Secure Endpoint

(formerly AMP for Endpoints)

Cisco Partner
https://cs.co/1page

Cisco **Secure Endpoint** is a lightweight connector that works on your Windows, Mac, Linux, Android, and iOS devices It is a combined endpoint protection platform (EPP) and endpoint detection and response (EDR) software, providing a total endpoint protection solution.

Secure Endpoint Benefits:

- Continuously detect malware, immediately and retrospectively.
- Record file activity over time to track malware's spread and scope.
- Access global threat intelligence to strengthen network defenses.
- Gain visibility, context, and control to detect Command & Control.
- Defend against exploitation-based memory injections and ransomware.

Deployments:

- Management and analysis through an easy-to-use, web-based console.
- The solution is offered as a subscription on endpoints, including coverage for Windows, Mac, Linux, servers and mobile devices (Android and iOS).

Secure MDR for Endpoint:

- 24x7x365 analysis, and response to improve response time to threats.
- Integrated security architecture that provides greater visibility.

Secure Endpoint Packages:

	Essentials	Advantage	Premier
Antimalware	✓	✓	✓
Next-generation endpoint protection	✓	✓	✓
Application Control	✓	✓	✓
Continuous Monitoring	✓	✓	✓
Dynamic File Analysis	✓	✓	✓
Endpoint Isolation	✓	✓	✓
Device Control (USB)	✓	✓	✓
Risk-Based Vulnerability Framework (Vuln Mgmt)		✓	✓
Advanced search (Orbital)		✓	✓
Remote Scripts powered by Orbital		✓	✓
Secure Malware Analytics Cloud [1]		✓	✓
Threat Hunting by Talos			✓
Secure MDR for Endpoint		*Available*	*Available*
Support for Secure Endpoint Private Cloud	✓		

[1] **< 500** endpoints = 1 Malware Analytics Cloud account / **500+** endpoints = 3 Malware Analytics Cloud accounts

Discovery Questions:

- How do you protect endpoints when they are off the corporate network?
- How many malware infections do you deal with on a weekly basis?
- What is the average time it takes you to figure out how an attack originated, what endpoints were impacted, and what the malware did?
- Do you have a way to automatically detect malicious file behavior once that file is already on your endpoints?
- Can you identify where Malware has been and what systems were affected?
- Do you know what the threat did and what is it doing now?
- What happens to alerts after hours or on weekend?

Secure Endpoint Engines & Features:

		Windows	Mac	Linux
1:1 SHA Matching	Files	●	●	●
Machine Learning	SPERO	●	○	○
Fuzzy Fingerprint Engine	ETHOS	●	○	○
TETRA	AV Engine	●	○	○
ClamAV	AV Engine	◐	●	●
Exploit Prevention	ExPrev	●	○	○
Low Prevalence	Detection	●	●	●
Malicious Activity Protection	Detection	●	○	○
Network (Device Flow Correlation)	Feature	●	●	●
System Process Protection	SPP	●	○	○
Script Protection	Feature	●	○	○
Behavioral Protection	BP	●	○	○
Backend Detection Engines	Feature	●	●	●
Endpoint Isolation	Feature	●	●	○
Orbital Live Query	IOCs	●	●	●
Application Control	App Control	●	●	●
Device Control (USB)	Feature	●	○	○

● Available ◐ Partial ○ N/A

Resources:

SalesConnect Order Guide Data Sheet
Best Practice User Guide At-a-Glance Secure MDR
Secure Endpoint MSSP Competitive Comparison Deployment Strategy Guide Secure Endpoint Private Cloud
MSLA Program Feature Request 30-day Free Trial Public page

Example SKUs: ***AMP4E-SEC-SUB*** | ***AMP4E-EDU-SUB***