Cisco AMP for Endpoints

New packages fit for every organization

Cisco AMP for Endpoints offers cloud-delivered Endpoint Protection and advanced Endpoint Detection and Response that stops attacks and simplifies security operations. We understand that customers have varying levels of endpoint security requirements so we are introducing new product packages so you can choose the one that best fits your organization: Cisco AMP for Endpoints Essentials and Cisco AMP for Endpoints Advantage.

Select the package that best fits your endpoint security needs.

Cisco AMP for Endpoints 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
- ✓ Vulnerability Identification
- ✓ Endpoint Isolation

Cisco AMP for Endpoints Advantage (Recommended)

The highest level of AMP for Endpoints 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 Threat Grid Cloud.

- ✓ NGAV
- ✓ Continuous Monitoring
- ✓ Dynamic File Analysis
- ✓ Behavioral Monitoring
- ✓ Vulnerability Identification
- ✓ Endpoint Isolation
- ✓ Advanced Search
- ✓ Threat Grid Cloud

Frequently Asked Questions

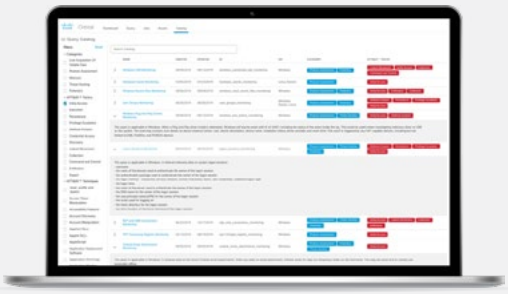
What value do I get from the Essentials package?

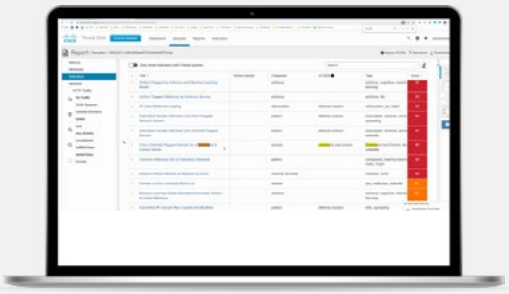
A full legacy AV replacement, the Essentials package allows you to:

- 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 indication 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 and Cisco Advanced Threat. 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:





- 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 finger-tips. Utilizing over a hundred specifically designed queries, security personnel have the ability to 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.
- Threat Grid Cloud console and API access allows security teams to perform in-depth static and advanced dynamic file analysis in order to identify malware quickly in a safe and secure environment.

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

With 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 are in compliance with current policies.

How does 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:

1. **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 at that point in time.
2. **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.
3. **Live search.** You can run complex queries on your endpoints for threat indicators, on demand or on a schedule, capturing the information you need about your endpoints in near real time.
4. **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 Threat Grid Cloud?

By integrating AMP for Endpoints with a Threat Grid Cloud subscription, customers gain the ability to perform comprehensive analysis of any potential malware attempting to compromise their endpoints. The Threat Grid 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. Threat Grid 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.

Threat Grid Cloud also the ability to enrich the other tools in your security environment through the use of 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 Threat Grid Cloud?

With Threat Grid, we help you do threat analysis and investigations more efficiently:

- **Security operations.** Threat Grid 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. Threat Grid Cloud also provides more advanced capabilities such as detailed sample analysis reports, process execution charts, and direct user interaction with malware through it's Glovebox feature.
- **Threat intelligence.** With access to a robust API to integrate sample submission, Threat Grid 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.** Threat Grid 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.** Threat Grid'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.

How do I get more information about these buying options?

- For more information about the new Cisco AMP for Endpoints packages, check our new Ordering Guide or contact your Cisco account manager.