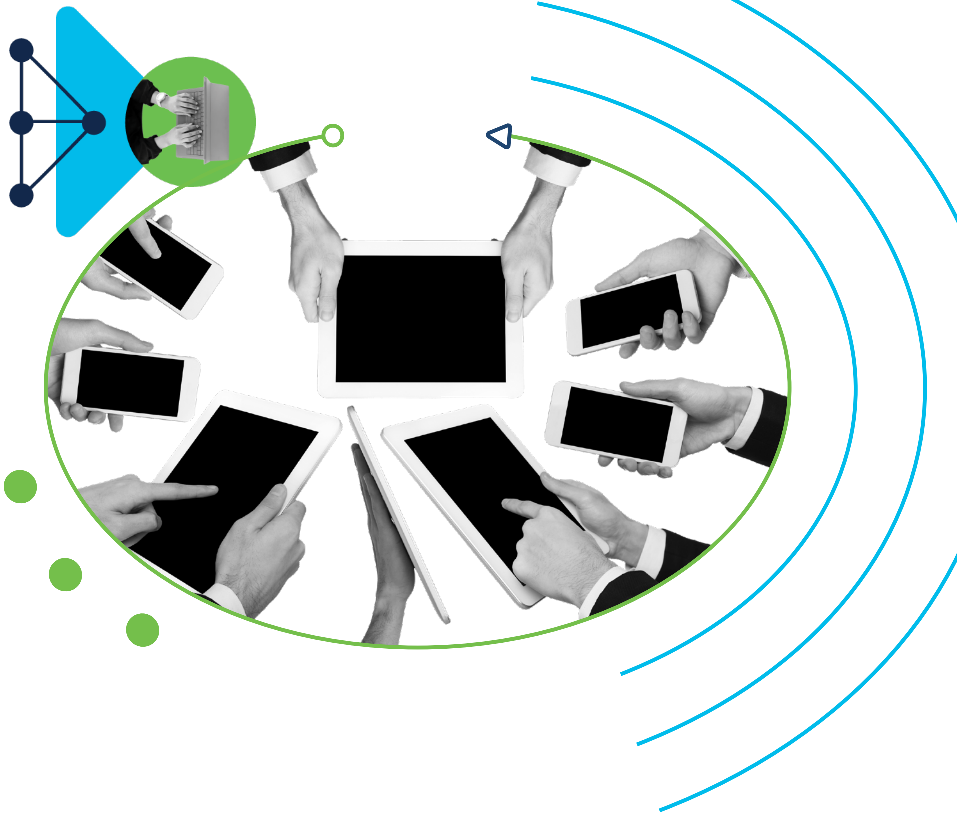
Cisco Secure Endpoint

New packages fit for every organization



Every Cisco Secure Endpoint (formerly AMP for Endpoints) package comes with Cisco SecureX built-in. It's our cloud-native platform that integrates all your security solutions into one view with the ability to orchestrate and deliver threat detection and response, meaning Secure Endpoint goes beyond EPP and EDR to give you Extended Detection and Response (XDR) capabilities. You'll be able to investigate and identify multiple files with context from multiple security products, for a deeper and wider view of what's happening. SecureX integration brings efficiency to your team for detection and response that's up to 85% faster.

Select the package that best fits your endpoint security needs.

Cisco Secure Endpoint Essentials

Replace legacy antivirus (AV) with our next-gen AV. Powered by Cisco Talos, the largest non-governmental threat intelligence in the world, we block more threats than any other security provider. See a threat once and block it everywhere – automating threat responses with one-click isolation of an infected host, while getting broader control beyond just the endpoint.

NGAV

Continuous Monitoring

Dynamic File Analysis

Behavioral Monitoring and Protection

Vulnerability Identification

Endpoint Isolation

Secure Malware Analytics

Cisco Secure Endpoint Advantage

Secure Endpoint Advantage includes all capabilities offered in the Essentials package, plus the ability to simplify security investigations with advanced endpoint detection and response (EDR), and easy access to our advanced malware analysis and threat intelligence portal –Cisco Secure Malware Analytics Cloud.

NGAV

Continuous Monitoring

Dynamic File Analysis

Behavioral Monitoring and Protection

Vulnerability Identification

Endpoint Isolation

Orbital Advanced Search

Secure Malware Analytics Cloud

Cisco Secure Endpoint Premier

Threat Hunting is now available to you through Cisco Secure Endpoint Premier. And, with SecureX Threat Hunting, you'll have elite human security experts from Cisco proactively searching for threats in your actual environment providing high-fidelity alerts with remediation recommendations.

NGAV

Continuous Monitoring

Dynamic File Analysis

Behavioral Monitoring and Protection

Vulnerability Identification

Endpoint Isolation

Orbital Advanced Search

Secure Malware Analytics Cloud

SecureX Threat Hunting

Frequently Asked Questions

What value do I get from the Essentials package?

A full legacy AV replacement, the Essentials package allows you to:

- Block known threats automatically using machine learning, exploit prevention, file reputation, antivirus, and a wide array of powerful protection engines that stop both fileless and file-based attacks.
- Use our patented technology to continuously analyze and monitor file and process activity. Automatically generate retrospective alerts at the first sign of malicious behavior.
- Identify Indicators of Compromise (IOC) at both the network and system levels, typically missed by single-purpose detection technologies.
- Stop threats from spreading with one-click isolation of an infected endpoint, without losing control of the device – shrinking the footprint of the attack.
- Leverage global threat intelligence from across Cisco's products and Services including Talos. Whether a threat originates on the Internet, in an email, or on someone else's network, our cloud-based global telemetry sees a threat once, anywhere in the world, and blocks it everywhere.

Why should I consider the Advantage package?

With the Advantage package, you get everything the Essentials package offers, plus the ability to simplify and accelerate security investigations and incident response using the following advanced EDR capabilities:

- Orbital Advanced Search allows Threat Hunters, SOC Analysts, and Incident Responders to do their jobs more efficiently by providing information about the endpoints they manage, all at their fingertips. Utilizing over a hundred specifically designed queries, security personnel can run complex queries on any or all endpoints. Advanced search provides deep visibility into what happened on any endpoint at any given time by taking a snapshot of its current state.
- Secure Malware Analytics Cloud console and API access allow security teams to perform in-depth static and advanced dynamic file analysis to identify malware quickly in a safe and secure environment.

In what ways (use cases) can I use the Orbital Advanced Search capability?

With Orbital Advanced Search, we can help you do the following important tasks better, faster:

- **Threat hunting**. Search for malicious artifacts in near real-time to accelerate your hunt for threats.
- **Incident investigation**. Get to the root cause of the incident fast, accelerating remediation.
- **IT operations**. Simply track disk space, memory, and other IT operations artifacts.
- **Vulnerability and compliance**. Quickly check the status of Operating Systems for things like versions and patch updates, ensuring your endpoints comply with current policies.

How does Orbital Advanced Search work?

Whether you are investigating an incident or hunting for threats we can help you simplify and accelerate these tedious processes in the following ways:

- **Forensics snapshots**. We can capture a snapshot of data from an endpoint such as running processes, open network ports, and a lot more at the time of detection or on-demand. You can think about it as a “freeze-framing activity” on an endpoint at the moment when something malicious was seen. This allows you to know exactly what was happening on your endpoint then.
- **Predefined and customizable queries**. We provide over a hundred predefined queries that you can quickly run as they are or easily customized as needed. These queries are simply organized in a catalog of common use cases and mapped to the MITRE ATT&CK.
- **Live search**. You can run complex queries on your endpoints for threat indicators, on-demand, or a schedule, capturing the information you need about your endpoints in near real-time.
- **Storage options**. The results of your queries can be stored in the cloud or sent to other applications such as Cisco Threat Response for further or future investigations.

What value do I get from having full access to Secure Malware Analytics Cloud?

By integrating Secure Endpoint with a Secure Malware Analytics Cloud subscription, customers gain the ability to perform a comprehensive analysis of any potential malware attempting to compromise their endpoints. The Secure Malware Analytics Cloud portal allows users to easily pivot and drill down on data elements, search for related samples and behaviors in their environment, and interact with malware in a secure way that avoids the latest malware evasion techniques. Secure Malware Analytics is powered by a globally sourced repository of malware samples and threat intelligence which offers crucial context to suspicious files that have been observed on a customer's endpoints.

Secure Malware Analytics Cloud also has the ability to enrich the other tools in your security environment leveraging premium threat feeds and an easy-to-use REST API. Users can automate sample submissions from 3rd party products and feed the resulting analysis into a variety of security and threat intelligence tools. This allows you to have a common analysis platform and gain a holistic view of all malware samples within their network. For a list of supported 3rd party integrations, view the link here.

In what ways (use cases) can I use Secure Malware Analytics Cloud?

With Secure Malware Analytics, we help you do threat analysis and investigations more efficiently:

- **Security operations**. Secure Malware Analytics provides an intuitive analysis environment that allows all types of analysts to quickly understand the details and scope of a threat using an advanced threat scoring system and behavioral indicators that are backed by advanced search capabilities across processes, file, disk, memory, network, and network artifacts and present findings in plain language. Secure Malware Analytics Cloud also provides more advanced capabilities such as detailed sample analysis reports, process execution charts, and direct user interaction with malware through its Glovebox feature.
- **Threat intelligence**. With access to a robust API to integrate sample submission, Secure Malware Analytics enriches security event and threat content, allowing customers to enhance the capabilities of their existing IT security infrastructure and to produce data feeds that can be ingested by SIEMS and other threat management tools.
- **Data enrichment**. Secure Malware Analytics leverages a robust store of analyzed malware content that is rich in historical context and fully correlated, enabling rapid development of actionable defense and IR remediation plans.
- **Drill down**. Secure Malware Analytics's depth of malware analysis and data pivoting capabilities provide reverse engineers and incident responders the context, depth of data, and malware analysis they require to be effective.

What is SecureX Threat Hunting?

SecureX Threat Hunting is an analyst-centric process, driven by Cisco Security experts, that enables organizations to uncover hidden advanced threats. Once threats are detected, customers are notified within their AMP Console, so they can begin remediation. Threat Hunting is a proactive approach to threat detection, which tells the incident responders a narrative of how an attack was spotted and how it evolved. The purpose is to discover and thwart attacks before they cause any damage. As a side-effect of leveraging regular and continuous Threat Hunting, an organization increases their knowledge of vulnerabilities and risks which further allows the hardening of their security environment.

What impact can I expect from SecureX Threat Hunting?

SecureX Threat Hunting is a feature embedded tightly inside the Cisco Secure Endpoint product and along-side all its other detection mechanisms.
As such it is designed to produce additional net new high-impact findings.

How do I get more information about these buying options?

For more information about the new Cisco Secure Endpoint packages, check our new Ordering Guide or contact your Cisco account manager.