



# Cisco Advanced Malware Protection (AMP) for Endpoints

Scott deLelys, CISSP

Chris Ireland, CSE

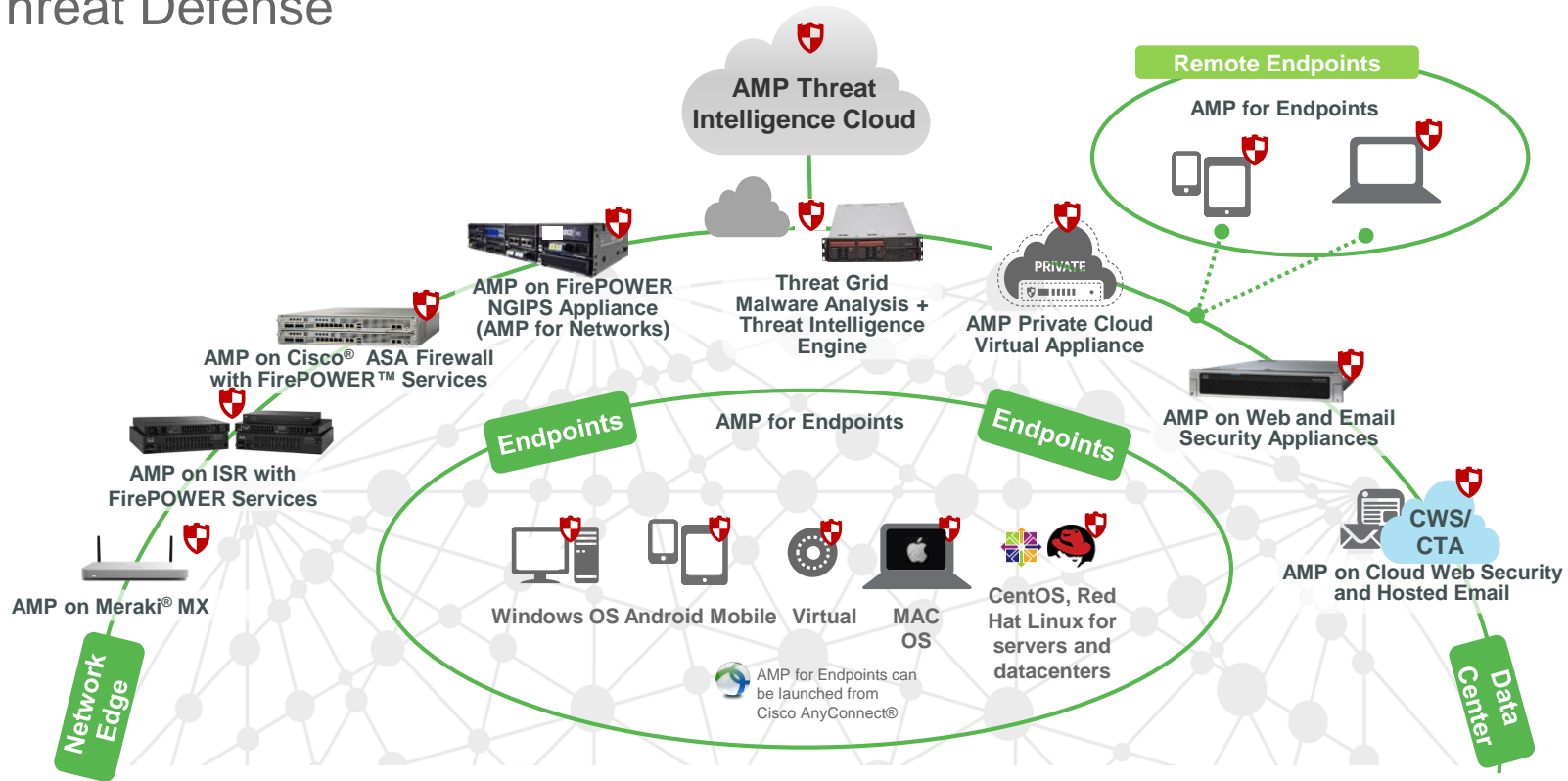
Cisco Security Business Group

Advanced Threat Solutions



# The AMP Everywhere Architecture

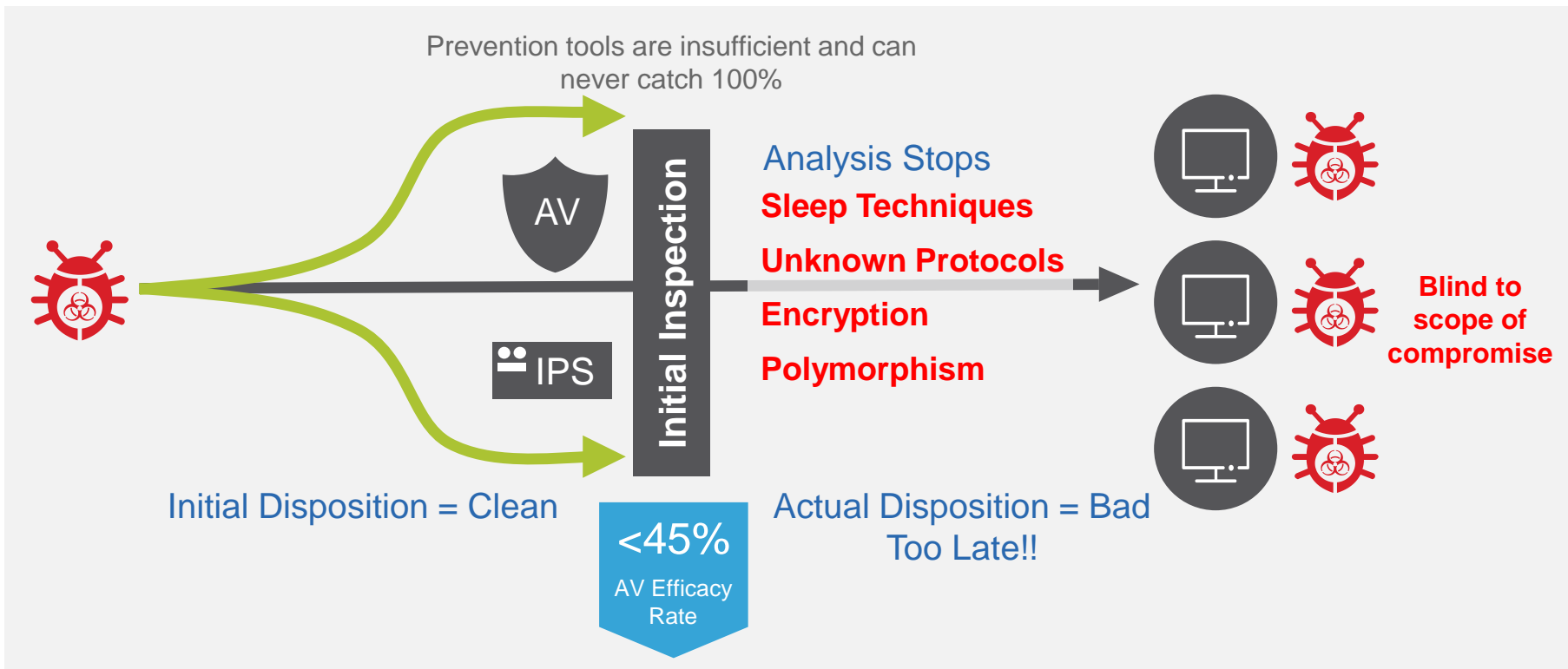
## AMP Protection Across the Extended Network for an Integrated Threat Defense



Every single attack that an organization experiences is either on an endpoint or it's headed there



# Malware is getting in. Prevention tools alone can't catch everything and provide limited visibility into threats once inside



# What Is Cisco AMP for Endpoints?



Software as a service (subscription)



Cloud managed



Lightweight connector



Protects Windows, Mac, Linux, Android and Apple iOS

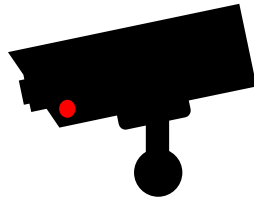


# AMP for Endpoints



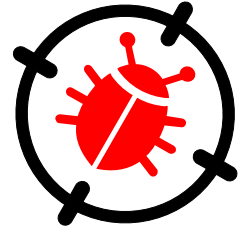
## Prevent

Prevent attacks and block malware in real time



## Monitor

Continuously monitor for threats on your endpoints to decrease time to detection



## Respond

Accelerate investigations and remediate faster and more effectively

# Harden Your Defenses with the Best Global Threat Intelligence



001 1101 1110011 0110011 101000 0110 00      1001 1101 1110011 0110011 101000 00  
 101000 0110 00 0111000 111010011 101 1100001 110 101000 0110 00 0111  
 00001110001110 1001 1101 1110011 0110011 101000 0110 00 1100001110001110

## TALOS



Cisco® AMP Threat Intelligence Cloud

Automatic updates in real time



Email

- 1.6 million global sensors
- 100 TB of data received per day
- More than 150 million deployed endpoints
- Experienced team of engineers, technicians, and researchers
- 35% worldwide email traffic



Endpoints



Web

- 16 billion web requests
- 24x7x365 operations
- 4.3 billion web blocks per day
- 40+ languages
- 1.5 million incoming malware samples per day
- AMP Community
- Private/public threat feeds



Networks

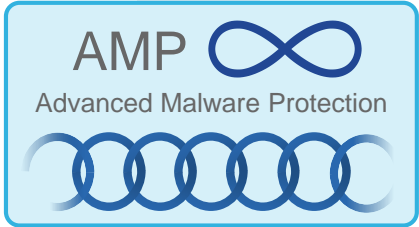


IPS

- AMP Threat Grid intelligence
- AMP Threat Grid dynamic analysis: 10 million files per month
- Advanced Microsoft and industry disclosures
- Snort and ClamAV open source communities
- AEGIS Program



Devices





# Plan A

## Prevention framework

```
##### mimikatz 2.0 alpha (x64) release "Kiv
## ^ ##
## \ ##
## / ##
## v ##
#####

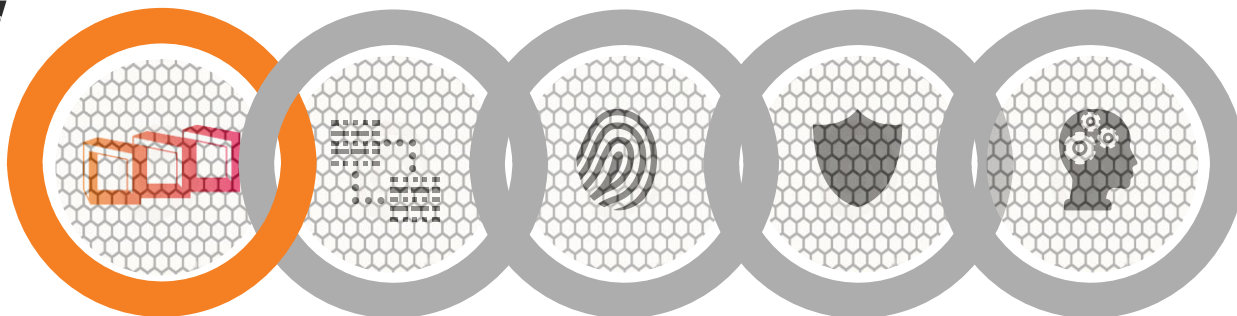
mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 : 147414 (00000000:00000000)
Session : RemoteInteractive from
User Name : administrator
Domain : ADSECLAB0
ID : S-1-5-21-186993273-13

msv :
[00000003] Primary
* Username : Administrator
* Domain : ADSECLAB0
* NTLM : 96ae239ae1f8f186a
* SHA1 : 0f3ecc3981e4bc63
[00010000] CredentialKeys
* NTLM : 96ae239ae1f8f18
* SHA1 : 0f3ecc3981e4bc6
```

Global File Reputation

Antivirus Engine



Exploit Prevention

Fuzzy Fingerprinting

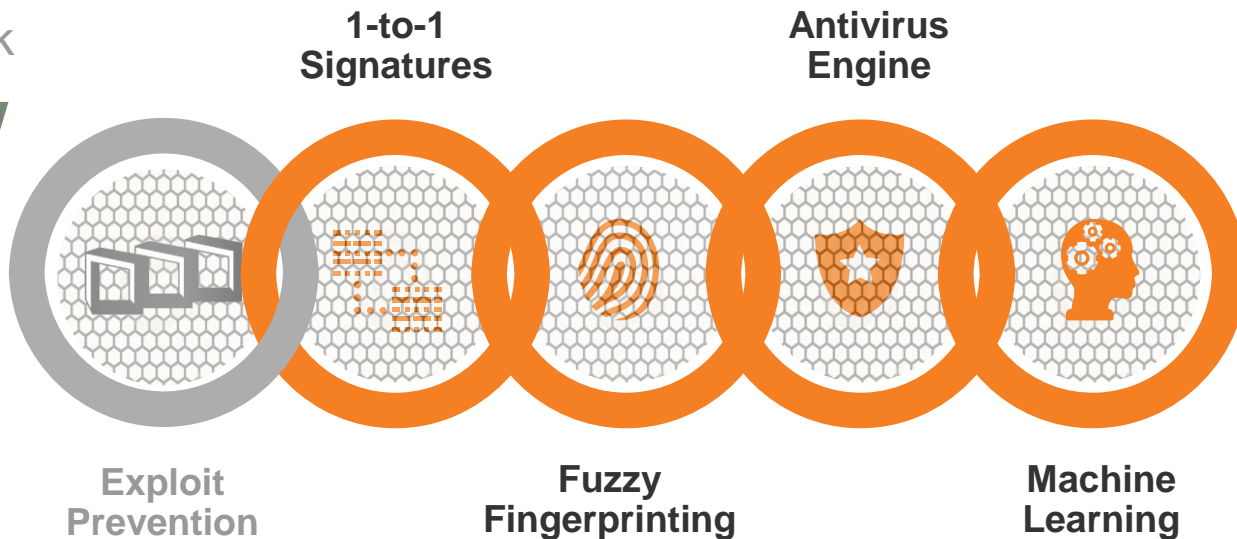
Machine Learning





# Plan A

Prevention framework



TIME TO DETECTION

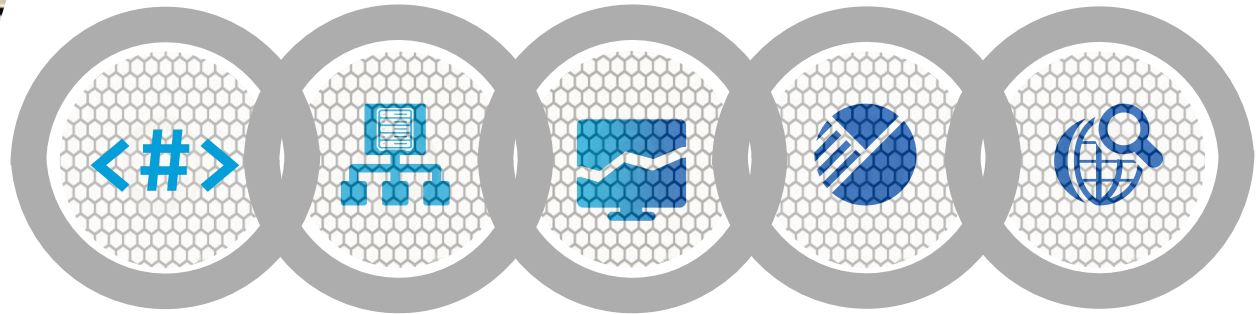
# Plan B

Detection framework



Device Flow  
Correlation

Advanced  
Analytics



Command  
Line Capture

Indicators of  
Compromise

Dynamic  
Analysis



# Proactive Protection Tools

Close attack pathways, uncover stealthy malware, and reverse-analyze suspicious threats.

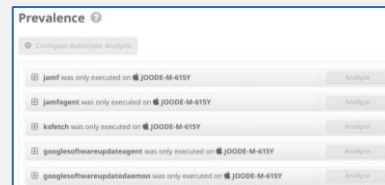
## Vulnerabilities

Our vulnerabilities feature shows you, across all of your endpoints, all the software on your system that's vulnerable to malicious attacks, so you can patch them and close any potential attack pathway.



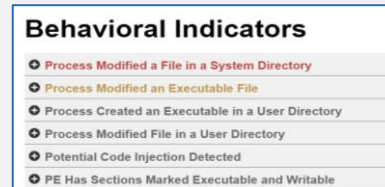
## Low Prevalence

Our low prevalence feature shows you applications on endpoints that are flying under the radar, and lets you take a closer look to see if there's any malicious behavior happening.



## Built-In Sandboxing

Built-in sandboxing capabilities powered by Threat Grid let you submit a file for analysis against over 900+ behavioral indicators so you can see what that file is trying to do and if it's bad. Then AMP will automatically block and quarantine the file.



But Prevention Alone Will  
Never Be 100% Effective

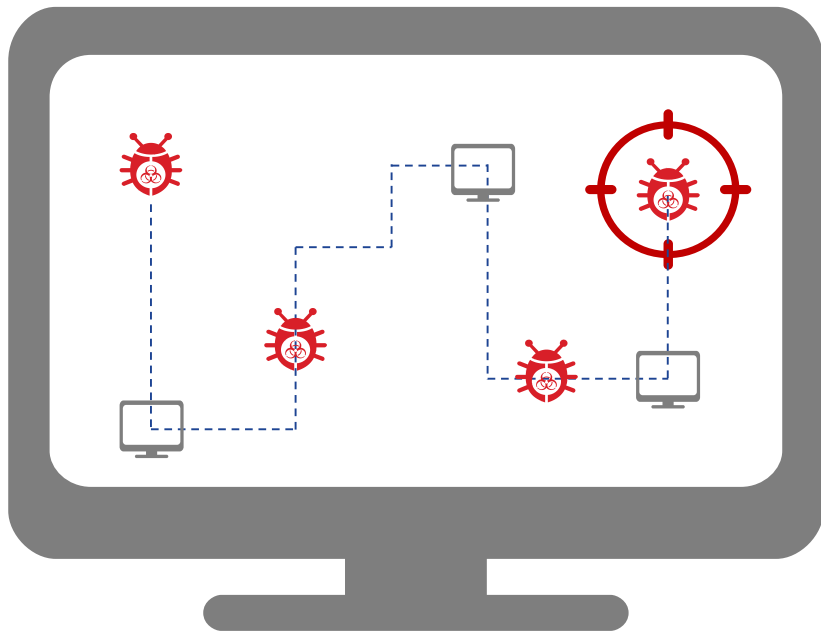
# Continuous Analysis and Retrospective Security

AMP for Endpoints Continuously Monitors, Records, and Analyzes All File Activity, Regardless of Disposition, to catch threats that got in



Monitor  
+  
Detect

● Recording



# If Something Gets in, Continuous Analysis and Retrospective Security Helps You Find Answers to the Most Pressing Security Questions



Monitor  
+  
Detect

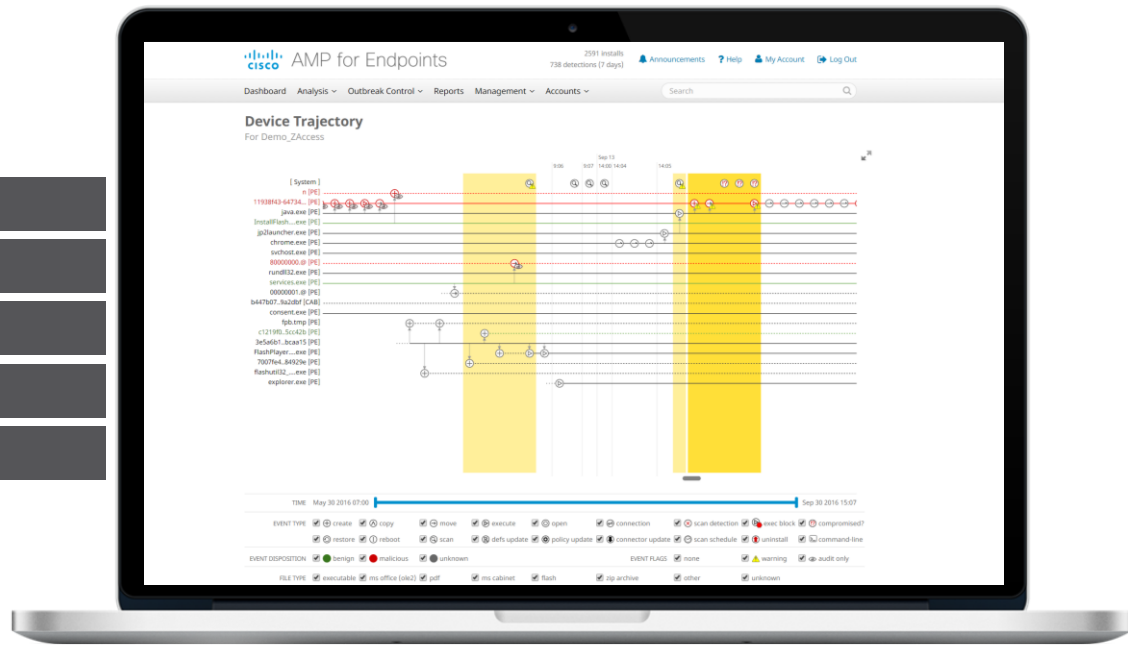
What happened?

Where did the malware come from?

Where has the malware been?

What is it doing?





How do we stop it?



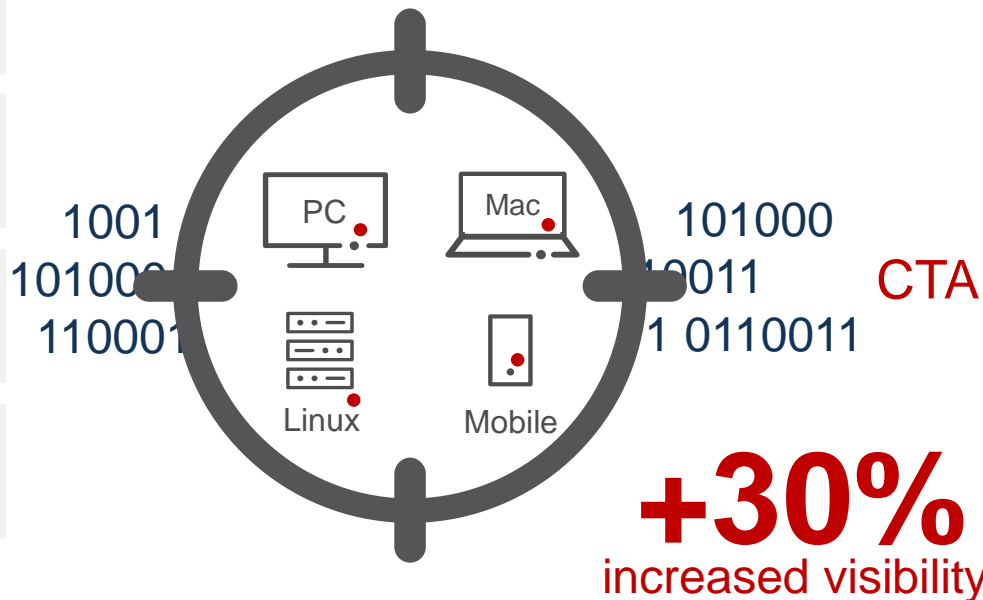
# Agentless Detection

Our Cognitive Threat Analytics (CTA) Integration Helps You See Threats on Endpoints Without an Agent Installed



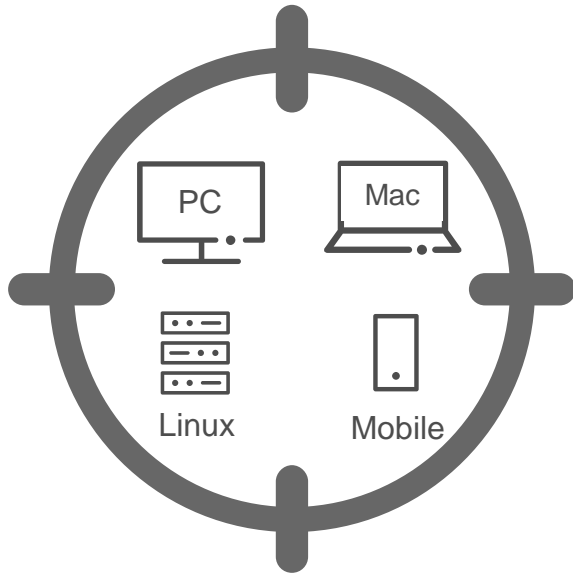
-  Get visibility into devices where you can't install an AMP for Endpoints connector
-  See more malware than before, like fileless or memory-only malware and infections that live in a web browser only
-  Catch malware before it compromises the OS level
-  Investigations are easier and faster because all detections and threat information are shown in the AMP for Endpoints console

## AMP for Endpoints



# AMP for Endpoints

in summary



- Prevention, Monitoring + Detection, Response
- Deep Visibility, Context, and Control if something gets in
- Continuous Analysis of File Behavior and Retrospective Security
- Turn on our AV detection engine in AMP for Endpoints to consolidate agents
- Containment and quarantine on endpoint
- Built-in sandbox powered by Threat Grid
- Open APIs for seamless integration
- Agentless protection via CTA
- More than just endpoint, it's the integrated security architecture of AMP Everywhere





[cisco.com/go/ampendpoint](https://cisco.com/go/ampendpoint)