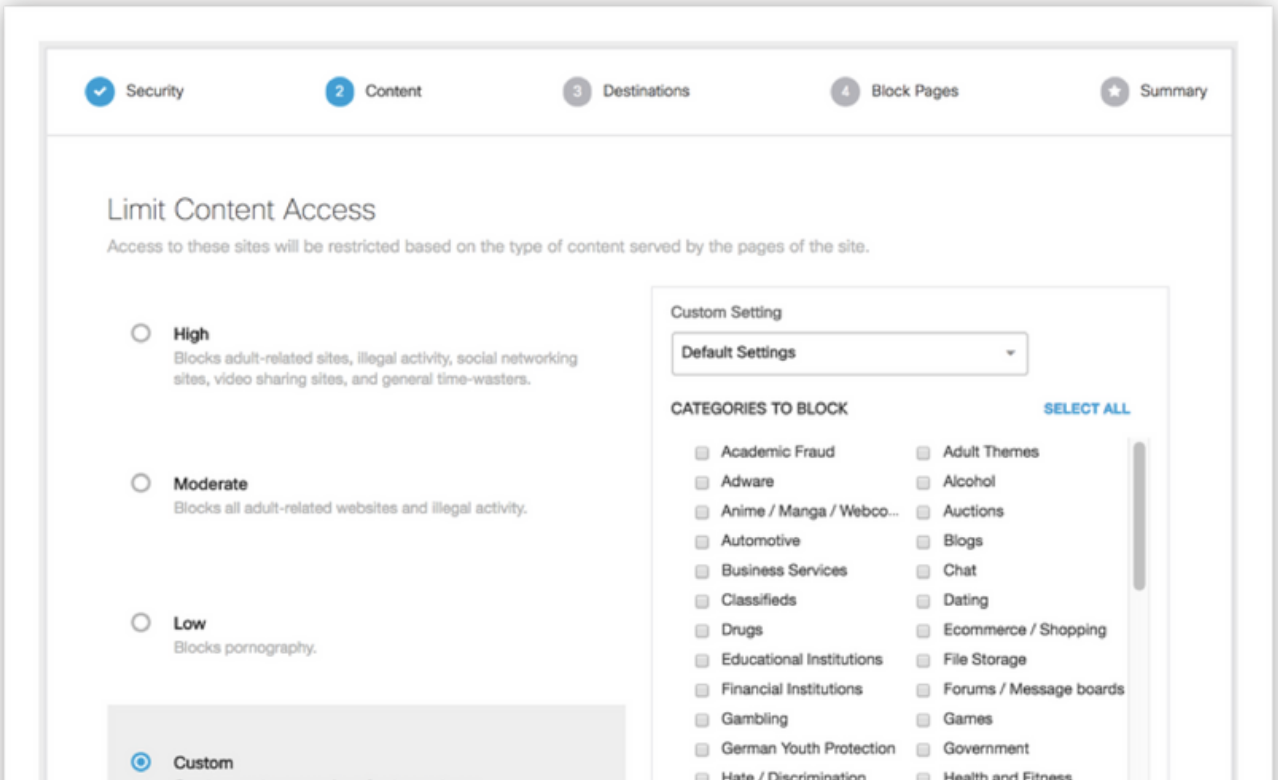
Guest Wi-Fi protection

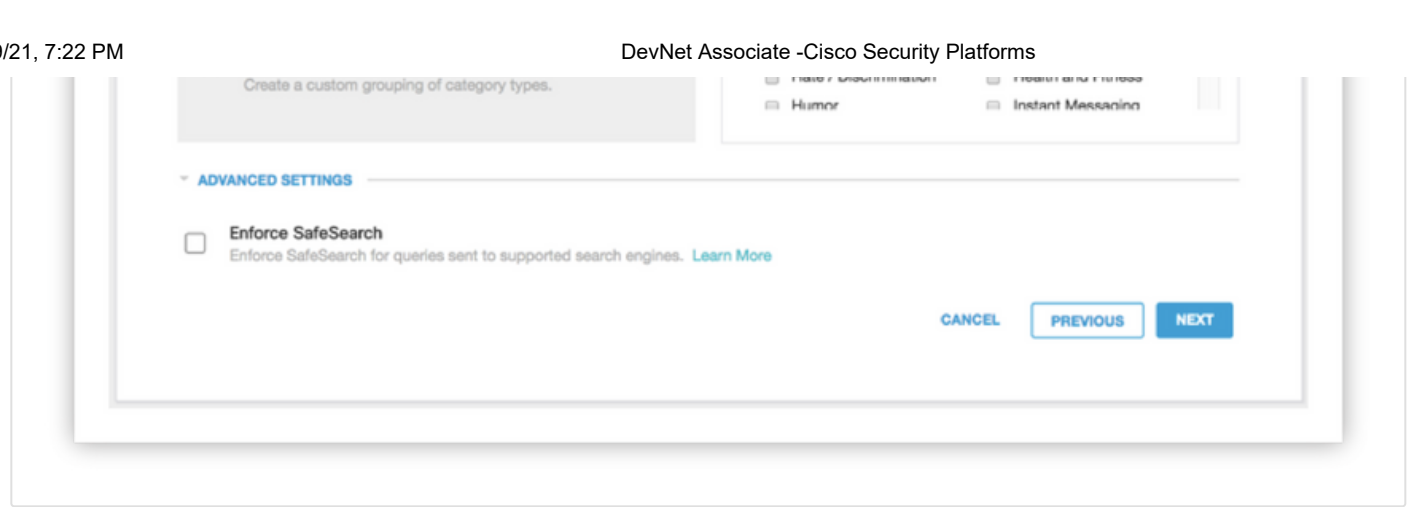
When providing guests with Wi-Fi, you must address security concerns but also legal liability protection. You also want to ensure your network cannot be infiltrated, which might enable identity theft or unwanted information access.

Application discovery and blocking

Umbrella lets you see what is being accessed, order the applications by risk elements, and then block as needed with an included automated blocking workflow. You can also have custom block lists you set up with the Umbrella user interface.

Cisco Umbrella Custom Block List





Use preset application-level reports to study a list of pre-categorized apps: Unreviewed, Under Audit, Approved, and Not Approved.

Off-network endpoint security

Umbrella can stop breaches from traffic from mobile devices not on VPN, or other endpoints not always using the VPN. It provides roaming protection for Windows, MacOS, and iOS devices outside the network security perimeter.

Web filtering and content filters

With Umbrella, you can filter content and also enable specific teams to access named sites as needed for their job role.

The Enforcement API helps create and maintain custom blocked and allowed lists. It goes through several decision points that work to update those custom lists.

- Is the domain already present on an allow list within the organization? If so, the allow list overrules any custom or Umbrella-owned block list. This override means that while a domain may be on the custom block list, no enforcement will be taken.
- Does the domain already exist in the Umbrella Security global block list under one of the security categories? Even if the domain does exist in the Umbrella global block list, it is still added to the customer's block list. You can check the status of a domain by submitting it to the Cisco Umbrella Investigate API or use the Umbrella Investigate Dashboard. If a score a score of -1 is returned, the domain is considered malicious.
- Is the domain considered benign, or safe, under Umbrella Investigate? A domain is considered safe when a score of +1 is returned from the Investigate API. Domains that are considered safe are not added to the block list. This is a fail-safe mechanism to prevent safe domains such as https://cisco.com from being blocked. Sometimes malware files contain clean domains being used to check for internet connectivity, which can trigger a false malicious positive by a Security Information and Event Management (SIEM) solution. Domains that are typically safe include ones that the Cisco security labs team has marked as safe or any domain found in the Alexa Top 1000.
- Is the status of the domain uncategorized? A domain is considered uncategorized when the Umbrella Investigate API returns a score of 0. If a domain is uncategorized, it is added to the Umbrella customer's block list.

8.6
Cisco Collaboration Platforms

8.8
Cisco Platforms and Development Summary