CROWDSTRIKE

CYPHORT

SOLUTION BRIEF

Benefits

- **Stop Breaches**
  Prevent both malware and malware-free attacks
- **5-Second Visibility**
  To discover and investigate current and historic endpoint activity
- **Cloud Powered**
  Lower cost and effective performance with cloud delivery 24/7

CONTINUOUS BREACH PREVENTION

STOP BREACHES AND GAIN THREAT KNOWLEDGE WITH THE INTEGRATED SOLUTION FROM CROWDSTRIKE AND CYPHORT

The threat landscape evolves constantly: Stay ahead of adversaries with an advanced, scalable joint solution that enables customers to seamlessly integrate CrowdStrike's Falcon Host into Cyphort's Adaptive Detection Fabric (ADF). ADF and Falcon Host will enable you to see whether a malicious file was executed, where it sits in the kill chain, and if it has moved laterally – all crucial steps in the detection to remediation timeline.

Immediate Time-To-Value

- Provide real-time threat detection and prevention of APT's within your environment
- Identifies targeted endpoints and contains threats before further lateral movement and infection occurs
- Prioritizes high-impact alerts, improving response time and preventing additional intrusions

Joint Solution Features

- Delivers comprehensive visibility pinpointing where a threat sits along the kill chain and whether it has been executed
- Provides network security featuring managed hunting and machine learning to identify potential threats in your environment
- Ensures a scalable layered security approach, with the ability to identify malware and non-malware based attacks

Combat Advanced Attacks with Crowdstrike and Cyphort

Harnessing next-gen endpoint security to prevent attacks from executing on your network

Falcon Intel fuels Falcon Host by providing real time intelligence on malware and non-malware based attacks, adversarial trends and targets, and attribution – all aggregated via CrowdStrike's ThreatGraph.

Falcon Host ingests endpoint data from Cyphort to verify that a malicious file has been executed on the endpoint.

Cyphort's ADF platform detects a malware object and queries Falcon Host to find out if the malware was executed on any endpoints.

Saving Invaluable Time From Detection to Remediation

Challenge

A suspected threat is identified within your environment and you need to understand how it got in, what systems are compromised and the potential exploit targets within your network.

Solution

Deploying a best-in-breed layered security solution that looks for the IOA's as well as IOC's of an attack within your network, allowing you to prevent an attack before it is executed.

Customer Benefit

Real-time network visibility coupled with the ability to detect and identify a potential threat provides you the insight to understand the intrusion point and lateral movement of the threat within your network.

Identifying Lateral Movement of Threats

Challenge

When a threat is discovered within your network it can take days to understand the sophistication and depth of an attack.

Solution

CrowdStrike and Cyphort work together to provide deep visibility of an attack and where it lies along the kill chain. Through this combined effort, you will have the ability to mitigate the attack before it spreads laterally – providing your team with a clear understanding of compromised endpoints.

Customer Benefit

With CrowdStrike and Cyphort working together remediation efforts can be prioritized, often reducing response times and preventing further damage to your network

About CrowdStrike

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR), and a 24/7 managed hunting service – all delivered via a single lightweight agent.

About Cyphort

Cyphort delivers the Adaptive Detection Fabric, an innovative, distributed software security layer which stops threats that go undetected by in-line security tools. Cyphort's open fabric integrates with existing security tools, delivering continuous insight and analysis of web and email traffic, prioritizing threat alerts for security teams, and providing auto-mitigation capabilities.

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