GLOBAL SECURITY SERVICES

The intelligence service for advanced threat detection and classification

Overview

Cyphort's Global Security Services (GSS) is a service offered by Cyphort's global security research team, Cyphort Labs. GSS works in conjunction with the advanced threat detection capabilities, integrated within the Anti-SIEM software solution. The GSS service ensures that the SmartCore multi-stage data correlation analytics engine is updated continuously with the latest threat detection and mitigation information produced by Cyphort Labs. The service is available to all customers with a SmartCore license and entitles them to receive all Cyphort Labs updates at no additional cost.

The Global Security Services Update Service

GSS provides customers with recurrent updates to SmartCore's machine learning models and threat intelligence engines. A sample of what the service includes is listed below. Please contact a Cyphort representative to get a comprehensive list of all GSS services.

- **Machine Learning Model Updates:** Cyphort uses machine learning analytics for analyzing malware behavior to determine if content is safe or malicious. The Cyphort Labs team continuously trains the machine-learning engine with millions of new samples of malicious and non-malicious code. This training increases the efficacy of our detection as we learn crucial characteristics of known good objects, as well as enable us to flag malicious object behavior falling outside the norm. Customers receive regular updates to the machine learning engine.
- **Advanced Web Filtering:** IP addresses, URLs, and other threat intelligence data is curated by Cyphort Labs and used to block external threats proactively.
- **Reputation Analysis:** Cyphort Labs reputation analysis determines if source URLs have a history of delivering malicious content.
- **Snort Signatures:** Global Security Services includes Snort signatures that can detect call backs to command and control servers.
- **Static Analysis:** This feature uses rules and signatures to assist in determining whether content is safe or malicious.

Threat Sharing Subscription

Customers can enhance the value of GSS by automatically sharing their anonymized metadata of new threats. Customers sharing threats found in their environment helps improve machine learning models. All metadata is limited to malware and malicious activities. No customer-distinguishable data is sent to Cyphort as part of the threat sharing subscription.

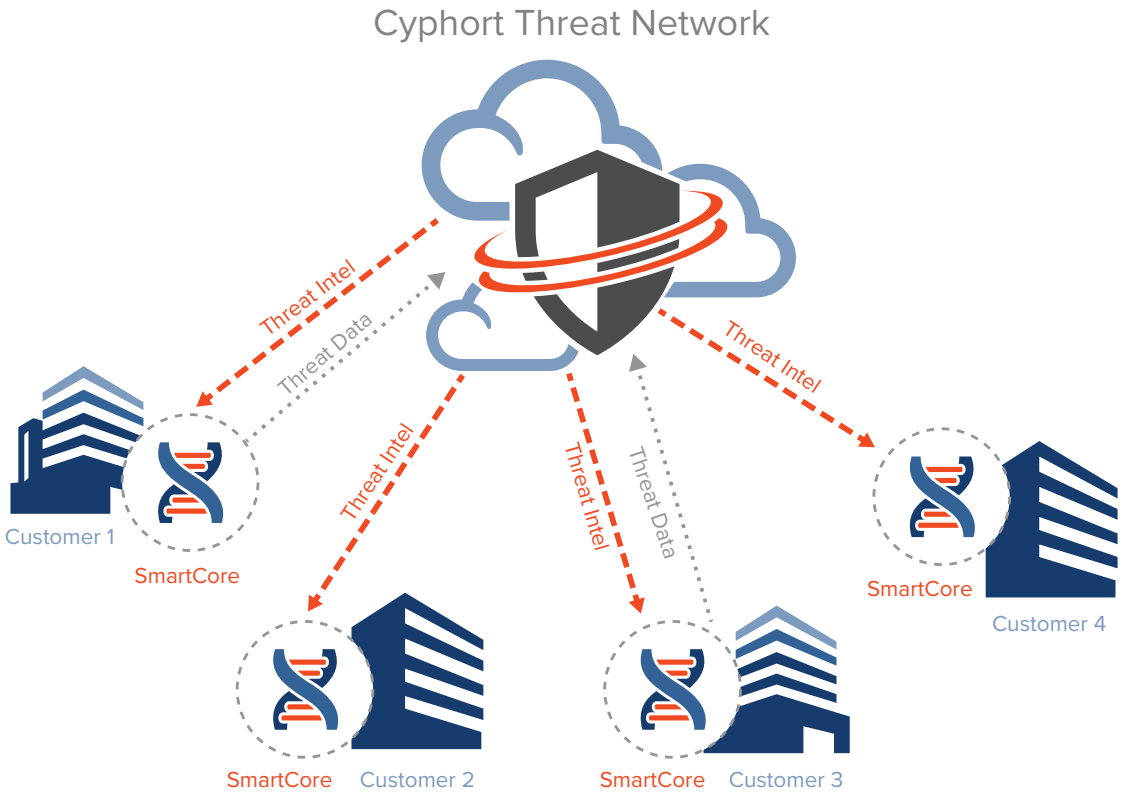
Customers can choose to opt-out of anonymized threat sharing by selecting the opt-out feature via the Anti-SIEM management application, although Cyphort does not recommend it.

Cyphort GSS Benefits:

- **Provides visibility** into threats that are early in their life cycle
- **Keeps the machine learning models updated** to identify yet unseen threats
- **Improves threat categorization and prioritization** to accelerate threat containment and remediation

Global Security Services Benefits

- **Provides visibility** into threats that are early in their life cycle
- **Keeps the machine learning models updated** to identify yet unseen threats
- **Continually improves threat intelligence categorization and prioritization** to accelerate threat containment and remediation



Global Security Services Information Flow

Cyphort Labs Overview

Cyphort Labs is made up of cyber security experts distributed throughout the world. We have assembled a team of security researchers, data scientists and ethical hackers from leading organizations. The Cyphort Labs' team works 24/7 monitoring the cyber world for malware events, their impact, and mitigation techniques. Their research results are incorporated into the detection capabilities of the Cyphort Adaptive Detection Fabric via static signatures, machine learning model updates, and algorithm optimization.

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.

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