Time for Integrated vs. Bolted-on IT Security

Cyphort Platform Architecture: Modular, Open and Flexible
Overview

This paper discusses prevalent market approaches to designing and architecting security products and their pitfalls. Most notably, as the security landscape evolves with new kinds of threats, new classes of products emerge to help organizations deal with them effectively. However most of these products are architected as standalone solutions giving rise to a bolted-on security implementation in most organizations.

In addition to being expensive to implement and maintain, bolted-on security implementations result in inferior security outcomes and are frequently the subject of IT organizations’ ire. Lately, vendors have started to offer “integrated” solutions. This is most evident in the areas of Next Generation Firewall and UTM products where Firewall, IPS and potentially other security products coexist and provide a unified interface to the security team. This approach however fails when discerning customers want to take a “best of breed” approach towards building their security infrastructure.

Cyphort advanced threats defense platform takes a significantly different approach that ties it closely with an organization’s overall security fabric, so that it functions in unison with customers existing security portfolio and processes while allowing organizations to completely leverage the functionality of related products.
What is a bolted-on architecture?

Bolted-on architecture is a consequence and not a design goal. It arises from the fact that organizations have to purchase, implement and maintain multiple security solutions, each with its own set of features and management interfaces. There is very little if any shared intelligence and coordination between disparate solutions. This approach results in a security architecture that has several disadvantages and results in an inferior security posture for an organization.

The pitfalls of a bolted-on security architecture

There are many issues related to bolt-on security architectures, many of which are obvious and some of which are less obvious and related to the effectiveness of a security posture. The following provides details on some of these pitfalls:

Inability to leverage synergy between solutions

While cost and management are frequently cited as major pain points for operating multiple solutions, it is the inability to utilize the technologies in disparate products in a meaningful way that is the biggest pitfall, and prevents organizations from unlocking the true value of their security investment. An example would be endpoint-based solutions that can protect from known malware and network-based solutions that detect unknown malware. Each have unique values, but combined would provide significantly more value to a customer. Network based solution can find zero-day threats, provide intelligence to the endpoint solution to identify and mitigate it in the future.

Management overhead and costs

Cost and overhead of operating multiple security products using their own management interfaces and paradigms is a major pain point for IT organizations.

Reduced visibility

Most security products claim to provide a “single pane of glass” view through their individual dashboards. However, this is done within the context of a specific product. How it matches up with the dashboards of other solutions is left to the security practitioners.

Redundancy

Security products frequently introduce redundant capabilities that are at best underutilized, and in the worst case compromise the reliability and security of an organization. For example, having multiple security products capable of blocking suspect Internet traffic can introduce additional points of failure thus reducing reliability. As another example, two separate security solutions that have discovered the same suspect activity through different means will effectively double the alert load for the incidence response teams resulting in over commitment to dealing with this particular threat, while potentially ignoring others thus reducing overall security effectiveness.
A new approach to building security

The issues discussed in the previous section leads us to discover a new architecture that will work in unison with an organizations overall security portfolio. In order to achieve this, a solution must be designed with the following principals in mind:

**Modular**

Monolithic security solution may pack a lot of features but they are prone to be underleveraged by the customers if individual functions cannot be accessed and matched up with other complementary technologies. One example would be to have threat detection solution that can export mitigation information so that existing enforcement solutions can provide protection based on the intelligence provided by the detection solution.

**Open interfaces**

The solution must be able to integrate with other solutions. This requires that the solution be built with a fundamental API layer. The intent would be to deliver API access to most of the functionality and adhere to standards based data exchange formats.

**Platform choices**

One requirement for a seamless solution is that it should be deployable in a variety of infrastructure scenarios. This includes deployment as a hardware appliance, virtual appliance or standard software images. This will ensure that security controls can be applied uniformly across the entire infrastructure.
Cyphort Advanced Threat Defense Platform

Cyphort Advanced Threats Defense Platform has been designed from the ground-up to become part of our customers’ security architecture. Cyphort Platform is designed around four modules namely:

**Collector(s):** This module collects network objects and metadata from network traffic using a SPAN or virtual TAP port where the traffic is to be inspected. These objects and metadata are combined and sent to the analysis module (known as the Cyphort Core) for detailed inspection and analysis.

**Core:** The Cyphort Core is the central brain of Cyphort platform. The Core module inspects, analyzes and correlates the data and objects sent from the Collector(s) to determine if it presents a threat, and produces the relevant risk score for your organization.

**Manager:** As the name suggests this is the management module for administering the solution, generating reports etc. This module co-resides with the Core, and is accessed via a Web browser.

**Mitigation:** Similar to the manager module, remediation also co-resides with the Core. This is the module that generates data from inspecting objects and receiving CnC signals from the collectors. This data can be “pushed” to existing network infrastructure controls for continuous protection across all users. The mitigation data includes –

- IP addresses for Firewall rules, URLs and Domains for Secure Web Gateways (SWG), and SNORT signatures for IPS solutions to block ongoing attacks
- A unique set of Indicators can be generated from each object evaluated in the analysis phase that can be used to evaluate if the intended target of the attack was indeed compromised. This is known as an Infection Verification Pack (IVP), used for endpoint verification

All modules function together using APIs that are available to our customers. Customers can replace some of these modules with their own custom modules or use the APIs to integrate with their existing infrastructure. Cyphort Platform provide complete flexibility of deployment and can be deployed as a hardware appliance, software or as a virtual machine to protect across the organization.
Cyphort APIs classification and use cases

Cyphort Platform APIs can be divided into three categories

1. Input APIs

These APIs pertain to sending potential malware carrying objects to the Cyphort core for inspection and analysis. Cyphort’s own Collector module uses these APIs to send network objects and metadata to the Cyphort Core.

One possible use case is if an organization has its own file carving capability, they can use the API to submit files directly to the Core for analysis. Here is a case study detailing this use case


2. Output APIs

These APIs provide detection and mitigation information as the Core and collectors identify active threats. Some of the use cases for these APIs include –

- Integration with existing security monitoring and alerting solutions so that the security teams can be notified of malicious events using a single mechanism
- Integration with Firewalls, Secure Web Gateways and IPS systems to automatically send mitigation information (IP addresses, URLs, Domains, SNORT signatures) to these devices to block malware communication.
- Integration with IT workflow and ticketing systems so tickets can be populated with the priority information and mitigation information and assigned to the appropriate personnel
- Integration of the infection verification functionality with the IT workflow systems so that the IVP binary can be sent to the endpoint for infection verification and results reported back and integrated with the remediation workflow
- Integration with existing antivirus solution management console so that malicious object MD5 can be added to the existing AV solution for blocking across the enterprise devices.

3. Management APIs

These APIs provide access to management, monitoring and reporting functions in the platform. This allows our customers to completely bypass Cyphort management interface and integrate the platform directly with their own management platform. Here is a case study where a Cyphort customer is using their existing management solution to manage Cyphort.


Conclusion

Cyphort’s Advanced Threats Defense Platform provides ideal security architecture for organizations that are using a diverse set of products for security. Cyphort’s open and modular architecture combined with RESTful APIs provides an ideal solution that can add powerful threat detection and mitigation while leveraging existing security and management systems.