USE CASE

How the Anti-SIEM's Integrated Detection Fabric Provides Advanced Threat Defense for Highly Distributed Organizations

Executive Summary

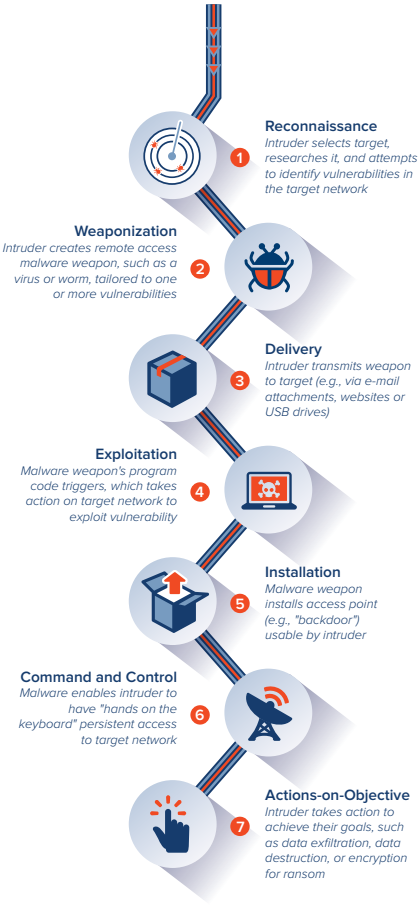
Most large organizations have employees distributed across multiple office locations. This can make it difficult for security teams to create a distributed, multi-site security architecture that can be managed as a single system. This use case looks at how the Anti-SIEM solution can protect distributed organizations against evasive advanced attacks that bypass the first line of defense.

The Challenge: Advanced Cyber Attacks and Their Growing Damage

Sophisticated cyber criminals continue to target organizations around the world. According to the Verizon 2017 Data Breach Investigations Report[1], 75 percent of data breaches are attributed to external actors, and 73% of attacks were financially motivated.

The crux of the issue is that cyber attackers continue to employ evasive, multi-pronged attacks, and security teams are often unable to prevent these threats with the tools in their traditional first line of defense (firewalls, IPS, secure web gateways, etc.).

Once they gain access to the internal network, today's targeted and highly sophisticated advanced persistent threats (APTs) typically move through the seven stages of the cyber kill chain as attackers pursue their objectives of stealing sensitive data. Most often, malware is delivered via email or web traffic (or a combination of both), and once a host is compromised, malware is spread across a network laterally. Ultimately, communications with a command-and-control server are established, which enables the attacker to pursue their objectives of surveillance and theft.



Summary of the Seven CKC Phases

Customer Problem

While these approaches are well understood, security teams are hard-pressed to stop them – especially when trying to protect thousands of employees across many different locations. Part of the problem is the static, rules-based nature of many of the defenses currently in place. Over the years, organizations have come to rely on a

1 Verizon, "2017 Data Breach Investigations Report. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/2

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

Cyber criminals continue to evolve their malware with increasing rapidity to evade security defenses. In fact, the 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 the packaging of their code so it 'looks' different enough to avoid detection.[2]"

Quite simply, 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.

Further, if and when a threat is detected, these defenses lack the more cohesive visibility needed to collect, correlate, and analyze traffic from Web, email, and lateral spread sources to understand where a given attack is within the cyber kill chain. This makes it difficult for security staff to identify which steps to take to mitigate the damage most effectively.

The Solution: The Detection Fabric within the Anti-SIEM

Cyphort's Anti-SIEM combines advanced threat detection, comprehensive threat analytics, and one-touch threat mitigation into an open, distributed software platform that addresses time, cost, and complexity challenges associated with traditional SIEMs. The detection fabric within the Anti-SIEM uses machine learning and behavioral analysis technologies to detect advanced threats in web, email, and lateral spread traffic. Threat data is correlated with event and log data collected from other security devices in the network. Results are consolidated and presented as a timeline view of each security incident. One-touch mitigation can contain breaches and strengthen existing tools. The Anti-SIEM works with or without an existing SIEM to reduce noise, improve productivity, and accelerate response.

Benefits

Cyphort's Anti-SIEM equips your organization with a number of unparalleled advantages:

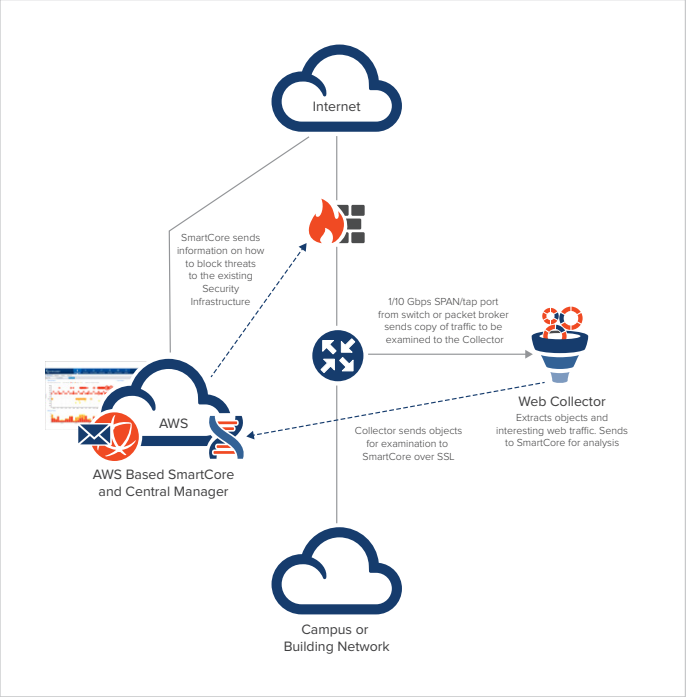
- **Distributed architecture, centralized management.** It is designed for fast, scalable deployment across virtually any number of locations, offering customers the flexibility of leveraging VMs, commercial servers, and cloud resources to ensure all locations and all users are protected against advanced threats from web and email channels.
- **Continuous protection.** It continuously collects and correlates data from multiple sources throughout the network, then employs a combination of behavioral analysis plus machine learning to identify virtually all categories of malware, including malware variants and entirely new malware families.
- **Scalable, flexible deployment.** Its deployments feature the SmartCore analytics engine and Cyphort collectors, which are used to capture and forward files and URLs to the SmartCore engine. It supports flexible implementation options, so your organization can implement the solution in a manner that's well-suited to your objectives and infrastructures.
- **Easy integration.** Its open architecture enables organizations to leverage the threat intelligence that gets captured. For example, when Cyphort captures intelligence on a new threat, you can automatically update other tools within your security architecture so they can block future attacks. The list of these tools includes firewalls, secure web gateways, intrusion prevention systems, and endpoints. The solution also integrates with network access control (NAC), content access service brokers (CASB) and security information event management platforms (SIEM).
- **Consolidated analytics.** Its open architecture allows it to ingest information (e.g. alerts and event data) from virtually any security tool in the network, then correlate all disparate data into a single consolidated, contextual view of the malicious incident across hosts and users.
- **Usage-based pricing.** It's purchased under an aggregate bandwidth pricing subscription model, which means your organization only pays for what it's using, regardless of how many locations you may be supporting.

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

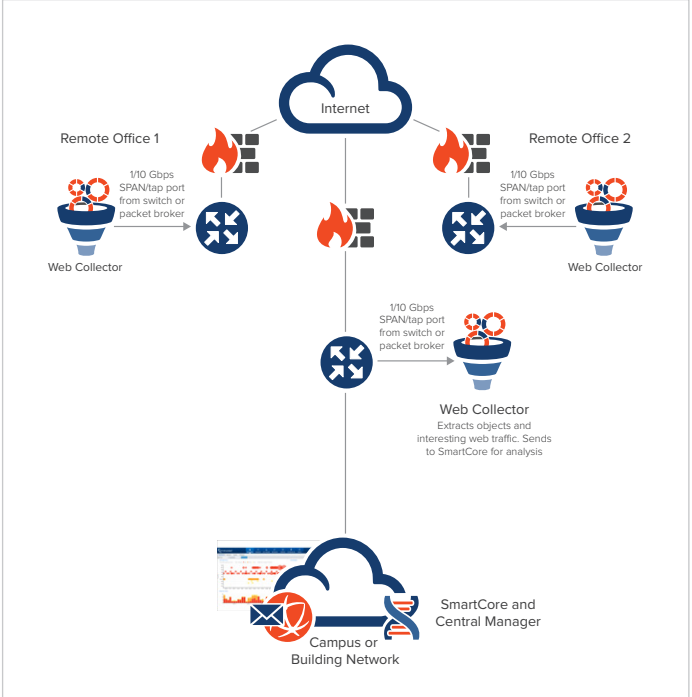
Deployment Options

The Anti-SIEM's SmartCore engine and collectors can be run on a range of systems, including general-purpose appliances, virtualized servers, and in private and public clouds. As a result, you can cost-effectively scale your deployment as workloads dictate.

Single Site AWS-Based SmartCore



Multiple Sites On-Premises SmartCore



Conclusion

With the Anti-SIEM, security teams can get the actionable intelligence needed to block advanced attacks—including those being transmitted via email and the web and those traversing distributed multi-site corporate networks. With the solution, you can gain the rich intelligence you need to address your organization's most critical threats while optimizing operational efficiency.

For an introduction to all components and features of the Anti-SIEM, be sure to download the product data sheet.

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