Fortune 500 with cloud infrastructure lowers APT risk while containing costs

The Customer

The company is a very successful F500 multinational, serves millions of customers, has branched its business model to enhance services to its core of loyal customers, and commands a dominant presence in its market space.

The Challenge

If a targeted attack is successful, the customer could suffer significant damage to its global brand, customer privacy and trust, and financial picture. What's really at stake? Key intellectual property and credit card information on millions of its customers.

Solution Requirements

The customer has a mix of Windows and Mac OSX devices while most of the data center infrastructure is hosted in the public cloud. The challenge was to find a solution that would defeat advanced attacks across its physical and cloud infrastructure while causing minimal changes to its current monitoring and incident response processes—a completely open and adaptive architecture was needed. Additionally, since the customer is global with multiple locations, the cost of a global deployment was a major concern to address.

The customer evaluated Cyphort's Adaptive Detection Fabric (ADF) as well as available competitive solutions in the marketplace including those that were appliance-based. While malware detection accuracy was a top requirement, they also needed a solution that would protect them across their entire global infrastructure. The key elements included:

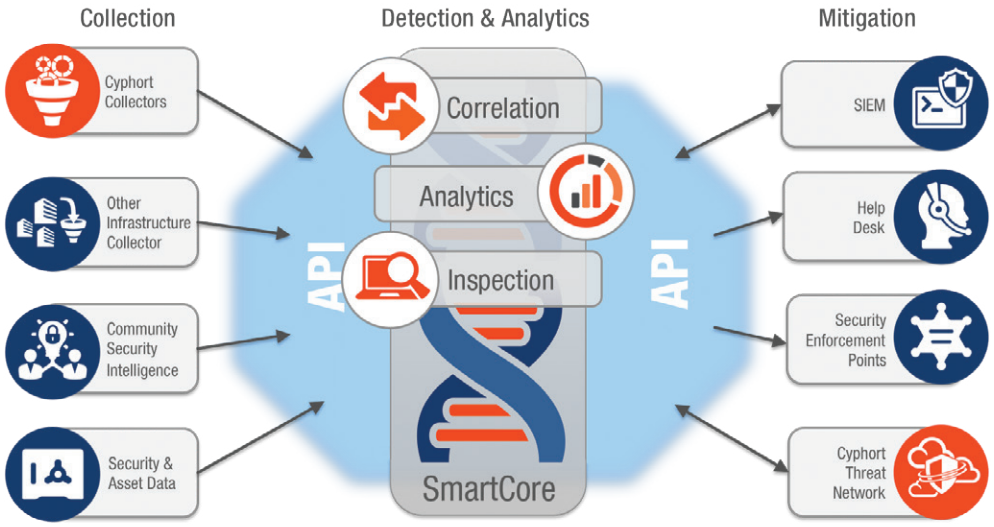
- **Detection of advanced armored malware:** The customer wanted a solution for identifying advanced malware with high efficacy. Signature-based solutions, which can't identify today's evasive malware, were not the right solution. Cyphort's solution detects evasive and stealthy malware—detecting unseen malware and identifying already compromised systems.
- **Ease of use and cost of operating:** The customer wanted to ensure that the solution would fit seamlessly within their existing infrastructure and not require a large team of remediation experts to evaluate and mitigate threats.
- **API-based integration:** The customer wanted to integrate their monitoring and remediation capabilities with their in-house tools and did not want to introduce a new dashboard and interface into its existing processes. The result they were looking for from an open API architecture was to reduce friction across the various teams as well as to contain any new training costs.
- **Use-based licensing:** The cost of a distributed deployment was a big concern for the customer and they wanted to ensure that the licensing model matched the value they received from the solution.
- **Software model:** Although, not a primary requirement, the customer preferred to have a software-based solution deployed in its public cloud infrastructure.

The customer implemented a Cyphort ADF solution in distributed mode. Each location received its own Cyphort Collector running on commodity hardware and the Cyphort SmartCore™ was deployed at the customer's public cloud.

The customer concluded a new security solution was required. What drove the need to change? Their intellectual property (IP) and customer privacy. IP is the lifeblood of their business and protecting it, along with their customers' credit card and privacy information, was what they had to do at all costs.

One of the primary requirements the customer needed to achieve with a stronger security solution was to minimize changes to its current monitoring and incident response processes. Any solution chosen had to have an open and adaptive architecture to meet the requirement.

To learn more details about the results and benefits this customer experienced, call us at 1.855.862.5927 or email Cyphort at info@cyphort.com.



ADF is a completely open API architecture and seamlessly integrates with existing security infrastructure.

Results & Benefits

Cyphort satisfied several requirements. After demonstrating the efficacy of ADF, the customer considered other aspects of the ADF solution—namely cost, context, and coverage. The following are the four factors that tilted the decision in Cyphort's favor.

- **Software-based scalable model:** Software delivery and potential deployment as a virtual machine (VM) was very attractive to the customer.
- **Actionable intelligence and threat prioritization:** ADF's automatic threat prioritization and mitigation information were clear winners when compared to competitive solutions.
- **Flexible licensing:** ADF's distributed software approach allows for a flexible licensing model. Cyphort licenses by network bandwidth and not by the number of locations it protects. Most appliance-based solutions are too rigid and prohibitively expensive in comparison.
- **API-based integration:** ADF has an open architecture that enables it to work with other third-party solutions. The open API approach allows the customer to directly integrate the solution with their existing monitoring and remediation applications without introducing a new interface to learn and use.

The customer is pleased that they don't have to add resources to their Incident Response team at this time—as this was a primary concern for them. The Cyphort ADF solution included SmartCore™, which provides automatic correlation, prioritization, and actionable intelligence—all very attractive capabilities for the customer. Their overall staffing requirements are not expected to grow significantly in the future as a result of Cyphort's ADF SmartCore™.

About Cyphort

Cyphort, Inc. is a network security company providing mid- and large-size enterprise customers with the innovative Adaptive Detection Fabric, a scalable software solution designed to integrate with existing security tools to discover and contain the advanced threats that bypass the first line of security defense in an organization. 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