# Exhibit 32

CYPHORT™

Next Generation APT Defense

Data Sheet

## What Makes Us Different

Single pane of glass threat visibility and correlation across perimeter and internal networks allowing you to see the initial compromise and scope of an attack

Adaptive sandbox array and machine learning analytics detection that evolves with threats ensuring the latest threat techniques are detected

Contextual risk quantification for prioritization and optimized workflow minimizing unnecessary remediation activities

Customer created Golden Image capabilities giving customer real-world endpoint detection context

Endpoint infection verification to focus remediation efforts on truly compromised systems

Flexible deployment as VM, software or hardware

# Cyphort and Next Generation Advanced Persistent Threat Defense

Cyphort network-based, next generation APT defense solution evolves as rapidly as the threats it is designed to detect, providing a unique experience by utilizing a single “pane of glass” for threat visibility across an enterprises perimeter and internal networks, ensuring the identification of initial compromised systems, and the ongoing internal threat progression.

Cyphort eliminates alert overload by utilizing extensive threat correlation and in-depth context for your infrastructure. The result is a solution that reduces time from detection to remediation and is able to be deployed across an enterprises global infrastructure quickly as flexible physical, virtual or cloud appliances.

## Highlights of the Cyphort Solution

**Detection That Evolves With Threats:** Cyphort has innovated a machine-learning based detection engine that adapts with the changing nature of threats, ensuring new zero-days, APTs and evasive threats are always detected without having to wait for new software or system updates.

**Single Pane of Glass Correlating All APT Activity:** Cyphort provides a single pane of glass for perimeter (North/South) and lateral (East/West) threat activity across enterprise organizations. Built-in correlation provides security professionals with a comprehensive view of their current security posture with respect to advanced attacks while eliminating unnecessary alert overload.

**Flexible Deployment:** Cyphort’s solution is easily and cost-effectively deployed in single locations, across distributed enterprises and/or virtualized cloud environments for ultimate flexibility and scalability. By developing a distributed architecture and leveraging software eliminates the need for physical appliances, dramatically reducing complexity while optimizing customer ROI.

# Dynamic Detection™

## Machine Learning + Behavioral Inspection = Dynamic Detection™

Unlike 1st generation behavioral systems that leverage heuristics based analysis for threat detection, Cyphort's innovative Dynamic Detection™ method utilizes a Machine Learning engine combined with Behaviorial Inspection analytics to adapt to evolving malware and new threat techniques, including evasion tactics.

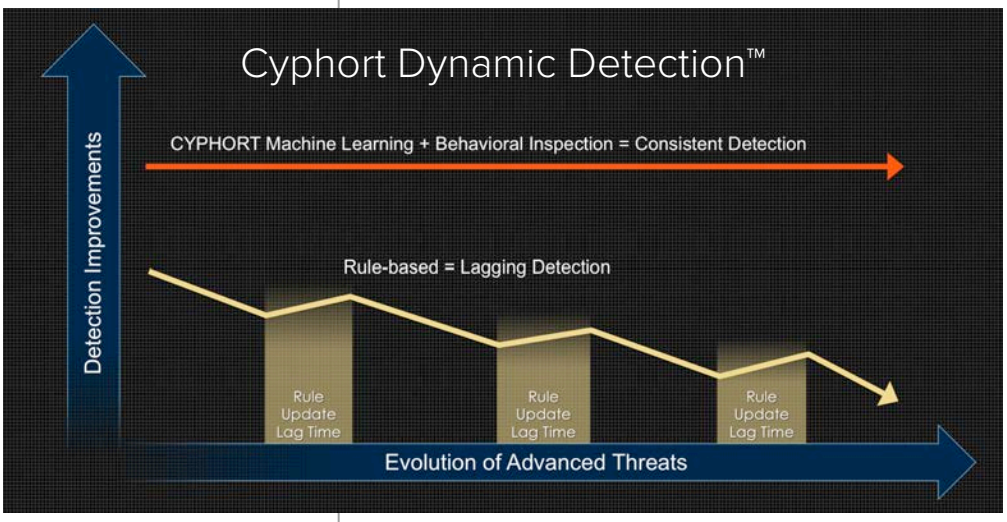
## Defeat evasion with adaptive sandbox array

Cyphort's Array of Sandboxes including virtualization and system emulation combined with a deep understanding of evasion and cloaking techniques allows the detection of evasion by ensuring that malicious code elicits enough behavior to make a determination.

## Detect obfuscated, multi-part threats

Cyphort's architecture has the capability to track multi-part attacks that employ obfuscation, or fragmentation to avoid detection with first generation APT solutions. By tracking users interaction with external sites, the system can effectively "replay" the entire interaction the same way an endpoint would be compromised, ensuring the inspection environment is able to retrieve the same payload that would detonate on an endpoint.

Cyphort Dynamic Detection™ method consistently finds next-gen threats with combined Machine Learning and Behavioral Inspection.




## Unsurpassed relevance with Custom Golden Image Sandbox

Cyphort allows customers to create and customize their own behavior analysis sandbox environments (Golden Image) mimicking the applications and endpoint protection solutions they have on their actual endpoints. This ability helps customers assess the impact of malware crossing the network in their own environment allowing laser focus to the threats that are "known" to compromise the endpoint systems, optimizing incident response resources to deal with the threat.

# Correlated Visibility

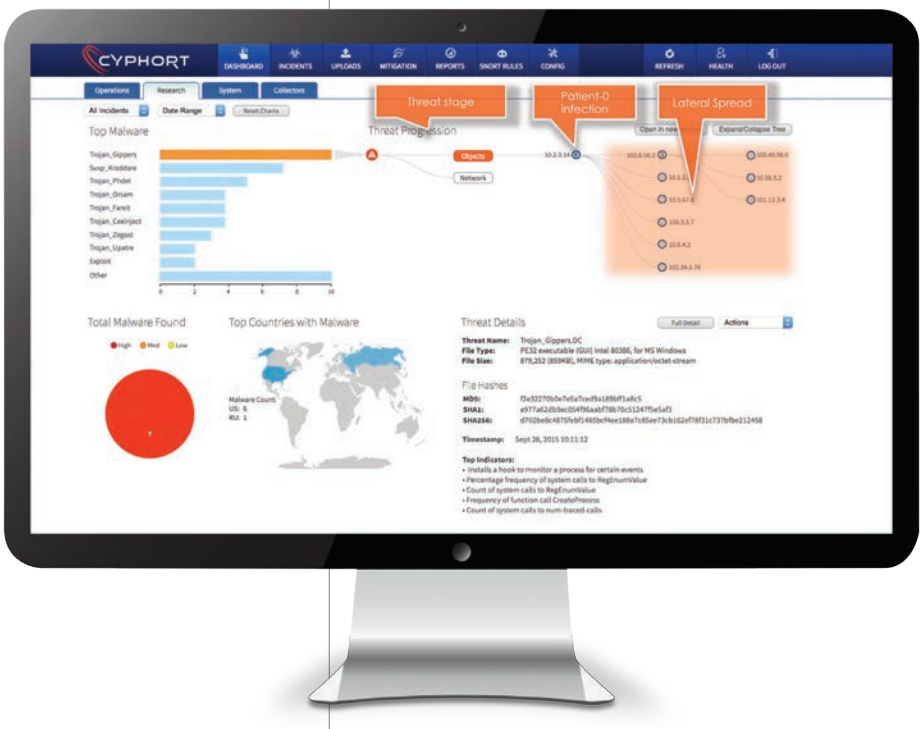
## View all correlated lateral and perimeter threat activity

When coupled with Cyphort's lateral-spread capabilities, customers are able to trace not only how threats enter an organization, but how they are progressing inside the organization, including additional devices that become compromised.

## Find threats across multiple threat vectors and platforms

See all threats irrespective of which vectors (web, email or file share) they utilize to spread and the platforms (Windows, Mac, Android, Linux) they are targeting.

Cyphort Advanced Threat Defense user interface provides complete visibility of correlated threats.




## View threats across their Cyber Kill chain lifecycle

Cyphort detects threats across the threat lifecycle and correlates the information as threat changes state across Exploit, Download, Command & Control, Lateral Spread and Internal Threat Activity.

## Eliminate alert overload

Cyphort dramatically reduces false positives and suppresses the noise from irrelevant threats. Accurate detection combined with the knowledge of intent, target value, cyber kill-chain stage and security posture of the target yields risk-based prioritization for incidence response.

# Deployment Versatility

## The Cyphort decoupled architectural advantage

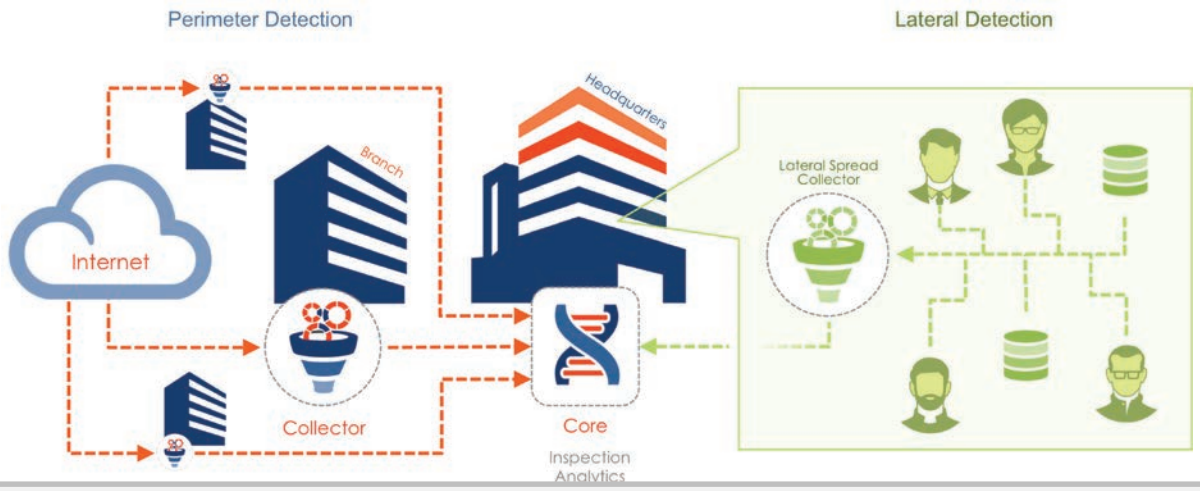
The Cyphort solution is delivered as software that can be installed on general-purpose servers, virtual machines and AWS cloud environments. The solution is designed to be scalable and distributed across distributed locations. The two key components of the solution are Cyphort Collectors and the Cyphort Core.

## Cyphort Collectors

Collectors are software-based sensors typically installed on commodity, low cost hardware or as virtual appliances, and are deployed at strategic network locations throughout a customer's network Internet egress points, data centers or branch offices. Collectors monitor network traffic out of band, collecting 'objects' to be inspected for the presence of malware or other threat activity. The collectors also monitor outgoing activity for the presence of malicious callbacks from compromised hosts.

## Cyphort Core

The Cyphort Core is the centralized detection component and contains the advanced threat detection and mitigation logic. Collectors forward the collected network objects and associated metadata to the Cyphort Core for analysis. The Cyphort Core also includes an analytics engine for accurate threat classification. The Cyphort Core then correlates the aggregated data across all collectors for verification and mitigation of attacks.



DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

**LAW FIRMS**
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

**FINANCIAL INSTITUTIONS**
Litigation and bankruptcy checks for companies and debtors.

**E-DISCOVERY AND LEGAL VENDORS**
Sync your system to PACER to automate legal marketing.