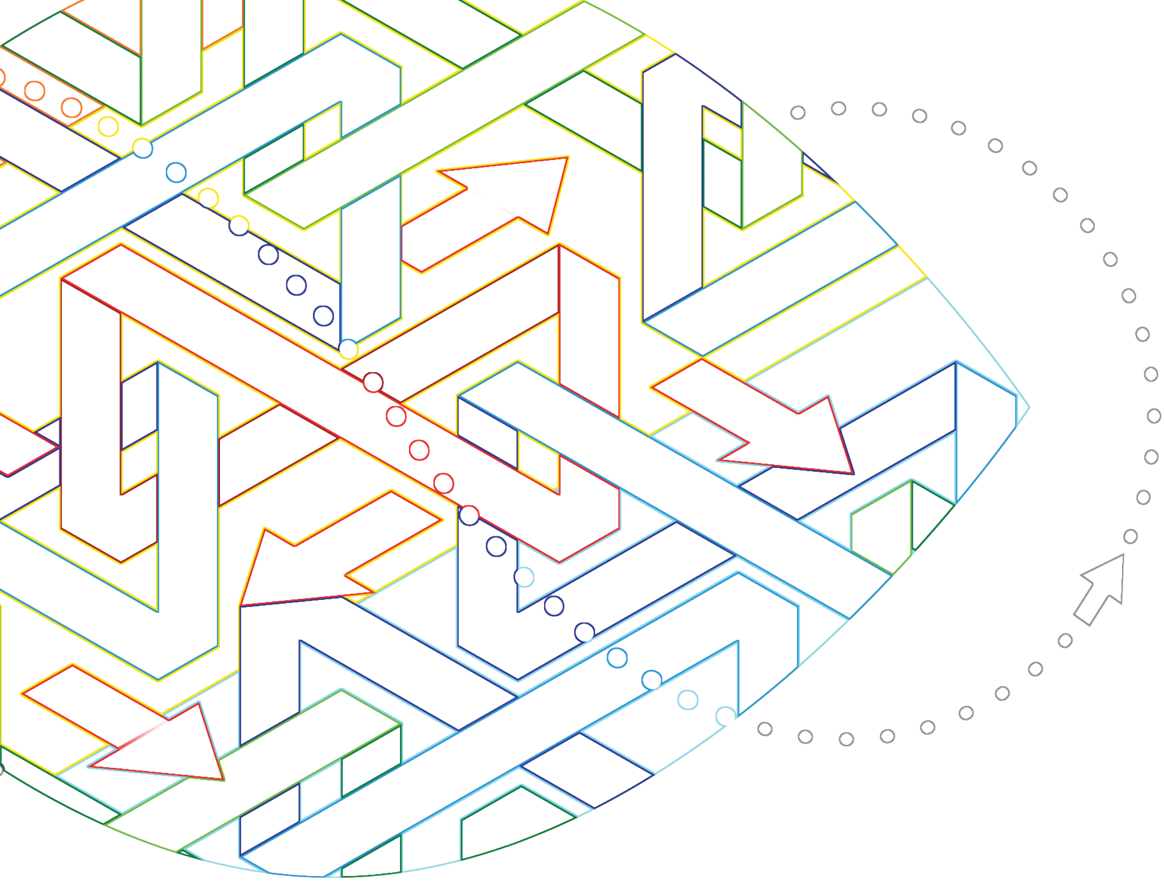
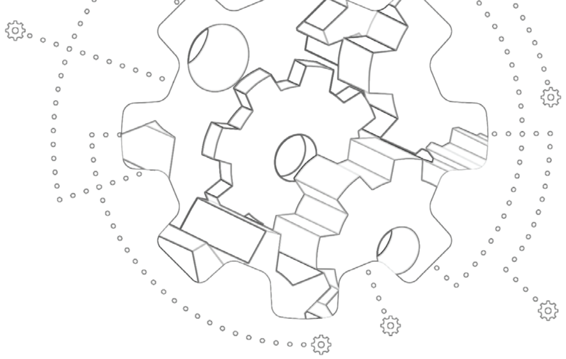


Continuous Endpoint Threat Detection and Response in a Point-in-Time World

SOURCEfire®

Sourcefire is now part of Cisco.

CISCO



A New Model to Protect the Endpoint

Sourcefire is not a newcomer to security innovation nor have we been sitting idly by while attackers have continued to innovate. In fact, as early as 2003 we had a vision for what would be required to combat advanced threats and pioneered the concept of continuous network discovery which became foundational to Next-Generation IPS. Today, targeted, advanced malware and sophisticated attacks are relentless as they compromise environments using new and stealthy techniques. Once again, Sourcefire is changing the way we must think about security, building on our continuous capability and introducing a new model for the way we need to combat these attacks.

Continuous Protection in a World of Continuous Change

When Sourcefire introduced real-time network awareness more than a decade ago, the standard for network visibility was to use invasive network point-in-time scanning tools. These scanning tools took significant time to complete a full scan and were disruptive to network and systems being scanned. More troublesome, because of the dynamic nature of networks, the data quickly became out of date, so the whole process would have to be run again and again. Finally, the data was wrought with blind spots and hard to correlate against live threat data.

Sourcefire recognized that the fundamental security problem that many defenders face is not securing their environment but gaining sufficient understanding of what they're protecting and how it's arranged so that they can begin the continuous process of securing it as it evolves. With continuous real-time network awareness, for the first time visibility was tightly integrated with threat detection, changing the network threat defense conversation forever. Real-time network awareness became a key requirement for Next-Generation IPS, as defined by Gartner, and now is our FireSIGHT® technology.

In 2013, Sourcefire introduced yet another paradigm-shifting security model to address the plague of advanced threats. Based on the concept that today's threat landscape and IT environment are dynamic and ever expanding, this new security model addresses the full attack continuum – before, during, and after an attack.

Building on real-time network awareness, this new model is transforming a traditional point-in-time methodology into a continuous approach:

- driving unique innovation in the battle against today's advanced threats;
- delivering visibility into compromise and attack persistence like never before;
- allowing security teams to quickly and surgically contain and remediate infection without disrupting end users and security personnel; and, ultimately
- empowering security teams to be the hunter, not the hunted.

Expecting Different Results

The world of endpoint threat detection and response is awash in high-level branding and messaging that all sounds the same. Everyone is claiming to be leading the next revolution in the detection of malware. Much akin to network scanners back in the day, each claims they are more real-time and continuous than the other, when in reality they were just incremental improvements on the same tool with the same fundamental limitations.

> *"Insanity: Doing the same thing over and over again, and expecting different results."*
> *– Albert Einstein*

The latest improvements in threat detection have involved executing files in a sandbox for detection and analysis, the use of virtual emulation layers to obfuscate malware from users and operating systems, reputation-based application whitelisting to baseline acceptable applications from malicious ones, and, more recently, attack chain simulation and analysis detection. But predictably, attackers fundamentally understand the static nature of these security technologies and are innovating around the limitations associated with them to penetrate network and endpoint defenses.

Unfortunately, it's the end user that is left with less than revolutionary improvement over the previous "bleeding-edge" detection technology of last year and the cycle repeats itself without addressing the underlying limitation. Today's detection technology is stuck in time, point-in-time to be exact.

Malware is dynamic and three dimensional. It doesn't just exist in a two dimensional point-in-time 'X-Y' plot waiting to be detected, where X is time and Y is the detection mechanism. Malware exists as an interconnected ecosystem that is constantly in motion. To even be remotely effective, malware defenses have to be multi-dimensional and just as dynamic, taking into account the relationship dimension as well. We have to let go of the hope that an 'uber' detection technology will make the problem go away and understand that we need continuous protection and visibility from point of entry, through propagation, and post-infection remediation.

What's needed is a truly transformational change in how we approach detecting advanced threats and breach activity.

Point-in-time Paradigm Shift

Today's advanced malware compromises environments from an array of attack vectors, takes endless form factors, launches attacks over time, and can obfuscate the exfiltration of data. As it unfolds it leaves in its wake massive volumes of data that we can capture, store, manipulate, analyze, and manage in order to understand these attacks and how to defeat them. Based on a model of delivering protection before, during, and after an attack, Sourcefire's Advanced Malware Protection for Endpoints solution leverages a big data architecture combined with a continuous approach and advanced analytics to overcome the limitations of traditional point-in-time detection and response technologies.

In this model, process-level telemetry data is continuously collected as it is happening, while it is happening across all sources, and is always up to date when it is needed.

A True Continuous Model Answers Key Questions

- What was the method and point of entry?
- What systems were affected?
- What did the threat do?
- Can I stop the threat and root cause?
- How do we recover from it?
- How do we prevent it from happening again?
- Can I quickly hunt down IoC's before they impact my operation?

Benefits of Continuous Analysis

- Less focus on data collection
- Automation of advanced analytics
- Better threat prioritization
- Faster time to remediation

Analysis can be layered to work in concert to eliminate impacts to control points and deliver advanced levels of detection over an extended period of time. Analysis is more than event enumeration and correlation; it also involves weaving telemetry data together for greater insights into what is happening across the environment. Tapping into a broader community of users, Collective Security Intelligence is continuously updated globally and is shared immediately. This global intelligence is correlated with local data for even more informed decision making.

In this model, detection and response are no longer separate disciplines or processes but an extension of the same objective: to stop advanced threats before they stop you. Going beyond traditional point-in-time methodologies, detection and response capabilities are continuous and integrated.

Detection

No detection method is 100% effective as attackers continue to innovate to evade these front line defenses. Yet despite the limitations of point-in-time detection, it maintains an important role in eliminating a large majority of potential threats. Moreover, by applying a continuous approach to traditional detection, defenders can improve upon point-in-time technologies, enabling them to be more effective, efficient, and pervasive.

But this is just the beginning of how Sourcefire's continuous approach transforms advanced malware protection. More importantly, it lets us deliver a range of other innovations that enhance the entire advanced malware protection process from detection through response.

Continuous Capabilities Enable Innovation

The only way to defeat advanced threats is to address them holistically across the full attack continuum – before, during, and after an attack. Our continuous approach in combination with a big data architecture is foundational to this model and enables a spectrum of additional innovation as it relates to advanced malware protection, including:

- **Retrospection** – The ability to conduct analysis at an initial point-in-time and over an extended period of time, not limited to files but also including processes, communications, and other telemetry data, something traditional point-in-time models simply can't do.
- **Attack Chain Weaving** –The method for weaving together the file, process, and communication retrospection streams as they happen over time to capture the relational dimension that is missing in two dimensional point-in-time technologies.
- **Behavioral Indications of Compromise (IoC's)** – More than static artifacts used to query against, these are complex behavioral clues that attack chain weaving captures and behavioral IoC's can detect as they are happening in real-time.
- **Trajectory** – Trajectory is more than a fancy marketing term for tracking. Tracking is an enumerated list of point-in-time events to show where something has been. On the other hand, Trajectory is the contiguous path an object moves, in this case malware, as a function of time. It is substantially more effective at showing the scope and root causes of malware in relationship to where it has been and what is has done.
- **Threat Hunting** – With the dynamic nature of malware captured over time, and the breadth of that data always up to date, the ability to zero-in on elusive malware IoC's is as simple as "Googling" your favorite style of takeout.

As important as each of these innovations is individually to combat malware and the advanced threats they represent, it's when they are combined together in an integrated workflow that the real impact across malware detection, monitoring, analysis, investigation, and containment becomes apparent.

Monitoring

The ability to collect telemetry data from the endpoint as it is happening and analyze it for threat activity as it comes in as well as over an extended period of time is a capability called retrospection and an innovation that Sourcefire is the first to deliver. It's a major leap forward from event-driven data collection or scheduled scans for new data and it captures attacks as they happen, analogous to a video surveillance system.

Automated, Advanced Analytics

To detect advanced attacks as they move laterally through the network and across endpoints, defenders need technologies that automatically look for Indicators of Compromise (IoC's) left behind by malware and exploits, as well as more advanced behaviors of compromise that happen over time. Sourcefire's continuous approach delivers this level of automation through advanced behavioral detection capabilities, not with the aim of providing yet another list of alerts to investigate but, rather, to deliver a prioritized and collated view of top areas of compromise and breach activity. The use of big data analytics and continuous capabilities identify patterns and indications of compromise as they emerge so that security teams can focus their efforts on the threats with the greatest potential for damage.

Threat Hunting vs. Investigation

Without the context and capabilities of a continuous approach, using the term "Investigation" is liable to cause a few involuntary twitches from security teams that have experience with the painstaking process of trying to track down a breach with very little contextual evidence. Often, the hardest question to answer is: "Where do we start?" In a continuous approach, investigations can be more targeted, fast and productive.

Innovation delivers advanced levels of detection, visibility and control to eliminate blind spots and workload.

A continuous approach shifts activity from looking for elusive facts and clues as part of an investigation, to a very focused hunt for breaches based on actual events like malware detections, and static and behavioral IoC's. Continuous capabilities backed by a big data architecture enable all data to be easily searchable anytime and all the time. With a continuous model and using the previous capabilities discussed (including behavioral and point-in-time detections as well as retrospection) hunting down malware can be fast and effective. Investigation, or threat hunting, involves visually understanding the point of entry, scope, and root causes of infection. It also includes the ability to identify a time window for the hunt, expand or contract that window, and pinpoint and pivot the hunt with filters. This becomes an important tool and an efficiency multiplier as security teams move from blindly responding to alerts and incidents to quickly hunting down malware before an attack escalates.

Outbreak Control vs. Containment

The concept of investigation is overwhelming when limited by point-in-time detection and forensic technologies. So too is the notion of containing malware or suspected malware without having to reimage everything in sight to get it done. Because point-in-time technologies are blind to the chain of events and contextual information that goes along with it, the ability to surgically contain malware isn't even within the realm of possibility.

With the level of visibility the continuous approach provides, coupled with the ability to target specific root causes, breaking the attack chain is not only quick but easy. What's more, even if the standard operating procedure is to reimage a device experiencing severe compromise, all the detection and telemetry data is still preserved and containment can still be enacted to prevent any future compromise by attackers using the same infection gateway.

Lastly, there are use cases where traditional point-in-time technologies have failed to detect an attack and an organization is in the midst of an active breach. Typically many endpoints have been infected over an extended period of time and the incident response team has been engaged to investigate and remediate the situation. As with detection and discovery, time is of the essence in this scenario and the same fundamental questions still apply, "Where do we start and how bad is the situation?" However, responding and containing in this outbreak scenario often involves understanding scope and root causes very quickly without tipping your hand to attackers. Once understood, quickly shutting down all points of compromise and infection gateways simultaneously is critical to prevent lateral movement of an attacker.

From the moment of deployment, a continuous approach immediately starts gathering vital detection and telemetry information that will help responders understand how bad the outbreak is, where the hotspots are, and most importantly, establish a containment profile that can be flipped on instantaneously. All the advanced behavioral detection, tracking and visualization capabilities begin immediately, but unlike the detect and protect scenario, they are all in audit mode. Still detecting and alerting but instead of actively blocking, they are capturing evidence like detectives on a stake out gathering information for the SWAT team to swoop in and close down the operation.

The fundamental difference between continuous and point-in-time when it comes to response, is that continuous provides a robust outbreak control capability that includes surgical containment where point-in-time only provides enumerated lists of facts and evidence. While these lists can be used by security teams, they are tedious to make actionable for containment.

Integration and Reporting

Sourcefire AMP for Endpoints is designed from the ground-up to support a continuous approach and big data architecture. It leverages a cloud model to enable a lightweight connector versus a heavy agent architecture at the endpoint. The connector is more akin to a collector of file and telemetry data, rather than a heavy detection agent limited in scope and effectiveness by computation and memory impacts on the endpoint and users. This frees up resources to allow the connector to continuously monitor, collect, and efficiently transmit telemetry data to the cloud for big data analytics.

The lightweight connector model also enables connectors to be supported on a variety of endpoint platforms, like Windows, Mac, Android, and virtual environments with a high level of parity across platforms. This connectivity extends malware detection and protection across other control points, like email and web gateway appliances, next-generation intrusion prevention systems and firewalls, and cloud services with high volumes of file transactions.

Pervasive collection and advanced analytics of file and telemetry data across control points enriches the level of collective intelligence that can be shared locally within an environment and globally across customers through the broader Sourcefire Collective Intelligence Cloud. Sharing intelligence in real-time helps security teams stay ahead of broad attacks that use techniques like phishing where many users could potentially be infected with the same initial payload but then receive different subsequent downloads or commands. Going beyond just file data analysis, other telemetry data can be analyzed across control points to more accurately determine the scope of an outbreak.

Once in the cloud, the depth of telemetry information collected across control points can be shared with all control points to provide contextual information equally, even at control points that might not be able to collect that level of information. For example, telemetry data and behavioral detections collected from an endpoint can be used by network security to determine the scope of exposure to a specific malware. From the endpoint, information indicating whether the file has been downloaded, opened or even moved can provide a more complete lineage of information to network security teams than is possible with generic alert data. Endpoints that have executed the malware are going to be a higher priority than those that merely down loaded it. Rich contextual information from the endpoint shared in real time with other control points for better threat determination and decision support is in sharp contrast to simply providing the typical list of events that may or may not be an actual threat.

A continuous approach extends to reporting capabilities as well. No longer are reports limited to event enumeration and aggregation, but can include actionable dashboards and trending that highlights business relevance and impact from a risk perspective. While point-in-time technologies can also provide dashboards and risk relevance, they typically require an additional layer of complexity in the way of SEIM integration to sift through and correlate the voluminous amounts of event data.

A big data architecture handles the ever-expanding volume of data that is essential to effective malware detection and analytics, while a continuous approach uses that data to provide context and most importantly, prioritization when and where you need it.

Conclusion: It's True, One + One Doesn't Equal Three. Sometimes, It Equals Six

A continuous approach plus a big data architecture enables six key areas of transformative innovation in the battle against advanced threats that target the endpoint:

1. **Detection that moves beyond point-in-time.** A continuous approach enables detection to become more effective, efficient and pervasive. Behavioral detection methods like sandboxing are optimized, activity is captured as it unfolds and intelligence is shared across detection engines and control points.
2. **Monitoring that enables attack chain weaving.** Retrospection – continuously monitoring files, process and communication – and then weaving that information together to create a lineage of activity provides unprecedented insights into an attack as it happens.
3. **Automated advanced analytics that look at behaviors over time.** Combing big data analytics and continuous capabilities to identify patterns and indications of compromise as they emerge enable security teams to focus their efforts on the threats that matter most.
4. **Investigation that turns the hunted into the hunter.** Transforming investigation into a focused hunt for threats based on actual events and IoC's gives security teams a fast and effective way to understand and scope an attack.
5. **Containment that really is simple.** Breaking the attack chain is fast and effective with the level of visibility the continuous approach provides combined with the ability to target specific root causes.
6. **Dashboards that are actionable and contextual.** Reports based on the pervasive collection and advanced analytics of file and telemetry data across control points, and overlaid with contextual information, highlight trends, business relevance, and impact on risk.

Building on our pioneering efforts in continuous capabilities and coupling that with a big data architecture, Sourcefire is delivering a new model to address today's advanced attacks. In this model, detection and response are no longer separate disciplines or processes but an extension of the same objective: to stop advanced threats before they stop you. Going beyond traditional point-in-time methodologies, detection and response capabilities are continuous and integrated. It's what's required for endpoint threat detection and response for the real world.

To learn more, contact us at: info@sourcefire.com

Detailed Comparison

What follows is a detailed comparison of capabilities that differentiate a continuous approach from a point-in-time model. Enhancements to detection as well as additional innovations related to advanced malware protection are covered.

Detection

CONTINUOUS APPROACH	POINT-IN-TIME MODEL LIMITATIONS
· Can perform as an integrated lattice of engines working in concert, sharing context for improved detection capabilities. · Optimizes behavioral methods of detection like sandboxing by reducing the workload and latency involved and eliminating the need to sandbox every new file. · Can perform detection over an extended period of time which is exactly how attacks unfold – over time. · Transforms audit mode from simply a tuning parameter used to reduce false positives to an incident response collection tool to capture real-time activity without tipping off attackers. · Collective sharing of detection intelligence is instantaneous across multiple control points.	· Engines, if there is more than one, work as a stack, operating serially in independent silos which reduces efficacy and impacts performance at the endpoint. · Requires updates from vendors which take time and create additional gaps in security.

Monitoring

CONTINUOUS APPROACH	POINT-IN-TIME MODEL LIMITATIONS
· File retrospection – After initial detection analysis a file continues to be interrogated over an extended period of time with the latest detection capabilities and collective threat intelligence, allowing for an updated disposition to be rendered and further analysis to be conducted well beyond the initial point-in-time it was first seen. · Process retrospection – Similar to file retrospection, process retrospection is the ability to continuously capture and analyze system process I/O over an extended period of time for attack chain analysis and behavioral IoC detection. · Communication retrospection – Continuously captures communication to and from an endpoint and the associated application and process that initiated or received the communication for added contextual data as part of attack chain analysis and behavioral IoC detection. · Attack Chain Weaving – AMP for Endpoints does more than retrospection, it introduces a new level of intelligence, linking and weaving together the various forms of retrospection into a lineage of activity that is available for analysis in real-time, anytime it is needed. Specifically, different forms of retrospection can be woven together through analysis to look for patterns of behavior from an individual endpoint or across the community of endpoints.	· Blind to the relational activity at the endpoint beyond detection activity. · Completely blind to anything that is happening within the network after it has crossed the control point.

Automated, Advanced Analytics

CONTINUOUS APPROACH	POINT-IN-TIME MODEL LIMITATIONS
· Happens in real time – as real-time endpoint telemetry data is continuously collected and added to the data store it can be automatically compared against static and behavioral IoC's. The advantage is time to detection of either a static or behavioral IoC can be dramatically reduced. · Behavioral Indications of Compromise – Leveraging Attack Chain Weaving capabilities, Behavioral IoC's, look for sophisticated patterns of activity across detection events, static IoC's and telemetry data that indicate potential compromise. A classic example is a dropper that has slipped through initial detection. · Trajectory – Records what happened leading up and after the triggered Behavioral IoC. As described later, the security team can quickly pivot from an alert that is meaningful to a full understanding of the scope of an outbreak and the ability to surgically contain the problem. · Open IoC's – The ability for customer to leverage their custom static IoC detection lists within the continuous model. · Intelligence-based IoC's – More than static intelligence, black lists or detection scripts, these IoC's are based on behavioral algorithms that look for specific malicious actions and related actions over time. Intelligence-based IoC's are developed and fully supported by the Sourcefire VRT® (Vulnerability Research Team.) · Prevalence – Advanced analysis engine that determines a detected malware's prevalence in relation to the organization and the broader global community. Often, malicious files with low prevalence are indicative of targeted malware and a targeted attempt at compromise and are typically missed by security teams. Prevalence analysis highlights these sorts of attacks, especially if correlated with other static or behavioral IoC's involving those systems as well.	· Some point-in-time technologies can look for Static IoC artifacts, but are not able to do it in real-time and often require time-consuming data collection before the IoC can be run. · May be able to show how many times or where malware has been seen but lacks relational information on root causes. · Not able to show the significance of the threat on prevalence. · If prevalence capabilities do exist, not able to do it real time or continue to track a specific file, process or even communication. · Not able to identify Behavioral IoC's.

Threat Hunting vs. Investigation

CONTINUOUS APPROACH	POINT-IN-TIME MODEL LIMITATIONS
· File Trajectory – Quickly understand the scope of exposure to malicious or suspect files based on time, method and point of entry; systems impacted; and prevalence. All, without the need to scan or snapshot endpoints. · Device Trajectory – Building on the level of scope provided by file trajectory, Device Trajectory provides robust time window analysis into system processes to understand root cause history and lineage with the ability to expand or contract the time window and filter to quickly pinpoint the exact cause of compromise. · Elastic Search – Elastic Search provides a fast and simple method of asking "Where else has this indicator been seen?" without the typical boundaries of relational database queries. Everything from host name, file name, URL, IP address to text strings can be searched across the entire dataset and across the global collective intelligence. Given the millions of files that are analyzed on a regular basis, it becomes a power tool for quickly hunting down advanced threats before it's too late.	· This is where traditional point-in-time detection technologies fall short. They fail to provide any post detection monitoring or contextual information. · Detections are often captured independent events added to an event-enumerated list. Yes, the list is updated continuously but without any contextual retrospection. · No ability to see events leading up to and after the detection. · Lack ability to fully analyze file for behavior and then quickly search across all endpoints for unique IoC's. · Some technologies may be able to provide limited scope capabilities, for example when and where the malware was detected based on event enumeration data, but they lack the ability to time window events leading up to and after compromise.

· File Analysis – First, it provides a safe mechanism to execute a file in a sandbox in order to fully analyze behavior and score the threat level of that behavior. Second, it provides the output of that analysis in detailed report. Third, all analysis results are added to the collective intelligence. And fourth, all analysis results are searchable via Elastic Search. Once again, security teams can quickly pivot from an indicator in a file analysis report to see where else in their entire enterprise this indicator may have been seen. This is critically important when an attack is targeted but uses a generic infection method.	· Traditional point-in-time forensic and investigation tools don't fare much better than their detection counterparts, even if they claim to be continuous. · Lack any advanced means of threat detection. Detection if combined with continuous contextual information can be an important starting point, but forensics tools are built for finding artifacts and clues not relationships. · Lack the ability to provide time-window visualization of events leading up to and after compromise. · Lack the ability to quickly search for unique IoC's without requiring all data be updated..

Outbreak Control vs. Containment

CONTINUOUS APPROACH	POINT-IN-TIME MODEL LIMITATIONS
· Simple Containment – Suspect a file is malicious? No problem and no waiting. Use the file's SHA256 to immediately block it on all, a group, or only one endpoint with a few mouse clicks. · Advanced Containment – Similar to Snort® scripts, advanced custom detections provide the ability to deal with families of malware without waiting for a signature update delivering Advanced Containment capabilities. · Application white and black listing – With rich contextual information the use of control lists for good applications being used as gateways for malicious activities or for specifically stopping suspected bad actor applications is much more manageable and effective as an extension of robust, continuous detection analysis and telemetry data. Security teams can quickly control a situation while standard procedures for response are engaged. · IP Black list – Similar to application control lists, IP blacklists can be more effectively used in the context of an actual event or corporate policies to control an outbreak and monitor endpoints for suspicious communications emanating from an endpoint. This is critically important in the breach scenario where any cross communication an attacker was using needs to be killed when the containment plan is executed.	· Point-in-time technologies are severely limited in their ability to contain malware or suspected malware because they're designed to focus on the point of detection not later in the attack continuum where containment is a critical requirement. · Some point-in-time detection technologies enable blacklisting of applications. This is a good method for containing applications that pose risk to an organization or suspicious applications that are not yet determined to be good or bad but should be blocked as a precaution. However, it is most effective when informed by a robust set of file and behavioral detection capabilities to do the primary functions of detection, analysis and containment. The primary reason is it becomes incredibly labor intensive to manage these technologies as a primary layer of protection and they are prone to missing attacks and are blind to attack chain activity. · Finally, point-in-time forensic and response tools are not built for rapid outbreak control required for the types of advanced threats seen today. They are useful in an investigation but are not able to pivot from data enumeration to containment action. This step often requires labor intense activity, which is typically avoided for the simpler, reimage approach.

4.14 | REV1