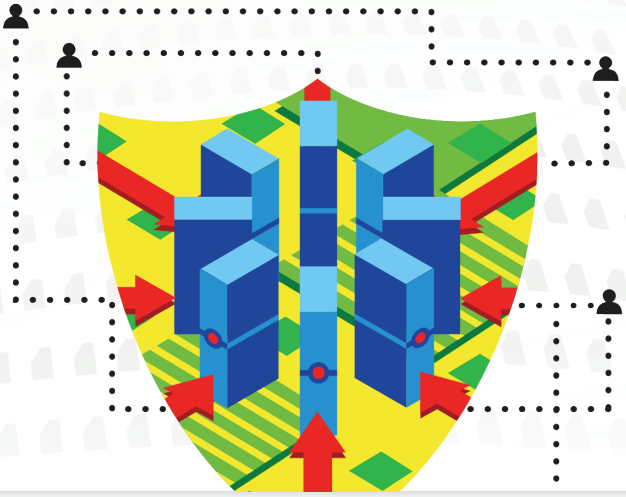
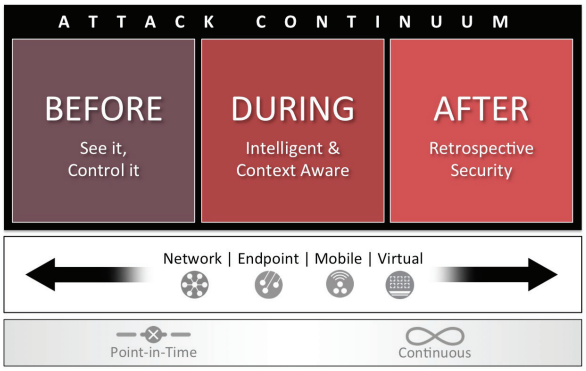
Buyer's Criteria for Advanced Malware Protection



Introduction

It's not a secret that today's advanced attackers have the resources, expertise and persistence to compromise any organization at any time. Traditional defenses, including firewalls and endpoint protection, are no longer effective against these attacks, which means the process of handling malware must evolve, and quickly at that. This involves a realization that detecting malware and the targeted, persistent attacks they represent 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.

The problem is going to 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 successfully compromise a device. The blacklist approach of matching a file to signatures of known bad malware no longer scales to keep pace and newer detection techniques, like sandboxing, are not 100% effective. In this Advanced Malware Protection Buyer's Criteria, we'll identify the key questions you should ask your advanced malware protection vendor, and we'll describe how Sourcefire combines big data analytics, collective security intelligence and enforcement across networks, endpoints, virtual systems and mobile devices, as well as unique Retrospective Security to combat the scourge of malware attacks.



Retrospective security is unique to Sourcefire and is fundamental in combating advanced malware. It delivers continuous capability which utilizes big data analytics to aggregate data and events across extended networks for constant file tracking and analysis, alerting on and remediating files initially deemed safe but now known to be malicious.

Key Questions to Ask Your Advanced Malware Protection Vendor

1. How are you leveraging big data for persistent malware determination?
2. How is malware analyzed to determine exactly what it does?
3. How does your malware analysis automatically update detection capabilities across control points and across all customers?
4. How do you gather intelligence on emerging malware threats?
5. How do you perform continuous analysis for retrospective malware detection?

Applying Big Data Analytics and Collective Security Intelligence to the Malware Problem

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 anti-virus" capability that basically 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.

Another limitation of the cloud assisted anti-virus model is the reality that attackers can use time and patience to their advantage. Most anti-malware technologies suffer from a lack of persistence and context, focusing solely on detection the first time a file is seen (point-in-time). However, what may not look like malware today can easily become maliciously repurposed tomorrow (or the next day). What's required is a continuous analysis capability that constantly monitors and can change file status from initially benign to malicious based on the latest threat intelligence.

Advanced malware writers use and innovate a variety of techniques to obscure the intent of malware and make it much harder to detect. This includes polymorphic files changing just enough to fool the signature engines, sophisticated downloaders which obtain malware on demand from command & control (CnC) networks, and erasable Trojans, which delete their own components making it difficult for forensics investigators to find and analyze the malware. These are but a few examples. Since malware can longer be identified based on what it "looks" like, new techniques are needed to capture and analyze the malware over its lifecycle to understand what it does, where it goes and identify malicious actions and indications of compromise that may happen well after the initial detection period, and therefore missed by point-in-time detection technologies.

Sourcefire has taken a new, more comprehensive approach to address these challenges in detecting malware. Enabled by a customer base of thousands of global enterprises and millions of endpoint malware protection agents in use, Sourcefire collects millions of malware samples every month. Tens of thousands of software attributes are analyzed within Sourcefire's Collective Security Intelligence Cloud to separate malware from benign software. Network traffic characteristics are also analyzed to identify malware searching for CnC networks. Sourcefire also leverages its vast installed base to determine what normal file and network activity looks like, both globally and within each specific customer organization, for comparison.

Further sophistication is required to detect malware designed to evade traditional detection tactics. Sourcefire uses purpose-built models constructed to identify malware based on what it does – not what it looks like – enabling new types of attacks to be detected, even zero-day attacks. To keep pace with the rate of change of malware, these models are updated automatically in real time based on new attack methods discovered by the Sourcefire VRT® (Vulnerability Research Team).

The benefit of Sourcefire's Collective Security Intelligence doesn't end when a file passes through any of the detection points. Sourcefire's cloud analytics continue to evaluate the file against the latest threat intelligence for an extended period of time allowing Sourcefire's Advanced Malware Protection solutions (Sourcefire AMP) to alert well beyond the first time the file is analyzed.

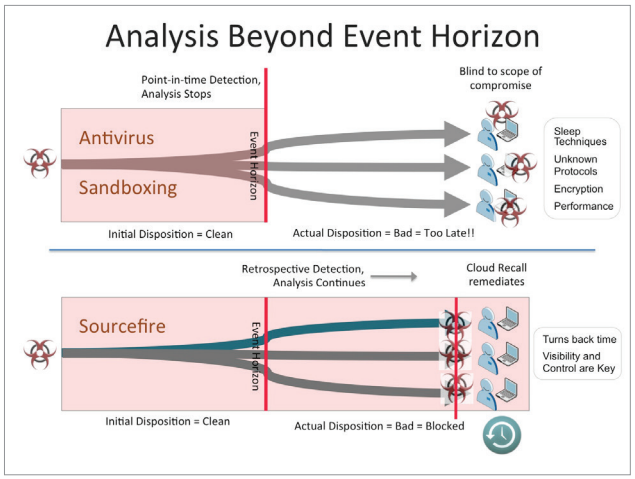
Finally, these benefits accrue to the entire Sourcefire AMP community, which is alerted whenever the disposition of a file is changed. In this situation, all organizations leveraging the Collective Security Intelligence Cloud immediately become aware of the malicious file, providing "collective immunity" enabled by the power of the cloud.

Retrospective Security: The use of continuous analysis capability to alert on files initially deemed benign or unknown, yet subsequently determined to be malicious. Retrospective security determines the scope of outbreaks, contains them and ultimately turns back the clock enabling automatic malware remediation.

Retrospective Security Turns Back the Clock on Attackers

Attackers do not stand still. They constantly evaluate the security controls in place and change their tactics to stay a step ahead of the defenses. In fact, most attackers test their malware against the leading anti-malware products before launching attacks, ensuring success. As the efficacy of blacklist approaches has waned, more and more security companies rely on virtual machine-based (VM-based) dynamic analysis to explode and study the malware. As such, attackers have adapted their tactics to either do nothing or delay the execution of the attack for a period of hours (or days) when running in a VM, assuming the file will be determined to be safe as the file did nothing malicious during the evaluation period. Of course, once the waiting period expires the victim's device is then compromised. Unfortunately there is no way for these point-in-time technologies to analyze the files again. Once a file is deemed safe, it's safe 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 propagation within the environment, understand root causes or identify potential malware gateways (systems that repeatedly become infected with malware or serve as the launching pad for broader infection).

Although that's just one example of how the malware writers manage to stay a step ahead of security companies and the limitations of existing anti-malware controls, the best approach is to assume no detection-defense is going to be 100% effective. To assume full protection based solely on detection both overestimates your ability to defend your critical assets and underestimates your adversaries' abilities to attack them. Thus, organizations need to plan for their defenses to be evaded, and ensure they can understand the scope and context of an infection, contain the damage quickly and eliminate the threat, root causes and malware gateways, which requires "Retrospective Security."



Key Questions to Ask Your Anti-Malware Vendor

1. What is your approach to determine the extent of malware proliferation across the network and on compromised devices?
2. How can you determine which devices have been exposed to malware if detection happens hours or days later?
3. How do you deal with malware, which has evaded initial detection or is not blocked at the network?
4. How are you able to quickly perform root cause analysis for suspicious activity?
5. What forms of controls do you have to stop an outbreak and root causes?

Retrospective Security allows an organization to, in essence, travel back in time, determining which devices have been exposed to malware regardless of when the file is identified as malware. This requires tracking every file crossing the protected network combined with a full lineage of every action that happens on every protected device and visually mapping how the files travel through the organization and what the files do on the system.

With traditional anti-malware defenses, if a file is determined to be malware at some point in the future, your options are usually limited since you can't get into a time machine and block the file upon entrance – it's already in the environment potentially wreaking havoc. This is where most anti-malware controls stop, leaving you blind to the full scope of the problem and stuck answering the question, "Now what?"

This is where the big data analytics underlying Sourcefire AMP pays dividends. Being able to quickly determine exactly how the file has traversed the organization via a capability called "Trajectory" enables malware to be tracked and the affected devices to be cleaned immediately (and in some cases automatically). Even more importantly, since Sourcefire AMP tracks every use of every file, organizations can find "Patient Zero" (the first malware victim) and every other infected device, which ensures 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 is significant.

Additionally, Trajectory doesn't just analyze information related to file activity, but also can track information about file lineage, usage, dependencies, communications, protocols and which files install malware to facilitate quick, root cause analysis of detected malware or suspicious activity. This enables security teams to instantly switch from detection to control during an attack, quickly understanding the scope of an outbreak and root causes to effectively stop further infection.

Another challenge when inundated with a number of detection events, especially with malware, is determining which event really requires prioritization and response. 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 together the result can significantly raise the risk that a system is compromised and a breach is imminent or in progress.

Indications of Compromise is yet another capability of Sourcefire AMP, performing deeper analytics to find systems that demonstrate symptoms of active compromise. This goes far beyond what point-in-time detection technologies can deliver by continuing to capture, analyze and correlate malware related activity after the first time it is analyzed, giving security personnel automated analysis and risk prioritization.

Lastly, once 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 towards its intended target.

Sourcefire AMP monitors communications activity on the protected endpoint and correlates it against Sourcefire Collective Security Intelligence to determine if compromise has occurred and block 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, Trajectory and Indications of Compromise leverage the captured network activity to accelerate investigation and compromise prioritization.

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

No security control can live in a vacuum. In order to defend against advanced malware, significant coordination is required between the defenses on the network, the protections on the endpoint and the management console tracking threats and remediation activities. Sourcefire provides an integrated system leveraging the cloud-based Collective Security Intelligence, advanced network analytics and multiple enforcement points to ensure advanced malware doesn't slip through the cracks of your organization.

Sourcefire's broad AMP capabilities start at the network to detect/block malware as it crosses the wire. As every file enters (or exits) the network, Sourcefire AMP generates a file fingerprint and then consults Sourcefire's FireSIGHT® central management console to determine if the file has been identified as malicious.

If FireSIGHT has never seen the file, it checks with the Sourcefire Collective Security Intelligence Cloud and quickly makes a determination of whether the file has been seen within Sourcefire's Collective Security Intelligence network. This lightweight lookup provides a far more scalable approach and no impact to latency compared to sandboxing every file on the network. For those files identified as malicious, FireSIGHT delivers File Trajectory capabilities to understand the context and extent of exposure.

Sourcefire's lightweight endpoint malware protection agent (the FireAMP™ connector) can also be implemented on each protected device so that all file activity can be checked against the Collective Security Intelligence Cloud to identify those files known to be malware. FireAMP doesn't just look for malicious files, but also can detect and block malware behavioral characteristics on the devices, even if the file hasn't been seen before, protecting the endpoints against zero-day attacks. The FireAMP connector also leverages the retrospective detection and File Trajectory capabilities described above to identify the extent of any outbreak and identify devices requiring immediate remediation.

If the file is determined to be suspicious, then Sourcefire AMP will perform much deeper File Analysis. As described above, Sourcefire's cloud-based analysis determines exactly what the file does and if determined to be malicious will profile the attack, generating indicators of compromise and other attributes that can be searched for using powerful big data analytics capabilities.

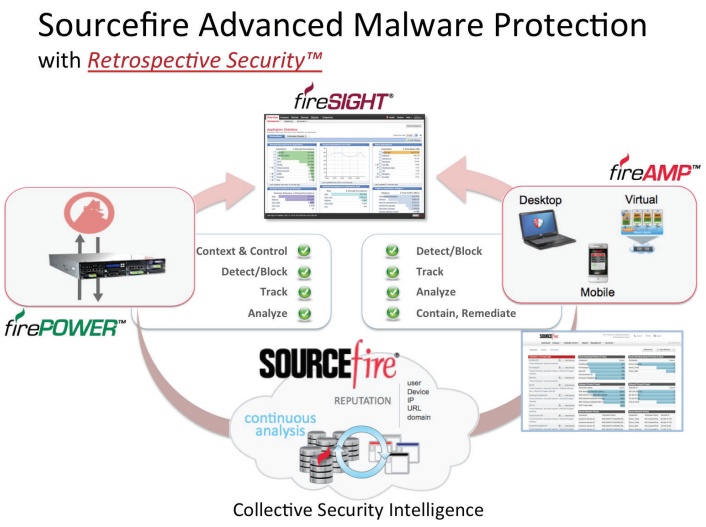
Leveraging these malware profiles, Sourcefire AMP provides the ability for an organization to take a proactive stance against a malware outbreak. If a file is determined to be malicious after the fact (using Retrospective Security) in another environment, the Collective Security Intelligence Cloud can send those determinations down to the FireSIGHT console in your organization enabling you to block the malware either at the network or endpoint achieving collective immunity with the rest of the Sourcefire AMP community. Additionally, organizations can set up custom rules to block specific files and IP addresses if local administrators identify a localized attack and need to take immediate action.

Key Questions to Ask Your AMP Vendor

1. Are you able to block, track, analyze and remediate malware and root causes at the network, on physical and virtual endpoints, and mobile devices?
2. How do you protect devices that roam outside of the protected network?
3. How do you determine which devices are actively compromised?
4. How are you able to confirm if a system is actively compromised and perform remediation?
5. Are custom malware detection rules to remediate unique attacks supported? How?

The FireAMP™ Mobile connector relies on the same Collective 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 are infected and which applications are introducing the malware into the system. When you want to remediate the attack, FireAMP Mobile includes powerful controls to block (blacklist) specific applications so you can enforce which applications can be used on mobile devices accessing corporate resources. The FireAMP™ Virtual connector extends the same capabilities and advanced malware protections to VMware virtual instances.

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



Advanced Malware Protection in Action

The best way to understand the capabilities of integrated advanced malware protection is to see how it worked to detect a Java zero-day attack TWO DAYS before it was publicly announced. In this instance, a customer looking at the FireAMP Console (the management console for endpoint, mobile and virtual connectors) detected some strange activity on a few of their devices, which looked like the behavioral patterns of malware. The customer analyzed the files using the Collective Security Intelligence Cloud and got a clear determination of malware.

The next step was to determine the extent of the attack and to clean it up as quickly as possible. The customer then used FireAMP's Trajectory capability to find which devices were exposed to the file(s) and/or showed the behavioral patterns of the attack. Once the affected devices were cleaned, the customer set up custom rules to block both those files, as well as the indicators of compromise of the malware.

But those custom rules were only needed for a short period of time since every Sourcefire AMP customer benefited from this collective immunity when these files and indicators were added to the big data analytics engine. This allowed customers to be alerted if this attack was found in their environment. Thus the entire Sourcefire AMP customer base was protected before there was even a public disclosure of the zero-day attack.

Summary

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

In order to have any chance of effectively defending against modern day attacks, the solution must leverage a big data analytics capability 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, enables customers to more effectively contain and remediate the damage of these advanced attacks.

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

Sourcefire's Advanced Malware Protection provides:

- **The flexibility of deployment on endpoints, network and mobile devices and virtual systems, utilizing a consistent policy;**
- **The benefits of the Collective Security Intelligence Cloud to identify and analyze emerging attacks, even before the industry discovers it;**
- **The ability to retrospectively identify malware and, via Trajectory, find every instance of that malware within your organization, before it spreads;**
- **The leverage of Collective Immunity by participating in the Sourcefire AMP community to access cutting edge research derived from the Sourcefire VRT and file samples seen by the millions of endpoint malware protection agents deployed globally within thousands of customers.**

To include Sourcefire AMP solutions in your advanced malware protection evaluation, contact us at info@sourcefire.com.

5.13 I REV1 B