Advanced threats call for Advanced Malware Protection (AMP)

Prevention alone can't protect organizations from attacks. Get deep visibility into activity on your system to quickly respond and remediate.

What you're up against

- **95%** **or more** of organizations have been targeted by malware
- **60%** of an organization's data is stolen within hours, when attacked
- **54%** of breaches remain undiscovered for months
- **55%** of organizations are unable to determine the cause of a breach
- **65%** of organizations say attacks evaded existing preventative security tools

Why prevention tools alone are not enough

Malware gets through via ever-changing tactics

Antivirus (AV) and Intrusion Prevention System (IPS) solutions have a <45% efficacy rate and provide limited to no visibility once malware gets in.

The new generation of hackers uses advanced malware—including polymorphic and environmentally aware malware—that can mask itself to evade traditional point-in-time security tools. This occurs when security tools make assumptions about what is safe and what is not, allowing malware that appears benign to get through.

AMP for Endpoints helps prevent malware from getting through, while providing protection against the threats that get in

Deep visibility
Increase visibility by 30% when using our machine learning engine

Context
Enable investigators to search historical data to correlate previous activity that may be related to a newly detected threat

Control
Quickly respond and remediate across all attack vectors to defend against today's most advanced threats

AMP for Endpoints decreases time to detection, improving response and mitigating threats

100 DAYS TO **6 HOURS** (or less)

Industry average time to detection

Cisco security time to detection

Full scope and history of an attack
Trajectory views show where it came from, where it's been and what it's doing

Investigation and threat hunting
Accelerate investigations and reduce management complexity by easily searching across all endpoints for Indicators of compromise (IoCs)

Contain and remediate
Surgical containment and remediation across PC, Mac, Linux, Android and iOS

Proven continuous analysis and retrospective Security

AMP for Endpoints continuously monitors, records, and analyzes all file activity, regardless of disposition, to catch threats that get in.

IDC Analyze the Future

AMP for Endpoints named a Leader by IDC for Specialized Threat Analysis and Protection due to it being one of the most robust, comprehensive security management consoles.

NSS LABS

AMP for Endpoints named the leader by NSS Labs in security effectiveness and fastest time to detection for three years in a row (2014-16) in a comparative test of breach detection systems.

Reduce costs
through flexible integration with multiple Cisco security and network infrastructure products.

Optimize your current investments
by easily integrating AMP Threat Grid (dynamic malware analysis and threat intelligence in a single solution) with your existing AMP infrastructure.

Cisco AMP for Endpoints provides full lifecycle breach prevention, detection, response, and remediation for the real world.

Call us today to schedule a meeting and learn more how Cisco AMP for Endpoints can protect your business