White Paper

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

What You Will Learn

The only way to defeat today's security threats is to address them holistically across the full attack continuum—before, during, and after an attack. Cisco's approach of continuous endpoint analysis in combination with a big data architecture is foundational to this model. Our innovations in advanced malware protection include:

- Continuous analysis
- Retrospection
- Behavioral indications of compromise
- Device and file trajectory
- Outbreak control
- Low prevalence

When these capabilities are combined in an integrated workflow, the real impact in malware detection, monitoring, analysis, investigation, and containment becomes apparent.

A New Model to Protect the Endpoint

Cisco 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 (formerly Sourcefire) had a vision for what would be required to combat advanced threats, and we pioneered the concept of continuous network discovery, which became foundational to next-generation intrusion prevention systems (NGIPSs). Today, targeted advanced malware and sophisticated attacks are relentless, compromising environments using new and stealthy techniques. Once again, Cisco is changing the way to think about security. We are building on our continuous capabilities and introducing a new model to combat attacks.

Continuous Protection in a World of Continuous Change

When Sourcefire (now part of Cisco) 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 tools took significant time to complete a full scan and were disruptive to the 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 More troublesome, because of the dynamic nature of networks, the data quickly became out of date, so the whole process would have to be run again and again.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 rife with blind spots and hard to correlate against live threat data.

Cisco 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, visibility could be tightly integrated with threat detection for the first time, changing the network threat defense conversation forever. Real-time network awareness became a key requirement for NGIPS, as defined by Gartner, and is our Cisco FireSIGHT™ technology.

In 2013, we 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, we are transforming a traditional point-in-time methodology into a continuous approach. This model:

- Fosters unique innovation in the battle against today's advanced threats
- Delivers visibility into compromise and attack persistence like never before
- Allows security teams to quickly and surgically contain and remediate infection without disrupting end users and security personnel
- Empowers 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 claims to be leading the next revolution in the detection of malware. Much akin to network scanners back in the day, each claims they offer more real-time and continuous protection than the others, when in reality they are 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, and using reputation-based application whitelisting to baseline acceptable applications from malicious ones. More recently, attack-chain simulation and analysis detection have come into play. But attackers understand the static nature of these security technologies and, predictably, 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 improvements over the "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 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 multidimensional and just as dynamic as the malware, taking into account the relationship between malware as well. We have to let go of the hope that an über-detection technology will make the problem go away.

What's needed is a truly transformational change in how we approach detecting advanced threats and breach activity. We need continuous protection and visibility from the point of entry through propagation and postinfection remediation.

A True Continuous Model Answers the Most Important 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 IoCs before they affect my organization?

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, the Cisco® Advanced Malware Protection (AMP) for Endpoints solution combines a continuous approach with a big data architecture to overcome the limitations of traditional point-in-time detection and response technologies.

In this model, process-level telemetry data is continuously collected while it is happening across all sources, and it is always up to date when it is needed. Analysis can be layered to work in concert to eliminate the impacts on control points and to deliver advanced levels of detection over an extended period of time. Analysis involves more than event enumeration and correlation; it also means weaving telemetry data together for greater insights into what is happening across the environment. Tapping into a broader community of users, Cisco 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. Detection and response capabilities are continuous and integrated, and go beyond traditional point-in-time methodologies.

Benefits of Continuous Analysis

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

Detection

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

But this is just the beginning of how Cisco'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 innovations in advanced malware protection, including:

- **Retrospection**: The ability to conduct analysis at an initial point in time and over an extended period of time is not limited to files. It also includes processes, communications, and other telemetry data, something traditional point-in-time models simply can't handle.
- **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 is missing in two-dimensional point-in-time technologies.
- **Behavioral indications of compromise (IoCs)**: These are more than static artifacts. They are complex behavioral clues that attack-chain weaving captures in real-time, and behavioral IoCs detect them as they are happening in real time.
- **Trajectory**: Trajectory is more than a fancy marketing term for tracking. Tracking produces an enumerated list of point-in-time events to show where something has been. "Trajectory" refers to the contiguous path on which an object, in this case malware, moves 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 IoCs is as simple as Googling your favorite style of takeout.

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

Figure 1 shows malware propagation with information about the point of entry, malware activity, and the affected endpoints.

Figure 1. Cisco AMP Network File Trajectory Screen

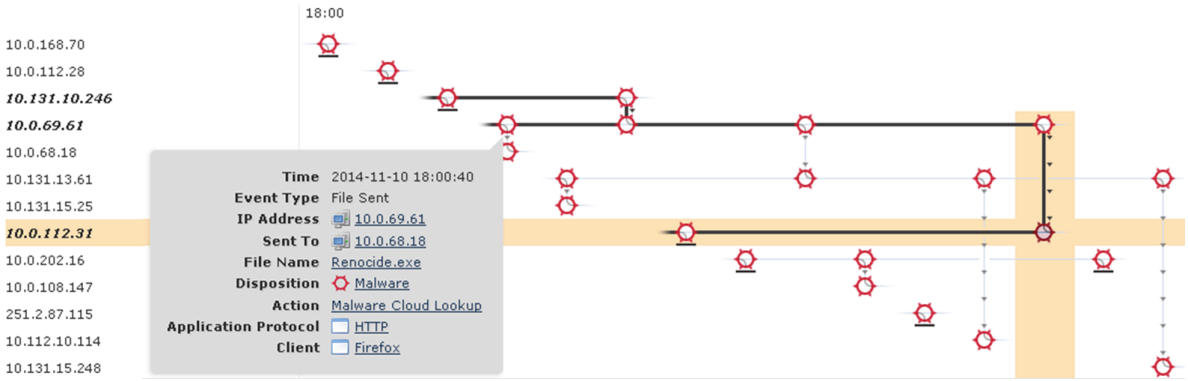
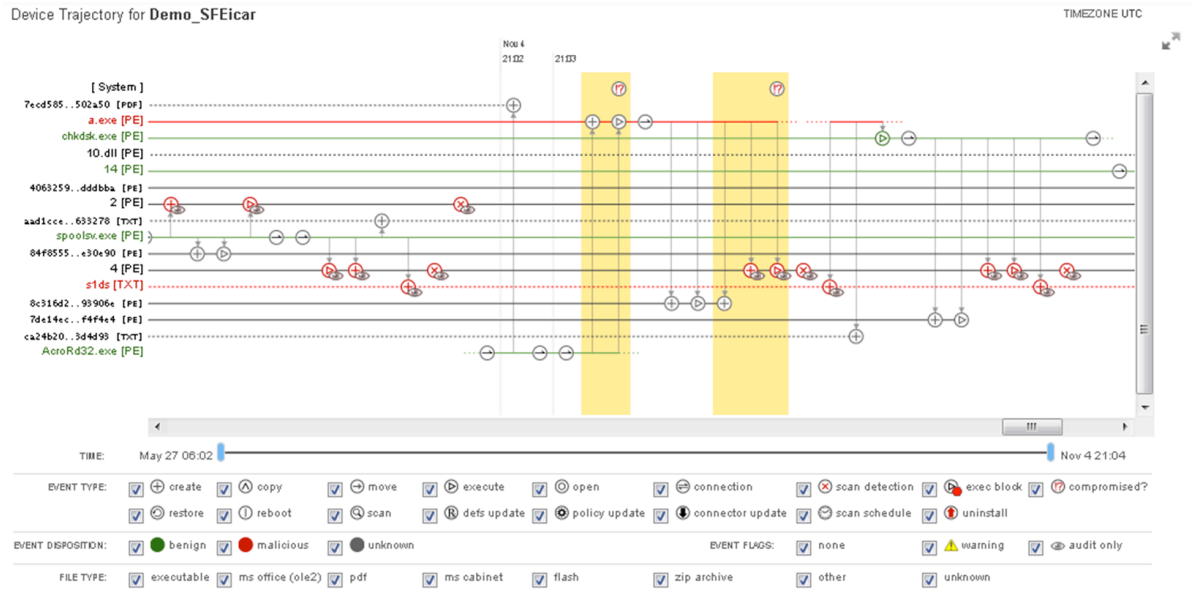


Figure 2 shows a device trajectory screen malware propagation with information about the point of entry, malware activity, and the binaries and executables affecting a specific endpoint. This information is correlated and shared between endpoints throughout the entire extended network and integrated with the network view in Figure 1.

Figure 2. Cisco AMP for Endpoints Device Trajectory Screen



Monitoring

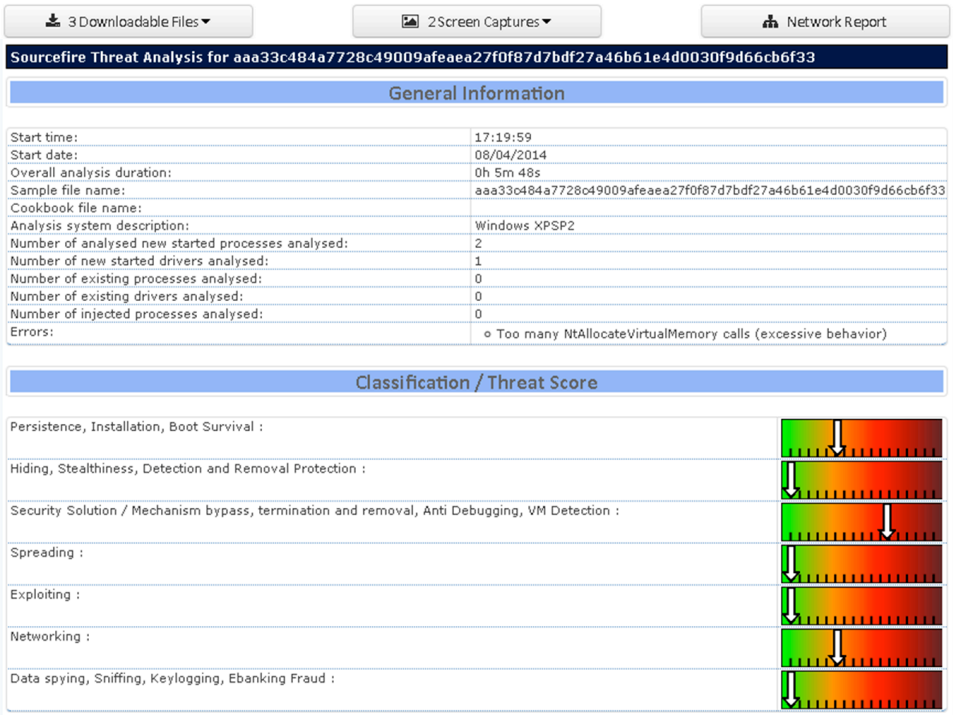
The ability to collect telemetry data from the endpoint and to analyze it for threat activity both as it occurs and over an extended period of time is a capability called retrospection. Cisco was the first to deliver this innovation. It's a major leap forward from event-driven data collection or scheduled 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 IoCs left behind by malware and exploits, as well as for more advanced behaviors of compromise that happen over time. Cisco's continuous approach delivers this level of automation through advanced behavior-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 the top areas of compromise and breach activity. With big data analytics and the use of continuous capabilities, patterns and IoCs can be identified as they emerge so that security teams can focus their efforts on the threats with the greatest potential for damage.

Figure 3 shows detailed information about file behavior, including the severity of behaviors, the original filename, screenshots of the malware executing, and sample packet captures. Armed with this information, you'll have a better understanding of what is necessary to contain the outbreak and block future attacks.

Figure 3. Cisco AMP for Endpoints File Analysis Screen



Threat Hunting vs. Investigation

Without the context and capabilities of a continuous approach, 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 little contextual evidence. Often, the hardest question to answer is: "Where do we start?" In a continuous approach, investigations can be faster, more targeted, and more productive.

A continuous approach shifts from a search for elusive facts and clues to a very focused hunt for breaches based on actual events like malware detections and static and behavioral IoCs. Continuous capabilities backed by a big data architecture enable all data to be easily searchable anytime and all the time. In a continuous model that uses the capabilities previously 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 capability to identify a time window for the hunt, expand or contract that window, and pinpoint and pivot the hunt with filters. This capability 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

Investigation can seem overwhelming if it is 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. 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 visibility that 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 that is experiencing severe compromise, all the detection and telemetry data is still preserved, and containment can still be enacted to prevent future compromise by attackers using the same infection gateway.

Lastly, traditional point-in-time technologies sometimes fail even to detect an attack, and an organization can be 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 apply: "Where do we start, and how bad is the situation?" However, responding to and containing the attack in this outbreak scenario often involves understanding the scope and root causes very quickly without tipping your hand to attackers. Quickly shutting down all points of compromise and infection gateways simultaneously is critical to preventing an attacker's lateral movements.

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 important, establish a containment profile that can be flipped on instantaneously. Advanced behavioral detection, tracking, and visualization begin immediately, but unlike the processes in a detect-and-protect scenario, they are all in audit mode. They are still detecting and alerting, but instead of actively blocking malware, they are capturing evidence like detectives on a stakeout who are gathering information for the SWAT team to swoop in and close down the operation.

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

Integration and Reporting

Cisco AMP for Endpoints is designed from the ground up to support a continuous approach and big data architecture. It uses a cloud model to enable a lightweight connector instead of a heavy agent architecture at the endpoint. The connector is 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 endpoints and users. This model frees up resources so that the connector can 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.

The 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 Cisco Collective Intelligence Cloud. Sharing intelligence in real time helps security teams stay ahead of broad attacks that use techniques like phishing, in which many users could be infected with the same initial payload but then receive different subsequent downloads or commands. Going beyond file data analysis, other telemetry data can be analyzed across control points to more accurately determine the scope of an outbreak.

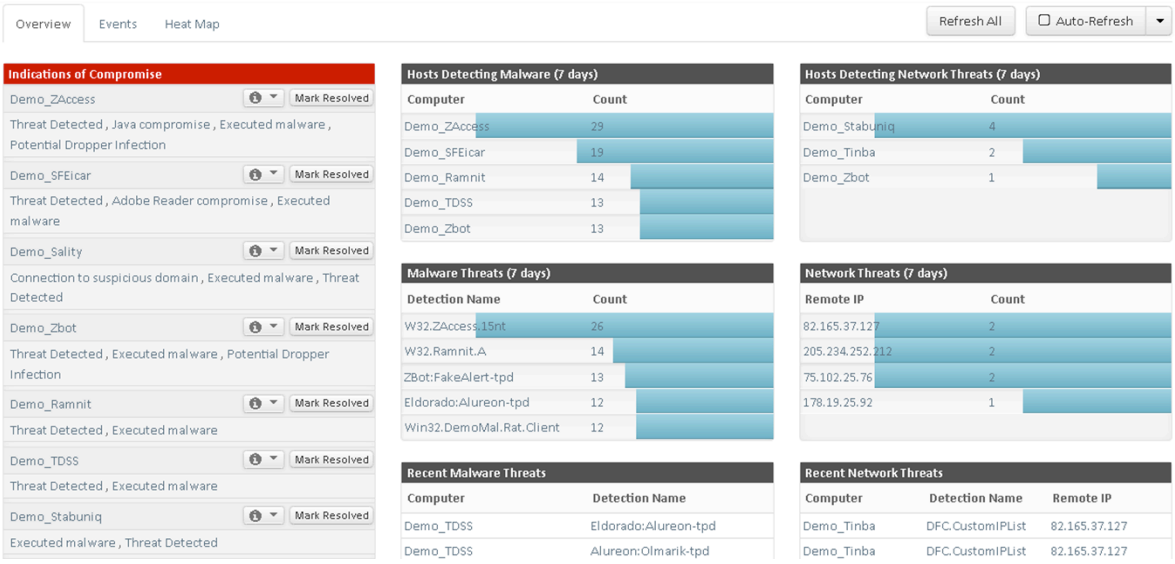
Once in the cloud, the depth of telemetry information collected across control points can be shared with all control points to provide contextual information equally, even at control points that might not be able to collect that level of information. For example, telemetry data and behavioral detections collected from an endpoint can be used by network security teams 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 picture to security teams than is possible with generic alert data. Endpoints that have activated the malware are going to have a higher priority than those that merely downloaded 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 the typical simple list of events that may or may not be actual threats.

A continuous approach extends to reporting capabilities as well. No longer are reports limited to event enumeration and aggregation. They can include actionable dashboards and trends that highlight business relevance and possible risks. Although point-in-time technologies can also provide dashboards and risk relevance, they typically require an additional layer of complexity in the way of security intelligence and event management (SIEM) 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 important, prioritization when and where you need it.

Figure 4 shows Cisco AMP for Endpoints actionable dashboards and trending that highlights business relevance and impact from a risk perspective. Reports are not limited to event enumeration and aggregation. In this view, we see prioritized indications of compromise, hosts detecting malware, and network threats among other data.

Figure 4. Cisco AMP for Endpoints Dashboards



Conclusion: It's True, 1 + 1 Doesn't Equal 3.Sometimes It Equals 6

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, processes, and communications 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 looks at behaviors over time.** Combining big data analytics and continuous capabilities to identify patterns and IoCs as they emerge helps enable security teams to focus their efforts on the threats that matter most.
4. **Investigation that turns the hunted into the hunter.** Transforming investigations into focused hunts for threats based on actual events and IoCs 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 that the continuous approach provides combined with the ability to target specific root causes.
6. **Dashboards that are actionable and contextual.** Reports that are based on the pervasive collection and advanced analytics of file and telemetry data across control points—and then overlaid with contextual information—highlight trends, business relevance, and the impacts on risk.

Building on our pioneering efforts in continuous capabilities and coupling those with a big data architecture, Cisco 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.

Comparing the Continuous Approach with the Point-in-Time Model

What follows are detailed comparisons of capabilities that differentiate a continuous approach from a point-in-time model. The descriptions also cover enhancements to detection as well as innovations in advanced malware protection.

Table 1. Detection

Continuous Approach	Point-in-Time Model
• An integrated lattice of engines can work in concert, sharing context for improved detection capabilities. • Behavioral methods of detection, like sandboxing, are optimized by reducing workloads and latency, and eliminating the need to sandbox every new file. • Detection is performed over an extended period of time, which is exactly how attacks unfold—over time. • The audit mode is transformed from a simple tuning parameter used to reduce false positives to an incident response collection tool to capture real-time activity without tipping off attackers. • Detection intelligence is shared collectively and instantaneously across multiple control points.	• Engines, if there is more than one, work as a stack, operating serially and independently, which reduces efficacy and slows performance at the endpoint. • Vendor updates are required, which take time and create additional gaps in security.

Table 2. Monitoring

Continuous Approach	Point-in-Time Model
• File retrospection: After the initial detection analysis, a file continues to be interrogated over an extended period of time with the latest detection capabilities and collective threat intelligence. An updated disposition can thus be rendered and further analysis can be conducted well beyond the point in time the file 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: Communications to and from an endpoint are continuously captured, as are the associated application and process that initiated or received the communication. This information provides added contextual data as part of attack-chain analysis and behavioral IoC detection. • Attack-chain weaving: Cisco AMP for Endpoints does more than retrospection; it introduces a new level of intelligence by 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.	• No retrospection: The model is blind to the relational activity at the endpoint beyond detection activity. • The model is also completely blind to anything that happens within the network after malware has crossed the control point.

Table 3. Automated Advanced Analytics

Continuous Approach	Point-in-Time Model
• Real-time response: Because endpoint telemetry data is continuously collected and added to the data store, it can be automatically compared with static and behavioral IoCs. The time to detection of either a static or a behavioral IoC can thus be dramatically reduced. • Behavioral Indications of Compromise (IoCs): Using attack-chain weaving, behavioral IoCs look for sophisticated patterns of activity across detection events, static IoCs, and telemetry data that indicate potential compromise. A classic example is a dropper that has slipped through initial detection. • Attack-chain weaving: Attack-chain weaving also records what happened leading up to and following the triggered behavioral IoC. 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 IoCs: With open IoCs, customers can use their custom static IoC-detection lists. • Intelligence-based IoCs: More than static intelligence, blacklists, or detection scripts, these IoCs are based on behavioral algorithms that look for specific malicious actions and related actions over time. Intelligence-based IoCs are developed and fully supported by the Cisco Talos Security Intelligence and Research Group. • Prevalence: An advanced analysis engine 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. These are typically missed by security teams. Prevalence analysis highlights these sorts of attacks, especially if correlated with other static or behavioral IoCs involving those systems.	• Some point-in-time technologies can look for static IoC artifacts, but they are not able to do so in real time, and they often require time-consuming data collection before the IoC can be run. • This model may be able to show how many times or where malware has been seen, but it lacks relational information on root causes. • The significance or prevalence of the threat is not shown. • If prevalence capabilities do exist, they cannot be implemented in real time, nor can they continue to track a specific file, process, or even communication. • Behavioral IoCs cannot be identified.

Table 4. Threat Hunting vs. Investigation

Continuous Approach	Point-in-Time Model
• File trajectory: The scope of exposure to malicious or suspect files is quickly understood with the time, method, and point of entry; the affected systems; and the prevalence—all without the need to scan or snapshot endpoints. • Device trajectory: Building on the level of scope provided by file trajectory, the device trajectory provides a robust time-window analysis into system processes to understand root cause history and lineage. It can also 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, and IP address to text strings can be searched across the entire data set and across the global collective intelligence. Given the millions of files that are analyzed on a regular basis, it becomes a powerful tool for quickly hunting down advanced threats before it's too late. • File analysis: First, the model provides a safe mechanism to run 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 a detailed report. Third, all analysis results are added to the collective intelligence. And fourth, all analysis results are searchable with 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.	• This is where traditional point-in-time detection technologies fall short. They fail to provide any postdetection monitoring or contextual information. ◦ Detections are often captured independent events that are added to an event-enumerated list. Yes, the list is updated continuously but without any contextual retrospection. ◦ There is no capability to see events leading up to and after the detection. ◦ There is no capability to fully analyze files for behavior and then to quickly search across all endpoints for unique IoCs. • Some technologies may be able to provide limited capabilities (for example, to determine 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 following the compromise. • Traditional point-in-time forensic and investigation tools don't fare much better than their detection counterparts, even if they claim to be continuous. ◦ They 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. ◦ The lack the ability to provide time-window visualization of events before and after a compromise. ◦ They lack the capability to quickly search for unique IoCs without requiring all data to be updated.

Table 5. Outbreak Control vs. Containment

Continuous Approach	Point-in-Time Model
• Simple containment: Do you suspect a file is malicious? No problem and no waiting. Use the file's SHA256 (secure hash algorithm) to immediately block it on all endpoints, a group of endpoints, or only one endpoint, with a few mouse clicks. • Advanced containment: Similar to Snort® scripts, advanced custom detections provide the capability to deal with families of malware without waiting for a signature update. • Application white- and blacklists: With rich contextual information, control lists can be used to more effectively determine whether good applications are being used as gateways for malicious activities and to stop suspected bad actor applications. These lists extend the continuous analysis and telemetry data. Security teams can quickly control a situation while standard procedures for response are engaged. • IP blacklist: Similar to application control lists, IP blacklists can be more effectively used in the context of an actual event or in corporate policies to control an outbreak and monitor endpoints for suspicious communications coming from an endpoint. This capability is critically important in the breach scenario where any cross-communication an attacker was using needs to be killed when the containment plan is implemented.	• 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 a 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, blacklisting is most effective when it is informed by a robust set of file and behavioral detection capabilities to do the primary functions of detection, analysis, and containment. The primary drawbacks are that managing these technologies as a primary layer of protection becomes incredibly labor intensive, and that 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 the rapid outbreak control that is required for the types of advanced threats seen today. They are useful in an investigation, but they are not able to pivot from data enumeration to containment. This step often requires labor-intensive activity, which is typically avoided for the simpler reimage approach.

For More Information

To learn more about the Cisco approach to security, email us at ciscosecurityinfo@cisco.com or call 800 553-6387.

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 C11-733649-00 02/15