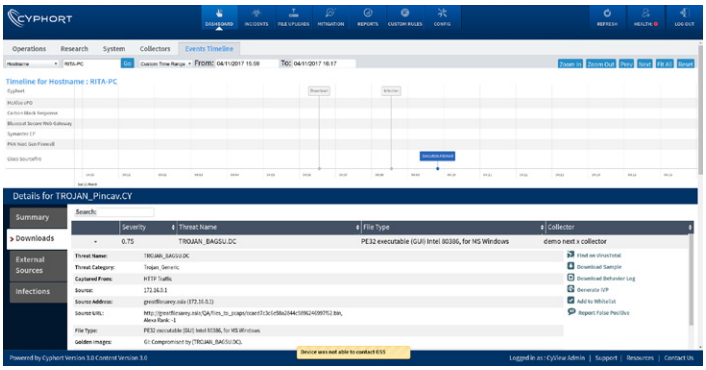
# ANTI-SIEM™

## It's everything you want in a SIEM – and less.
## Less cost. Less noise. Less complexity. Less wasted time.

Cyphort's Anti-SIEM is a distributed software platform that combines advanced threat detection, consolidated security analytics, and one-touch threat mitigation to address two critical requirements facing security teams in most large organizations:

1. **Productivity** – Security teams are typically flooded each day with hundreds of security alerts that must be triaged to determine which should be ignored and which require further investigation. Security analysts and incident responders require analytics capabilities that can effectively reduce the noise level and allow them to focus on incidents that pose the greatest risk to the organization.

2. **Security** – The alerts, logs, and events presented to security analysts typically indicate symptoms of potentially malicious activity in the network. What's missing is detailed visibility into the specific advanced threat itself. To strengthen the security posture of an organization, analysts require a platform with strong threat detection and actionable information necessary to respond to threats very quickly.




*Cyphort provides a consolidated timeline view of a security incident that combines threat detection with related events from other security devices.*

The Anti-SIEM addresses both requirements by first proactively detecting advanced threats that have compromised endpoints. Its analytics engine then correlates this threat detection with all related security events generated from other devices in the network. All relevant data is consolidated, along with host/user identity information, and presented to security analysts as a timeline view of a complete security incident relating to a named user. In addition, the Anti-SIEM prioritizes threats based on their progression through the cyber kill chain and their scope (threat impact on other endpoints). This automated process is often completed within 15 seconds – far less than the average of 2 hours of manual effort normally required, based on research conducted by Cyphort.

By consolidating all related events into a single security incident, security analysts and incident responders can then run interactive investigations that fully leverage this rich set of data. They can prioritize security incidents based on their risk levels, then implement response and mitigation plans for fast, effective threat resolution. The Anti-SIEM can assist in the mitigation process by working with security teams to automate policy updates to various security tools.

## Here are 7 key values of the Cyphort Anti-SIEM platform.

### 1. Threat Detection

Unlike traditional SIEMs, Cyphort's platform is built on strong advanced threat detection capabilities. The data ingested from Cyphort collectors – which continuously monitor web, email, and lateral spread traffic – are fed into the SmartCore detection engine, which consolidates all data and applies machine learning and behavioral analysis technologies to identify advanced targeted attacks, often within 15 seconds.

### 2. Security Analytics

Analytics has long been in the DNA of Cyphort. The SmartCore analytics engine complements its detection engine and is focused on making interactive investigations productive and efficient for analysts and incident responders. In addition to ingesting raw data from its own collectors, SmartCore ingests events from other detection and identity sources. It then employs correlation algorithms that enable data reduction, risk-based prioritization, and automation of many tedious manual processes.

### 3. Threat Visualization

The SmartCore analytics engine is paired with threat visualization capabilities that reveal threat progression through the cyber kill chain, as well as the scope and impact of a threat on named hosts and users. This provides useful context that enables faster and more accurate mitigation decisions.

### 4. Identity Information

Cyphort's Anti-SIEM also integrates with Active Directory and other identity sources, which enables the analytics engine to link specific security incidents to named users and host devices in the organization. This eliminates the need for security teams to deal with obscure IP addresses, thus saving time and providing more accurate insight into compromised hosts, users and assets.

### 5. One-Touch Mitigation

To help improve the productivity and response time of security teams, the Anti-SIEM also offers automated "one-touch" mitigation capabilities. For example, the platform can automatically create new rules and policies for inline devices to strengthen them against future attacks. Likewise, it can work with NACs to isolate or restrict the movement on infected endpoints until deeper forensics can be done.

### 6. Scalable Storage

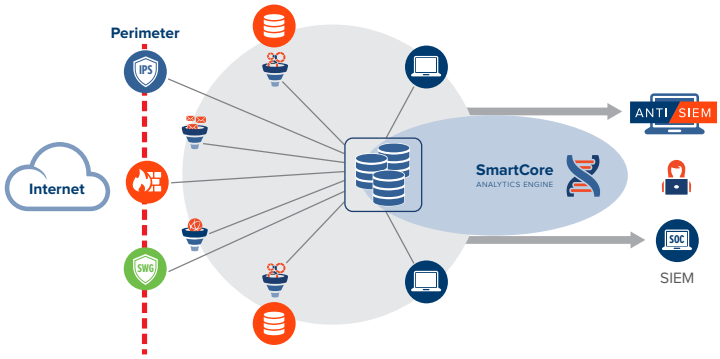
The Cyphort platform includes an integrated storage architecture that is easily scalable based on the requirements of each customer. For example, some companies only want 3 months of storage, while others prefer 3 years of storage to enable deeper historical forensics. The timeline view of security incidents noted above can also be extended to weeks, months, or more based on the historical data stored by the customer. Cyphort licenses are based on the number of users, not the volume of data stored or number of events ingested, so there is no data "tax" often associated with SIEMs.

### 7. Distributed, Open Architecture

Cyphort's distributed architecture leverages lightweight collectors that can be deployed at any number of branch offices, all feeding into an analytics engine deployed at headquarters or in the cloud. This ensures that the entire organization, even a five-person branch office, is protected. This is complemented by the Anti-SIEM's open architecture, which enables the platform to also ingest log and event data from the other network and endpoint security tools already deployed in the network.

## The Cyphort Anti-SIEM platform can provide values for 3 different use cases:

1. Organizations that currently do not have a SIEM deployed. In this use case, it is assumed that they would prefer not to deal with the cost and complexity of traditional SIEMs. Here, the Anti-SIEM can provide greater security and a faster time-to-value, all at a lower cost than traditional SIEMs.
2. Organizations that have a SIEM, but need better analytics and threat detection. In this use case, the Cyphort platform can work with the existing SIEM, ingesting data from it, and providing the necessary deeper dive threat detection, security analytics, and one-touch mitigation capabilities.
3. Organizations that have a SIEM and want to replace it. In this use case, the Cyphort platform could quickly deliver more value and less complexity. However, the Anti-SIEM does not currently support compliance reporting requirements, so it may not be an ideal fit for some organizations.




*Open architecture allows logs to be collected from multiple sources, including Cyphort collectors, then analyzed and correlated via the SmartCore analytics engine. Results are presented as a consolidated timeline view of multiple related events within one security incident. This can be viewed through the Cyphort management application or integrated into existing SIEMs.*

To see a demo or arrange a POC of the Cyphort Anti-SIEM platform, please contact your local Cyphort sales representative. Alternatively, call us at 1-408-841-4665, email us at info@cyphort.com, or visit us at www.cyphort.com.

## About Cyphort

Cyphort, Inc., provides a distributed security analytics solution that delivers advanced threat defense and improves operational efficiency for SOC and IR teams within mid- and large-size organizations. Based in Santa Clara, California, the company was founded in 2011 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