White Paper

Buyer's Criteria for Advanced Malware Protection

What You Will Learn

This document will identify the essential capabilities you should seek in an advanced malware protection solution, the key questions you should ask your advanced malware protection vendor, and shows you how Cisco combats today's advanced malware attacks using a combination of four techniques:

- Big data analytics
- Collective global security intelligence
- Enforcement across multiple form factors (networks, endpoints, mobile devices, secure gateways, and virtual systems)
- Continuous analysis and retrospective security

Introduction

It's no secret that today's attackers have the resources, expertise, and persistence to compromise any organization if given enough time. Traditional defenses, including firewalls and endpoint anti-virus, no longer work against these attacks. The process of handling malware must evolve—and quickly at that. Detecting targeted, persistent malware attacks is a bigger problem than a single point-in-time control or product can effectively address on its own. Advanced malware protection requires an integrated set of controls and a continuous process to detect, confirm, track, analyze, and remediate these threats—before, during, and after an attack.

QUESTIONS TO ASK YOUR ADVANCED MALWARE PROTECTION VENDOR

- How are you using big data for persistent malware determination?
- How is malware analyzed to determine exactly what it does?
- How does your malware analysis automatically update detection capabilities?
- How do you gather intelligence on emerging malware threats?
- How do you perform continuous analysis for retrospective malware detection?

The problem will get worse before it gets better. With the rise of polymorphic malware, organizations face tens of thousands of new malware samples per hour, and attackers can rely on fairly simple malware tools to compromise a device. The blacklist approach of matching a file to known malware signatures no longer scales to keep pace, and newer detection techniques such as sandboxing fall short of 100 percent efficacy.

Big Data Analytics and Collective Intelligence

In an attempt to better serve customers in the wake of the exponential rise in known malware, traditional endpoint-protection vendors introduced a "cloud-assisted antivirus" capability that essentially moved the signature databases to the cloud. This addressed the issue of needing to distribute billions of virus signatures to each endpoint every five minutes, but it didn't address the evolution of advanced malware designed to evade signature-based detection.

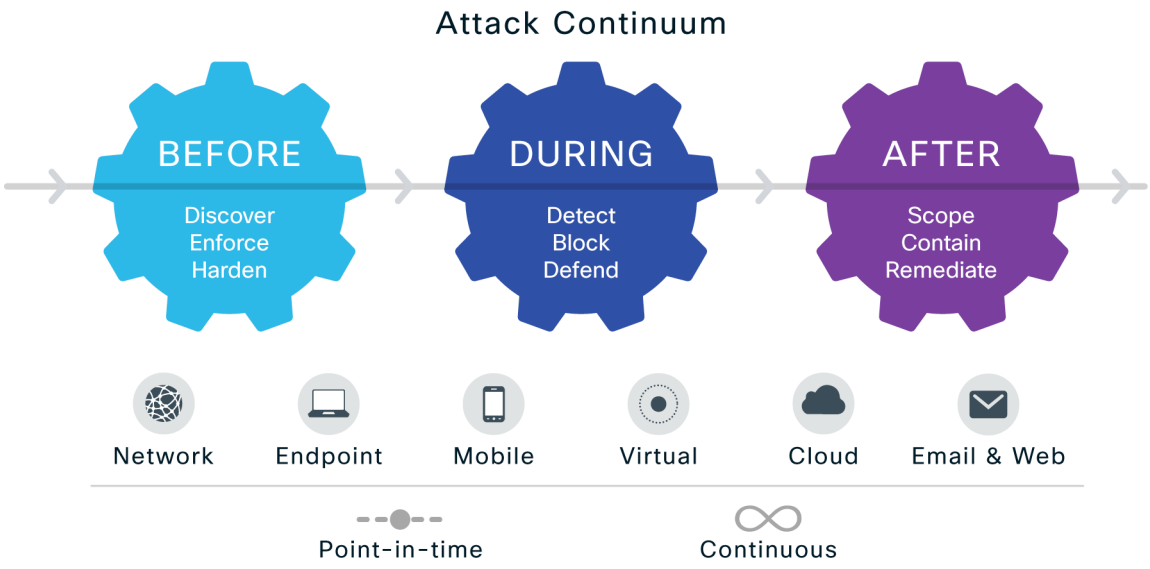
By designing malware that acts patiently, attackers exploited another limitation of the cloud-assisted antivirus model: Most antimalware technologies suffer from a lack of persistence and context, focusing solely on detection the first time a file is seen (point-in-time detection). However, what is benign today can easily become malicious tomorrow. True protection can be achieved only through continuous analysis. Constantly monitoring all traffic helps security personnel trace an infection back to its origin if a file's disposition changes.

Advanced malware writers use a variety of techniques to obscure the intent of malware and make it much harder to detect. These innovations include polymorphic files that change just enough to fool the signature engines, sophisticated downloaders that obtain malware on demand from command-and-control (CnC) networks, and erasable Trojans, which delete their own components, making it difficult for forensics investigators to find and analyze the malware. Those are but a few examples.

Since malware can no longer be identified based on what it "looks" like, an effective defense requires new techniques to capture and analyze the malware over its lifecycle. This new model of proactive security intelligence gains an understanding of what the malware does and where it goes. Threats today can evade defenses that deploy point-in-time strategies and will execute and indicate compromise in a system well after the initial detection period.

You need an approach to malware that adapts as quickly as the threat. Cisco has taken a new, more comprehensive approach to address these challenges in detecting malware. Supported by a global footprint of thousands of enterprises and millions of endpoints, we collect millions of malware samples every month. The Cisco Talos Security Intelligence and Research Group (Talos) and our Collective Security Intelligence (CSI) Cloud analyze tens of thousands of software attributes to separate malware from benign software. We also analyze network traffic characteristics to identify malware searching for CnC networks. For comparison, we use our vast base of Advanced Malware Protection (AMP) installations across our product lines[1] to determine what normal file and network activity looks like, both globally and within each specific customer organization.

Figure 1. The Cisco approach to advanced malware protection: protecting you before, during, and after an attack, across multiple attack vectors and providing continuous analysis and retrospective security in addition to traditional point-in-time detection techniques.



[1] AMP capabilities are now available as an additionally licensed feature on the Cisco Email and Web Security solutions. Learn more by visiting http://www.cisco.com/go/amp.

Detecting malware designed to evade traditional detection tactics requires even further sophistication. Cisco uses purpose-built models to identify malware based on what it does, not what it looks like. So new types of attacks, even new zero-day attacks, can be detected. To keep pace with the rate of change of malware, these models update automatically in real time based on attack methods discovered by our Talos Security Intelligence and Research Group.

Added benefits include cloud analytics that evaluate files over an extended period of time. Our AMP solutions can alert you well beyond the first time the file is analyzed, even if it has passed through a detection point.

Finally, these benefits extend to the entire Cisco AMP community. Whenever a file disposition changes, AMP sends an alert. In this situation, all organizations using Cisco AMP immediately become aware of the malicious file, providing “collective immunity” enabled by the power of the cloud.

Retrospective Security Turns Back the Clock on Attacks

Attackers do not stand still. They constantly evaluate the security controls in place and change tactics to stay a step ahead of defenses. In fact, most attackers test their malware against the leading antimalware products before launching their attacks. As the efficacy of blacklist approaches wanes, more and more security companies rely on virtual machine (VM)-based dynamic analysis to expose and study the malware. Attackers have responded by adapting their tactics: either they do nothing, or they delay the execution of the attack for a period of hours (or days) when running in a VM. They assume the file will evade detection because it did nothing malicious during the evaluation period. Of course, once the waiting period expires, the malware compromises the device.

Unfortunately, point-in-time technologies cannot analyze a file again. When a file has been deemed safe, its status doesn’t change regardless of whether detection techniques have improved or the file exhibits malware behavior. Even worse, once the malware evades detection, these controls have no way to track its propagation within the environment, provide visibility into the root causes, or identify potential malware gateways (systems that repeatedly become infected with malware or serve as the launching pad for broader infections).

The best approach is to assume that no detection measures will be 100 percent effective. To believe that such measures will fully protect you overestimates your ability to defend your critical assets and underestimates your adversaries’ abilities to attack them. Organizations need to assume their defenses will be evaded. They must have the capacity to understand the scope and context of an infection, contain the damage quickly, and eliminate the threat, root causes, and malware gateways. This capability requires retrospective security.

> Retrospective Security: The use of continuous analysis to constantly scrutinize file behavior, trace processes, file activities, and communications over time in order to understand the full extent of an infection, establish root causes, and perform remediation. This lets you look back in time and turn back the clock on would-be attacks. The need for retrospective security arises when any indication of a compromise occurs, such as an event trigger, a change in the disposition of a file or an IoC trigger.

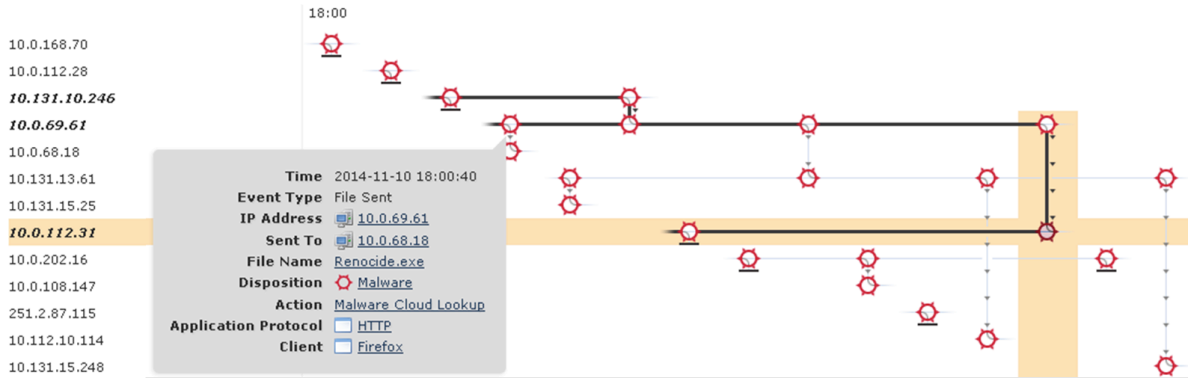
Our retrospective-security technology enables you to travel back in time and determine which devices have been exposed to a malware regardless of when the compromised file is identified. Two features provide this capability: file trajectory and indications of compromise. File trajectory tracks every file crossing the protected network and gives you access to a full history of actions from every protected device that has been exposed. Indications of compromise (IoCs) use the information from file trajectory to create a behavioral pattern that can be used to search your system for malware that is present but undetected.

Tracking Malware Through File Trajectory

If a file proves to be malware at some point in the future, you have limited options with traditional antimalware defenses. You can't get into a time machine and block the file upon entrance. It's already in the environment, and you have no idea how far it has spread or what it has done. This is where most antimalware controls leave you blind to the full scope of the problem and with no ability to figure it out.

Enter the big data analytics underlying AMP. A capability called file trajectory quickly determines exactly how the malware has traversed the organization. In some cases, you can immediately and automatically clean the affected devices. Trajectory provides you with a visual mapping of how the files traveled through the organization and what the files did on the system. It uses that information to identify other instances of the malware on your system. Even more important, since AMP tracks every use of every file, you can identify "patient zero" (the first malware victim) and every other infected device, helping to ensure the total eradication of the infection. It's well known that if even a single instance of the malware remains after cleanup, the likelihood of reinfection remains significant.

Figure 2. A file trajectory screen showing malware propagation with information on point of entry, malware activity, and which endpoints are involved.



Additionally, file trajectory doesn't just analyze information related to file activity. It can also track information about the file's lineage, use, dependencies, communications, and protocols. It can track which files are installing malware in order to facilitate a quick root-cause analysis of detected malware or suspicious activity. Security teams can switch from detection to control during an attack, quickly understanding the scope of an outbreak and root causes to effectively stop further infection.

Determining which event requires prioritization and an immediate response proves extremely challenging when you're faced with a high number of detection events, especially with malware. A single event, even a blocked malicious file on an endpoint, doesn't always mean compromise. However, when multiple events, even multiple seemingly benign activities, are correlated, the result can significantly raise the risk that a system has been compromised and that a breach is imminent or in progress.

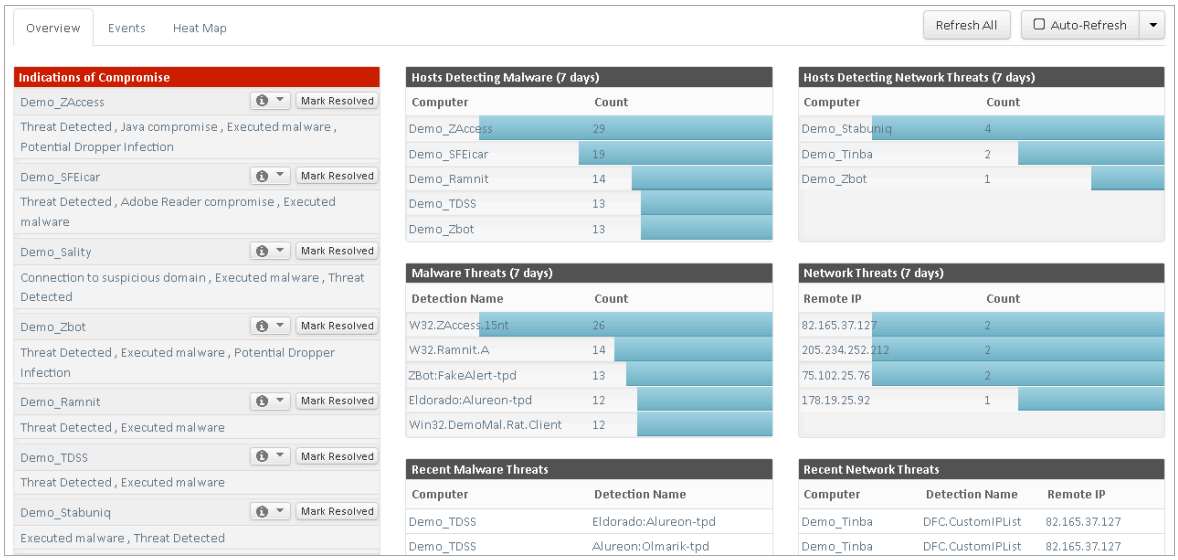
IoCs Identify Patterns, Not Fingerprints

AMP's Indications of Compromise (IoC) capability allows you to perform deeper analytics to find systems that demonstrate symptoms of an active compromise. This capability goes far beyond what point-in-time detection technologies can deliver because it continues to capture, analyze, and correlate malware-related activity after the first analysis, giving you automated analysis and risk prioritization.

Lastly, after malware has gained a foothold within an enterprise, it typically tries to communicate back to CnC servers or, if directly controlled by an attacker, begins reconnaissance activities to move laterally toward its intended target.

Cisco AMP monitors communications activity on the protected endpoint and correlates it against Collective Security Intelligence to determine if a compromise has occurred and blocks the communication and distribution of malware at the endpoint. This gives security personnel a distinct advantage controlling malware proliferation on endpoints that may not reside behind the protections of a corporate network, such as systems used by remote or mobile workers. In addition, file trajectory and IoCs use the captured network activity to accelerate investigations and prioritize threats.

Figure 3. A Cisco AMP dashboard screen showing Indications of Compromise on a system.



Better Together: Enforcement on the Network, Secure Gateway, Physical and Virtual Endpoints, and Mobile Devices

No security control can live in a vacuum. Defending against advanced malware requires significant coordination between the network, gateway, and endpoint defenses. You also need a central management console that tracks threats and remediation activities across all levels. Cisco provides an integrated system built on cloud-based security intelligence, advanced network analytics, and multiple enforcement points to help ensure that advanced malware doesn't go undetected in your organization.

Cisco's broad AMP capabilities start protecting at the network to detect and block malware as it crosses the wire. As every file enters (or exits) the network, AMP generates a file fingerprint and then consults the Cisco FireSIGHT™ Management Center (Management Center) to determine whether the file has been identified as malicious.

If Management Center has never seen the file, it checks with our collective security intelligence and determines whether the file has been seen within our security intelligence network. This lightweight lookup is a far more scalable approach and has no impact on system latency (as opposed to sandboxing every file on the network). For those files identified as malicious, Management Center delivers file trajectory capabilities to understand the context and extent of exposure.

Cisco's lightweight endpoint malware protection agent (the Cisco AMP™ connector) can also be implemented on each protected device so that all file activity can be checked against our collective security intelligence and known malware. AMP for Endpoints doesn't just look for malicious files, its also detects and blocks malware behavior on protected devices. Even if the file hasn't been seen before, the endpoints are protected against zero-day attacks. AMP for Endpoints also leverages retrospective security and file trajectory capabilities, as mentioned above, to identify the extent of any outbreak and identify devices requiring immediate remediation.

If a file is flagged as suspicious, AMP performs deeper file analysis. As described above, Cisco's cloud-based analysis determines exactly what the file does and profiles the attack if it is found to be malware. This process generates IoCs that can be used to find malware that might already be on the network.

Leveraging these malware profiles, AMP provides the ability for an organization to take a proactive stance against a malware outbreak. If a file proves malicious after the fact (using retrospective security), or if it is identified in another environment within the Cisco AMP community, the CSI Cloud sends the updated information to Management Center in your organization, so you can block the malware at the network or endpoint. By so doing, you achieve collective immunity with the rest of the Cisco AMP community. Additionally, you can set up custom rules to block specific files and IP addresses if local administrators identify a localized attack that necessitates immediate action.

Cisco AMP for Endpoints also protects mobile devices. The AMP mobile connector relies on the same security intelligence cloud to quickly analyze Android applications for possible threats in real time. With visibility extending to mobile devices, you can quickly understand which devices have been infected and which applications have launched malware into the system. You can remediate the attack with powerful controls to blacklist specific applications so you can enforce which applications can be used on mobile devices accessing corporate resources. The Cisco AMP virtual connector extends the same capabilities and advanced malware protections to VMware virtual instances.

AMP capabilities are also now available on Cisco Email and Web Security gateways, Cisco Cloud Web Security, and available as an added capability on Cisco ASA with FirePOWER Services. With AMP capabilities added to these appliances, you can enhance detection and blocking of advanced malware at these potential points of entry. Key AMP capabilities include file reputation and file sandboxing described above. In addition, retrospective alerting provides continuous analysis of files that have traversed these gateways, using real-time updates from the CSI Cloud to stay abreast of changing threat levels. When a malicious file is identified as a threat, AMP alerts the administrator and provides visibility into what areas and applications on the network may have been infected and when. As a result, customers can identify and address an attack quickly before it has a chance to spread.

As we've described, malware can enter the organization through multiple attack vectors. It's critical to have full visibility of activity throughout an entire organization. By leveraging our global security intelligence network and having an ability to detect, block, track, investigate and remediate outbreaks on the gateway, network, endpoints, mobile devices and virtual systems, organizations can eliminate the blind spots inherent to other security controls that lack broad coverage.

AMP in Action

A real-world example is often the best way to see the power of an integrated advanced malware protection solution. AMP worked to detect a Java zero-day attack 48 hours before it was publicly announced. In this instance, AMP for Endpoints detected strange behavioral activity on multiple devices. The customer analyzed the files using the CSI Cloud and determined that the file was indeed malware.

The next step was to investigate the extent of the attack and remediate the infection as quickly as possible. The customer used the file trajectory capability to find which devices were exposed to the compromised file(s) or showed the behavioral patterns of the attack. After cleaning the effected devices, the customer set up custom rules to block the files as well as the malware's IoCs.

But those custom rules were needed only for a short period of time. After the event, all AMP customers received the malware profile, inoculating them to that particular attack. Because the files and indicators were added to the big data analytics engine, every instance of that attack was blocked before it had a chance to enter the device or network. This process also alerted customers to the attack, enabling them to search their own environment for the threat. Thus, a single action resulted in global protection to the entire Cisco AMP customer base, even before a public disclosure of the zero-day attack.

Conclusion

Although the industry acknowledges that advanced malware attacks require innovative solutions to detect and remediate, far too many organizations default to focusing their efforts on detection, whether that involves traditional endpoint detection suites or "silver bullet" defenses. That is a sure path to failure, as the industry continues to witness with each front-page story about data loss and breaches.

To have any chance of effectively defending against modern-day attacks, the solution must use continuous analysis and big data analytics to track file interaction and activity across the network, in physical and virtual environments, and on protected endpoints and mobile devices. Given that many attacks lie dormant during the period of traditional detection, having the ability to go back and retrospectively change a determination to malicious, and then track the trajectory of those files and indicators through an organization, helps you to more effectively contain and remediate the damage of these advanced attacks.

Finally, advanced malware protection must be relevant not only to endpoint devices but also to networks, mobile devices, and virtual systems to provide a pervasive and consistent level of protection, given that you cannot predict the target of the next attack.

AMP provides:

- Flexibility in deployment, while using a consistent policy, on endpoints, networks, mobile devices, secure gateways, and virtual systems
- CSI Cloud, which helps you identify and analyze emerging attacks even before the industry discovers them
- The capability to retrospectively identify malware and, through file trajectory, find every instance of that malware within your organization before it spreads
- Collective immunity provided by the global Cisco AMP community, which accesses research derived from Talos and from the file samples seen by millions of AMP protection agents

To include Cisco AMP solutions in your advanced malware protection evaluation, visit http://www.cisco.com/go/amp.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-733364-00 11/14