Prevent Cybercrime with Cisco Advanced Malware Protection (AMP) for Endpoints

Defend your organization with the power of retrospective security

With polymorphic malware evading **more than 75%** of all current antivirus engines, businesses need a sophisticated approach to protecting their network and digital assets.[1]

Companies that still rely on outdated endpoint security measures don't stand a chance against polymorphic malware. They evade detection by morphing any identifying characteristics, such as types of files, file names and encryption keys, to trick pattern-matching detection antivirus software. Hackers can develop polymorphic malware as a virus, worm, bot, Trojan or keylogger, which makes them their tool of choice today.

Cybercriminals now take an entrepreneurial—even professional—approach to their work. With funding from organized crime and rogue nations, hackers have abundant resources that enable them to unleash mechanized, multifaceted attacks on the networks of businesses, organizations and governments, and at their time and choosing.

The accelerated development of cybercrime will force organizations to change.

Using what had until recently been considered endpoint security best practices no longer enables businesses to cope with current and future malware techniques. As hackers continue to evolve, they will devise malware with increasingly sophisticated masking abilities that evade traditional security tools.

While it may appear that hackers now have the upper hand, Cisco Advanced Malware Protection (AMP) for Endpoints using retrospective security empowers organizations to prevent, detect and respond to these new forms of cyberattacks.

On the following pages, you'll see how and why organizations are protecting their endpoints and digital assets with Cisco AMP for Endpoints.

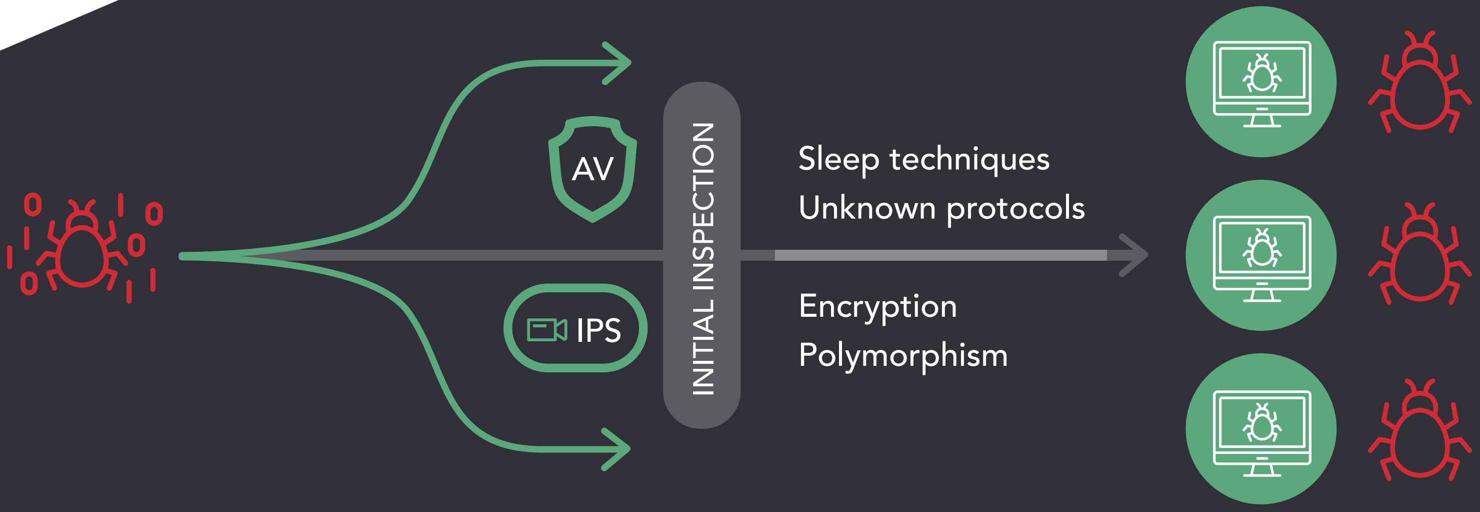
The changing face of cybercriminals

In the past, hackers could rely on brute force rather than elegant coding. That's changed. Today hackers are smarter, faster and more efficient at developing new forms of malware. We've reached the stage where less than 25 percent of current antivirus engines can detect these more advanced attacks—the type of which hackers now favor.

By using techniques such as polymorphic and environmentally aware malware, which masks itself to evade point-in-time security tools, hackers have created a way to fool traditional AV and IPS solutions into letting malware into their network. Through taking advantage of flaws in traditional security tools that make incorrect assumptions about what files are safe and what are not, hackers have found an effective way to get their malware through.

Malware gets through via ever changing tactics

The illustration below shows how current strains of malware get past most Antivirus (AV) and Intrusion Prevention System (IPS) solutions.



KNOW THE DIFFERENCE BETWEEN POINT-IN-TIME AND RETROSPECTIVE SECURITY TOOLS. **SEE NEXT PAGE.**

Point-in-Time security fails to address current malware technology

Malware today is not static. It's dynamic and can now be viewed as something three dimensional, because advanced malware no longer exists on a two dimensional plane where it can easily be detected. If malware protection does not take a similarly dynamic approach to security, then it cannot hope to be effective.

Point-in-Time vs. Retrospective Security

Point-in-Time Security Tools

examine files only at the point of entry. If the file appears to be safe, based on what the tool is looking for, the file is allowed to cross into the network. The problem is that the security tool is only as good as the information it has, and hackers have learned how to develop malware that appears safe.

Retrospective Security Tools

examine files not just the point of entry, but monitor them across the entire attack continuum—recording information before an attack as well as running continuous analysis and advanced analytics during and after an event.

WHY IS RETROSPECTIVE SECURITY BETTER ABLE TO DEFEND AGAINST ADVANCED MALWARE ATTACKS? **SEE NEXT PAGE**.

Look back for a leap forward in security

Retrospective security enables IT to look at their systems at any point in the past. Through a host of tools including retrospection, attack chain correlation, behavioral indications of compromise (IOCs), trajectory and breach hunting, IT can see exactly how their network has changed as opposed to viewing it without context and as a single point in time in history.

The increased visibility from retrospective security enables IT to:

- Methodically analyze what occurred during a breach
- Learn how the system was entered and what data was accessed
- Understand how to prevent future attacks

In the event of a breach, retrospective security can save a significant amount of money

Organizations using point-in-time security tools must hire independent security consultants to do the forensic detective work. If the same organization had retrospective security tools in place, such as Cisco AMP for Endpoints, their IT administrators would have had all of the information needed to investigate the breech on their own andformulate a remediation plan to address the problem.

By deploying an advanced malware solution with retrospective security, organizations can allocate more of their resources to profitable activities rather than paying for the increased costs of cybercrime remediation.

Companies using Cisco AMP for Endpoints also benefit by:

- Gaining access to real-time threat intelligence and big data analytics, compiled by the Cisco Talos Security Intelligence and Research Group
- Using this intelligence to make better decisions or to automatically take security actions
- Moving from a reactive to a proactive security stance

LEARN WHAT SECURITY AND BUSINESS BENEFITS YOU CAN GAIN THROUGH CISCO AMP FOR ENDPOINTS. **SEE NEXT PAGE**.

Cisco AMP for Endpoints offers security and business benefits

Organizations have boosted their endpoint protection and saved money by:

6 HOURS

Reducing time to detection from an industry average of 100 days to 6 hours or less with 98% detected in three minutes or less [2]

Adding context through historical data searches to correlate prior activity, which may be associated with a newly detected threat

Increasing visibility by 30% when using our machine learning engine

Reducing costs by integrating with multiple Cisco security and network infrastructure products as well as by enabling IT to perform tasks normally handled by independent security consultants

Enabling control to rapidly respond and remediate against the most advanced threats and across all attack vectors

Providing broad endpoint coverage across Windows, Mac OS, Android, and Linux operating systems

Results such as these demonstrate why organizations are choosing Cisco AMP for Endpoints over other security options.

WHAT DO THE EXPERTS SAY ABOUT CISCO AMP FOR ENDPOINTS? **SEE NEXT PAGE**.

The freshest intelligence delivers enhanced security

The Cisco Talos Security Intelligence and Research Group compiles the industry's leading collection of real-time threat intelligence and big data analytics. This data is pushed from the cloud to the AMP client, providing the latest threat intelligence to proactively defend against threats.

- **1.5 million incoming malware samples per day**
- **1.6 million global sensors**
- **100 TB of data per day**
- **13 billion web requests**
- **A global team of engineers, technicians, and researchers**
- **24-hour operations**

AMP correlates files, behavior, telemetry data, and activity against this robust, context-rich knowledge base to quickly detect malware. Security teams benefit from AMP's automated analysis by saving time and gaining the latest threat intelligence to quicklyunderstand, prioritize, and block sophisticated attacks.

The integration of our Threat Grid technology into AMP also provides:

- Highly accurate and context-rich intelligence feeds delivered in standard formats to integrate smoothly with existing security technologies
- Analysis of millions of samples every month, against more than 700 behavioral indicators, resulting in billions of artifacts
- An easy-to-understand threat score to help security teams prioritize threats

AMP uses this intelligence and analysis to inform your security decision making or automatically take action on your behalf. For instance, the system can block known malware and policy-violating file types, dynamically blacklist connections that are known to be malicious, and block attempts to download files from websites and domains categorized as malicious.

Industry analysts see high value in Cisco AMP for Endpoints

NSS LABS

"Based on our (Breach Detection Systems) reports, Advanced Malware Protection from Cisco should be on everyone's short list."

ESG

"… do any network security vendors understand data center and what's needed to accommodate network security? Cisco certainly does."

HARVEST

"Cisco is disrupting the advanced threat defense industry."

Gartner®

2016 Vendor Rating for Security: Positive.

FORRESTER®

"… AMP will be one of the most beneficial aspects of the [Sourcefire®] acquisition."

IDC Analyze the Future

"The AMP products will provide deeper capability to Cisco's role in providing secure services for the Internet of Everything (IoE)."

HOW DOES CISCO AMP FOR ENDPOINTS COMPARE WITH COMPETING SECURITY PRODUCTS? **SEE NEXT PAGE**.

A closer look at IDC MarketScape 2017

In their MarketScape 2017 vendor assessment for worldwide endpoint specialized threat analysis and protection, IDC says the following about Cisco AMP for Endpoints.

"Cisco has created one of the most robust comprehensive management consoles to support organizations with the wherewithal to support dedicated incident responders and active threat hunters. It provides investigators with rich, contextual information and the ability to conduct"retrospection," a search through historical data to correlate previous activity that may be related to a newly detected threat. The console can be configured to an investigator's preferences and has embedded workflow capabilities to track an investigation through to its conclusion."

"Cisco provides one of the most comprehensive and, more importantly, cohesive set of offerings to identify and block attacker activity and advanced malware across endpoint, web, messaging, and network-level avenues of attack. If properly deployed, tuned, and proactively managed and maintained, the solution should significantly improve a large enterprise's security posture."

"Cisco maintains one of the largest and highly skilled base of sales channel partners in the security industry. It invests heavily in its channel program to provide training to educatepartners about the technology behind its products. Many partners provide both managed and professional services and can assist customers with deploying and configuring AMP for Endpoints."[3]

FIND OUT HOW TO GET FIRST-HAND INFORMATION ABOUT DEPLOYING CISCO AMP FOR ENDPOINTS. **SEE NEXT PAGE**.

Learn more

Call us today to schedule a meeting, and we'll answer your questions.

[1] https://themerkle.com/emotet-banking-trojan-outsmarts-75-of-all-antivirus-software/
[2] 2016 Cisco Midyear Security Report - https://www.cisco.com/c/dam/m/en_ca/never-better/assets/files/midyear-security-report-2016.pdf
[3] https://www.cisco.com/c/dam/en/us/products/collateral/security/fireamp-endpoints/idc-marketscape-threat.pdf