DATA SHEET

ADAPTIVE DETECTION FABRIC

It’s the foundation of the Anti-SIEM and it focuses on detection of advanced threats, essential to empower security analysts and incident responders

Why a Detection Fabric is Critical to Solving Security Problems

The Anti-SIEM from Cyphort delivers three key values: advanced threat detection, comprehensive security analytics, and one-touch threat mitigation. In this document, we’ll focus specifically on the threat detection capabilities of Cyphort’s Adaptive Detection Fabric, the underlying threat intelligence layer that ensures Anti-SIEM users are empowered to quickly solve critical security problems.

Virtually every enterprise security architecture begins with a strong first line of defense. Security tools like next-generation firewalls, secure web gateways, and intrusion prevention systems are quite effective in recognizing and blocking most malicious web and email traffic trying to gain access to internal network resources. But these devices typically sit in-line and must use various rules to quickly make block/allow decisions without introducing latency. As effective as these tools are, none of them can block 100% of the advanced threats targeting your network. Once these threats gain access to internal resources, they can operate in stealth mode for months without ever being discovered. By the time the breach is discovered, the damage is done.

The Adaptive Detection Fabric (ADF) within the Anti-SIEM solution has been designed to close this security gap, deliver insight into advanced threats, and empower your security team to eliminate threats before they can execute on their mission.

A fabric, by definition, weaves together multiple components to create a unified whole, ideally greater than the sum of its parts. The fabric within the Anti-SIEM accomplishes this through a distributed software layer that works with what you already have in place. No rip-and-replace is required. The distributed software is built with patent-pending detection technology that provides continuous, multi-stage analysis of web, email, and lateral spread traffic moving through the network. In addition, this detection fabric can integrate with cloud-based email applications such as Gmail and Office365 to help protect organizations against malicious content delivered through those vectors.

The intelligent fabric – scalable and cost-effective to support any size organization – continuously collects information from multiple attack vectors, then uses advanced machine learning and behavioral analysis technologies to discover the advanced threats that other security tools miss. This can be done in as little as 15 seconds. Threats detected by the fabric are combined with data ingested from other security tools in the network, analyzed and correlated by the Anti-SIEM’s analytics engine, then presented to security analysts with a consolidated timeline view of all events related to an infected host. From there the fabric can also provide “one-touch” policy updates to in-line tools to strengthen them against a recurrence of advanced attacks.

ADF Solution Highlights

The Intelligent Fabric that Powers the Anti-SIEM

Cyphort's intelligent Adaptive Detection Fabric starts with virtual collectors that are deployed at critical points in the network – even across remote locations. These collectors, which can be configured based on the bandwidth and capacity requirements of your organization, capture web and email traffic originating from the Internet, as well as potentially malicious lateral spread traffic moving across your network. The ability to track lateral spread traffic is particularly important because it is often an indicator that the threat has progressed in its efforts to target and exfiltrate sensitive data. In addition, the fabric can collect raw web, email, and lateral spread traffic, as well as executables targeting endpoint devices in the network.

Data and related executables continuously collected across the fabric are delivered to SmartCore, which is the analytics engine used by the Anti-SIEM. The SmartCore engine (which can be deployed on-premises or in the cloud) employs a comprehensive, multi-stage data analysis process using machine learning, behavioral analysis, and other techniques to continuously correlate and analyze data from multiple sources and accurately identify previously undiscovered malicious content. Results from this process are delivered to security analysts via the Anti-SIEM management application (or can be integrated into existing SIEMs).

What they see is a consolidated timeline view of a security incident that combines insight into the advanced threat, identity information on the infected host, and information on all related security events gathered from other sources in the network. As the analytics engine continues to process more data, security analysts are provided with updated information on these threats, their risk levels, and their progression through the cyber kill chain. This near real-time, comprehensive view of advanced threat activity enables faster incident response and improved productivity of existing IT resources. That's the power of the Anti-SIEM.

The Adaptive Fabric

As noted earlier, the detection fabric within the Anti-SIEM seamlessly integrates with the security tools you already have deployed, which minimizes deployment complexity and eliminates unnecessary disruption to your operations. In essence, it adapts to what you already have in place through ADF's simple open API architecture, which provides two-way sharing of critical information.

For example, the information extracted from in-line security devices and endpoint security software allows the fabric to capture information from all relevant sources, and thus ensure that the Anti-SIEM's analytics engine provides a holistic view of all potentially malicious network traffic. Once advanced threats are identified, the Anti-SIEM can automatically create updated rules for in-line and endpoint devices, enabling them to adapt to newly discovered threats and prevent them from executing in the future.

The Analytics Engine within the Anti-SIEM

The effectiveness of this detection fabric is largely based on the power of the multi-stage threat analysis process, which includes:

- **Static analysis:** applying continuously updated rules and signatures to first look for known threats that may have bypassed in-line devices.
- **Payload analysis:** leveraging an intelligent sandbox array to gain deeper understanding of malware behavior by detonating suspicious web and file content, which would otherwise target Windows, OSX, or Android endpoint devices.
- **Machine learning and behavioral analysis:** Cyphort's patent-pending technologies recognize the latest threat behaviors (such as multi-component attacks over time) and are able to quickly detect previously unknown threats.
- **Malware reputation analysis:** results from the analysis are compared with similar known threats to determine whether the new threat is a variant of an existing threat or something completely original.

The Anti-SIEM's threat analysis process continuously adapts to the changing threat landscape through its connection to Cyphort's cloud-based GSS Service. Included at no additional cost to Cyphort customers, this service continuously examines millions of samples of potentially malicious code, then automatically updates SmartCore and each of the four stages in its threat analysis process to ensure that security analysts always receive fast, accurate insight into advanced threats discovered inside their network.

By consolidating threat detection from the fabric with event data from multiple data sources into a single integrated view, the analytics engine within the Anti-SIEM provides a comprehensive view of the latest threat activity, prioritized based on risk severity, asset targets in the network, endpoint environment, and progress moving through the kill chain. In addition, it's easy to determine the identity of specific users that may have been targeted by these advanced threats.

This actionable information can be viewed through the Anti-SIEM management application or seamlessly integrated into all leading SIEMs to provide consolidated, streamlined management and incident response workflows. The application also allows administrative access controls, enabling security managers to assign the appropriate level of privileged access to security administrators based on their roles in the organization. The information provided by the Anti-SIEM helps accelerate incident response and resolution, improve the productivity of security teams, and potentially eliminate the need for additional costly staffing resources.

Fabric Deployment Versatility

The software-centric architecture of the Anti-SIEM's Adaptive Detection Fabric provides benefits to organizations in three different ways.

- **Flexible:** The fabric can be deployed on general purpose servers, virtual machines, in the cloud, or in any architectural combination preferred by your organization. This also means that it can be deployed quickly and be operational the same day.
- **Scalable:** The fabric can scale to protect any number of users and assets in any number of locations, regardless of size or geographic separation. In any case, deployment is managed as a single system – or as multiple instances if desired.
- **Cost-Effective:** The fabric is included in the Anti-SIEM's subscription-based pricing model and is based on the total bandwidth required to support the deployment. This makes it simple and cost-effective to adjust deployment based on the needs of the organization.

Quilt Security Ecosystem

One of the design objectives of the Anti-SIEM and its detection fabric was to create a technologically advanced software security layer that would integrate seamlessly with your existing security architecture and the tools you already have deployed. Cyphort's commitment to a completely open API architecture has allowed us to achieve that objective. All threat intelligence processed by SmartCore is available to a wide range of off-the-shelf and custom tools, enabling organizations to build a best-of-breed, heterogeneous security infrastructure without being bound to a single-vendor siloed environment.

To extend the value of open APIs to all customers, Cyphort has created the Quilt Security Ecosystem, a vendor interoperability program that includes virtually all leading vendors delivering next-generation firewalls, secure web gateways, intrusion prevention systems, endpoint security software, SIEM tools, CASB, and more. The ecosystem ensures that ADF collectors can capture web, email, and lateral spread traffic from the right sources. And in many cases, it ensures that the Anti-SIEM can provide containment of newly discovered threats as well as updated security policies to strengthen in-line and endpoint devices against future attacks.

The Quilt Security Ecosystem continues to grow. Please contact your Cyphort sales representative for information on any specific vendors or products that may be important within your infrastructure.

Isn't it time to see what you've been missing? Learn more about how the detection fabric within the Anti-SIEM can close the security gap in your organization. To arrange a live demo or schedule a 30-day POC, please contact your local Cyphort sales representative or email us at sales@cyphort.com.

Anti-SIEM Subscription Offerings

The Adaptive Detection Fabric is a core part of the overall Anti-SIEM solution offering. A summary of features and license options are noted below.

Standard Level – 1 or 3 years

Protect critical attack vectors in your network with threat analytics

- License by bandwidth and users, unlimited locations
- Combined Web, Email, File Uploads and Advanced Threat Analytics
- Includes Windows, Mac, Linux and Android OS

Enterprise Level – 1 or 3 years

Extend visibility and protection across the enterprise with threat analytics

- License by bandwidth and users, unlimited locations
- All Standard Level features and Advanced Email
- Lateral spread detection across all locations
- Unlimited Scale for Email and Advanced Threat Analytics

Virtual Appliance Requirements

VMware General Requirements

Model	Versions
ESXi and vSphere versions	5.5.x and 6.0
vCenter versions (optional for .ova deployments)	5.5.x and 6.0

Virtual Fabric Collector

Model	Performance	Number of vCPU	Memory	Disk Storage*
FC-v50M	50 Mbps	1	1.5 GB	16 GB
FCv100M	100 Mbps	2	4 GB	16 GB
FC-v500M	500 Mbps	4	16 GB	512 GB
FC-v1G	1 Gbps	8	32 GB	512 GB
FC-v2.5G	2.5 Gbps	24	64 GB	512 GB

*Disks may be thin provisioned

Collectors require two Interfaces. One for management that can be shared. One dedicated hardware interface on the ESX server is required for the tap port.

Amazon Web Services Deployment Option

Model	Performance
Compute Optimized C4.4Xlarge	up to 45,000 objects/day
Compute Optimized C4.8Xlarge	up to 110,000 objects/day

Note that overall performance is a function of the type of disk volume chosen for the EC2 instances from which the vCore is running.

Virtual SmartCore Engine

Model	Performance (objects detonated)	Number of vCPU	Virtual Memory	Virtual Disk*
vSC-8	up to 40,000 objects/day	8	32 GB	Disk 1: 512 GB Disk 2: 1 TB
vSC-24	up to 140,000 objects/day	24	96 GB	Disk 1: 512 GB Disk 2: 2 TB

*Disks may be thin provisioned

Physical Appliances

SmartCore

Model	Performance* (objects detonated)
SC-R730	up to 175,000 objects/day

*Can be clustered to deliver more than 1M objects per day

All-in-One (SmartCore+Fabric Collector+Fabric Manager)

Model	Performance (objects detonated)	Performance (Gbps)
AIO-R430	up to 30,000 objects/day	1 Gbps
AIO-R730	up to 80,000 objects/day	2 Gbps

Fabric Web Collector

Model	Performance (Gbps)
Mac Mini	200 Mbps
FC-R330	1 Gbps
FC-R730	4 Gbps

For detailed ADF Physical Appliance Specifications, please consult the Quick Start Guide or contact support@cyphort.com

About Cyphort

Cyphort, Inc. is a security software company providing mid- and large-size enterprise customers with innovative security analytics for advanced threat defense. The solution is built with an open architecture that integrates with existing security tools to discover and contain the advanced threats that bypass the first line of security defense in an organization. Based in Santa Clara, California, the company was founded in 2011, is privately-held, and distributes its software through direct sales and channel partners across North America and international markets. Learn more at 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

Part#M1001-003US