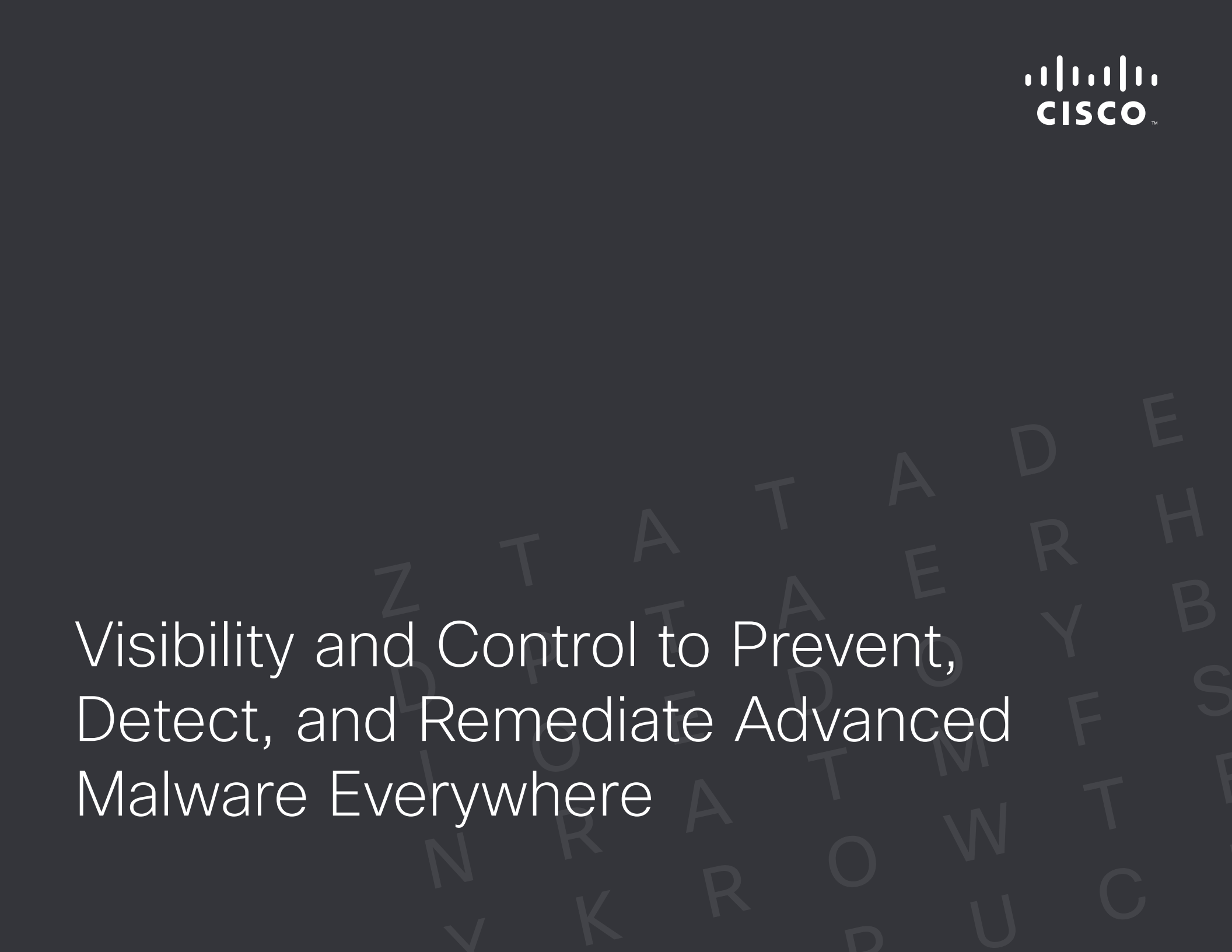

Visibility and Control to Prevent, Detect, and Remediate Advanced Malware Everywhere

What You Will Learn

Fighting malware today requires more than point-in-time security tools alone. It takes only one threat to evade detection and compromise your environment. Furthermore, point-in-time detection provides no insight into the scope of a breach after it has happened, leaving you blind and unsure of how to respond and contain the threat.

Cisco® Advanced Malware Protection (AMP) is different. This integrated solution provides:

- Global threat intelligence to strengthen network defenses
- Advanced analysis engines to block malicious files in real time
- The ability to continuously analyze file behavior and traffic in order to uncover threats faster

These capabilities provide visibility into potential threat activity and the control to rapidly contain and remediate malware. You get integrated protection before, during and after an attack across the extended network.

It's A Jungle Out There

Cybercrime is pervasive, hackers are organized, and malware is sophisticated, stealthy, and fast

Hacking is an industry powered by a community of professional, entrepreneurial, and resourceful cybercriminals. They share techniques, are well-funded, and work together to accomplish their objectives. Persistent and relentless, they launch mechanized, multifaceted attacks through multiple attack vectors against specific organizations.

This fast, effective, and efficient criminal economy uses a variety of systematic techniques that incorporate advanced malware. Such malware, including polymorphic and environmentally aware malware, is very good at masking itself and evading traditional security tools, which can lead to a breach.

> The question is no longer *if* you will be breached; the question is *when*.

So the question is no longer *if* you will be breached; the question is *when*. Just look at the numbers: 95 percent of organizations have been targeted by malware.[1] When attacked, 60 percent of an organization's data is stolen within hours; 54 percent of breaches remain undiscovered for months; and 55 percent of organizations are unable to even determine the source of the breach.[2] The longer malware is left undiscovered, the more damage it causes: the average cost of a breach in 2014 was $5.9 million, and that number continues to rise.[3]

If it isn't obvious by now, defenses against advanced malware are failing

If 54 percent of breaches remain undiscovered for months, and 55 percent of organizations are unable to even determine the cause of a breach, then the IT security tools being used are clearly no match for today's threats.

What's going on?

> **54** percent of breaches remain undiscovered for months.

Many organizations deploy only antivirus tools, traditional firewalls, and legacy intrusion prevention systems (IPS) to defend themselves. These point-in-time security tools scan a file at the point of entry into the extended network. They check the file's reputation against a list of known malicious files. If a known "bad" file is found, it's blocked. If a file's disposition is deemed "good" or "unknown," it is allowed entry into the network.

Unfortunately, that's where the analysis stops and where organizations get into trouble.

Based on what we know about advanced malware, what's deemed to be "good" or "unknown" could very well be malicious, and point-in-time tools might not know it. Perhaps there is no signature or threat intelligence to indicate that the file is bad, or maybe the advanced malware is so effective at masking itself as "good" that it evades detection. Even if a sandbox is deployed, advanced malware can use sleep techniques or polymorphism to evade it. Once the malware gets into the network, point-in-time tools provide limited or no visibility into the activity of threats after initial inspection. This leaves IT security professionals blind, with no way to continue to monitor these files and take action if the files exhibit malicious behavior later on.

1. 2014 Cisco Annual Security Report
2. 2014: A Year of Mega Breaches, Ponemon Institute.
3. Cost of a Data Breach, 2013/2014, Ponemon Institute.

Throwing multiple, disparate security tools at the problem just slows you down

Despite the insufficiency of point-in-time tools, organizations seem to keep throwing more and more of them at the problem. Caught in a cycle of layering on the latest security tool, it isn't unusual to find organizations with 40 to 60 different security products that don't–and can't–work together.

Disparate products cannot always communicate with each other. This means less sharing of information before, during, and after an attack, which slows down your ability to uncover threats. Instead of correlating information and prioritizing threat events to help your security teams identify the high-risk threats that are important, these disparate tools are firing off hundreds of siloed or duplicate alerts each day, which only creates more noise and unnecessary work for your security teams. Security tools should work together to help you make smarter security decisions and cut through the noise, not add to it.

Furthermore, multiple products mean multiple vendor relationships and multiple management systems for your IT security team to juggle. This results in a longer time to detect threats, increased capital and operating costs, and more administrative complexity. In the end, this disjointed approach doesn't provide you with the visibility, control, or manageability you need to quickly detect and eliminate threats before damage is done.

Detecting malware and the targeted, persistent attacks they represent is a bigger problem than traditional defenses or a set of fragmented solutions can address. Organizations need to approach the security problem in a completely different way. Advanced malware protection must be as pervasive as the malware it is designed to combat.

Advanced Attacks Require An Integrated, Advanced Security Approach

Prevent what you can

So how should you approach the problem? Start by preventing what you can. Expand your base of threat intelligence to strengthen your network's defenses so that you can block more known malicious files. Take care of the majority of nuisance malware that attacks your organization. Optimize how detection tools work to increase their performance and find threats more quickly. Despite the limitations of point-in-time detection, it maintains an important role in eliminating a large majority of potential threats.

But also face reality: relying on a prevention strategy alone will ultimately fail. No detection method is 100 percent effective as attackers continue to innovate to evade your front-line defenses. Something will get in.

The need for speed: Quickly detect, respond, and remediate

60 percent of an organization's data is stolen within hours of an attack.

Come to terms with the reality that something will get in. Malware is sophisticated, hackers are smart, and an attack can and will evade initial detection and other preventive measures. Once something gets in, it's now a matter of reducing the time to detection (TTD) and time to remediation (TTR). Malware acts fast, and your sensitive data and critical systems are on the line. Within hours of a breach, 60 percent of data is stolen. The longer malware is left in your environment unchecked, the more damage will be done. So it is essential that you not only detect, contain, and remediate malware in your environment, but also do so extremely rapidly.

However, we know that most organizations struggle to get visibility into the threats in their environment. If you can't see advanced threats, how can you even detect and remediate them? How can you avoid becoming tomorrow's headline news?

You need visibility and control everywhere and all the time

You need to go beyond what point-in-time tools can provide. You need to achieve visibility and control, quickly and efficiently: visibility to see what is happening within your IT environment, and control to stop malicious actors when you find them. But that can't be accomplished in a one-time approach. You need visibility and control everywhere and all the time: across all attack vectors (endpoint, mobile, web, email, network) and across the full attack continuum (before, during, and even after an attack).

You gain this ability by gathering and analyzing telemetry data continuously, going beyond signatures to identify known attacks, and looking at file behavior to expose indicators of compromise that would otherwise go unnoticed. Local data needs to be woven together with global intelligence for more meaningful insights into the nature of attacks. Information needs to be shared across the environment and multiple control points to speed detection and response before a high-level breach can materialize. Endpoints need to talk to the network device, which needs to talk to the firewall, and so forth. For example, suspected malware observed on an endpoint could be automatically inspected or blocked by network sensors. If one tool sees something, everything else should see it too.

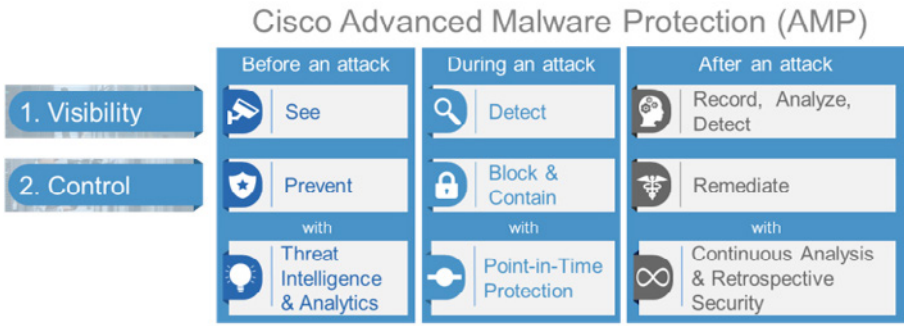
Once you can see how files are behaving and what they are doing, then you can identify them as malicious even after an attack. Then you need technology that allows you to rapidly contain the files and remediate them. This response can include a variety of activities, including identifying the root cause of the attack, prioritizing events by scope and severity to stop real threats sooner, and shutting down all points of compromise and infection gateways simultaneously to prevent lateral movement of the attacker. All this needs to be done extremely quickly in order to mitigate damage.

Having this visibility and control everywhere and at all times is essential to establishing a more systemic and integrated approach to threat defense so you can more effectively and efficiently protect your organization.

Have You Met Cisco Advanced Malware Protection?

Cisco Advanced Malware Protection (AMP) delivers the integrated, advanced security approach that you need. Cisco AMP is a technology that gives you the visibility and control to not only prevent breaches and block known and emerging threats, *but also* to quickly detect, contain, and remediate malware that has penetrated the extended network from a wide range of attack vectors. (See Figure 1.)

Figure 1. Continuous Visibility and Control



Protect your organization across the full attack continuum

BEFORE: Cisco AMP strengthens defenses before an attack using the best **threat intelligence and advanced analytics**. With a vast library of intelligence, known malicious files, and known behaviors, you can identify more threats when you see them, enhance defenses, and make better security decisions.

Cisco AMP is built on unmatched threat intelligence collected from Cisco's Security Intelligence organization, Talos Security Intelligence and Research Group, and Threat Grid intelligence feeds. Cisco monitors 35 percent of worldwide email traffic, scans 100 terabytes of data and 1.1 million malware samples per day, and has a group of threat analysts and researchers working around the clock to provide AMP with the latest threat intelligence. Cisco AMP correlates files, behavior, telemetry data, and activity against this robust, context-rich knowledge base to quickly detect malware and help you understand, prioritize, and block sophisticated attacks when they occur.

DURING: Cisco AMP combines this intelligence with proven detection techniques to take **point-in-time protection** tools to the next level. File reputation, one-to-one signatures, fuzzy fingerprinting, and static and dynamic analysis using sandboxing technology are all built into Cisco AMP as a first line of defense. This allows the organization to automatically block as many known and emerging threats as possible before they manage to infiltrate the network. With a constant feed of new threat intelligence, 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.

But no point-in-time detection method alone will ever catch 100 percent of malware. While point-in-time detection is essential, modern security solutions need more. Cisco AMP goes beyond point-in-time to allow you to quickly detect, contain, and remediate even the most elusive malware if it manages to slip by your front-line defenses.

AFTER: Unlike any other technology available today, Cisco AMP provides **continuous analysis and retrospective security** to help you detect malware even after it slips into the extended network. After a file traverses the security control point and is inspected by point-in-time engines, deemed "good" or "unknown", and allowed into the network, AMP continues to watch it, scrutinizing its every move throughout your environment.

The AMP system continuously monitors, analyzes, and records all file activity and communications on endpoints, mobile devices, and in the network in order to quickly uncover stealthy threats that exhibit suspicious behavior. At the first sign of trouble, AMP will retrospectively alert security teams and provide detailed information on the behavior of the threat–how the event occurred, where the malware came from, where the malware has been throughout your network, and what the malware is trying to do. Most importantly, AMP then gives you the ability to stop it. You can categorize the file as "bad" based on the evidence collected and analyzed, and surgically remediate it.

This capability, unique to Cisco AMP, is called **retrospective security**. It's the ability to record the activity of every file in the system and, if a supposedly "good" file turns "bad", the ability to rewind the recorded history to see the origin of the threat and the behavior it exhibited over time. Then, AMP lets you take action with built-in response capabilities. AMP also remembers what it sees, from the threat's signature to the behavior of the file, and logs the data in AMP's threat intelligence database to further strengthen front-line defenses. This file and files like it will not be able to evade initial detection again.

AMP is everywhere, integrated, and connected

Visibility and control like this, from beginning to end, is exactly what you need to quickly uncover stealthy malware and eliminate it. But you also need coverage and visibility across a broad range of attack vectors and the ability to share information across your security infrastructure for thorough and quick action.

Cisco Advanced Malware Protection is "everywhere" now. You can deploy the AMP technology across your entire security infrastructure or at certain strategic control points to meet your specific security needs. From the endpoint to the network, mobile devices, and virtual environments, there are multiple ways to consume the technology. (See Table 1.)

What's important to note here is the interconnectivity, communication, and integration among all these solutions. These are not point products that live in a vacuum. When deployed together, the solutions work together to provide an integrated defense that systematically and rapidly responds to threats. An ecosystem is created whereby the AMP solutions automatically share threat intelligence, indications of compromise, event information, and quarantine information across all the deployments. With AMP "eyes everywhere," organizations can drastically reduce TTD and TTR.

Table 1. Deployment Options

Solution	Deployment
AMP for Endpoints	Protect PCs running Windows, Macs, Android mobile devices, Linux, and virtual environments using AMP's lightweight connector, with no performance impact on users.
AMP for Networks	Deploy AMP as a network-based solution integrated into Cisco FirePOWER™ NGIPS security appliances.
AMP on ASA with FirePOWER Services	Deploy AMP capabilities integrated into the Cisco ASA firewall.
AMP Private Cloud Virtual Appliance	Deploy as an on-premises, air-gapped solution built specifically for organizations with high-privacy requirements that restrict using a public cloud for disposition lookups.
AMP on Email Security Appliance (ESA), Web Security Appliance (WSA), and Cloud Web Security (CWS)	For Cisco Cloud Web Security (CWS), Email Security Appliance (ESA), or Web Security Appliance (WSA), Advanced Malware Protection capabilities can be turned on to provide retrospective capabilities and malware analysis.
AMP Threat Grid	AMP Threat Grid is a standalone malware analysis and threat intelligence product that can be deployed in the cloud or as an on-premises appliance. Threat Grid threat intelligence and advanced malware analysis capabilities are built into the other AMP deployments in varying capacities.

Conclusion

To effectively protect against today's advanced threats, you need a solution that covers multiple attack vectors, shares information, reduces complexity, increases ease of use for management, and ultimately, provides your organization with the deep visibility and control you need to not only prevent breaches, but in the case that malware gets in, the ability to quickly detect, contain, and remediate it. Cisco Advanced Malware Protection provides this, allowing you to protect your organization before, during, and after an attack.

For More Information

To learn more about Cisco Advanced Malware Protection and how it can help your organization, watch this short overview video, see a concise or detailed demonstration of the technology, hear from customers, see how AMP stacks up against the competition, or reach out to your Cisco sales representative to set up a POV with a Cisco AMP specialist.

C11-735641-00 08/15