SOLUTION BRIEF

How Cyphort Advanced Threat Detection Helps Close Critical Security Gaps

A Technical Overview of the SmartCore Analytics Engine

In the battle to combat advanced, dynamic malware, security teams continue to adapt their defenses. The problem is that cyber attackers continue to advance their approaches as well—and so the breaches continue. This solution brief shows how the Cyphort Anti-SIEM software platform—and specifically its SmartCore analytics engine—helps close the critical gap inside the network exploited by cyber attackers today. The brief offers a detailed look at Anti-SIEM and SmartCore, revealing how the solution's unique combination of threat detection, data correlation, behavioral analysis, and machine learning enables customers to establish persistent safeguards against today's dynamic attacks.

Introduction: The Evolution of Threats and Defenses

In years past, a familiar pattern emerged in the cyber security landscape. Defenses were erected, and soon new malware was being devised to circumvent those defenses. Once new or enhanced systems were employed, new malware emerged to circumvent the new defense—and the cycle continued.

While the cycle has been referred to as a cat and mouse "game," the stakes are high, particularly as nation states and well-funded cyber-criminal organizations apply increasing resources and expertise to their attacks. As a result, the task of detecting and stopping malware continues to get tougher.

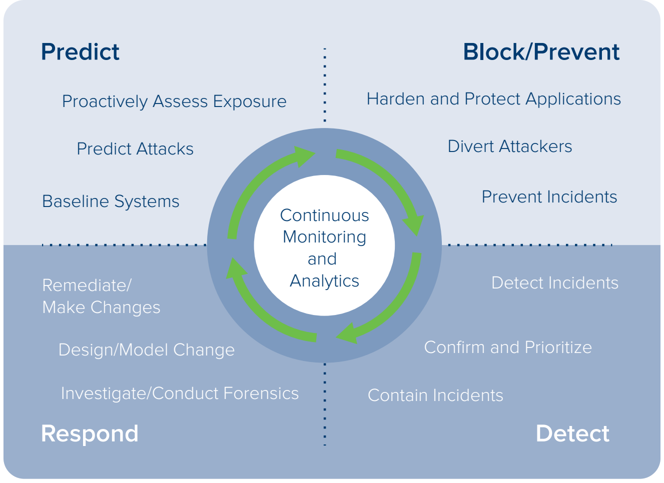
As the sophistication of attacks grows, malware exhibits constantly evolving attributes that enable it to evade static signatures or rule-based approaches. In the past, for example, when malicious emails were found that were sent from a particular domain, the domain could be blacklisted or blocked by an anti-virus platform. Today, however, attacks are too dynamic for static, rules-based approaches like URL blacklists to offer any real protections.

Understanding the Gaps in Security Defenses

Limitations of In-line Defenses

To help organizations strengthen their security posture, analyst firm Gartner has described the attributes of an adaptive security architecture, which is comprised of four key capabilities (or layers): prevent, detect, respond, and predict.[1] The key intent of the Gartner model is to clearly define the components of a strong security defense, underscoring the fact that no single approach is sufficient. Organizations need to take a comprehensive approach to security that goes well beyond a prevention layer to establish strong defenses.

At the prevention layer, organizations have come to rely on a range of in-line defenses, such as firewalls, secure web gateways, and intrusion prevention systems (IPS), and these mechanisms are proving to have limitations. While the specifics of these in-line technologies vary, at a high level these systems apply a pre-defined set of rules to make immediate decisions as to whether to block or allow a specific transmission or object.



Gartner Adaptive Security Architecture[1]

[1] Gartner, "Designing an Adaptive Security Architecture for Protection From Advanced Attacks," Neil MacDonald and Peter Firstbrook, January 28, 2016, ID: G00259490, URL: https://www.gartner.com/doc/reprints?id=1-279SLRJ&ct=150109&st=sb

Given the time-sensitive nature of so much of today's network traffic, the reality is that in-line detection tools have very limited time to do their inspection and determine whether or not a given transmission or object is malicious. Even brief delays can result in a degraded network performance and user experience. Consequently, these defenses can't do more exhaustive analysis, and notably, can't run any potentially malicious code and inspect its behavior. Most in-line defenses typically have less than a tenth of a second to decide, which is not enough time for the behavior of malware to be run, monitored, and detected. This lack of behavioral analysis is posing an increasingly significant obstacle.

Cyber criminals have continued to evolve their malware with increasing rapidity. In fact, the Verizon 2016 Data Breach Investigations Report stated, "Analysis of one of our larger datasets showed that 99% of malware hashes are seen for only 58 seconds or less. In fact, most malware was seen only once. This reflects how quickly hackers are modifying their code to avoid detection.[2]"

In-line defenses that rely on rules and signatures can only capture malware that has already been identified and disseminated repeatedly. As the report above indicates, those types of attacks are starting to be very rare indeed.

However, while the static binaries of malware are constantly changing, the behavior of malware is remarkably consistent. Ultimately, attackers have similar objectives, that is, surveillance, the capture and theft of data, and so on.

Limitations of Sandboxes

In recent years, many organizations have augmented in-line defenses with sandbox-based approaches. At a high level, these systems take potential malware and run it in an isolated laboratory environment meant to mimic the platform of an end user. As the code is run in the sandbox, security analysts or automated monitors may be employed to inspect behavior, flagging such activities as the modification of a registry, the execution of a new script, communications with a command-and-control server, and so on. If malware is detected in the sandbox, the system will update rules so that the same malware will be blocked the next time it surfaces.

Limitations in these approaches occur because they inherently rely on static rules to detect malware. Malware authors are increasingly adept at circumventing these static risk indicators. Further, many solutions are ultimately reliant on analysts, who are inherently limited in terms of the number of details and behaviors they can observe, and in how fast they can process their analysis and findings. For example, an analyst may miss the fact that an executable is saved into a temporary folder and run in the background.

The Four Categories of Malware: What's Being Stopped and What's Not

In assessing your organization's security, it's important to map the categories of malware that may be employed by threat actors, and what types of defenses are equipped to detect or stop them.

Following is a high-level breakdown of the different forms malware can take and the types of solutions that can stop them:

- **Known.** These are effectively the same malware objects that existing defenses have captured, identified, and established defenses against. In-line detection systems can block these known threats. However, as outlined above, serious malware authors have pretty much completely moved away from reusing malware in this way.
- **Repacking.** Malware authors often repack their existing code sets. When executing a repacked sample, it will behave the same as the original; however, the code streams themselves differ, which can enable them to evade detection by some anti-malware systems. Traditional anti-virus solutions can detect some repacked code. However, if a system relies solely on doing pattern matching on the static code, the bytes will be different enough to evade detection.
- **Variant.** This is malware that's part of an existing family, but that will behave differently when executed. Sandbox-based solutions can catch some of these malware variations. Also, some solutions that employ static code analysis can identify patterns in bytes of code to detect some malware variants.
- **New family.** This represents a new set of malware code that looks and behaves in a fundamentally different way from prior families. No traditional in-line detection systems or sandboxes are equipped to catch these new families.

Cyphort Advanced Threat Detection and SmartCore Analytics

Cyphort offers a solution that enables organizations to address a critical gap in their security defenses. The Cyphort Anti-SIEM solution includes integrated advanced threat detection technologies which, in combination with SmartCore analytics, enables your organization to detect and stop not only repacked and variant malware—but entirely new families of malware.

The Anti-SIEM doesn't rely on the static content analysis or rules that are proving increasingly vulnerable to evasion. Instead, the solution uses a distributed software layer to capture information from a range of important network, endpoint, and cloud sources, establishing a holistic, comprehensive security fabric in the environment. Instead, it is built with patent-pending technology that provides continuous, multi- stage analysis of web and email traffic, as well as traffic

[2] Verizon, "2016 Data Breach Investigations Report," page 48, URL: www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

traversing the network laterally. Also, the solution features open APIs that enable you to automatically update your existing in-line defenses with new threats as soon as they are discovered.

The Power of SmartCore

SmartCore continuously collects and correlates data from multiple sources, then employs a combination of behavioral analysis plus machine learning to identify virtually all categories of previously undetected malware. While many vendors are starting to capitalize on the advantages of machine learning, Cyphort harnesses this approach in a fundamentally unique way. The SmartCore multi-stage data correlation and threat analysis engine leverages machine learning in combination with advanced behavioral analysis. Cyphort collectors and the SmartCore engine are deployed across the customer environment—including on virtual machines (VMs), commercial servers, or in the cloud—where samples are continuously collected and inspected to detect malware.

In the fall of 2016, a new malware attack that came to be named TrickBot was discovered and analyzed. Through this analysis, malware researchers found there was a strong connection to the Dyre Banking Trojan, but that the malware was rewritten from scratch. While this new variant hadn't made it into Cyphort customer environments, the threat research team at Cyphort ran the malware in their labs, using the same version of SmartCore deployed in customer environments. By identifying the programming techniques that characterize malware, SmartCore immediately detected the malicious nature of this code, even though it represented an entirely new malware family. This is a pattern that has been repeated consistently whenever new malware families are discovered.

The Benefits of the Anti-SIEM

Cyphort has put the "S" back into the SIEM, making it a powerful security platform. Organizations can realize many significant advantages:

- **Stop new malware.** Gain immediate protection against malware, whether it's known or an entirely new malware family. Further, because this intelligence is employed on the product, there's no lag time between the discovery of an exploit and the ability to gain protection against it.
- **Optimized detection accuracy.** The combination of behavioral analysis plus machine learning enables deep inspection of large numbers of attributes, and in-depth correlation of this intelligence. This intelligence is used to establish optimized classifier models, which are continuously updated via Cyphort's cloud-based GSS service. Through these capabilities, the solution continues to maximize detection accuracy while minimizing false positives.
- **Leverage investments.** Close critical security gaps, while at the same time strengthening the security realized from your existing in-line defenses, including network security devices and endpoint security systems. As a result, an investment in Cyphort means you address a critical security gap and maximize the value of many of your existing systems.

Process: How the Anti-SIEM Leverages SmartCore

Collection and Inspection

The Anti-SIEM uses virtual collectors at critical points across the distributed enterprise. These collectors capture web and email transmissions and traffic traversing laterally in a network. These collectors then feed this information to the SmartCore analytics engine, which employs a multi-stage analysis process. SmartCore inspects content, such as the bytes of an object, whether it's a document file, or it's an executable.

Behavioral Analysis

As opposed to time-constrained in-line devices, SmartCore can do a rigorous analysis of suspicious data and objects. The SmartCore engine features a multi-stage analysis process. For example, it can open files in associated applications and OSs, such as opening a document in a word processing program. If it's an executable or script, the engine will initiate the code. SmartCore then logs and records all the actions and behaviors that the code exhibits. The engine will track such aspects as a piece of memory being allocated, a registry item being queried, a file being opened, and much more.

Machine Learning

The SmartCore engine then applies machine learning to the extensive behavioral and attribute data captured. Through the use of extensive algorithms and processing power, the machine learning functionality can far surpass the analysis capabilities of any individuals or teams, both in terms of depth, breadth, and speed. SmartCore's algorithms and classifiers were developed based on the analysis of hundreds of specific attributes and hundreds of thousands of unique samples, including both benign and malicious code. The resulting machine learning classifiers are part of the SmartCore engine that is deployed in the customer environment.

As new samples emerge, they are fed into the machine learning engine's classifiers, where automated, extensive analysis is run to determine whether the code is benign or malicious. Further, the classifiers are continually optimized to improve detection accuracy rates, while minimizing false positives.

Through machine learning, SmartCore looks for direct and indirect indicators of compromise. Following is more on each of these indicator types.

Direct Indicators of Compromise

These can be considered traditional indicators of compromise. For example, it's long been observed that benign applications typically use MFC (Microsoft Foundation Classes) and other high-level programming abstractions, while malware most commonly only uses Win32 APIs. The creation and execution of a file in a temporary folder is one of the common traits of malware. While the benign code may perform these tasks, malware tends to do so with much higher regularity.

Also, there are specific function calls that are used in Windows environments to enumerate all the processes currently running on the system. The latter command serves two purposes for malware: identifying which processes are running and available to target, and to see what security monitoring capabilities may be running, so they can be evaded. Many benign applications won't take this step; they'll just start running.

Indirect Indicators of Compromise

Seasoned poker players will often look for so-called "tells," distinct mannerisms that indicate their opponents may have a strong hand or be bluffing about a weak hand. Indirect indicators of compromise can be viewed as tells in the cyber security arena, the behavioral flags that point to the malicious nature of a piece of code. To find these indirect indicators, SmartCore looks at a range of aspects:

- How many memory allocations were made?
- What is the average memory size allocated?
- What's the standard deviation of memory size?
- What is the granularity of rules assigning memory allocation?
- What percentage of calls was made to create files compared to instruct a process to sleep?
- What was the percentage of calls to a particular function?
- Are small chunks of memory allocated frequently or big chunks allocated infrequently?
- How many memory allocations are pinned?
- And much more

By analyzing this kind of abstract behavioral information, SmartCore ascertains how programs are run and the kinds of programming techniques that have been employed. As with the direct indicators of compromise, any one of these attributes isn't an absolute sign of malware. However, by classifying all these attributes and the patterns evidenced, clear indications emerge. For example, while making a call to a specific function in and of itself doesn't mean it's malware, the call represents one factor, but if the call is made with a certain frequency or sequence, it can provide a strong indicator of malware.

By feeding this intelligence into the machine-learning engine, Cyphort developers saw detection accuracy improve significantly. SmartCore's machine learning classifiers can correlate these subtle and numerous behavioral attributes and detect malicious samples. Ultimately, what was found is that malware developers use very different techniques and approaches than developers of benign programs. SmartCore can capitalizes on this fact, establishing a fast, highly effective way to analyze code and determine if its malware.

Cyphort Differentiators

By leveraging a unique combination of behavioral analysis and machine learning, the advanced threat detection capabilities, in combination with SmartCore analytics, helps close the critical visibility gaps left by traditional solutions. Following is a summary of the key differentiators:

Compared to In-line Prevention

In-line prevention tools just have time to compare content against existing rules and determine whether to block or allow a specific element. By contrast, Cyphort observes and detects malware based on its behavior, which is much harder for malware authors to change than its "looks."

Compared to Sandboxes

Rather than employing the static rules of sandboxes, Cyphort employs continuously updated machine learning models and combines them with the behavioral intelligence that gets captured. This enables the Anti-SIEM to detect new malware families that sandboxes miss.

Compared to Machine Learning

The detection capabilities of the Anti-SIEM fully leverage the value of machine learning as compared to other vendors. For example, some AV vendors are funneling data captured at end points into a machine-learning environment within their internal labs. Based on this machine learning, the AV vendor may then generate new rules and signatures, and use them to update the products employed in customer environments. However, these approaches still pose some disadvantages:

- This machine learning isn't embedded within the in-line inspection processes being employed. The results of machine learning still need to be analyzed and interpreted by staff members, who are then tasked with initiating the product updates required.
- Ultimately, these approaches don't fundamentally address the potential delays that can occur between the detection of a threat and the implementation of the updates needed to combat the threat. Further, because they require ongoing efforts of staff members, they're susceptible to delays, mistakes, and oversights.

In contrast, the SmartCore engine employs machine learning within its immediate threat analysis processing, which occurs within the customer environment. The result is that the Anti-SIEM delivers an unparalleled ability to offer fast, actionable protection and insights.

Cyphort Advantages

Cyphort customers can realize a significant number of advantages when they implement the Anti-SIEM to gain actionable insight into security incidents:

- **Powerful insights.** Delivers rich contextual intelligence that fuels fast, effective response. The solution helps security teams identify malware earlier in the cyber kill chain and get the context needed to understand where it has spread, so they can prioritize response and effectively limit any potential damage.
- **Extensive automation.** Fully automated, and not reliant on laboratory teams to track environmental variables, analyze new samples, or build new rules. Because the solution's not as susceptible to human oversights and delays, Cyphort offers significant advantages in reliability and scalability.
- **Imperviousness to reverse engineering.** Over the years, malware authors have become adept at detecting the approaches of security systems being used and developing tactics to evade them. However, the proprietary algorithms and classifiers used in the SmartCore engine's machine learning processing can't be readily dissected and understood. There isn't any simplistic formula that an attacker can uncover that details exactly what mix of attributes may trigger a positive determination in the SmartCore engine. Fundamentally, changing how malware behaves isn't a trivial effort. While it can be easy to create dynamically generated domains to bypass URL blacklists, for example, it's much more difficult for malware authors to change their underlying programming approaches, behaviors, and objectives.
- **Immediate detection.** Through the SmartCore engine and its powerful machine learning capabilities, Cyphort has discovered that malware behaves in a fundamentally different manner than benign applications—and these differences are detectable as soon as code starts running. With the Anti-SIEM solution and SmartCore analytics, these differences can be detected immediately. Over the years, in their ongoing efforts to enhance the product, the Cyhport development team has periodically tested varying intervals of behavior observation. For example, they've run extensive tests and tracked the results depending on whether code behavior was tracked for 15 seconds, 30 seconds, one minute, or two minutes. While the platform could keep capturing more observational data the longer it ran, staff scientists found that overall efficacy in malware detection didn't change. Ultimately, malware is consistently discovered within 15 seconds.

Conclusion

Today, malware is constantly evolving, leaving static rules-based defenses, well, defenseless. By delivering a unique combination of behavioral analysis and machine learning, the SmartCore analytics engine provides a fundamentally differentiated solution that addresses a critical vulnerability in most organizations today.

To understand more about the Anti-SIEM, all of the components and features of SmartCore, and its value to your organization, be sure to visit the resources section on the website. To arrange a demonstration, please call us at 1-408-841-4665 or email info@cyphort.com.

About Cyphort

Cyphort is a privately held cybersecurity company founded in 2011 and based in Santa Clara, CA. The company provides SMB and enterprise customers with the Anti-SIEM, an open, scalable software platform that combines advanced threat detection, analytics, and mitigation capabilities. The solution minimizes the cost and complexity of traditional SIEMs, while delivering immediate, actionable insight into security incidents for fast threat resolution. www.cyphort.com

CYPHORT

5451 Great America Pkwy, Suite 225, Santa Clara, CA 95054 | P 1.408.841.4665 | F 1.408.540.1299 | info@cyphort.com
Sales/Customer Support P 1.855.862.5927 | F 1.408.540.1299 | support@cyphort.com