# AMP *for Endpoints*

**Advanced Malware Protection**

Cisco ***Advanced Malware Protection*** (AMP) for Endpoints is a combined endpoint protection platform (EPP) and endpoint detection and response (EDR) software, providing a total endpoint protection solution.

## 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 quickly detect, analyze, and remediate breaches.
- Agentless detection to catch malware before it compromises the OS level.
- Defend endpoints from all exploit based, memory injection attacks, including ransomware using in-memory techniques.

## Deployments:

- Managed through an easy-to-use, web-based console.
- Deployed through lightweight endpoint connector, no performance impact on users.
- Analysis is done in the cloud, not on the endpoint.
- The solution is offered as a subscription on endpoints, including coverage for Windows, Macs, Linux, servers and mobile devices (Android and iOS).

**Prevent**: Zero-day Ransomware, Fileless malware attacks, Viruses, Other known malware

**Detect**: Command & Control communications, Suspect behaviors that should be investigated further.

**Reduce Risk**: Highlight active vulnerabilities, analyze (sandbox) suspect executables, investigate web proxy traffic for suspect behaviors

## AMP *for Endpoint* Use Cases:

- **Endpoint Malware Protection**
  - Windows
  - Linux
  - Android
  - Apple
- **PCI-DSS, HIPAA & GDPR Compliance**
- **Endpoint Visibility / Isolation**
- **Blocking the latest Malware**
  - Ransomware protection
  - Fileless malware
- **Advanced Search (Orbital)**
- **Threat Hunting**

## Challenges you may face:

- 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?
- How long does it take your team to identify unknown malware?"
  *An average cost of $2,000 per machine and 1-2 days of lost productivity.*


*Regardless of Operating System – from Servers to Desktop to Mobile Devices*

**More Information:** http://cisco.com/go/amp