Financial Service Provider Deploys Powerful Adaptive Detection Fabric to Stop Threats and Protect Customer Data

The Customer

The customer is a successful financial services company using innovative technology to change the way consumers and businesses obtain credit. Since their beginning, they have facilitated billions of dollars of loans. The customer has received considerable recognition from the financial services industry for their focus on providing a unique way of lending that results in a delightful customer experience.

The Challenge

The customer knew it could be a high-value target for criminal activity due to their use of innovative technology, and they decided to evaluate new security solutions to strengthen against and combat cyber attacks. What was concerning to them was that even a minor breach in their network could result in the loss of financial data associated with thousands of its clients, and it could set in motion a devastating effect on its reputation and business performance.

To protect vital assets like their online financial services and intellectual property (IP) as well as client financial and banking information, the customer decided it had to strengthen its network defense by adding a detection layer focused on stopping advanced threats. This new detection layer would give them the preparedness they were looking for to stop attackers from doing serious damage to their company.

Solution Requirements

Their requirements specified that any solution must have the capabilities to prioritize risk on already-compromised systems as well as detect never-before-seen malware. They also needed a solution to have the ability to respond to threats rapidly as well as provide financial benefits to lower overall capital and operational expenses.

They decided to evaluate and ultimately deploy Cyphort's Adaptive Detection Fabric (ADF) solution, an innovative, distributed software security layer that stops threats undetectable by traditional in-line security tools. ADF provides continuous insight and analysis of Web, email, and lateral spread traffic to discover and prioritize advanced threats early in their life cycle. This process reduces the time from detection to remediation and enables ADF to provide auto-mitigation capabilities that strengthen existing in-line security tools against similar threats in the future. Finally, ADF delivers significant economic value with a cost-effective deployment model, as well as cost savings resulting from fewer breaches and faster incident response time.

Their key solution requirements included:

- **Detection of advanced armored malware:** The customer wanted a solution for identifying advanced malware with high efficacy. Signature and rules-based solutions, which can't always identify today's evasive malware, were not an option. Cyphort's ADF solution detects evasive and stealthy APT malware on already compromised systems as well as detecting never-before-seen malware.
- **Ability to respond to threats quickly:** The customer did not have a team of security incident response experts and did not want to invest in one if not required. The ability to respond to newly found threats using existing staff and systems was of paramount importance. ADF's open API architecture which integrates with existing enforcement infrastructure and SIEM were features highly valued by the customer.
- **The cost of ownership:** The customer wanted a solution that could be rolled out deep and wide across its entire infrastructure without having to starve other important initiatives. ADF can provide detection and mitigation across the entire enterprise including East/West traffic.
- **Deployment flexibility:** The customer was running its servers in a Virtual Machine (VM) environment, so protecting these servers was important. The ability to run ADF Collectors on VMs in the data center was an essential requirement.

The customer faced two challenges. Both were equally important: protect itself and protect its customers' banking information.

What was concerning to them was that even a minor breach in its network could set in motion a devastating effect on its reputation and business performance.

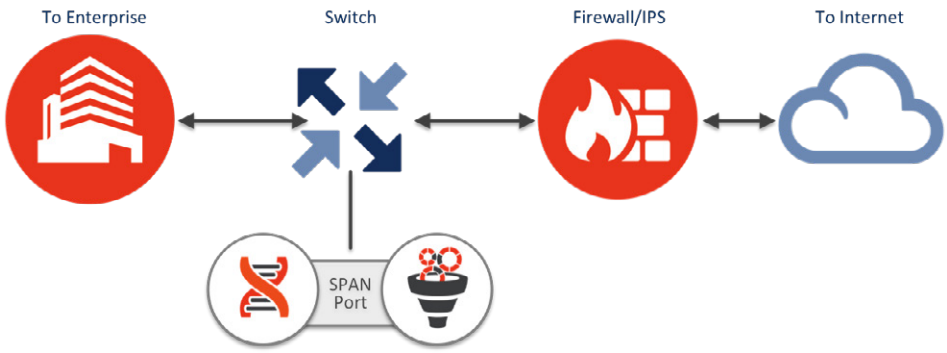
To learn more details about the results and benefits this customer experienced, call us at 1.408.841.4665 or email Cyphort at info@cyphort.com.

After first deploying Cyphort's Adaptive Detection Fabric as a proof-of-concept, the customer could see it met their requirements and decided on a full ADF implementation in a phased approach.

Phase 1: The customer deployed Cyphort's ADF SmartCore machine learning and behavior analysis engine as well as a virtual Collector running on commodity hardware at its primary Internet egress point. This provided the company with the ability to scan both inbound and outbound traffic for threat activity including Web, email, and other executables. Once it perfected its internal processes to handle unseen threats, the company moved to phase two.

Phase 2: Delighted with ADF's results thus far in the deployment, the customer decided to expand the implementation by going deep and wide in its network to include lateral spread traffic. The customer deployed two new Collectors as VMs that oversee the data center traffic from a virtual SPAN port.

Even with increased traffic, the customer has not experienced the need to upgrade its SmartCore because it easily picked up the traffic load from the new VM Collectors.



Cyphort's ADF solution uses an Open API architecture that seamlessly integrates with existing security infrastructure. ADF is designed to close the detection and mitigation gap across a diverse and distributed organization.

Results & Benefits

The Adaptive Detection Fabric satisfied the customers' requirements. After demonstrating its malware detection efficacy, the practical aspects of deployment and pricing became the main deciding factors. The following factors are what influenced the decision for ADF.

- **Unmatched threat detection:** The customer evaluated the detection capabilities of all contenders side by side for an extended period. SmartCore came out ahead or equal in its threat detection capabilities.
- **Flexible, software-based, and scalable deployment:** Software delivery and deployment as a VM was very attractive to the customer. SmartCore can scale up and down based on volume.
- **Reduced cost of ownership:** ADF reduced the cost of ownership for this customer by not only reducing the capital expenditure on solution procurement that it would have to make but also reduced the operational spending on monitoring and incident response.
- **The speed of threat resolution:** SmartCore provides rich contextual information and risk prioritization for each detected threat with clear steps for mitigation. This greatly simplified the life of IT staff involved in security response and allowed them to enhance their security posture without adding staff.

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