DATA SHEET

# QUILT SECURITY ECOSYSTEM

## Vendors Collaborating with Cyphort to Provide Customers with a Stronger Security Posture

Security has always been about layers to create an intelligent defense-in-depth architecture. No one security solution will deliver 100% protection against all attack vectors. The ideal security architecture requires seamless integration of multiple complementary security technologies creating a whole that is greater than the sum of its parts to provide maximum protection against cyber attacks.

This is the strategy behind Cyphort's Quilt Security Ecosystem, a collaboration with vendors in all major security product categories, including endpoint, secure web gateway, NGFW, IPS, NAC, CASB, SIEM, and more. These technologies integrated with Cyphort's Anti-SIEM software platform, which combines advanced threat detection, analytics, and mitigation, strengthen security postures and accelerate incident response. Each Quilt partner leverages customer's existing investments and enhances the value of the Anti-SIEM.   The greater the interoperability and sharing of information, the stronger the correlation and ability to catch new threats. Much like a quilt, the combined effort of all participating vendors weaves together an incredibly strong security architecture.

The Quilt Security Ecosystem is made possible by Cyphort's open software architecture, which enables Cyphort and its partners to share critical information necessary for fast, accurate threat detection and remediation. Cyphort and its partners have essentially created an intelligent fabric—a distributed software layer that is scalable and cost-effective to support any size organization—leveraging Cyphort technology to continuously collect and correlate data from multiple sources throughout the network.  It then  employs a combination of behavioral analysis and machine learning to identify virtually all categories of malware.

Cyphort offers pre-built integrations with a broad set of Quilt Ecosystem partners, enabling the software fabric of Cypohort's Anti-SIEM to weave together multiple technologies so that security analysts can gain a holistic view of threat activity from diverse information sources. This holistic view provides incident response teams with rich data that includes threat profile and prioritization, the identity of the host and end user, its progression through the cyber kill chain, and a consolidated timeline view of all events related to a single security incident.

By taking full advantage of the Quilt Ecosystem, security teams can leverage data from multiple security tools deployed in their network and have the actionable intelligence needed to detect and contain advanced attacks—including those transmitted via email and the web and those traversing distributed multi-site corporate networks. This can help optimize the use of limited SIEM, SOC, and IR resources.

There are three categories of Quilt Ecosystem partners: Network, Endpoint, and Infrastructure. Each type is summarized below.

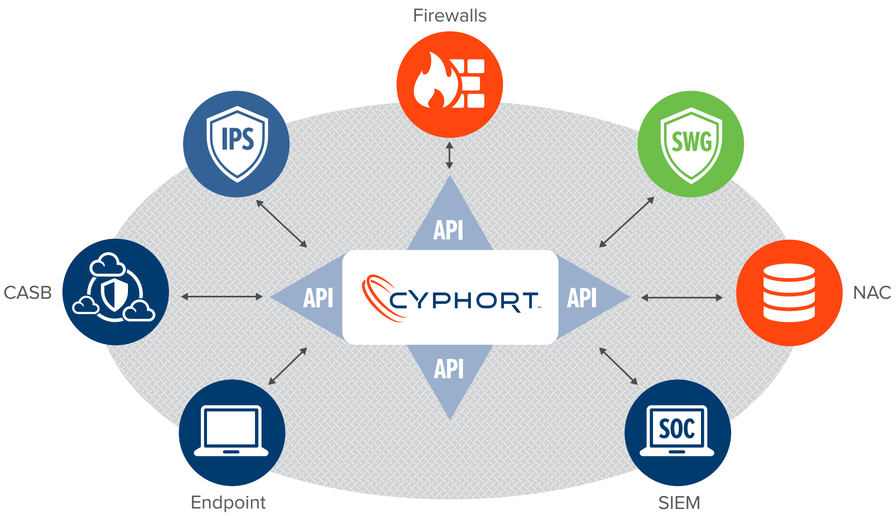
### Cyphort Anti-SIEM Features and Benefits:

- **A "lean-forward" security solution** designed to close security gaps and accelerating incident response
- **Threat detection** continuously ingests web, email, lateral spread traffic to find advanced threats
- **Security analytics** SmartCore engine correlates data from multiple sources, then presents timeline view of security incident
- **Threat mitigation** automatically creates updated policies to strengthen inline devices against future attacks
- **SOC productivity** eliminates manual steps, presents actionable information, accelerates incident response

- **Network** – These include perimeter and cloud partners in areas ranging from Next-Generation Firewalls (NGFW), Secure Web Gateways (SWG), Network Access Control (NAC), Cloud Access Security Brokers (CASB), and Intrusion Prevention/Detection Systems (IPS). These partnerships take advantage of the Anti-SIEM's ability to deliver automated action for prevention, isolation, enforcement, file uploading, and SSL inspection. This automation helps to lower administrative burdens on your security team.
- **Endpoint** – This category covers technologies that include Endpoint Detection and Response (EDR), User Behavior Analytics (UBA), and Next-Generation Anti-Virus (NGAV). Many integration options are possible. These include uploading files to Cyphort's advanced SmartCore data correlation and analysis engine, searching for malicious file hashes, analyzing file execution, and sharing indicators of compromise that are detected during detonation for infection verification. The results of SmartCore's analysis gives endpoint partners a wide range of policies they can apply including blocking or isolating infected machines.
- **Infrastructure** – These partners provide a multitude of joint functionality and interoperability with Cyphort. Because the Anti-SIEM is a software solution, it can work on hypervisors, in cloud environments, and on off-the-shelf commercial hardware. The software is designed to be elastic and leverage scalable cloud computing resources when high workloads are required. Security Information and Event Management (SIEM) vendors are also part of the network infrastructure partnerships, and the Anti-SIEM can enhance the value and performance of those investments.

Many partners span all three categories of integration providing several product offerings that work with the Anti-SIEM. Also, Cyphort provides the capability for multiple partners to work together seamlessly. The program is an ever-growing, interconnected fabric creating multiple layers of security, which is the most effective strategy for detecting and mitigating advanced threats.

To learn more about interoperability with specific vendors in your security infrastructure, please contact us at 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