

Online Storage Provider Relies on Adaptive Detection Fabric for Security

The Customer

The company is a leading online file sharing and content management service. It serves the enterprise and consumer markets and supports millions of users and tens-of-thousands of companies.

The Challenge

Enterprises now face another threat vector: file-sharing services offered by cloud service providers. These services are often used in the shadows by company employees for collaborating and sharing files with outside parties. Of particular concern to security-conscious enterprise customers is the risk it presents to network security. One illustration of the danger involved is DropSmack, a malicious program that uses a file sharing service to steal data and deliver malware. This type of collaboration and sharing process demonstrates the possibility that attackers can bypass an organization's prevention infrastructure entirely.

Given this situation, the cloud service provider wanted to accomplish the following goals:

- ▶ Position their service as an enterprise-ready, highly secure solution for security-conscious customers.
- ▶ Create a value-added premium secure file service to expand revenues and gross margins.

Solution Requirements

The customer evaluated Cyphort's Adaptive Detection Fabric (ADF) as well as other options in the marketplace including costlier, appliance-based options. While advanced malware detection accuracy was a top requirement, they also wanted a practical solution that would fit their SaaS business model—which needed a flexible, scalable solution. The customer's key requirements 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. The ADF solution discovers evasive and stealthy malware—detecting unseen malware and identifying already compromised systems.
- ▶ **API-based integration:** The customer wanted to scan files already stored on their cloud-based storage service. Most network-based solutions were found to be incompatible with this approach as they only operate on live network traffic. Cyphort's ADF, usually deployed as a network-based solution in most environments, provided the customer the ability to feed files to the ADF SmartCore analysis engine through its open API architecture.
- ▶ **Scalable scanning engine:** Scalability was a significant requirement as the volume of files uploaded to the service is high, the performance of the solution had to scale with the volume of files without having to over-provision initially or having to make additional upgrades later on like appliance-based solutions.
- ▶ **Integration with the infrastructure:** The customer did not want to have an additional tool and management interface to manage the solution. They preferred a solution that would integrate with their own management interface. The customer recognized that ADF's open API architecture was a great match to meet this requirement.
- ▶ **Use-based licensing:** The unpredictability of scanning volumes necessitated that they find a solution that is priced based on usage and does not require over-provisioning just to deal with

A leading online file sharing and content management service provider puts enterprise customers' minds at ease by analyzing files for advanced malware before delivering them.

Scalability was a significant requirement as the volume of files uploaded to the service is high, and the performance of the solution had to scale with the volume of files without having to over-provision.

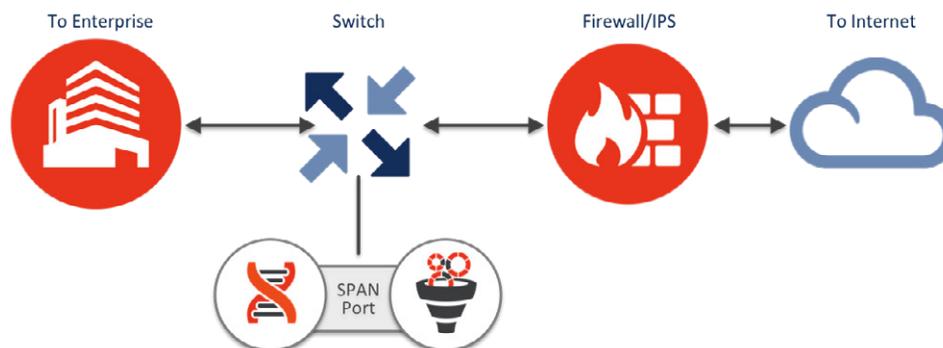
Software delivery and deployment as a VM was a very attractive feature to the customer.

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.

the expected peak load. ADF's software model and flexible licensing provided an excellent fit to meet this requirement.

The customer implemented the ADF SmartCore software running as a virtual machine in their environment. With clustering built in, they can quickly scale their deployment as they sign up more customers.

Instead of using ADF Collectors, the customer opted to utilize the open API architecture and feed files to the SmartCore malware detection engine. As the SmartCore open API returns the detection results, the customer can quarantine malicious files. The ADF open API architecture also provided access to management and reporting capabilities that the customer could then integrate with their third-party security management tools.



Results & Benefits

The Adaptive Detection Fabric satisfied several requirements that the customer had specified. After demonstrating the efficacy of ADF malware detection, pricing and ease of deployment in a SaaS environment became the main deciding factors. The following are the major factors that influenced the decision in Cyphort's favor.

- ▶ **Software-based scalable model:** Software delivery and deployment as a VM was a very attractive feature to the customer. ADF SmartCore can scale up and down based on the volume. Built-in clustering combined with the VM-based deployment provided the best deployment option to the customer.
- ▶ **Flexible licensing:** ADF's software approach allows for a flexible licensing model offering significant value to the customer. ADF is licensed by network bandwidth, and is not tied to the number of locations it protects. In contrast, most appliance-based solutions are too rigid and prohibitively expensive.
- ▶ **API-based integration:** ADF has an open architecture that enables it to work with third-party solutions. This approach provides a platform with API's for submitting files for scanning, retrieving results, and managing the solution—and this was a great fit for the customer.

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.

