# Cisco AMP for Endpoints – Premier

## Cisco SecureX Threat Hunting

As advanced threats continue to proliferate throughout an organizations’ IT infrastructure, threat hunting as a practice has emerged. For an elite security organization, threat hunting takes a more proactive stance to threat detection. Threat hunting was a natural, security progression saved for the most mature environments where skilled personnel leverage knowledge and tools to formulate and investigate hypotheses relating to their organization’s security across the threat landscape. With technology advancements and automation, threat hunting is now within the reach for every organization.

Threat Hunting is an analyst-centric process enabling organizations to uncover hidden advanced threats. It takes a proactive approach to security through hypothesis-driven playbooks. Threat hunting formulates hypotheses from a variety of input variables spanning the hunter’s subject matter expertise. These hypotheses are then applied to a repeatable process and run against previously collected telemetry to find signs of compromise that have evaded detection. It produces new high-fidelity incidents escalated to the security staff for further investigation and triage.

## Benefits

- **Uncover hidden threats faster across the attack surface** – Using MITRE ATT&CK™ and other industry best practices
- **Improve security posture instantly** – Adding an established threat hunting practice significantly advances your security maturation
- **Reduce alert fatigue** – Through SecureX Threat Hunting your organization receives fewer, high confidence, and high impact actionable alerts

## Why Threat Hunting is Critical

- Legacy security tools fail to stop advanced threats
- Sophisticated attackers make detection extremely difficult
- Even artificial intelligence and machine learning techniques may fall short in stopping all attacks

Atomic indicators are a level of indication that should and must be automated. The sheer volume of these alerts that overwhelm analysts regularly and provide an endless stream of busy work is best served through automation. Normally, the presence of a positive alert suggests a compromise, but it does not take into account the ingestion, validation, and time.

### Automated Methodology

Through the SecureX Threat Hunting feature, Cisco automates this process, as it is a simple, effective mechanism to introduce a level of atomic indicators to search back as intelligence is introduced. That is, it was not in the product or known about when it may have hit.

### Analytics Methodology

SecureX Threat Hunting takes and applies a level of subject matter expertise coupled with data science mechanisms to take seemingly benign or normal activity and easily identify areas that may be cause for concern. With the significant volume of telemetry points, a human analyst alone can’t go through the amount of data without the use of data science mechanisms. Not only does analytics apply a means to identifying outliers, but it also allows us to apply, at a data science level, questions to the data which we want a faster answer on a global level.

### True Threat Hunting

Threat hunting revolves around points of research and knowledge of the domain. Cisco applies subject matter expertise to backfill both the Automated and Analytics methods, and conduct contextual hunts, research possibilities, and dive deeper into problems which may have bypassed traditional means of detection.

## How to Buy

To view buying options and speak with a Cisco sales representative, visit Packages Comparison.

## Next Steps

Talk to a Cisco sales representative or channel partner about how Cisco AMP for Endpoints can help you defend your organization from advanced cyber attacks. Visit our website to learn more.