Security 2.0
A Multi-Dimensional Approach to Advanced Threat Protection
Executive Summary

Year after year, as cyber criminals and their attack strategies outpace detection and challenge cyber security efforts worldwide, the global threat landscape continues to evolve. Just a few years ago, cyber threats were the domain of hackers gaining technical supremacy or simply having fun. Today, hacking is a highly organized, malicious profession with clear economic and strategic objectives. These attacks may consist of stealing an organization’s intellectual property, or confiscating online bank accounts and customer information, creating and distributing viruses on other computers, and more. Often financed by large criminal organizations, political cohorts and even nation states, there is an abundance of resources and sophisticated talent at work in the cyber world, and it costs companies today dearly. Global cyber crime and espionage activity costs the global economy anywhere from $100 billion to $500 billion annually, according to most industry reports. The average annualized cost of cyber crime in a study conducted by Ponemon Institute on 60 U.S. companies was $11.6 million a year, with a range of $1.3 million to $58 million.

The nature of cyber threats is also changing from widely applicable single-method attacks, to stealthier, multi-phase and targeted threats, many of which frequently use zero-day vulnerabilities and evasive metamorphic or polymorphic malware propagation. These attacks are invariably immune to traditional, signature-based detection methods and are increasingly undetectable by session-based, stage-specific network security appliances and services.

Advanced cyber attacks typically unfold in a series of stages, popularly known as a “kill chain.” Security efforts that focus on a specific stage or detection mechanism in the chain are egregiously ineffective because a comprehensive view of all threat stages is required for effective detection and mitigation. Moreover, as cyber attacks continue to advance, the tools available in the cyber security and cloud marketplace have not kept pace, evolving slowly, if at all, and usually focus on only one threat stage or aspect. Today’s cyber security solutions tend to exhibit one or more of the following:

- **Single Presence**: A cyber security tool installed at one or select egress points in a network, without visibility to all malicious traffic, and thus incapable of comprehensive threat analysis or full-chain correlation.

- **Single Method**: A cyber security tool that is overly reliant on one method of malware detection (e.g., sandboxing, signature matching, etc.) that smart malware then learns to anticipate and evade.

- **Single Event**: A cyber security tool that focuses on one stage of the “kill-chain” (e.g., malware delivery), thus missing valuable information for more expansive and comprehensive detection and mitigation.

- **Single Signal**: A cyber security tool that inundates security professionals with security event alerts to “root-cause” without correlating the event to specific attacks, thus falling short on providing immediately actionable intelligence.
At Cyphort, we understand the advanced threat protection space for enterprises — we have pioneered solutions in this field and understand how modern enterprise threat problems should be solved. It requires continuous monitoring and risk mitigation with actionable and business-relevant intelligence. We have created a software- and cloud-based solution that will put enterprises back in control of their threat protection.

The Cyphort solution offers comprehensive visibility into all relevant network data: Cyphort’s one-of-a-kind machine learning, big-data correlation engine accurately detects advanced malware threats and generates actionable intelligence for immediate mitigation. In addition, the Cyphort solution includes coverage of threats for a wide variety of software platforms, including Windows, Mac OSX, Android and Unix, thus securing the enterprise’s entire infrastructure.

This paper provides perspective on the advanced threat landscape, outlines competitive approaches that often fall short, and highlights Cyphort’s comprehensive approach — from visibility and detection to actionable threat intelligence.

The Struggle With Advanced Threats

Corporate networks are highly interconnected, often global in nature, and use a variety of Internet egress points, extranet partners, remote workers, mobile devices, and applications in the cloud. Critical applications also require access to diverse business partner sites and customers across the Internet. Employees frequently work from home, using their own Internet connections to browse the Web via a corporate VPN that provides direct access to confidential business data and intellectual property. While on business travel, your employees can use any available means to get online: a hotel WiFi or a coffee shop hotspot. Increasingly, employees are using their personal smart phones, tablets and a bring-your-own-device (BYOD) strategy for business purposes, accessing sensitive enterprise data with these mobile devices through a separate carrier’s cellular networks.

Further, with global business today, an enterprise’s main campus network often connects to many different remote offices and sites, ranging from small sales groups to vast development centers spread around the globe. These corporate networks are designed to optimize business productivity across all connected and remote sites. The problem? Sophisticated threat actors see these networks as an enticing, prime target. They will perform targeted attacks that take advantage of every manner of network entry point and vector vulnerability. Many of these attackers are well-paid professionals, backed by criminal organizations or even governments. Ironically, the better an IT infrastructure has been deployed to support online business relationships and employee productivity or collaboration, the more options are available to a threat actor seeking inroads into the organization. When an attack successfully infects its first client machine (laptop, tablet, etc.), it immediately attempts to remain unseen while spreading laterally from its initial foothold into more sites, servers, shares, and networks, where it performs a sequence of activities to patiently identify and exfiltrate high-value, digital assets from the targeted company.
Unfortunately, there is a huge imbalance between the threat actor’s objective and those of the enterprise. A threat only needs to find a single available path into the corporate environment to infect a single device, and from there, the attack can successfully spread throughout the enterprise. Meanwhile, the enterprise is faced with the daunting task of protecting all access vectors and all corporate assets from any given attack path.

Where Network Security Products Fall Short

Today’s security products are ill equipped to defend an enterprise against the imbalance of sophisticated and well-funded threat actors. Security products are still predominantly single-presence, single-method, single-event, and single-signal based. Let’s examine these in turn:

**Single Presence**

A single-presence security product is a self-contained network appliance, collecting, analyzing, and controlling network traffic at its point of presence. However, to detect and protect against advanced threats, a detection and analysis engine must be present at every possible inbound network path. Even the most advanced detection and protection technologies are useless if their deployment cannot see and inspect all threat traffic. As a result, distributed corporate networks and mobile connections are invisible to a single-presence appliance. Therefore, providing comprehensive visibility with a single-presence network security appliance is technically challenging or realistically impossible — depending on the enterprise’s network architecture. It is also prohibitively expensive for corporate capital and operational budgets to distribute single-presence appliances everywhere they would be relevant.

**Single Method**

Threat actors and proactive detection are locked in an arms race, with the corporate enterprise frequently outgunned. Threat actors continuously study every new single method detection process and tool to refine their attack code capabilities and evade detection mechanisms, referred to as “armoring.” This is true not only for static analysis single-method tools, such as signature-based engines, but also for single-method sandboxing technology, used for behavioral analysis. Attacks are also evolving their malware behavior to evade the abilities of the detection engine that is monitoring the sandbox. Attacks are now highly adaptive with regard to sandbox detection, able to cleverly halt attack code execution if it is discovered. In this context, threat actors are launching attacks that invariably slip past single-method detection technology unnoticed (and can often bypass even multiple method detection technologies). Single-method detection is ineffective if it is unable to dynamically adapt to the relentlessly fast-paced and evolving threat landscape.

**Single Event**

A threat evolves along well-understood phases — reconnaissance, weaponization, delivery, exploitation, malware installation, command and control callback and payload drop, and execution of hostile actions (e.g., exfiltration of digital assets and IP) — as depicted in Figure 5 in the context of a kill chain. A single-event methodology is typically focused only on malware delivery. As previously mentioned, the first few phases of an attack are designed to obtain control of an employee’s device and malware delivery may not always occur inside the enterprise’s boundaries. In any event, most advanced single-event solutions are focused only on detecting the exploit and are therefore ineffective against all attack vectors at all attack stages.

**Single Signal**

The Cyphort argument, thus far, posits that a single-presence or single-event solution is unable to provide comprehensive detection or protection capabilities. Now, allow us to flip the coin and show how a single-signal solution often inundates and overwhelms an enterprise with its barrage of alerts and threat data.

A single-signal solution generates a separate alert for every single suspicious signal it identifies. When installing advanced single-signal threat detection system into a network, it is often the case that a flood of potential malware alerts demonstrate an impressive and shocking spread of attacks throughout your network; you were blind but now you see. Initially, this epiphany is exciting — and alarming at the same time. So what happens? In most cases, the IT checkbooks come out ready to fund a solution. But enterprises soon realize that operationalizing these alerts is massively time-consuming and costly. And perhaps just as important, they fail to acknowledge the relationship between such an alert and loss of IP or compromised digital assets. In many
cases, the alert may be triggered by a threat that cannot succeed in your environment (for example, it exploits an old version of a browser that is no longer in use in your company) or by a threat that has already been identified and blocked on the targeted host by your corporate AV tool. In both these examples, time is spent researching mitigation efforts for an alert that should have been immediately de-prioritized so that time is better spent on an attack that actually infected several client machines and located valuable assets for stealthy exfiltration.

On the other hand, some alerts are triggered by unusual but harmless code. If an enterprise unnecessarily wipes employees’ machines as a result of alert overload, it is incurring excessive workloads for the IT team and causing a loss of employee productivity.

Cyphort’s Comprehensive Approach

Given the state of the world’s cyber security challenges, any effective solution for threat detection and protection must be fundamentally multi-dimensional. This multi-dimensional aspect of continuous inspection, detection and mitigation is the core of Cyphort’s cyber security solution. Delivered as software that can be installed on general-purpose hardware, virtual machines and cloud environments, our solution consists of four components:

- **Collectors** — software-based probes that monitor traffic across web, email and file-sharing applications, and ‘collect’ the suspect malware data.
- **Cyphort Core** — the centralized detection component of our solution.
- **Cyphort Manager** — the web-based administrative interface for managing distributed deployment, and access to reports and functions.
- **Cyphort Threat Network** — cloud service that feeds global threat intelligence to the Cyphort Core.

Here are the benefits of our approach:

- **Comprehensive Visibility**: The Cyphort solution decouples its inspection sensors, the Collectors, from its analysis engine, Cyphort Core, providing the ability to collect object-based (not merely session-based) network traffic from multiple points of presence in an entirely non-intrusive and significantly cost-effective manner. Optionally, the Cyphort architecture is available as a cloud-based SaaS deployment.

- **Accurate Detection**: The Cyphort analytics approach correlates collected threat data along the entire kill chain (Figure 5) thus increasing the reliability with which Cyphort detects malware and infections in an environment. This approach enables corporate networks to detect threats outside the corporate boundaries on exploited remote or mobile devices such as employee laptops, tablets, or smart phones (BYOD).

- **Multi-Platform Coverage**: Cyphort uses machine learning to automatically adapt to the threats it observes instead of using hard-coded detection rules. This strategy enables Cyphort to quickly adapt to evolving threats, including evasive armored malware attacks, while simultaneously operating with the flexibility required to detect threats that target a wide range of platforms (such as Windows, OSX, Unix, and Android).

- **Actionable Threat Intelligence**: The Cyphort solution ascertains true security threats by using a tertiary (not simply binary) Hierarchical Reasoning Engine (HRE) to aggregate and correlate behavioral analysis results, static analysis information, network command and control (C&C) callback data, and reliable reputation scores to determine actual risks or relevance of detected threats in an enterprise network. The HRE alerts also support existing SIEM and security controls by providing the intelligence needed to successfully block and mitigate an attack. Additionally, Cyphort follows up its alerts when an infection is detected by deploying a component that assists with mitigation; it assesses all hosts in a domain and identifies which hosts, if any, are specifically infected.

The Cyphort Approach: **Comprehensive Visibility**

Cyphort’s architecture is designed to break the kill chain and adapt to the enterprise’s network configuration. First, Cyphort separates continuous inspection of traffic data and objects from threat detection and analytics, and then Cyphort Collectors use object-based technology, so they are not limited to session-based inspection. This is a significant advantage over existing analysis and detonation technologies because it allows for the deployment of various collectors throughout the network, in a substantially cost-effective manner, with less latency during behavioral analysis cycles. **Figure 2** depicts a typical main campus deployment where collectors...
are placed at various attack vector-specific locations on the perimeter (Internet, Extranet) as well as located internally.

Moreover, if most of an enterprise’s employee network traffic is encrypted until it reaches its internal VDI destination servers, Cyphort Collectors can be deployed at the point of decryption to inspect that network traffic at the VDI. Meanwhile, an email Collector can be inspecting email content simultaneously, providing deep and continuous surveillance of the critical email threat vector while also providing visibility of the entire correlated Web and e-mail kill chain.

**Figure 3** depicts a distributed enterprise deployment. Attackers often attempt to get a foothold in your environment via a remote site’s vulnerabilities, hoping that such a site may have weaknesses in their security posture not found at the main campus site. Therefore, deploying Collectors extends protection of the main campus. This also enables Cyphort to correlate global activities from any corporate site.
Cyphort designed its cyber security product to specifically break the threat kill chain by focusing on delivery, exploitation, malware, and command and control. This differentiates Cyphort from all competing cyber security products. With Cyphort, enterprises are able to surveil all phases of a cyber threat while providing deep, instrumented analysis at its Core with unique, machine learning correlation capabilities that generate actionable intelligence for every phase of an attack:

**Kill Chain Exploitation**

Malicious exploit code typically installs on a client machine with the sole purpose of indicating “I’ve arrived” to a C&C server, from which, it later downloads and installs the malware payload. This exploit code typically takes advantage of vulnerability in a web browser, plug-in, media player, PDF reader or the like. Exploit code today has achieved a high degree of evasion (see Figure 5), making it hard to detect reliably — various evasive techniques, such as java script obfuscation and redirection inside a browser, have become widespread.
Kill Chain Malware Installation

The malware installs on a client machine for the purpose of identification and exfiltration of digital assets, possibly gaining privilege and access to other processes for secondary or simultaneous threat objectives. The malware uses techniques such as root kits and backdoors. Attack code is often delivered as an .exe file, and it is frequently obfuscated via encryption or by embedding into other files (see Figure 6).

Figure 6: Challenges in Breaking the Kill Chain

Prevalent Behavioral Techniques

Most behavioral solutions and products are focused on detecting advanced threats by executing exploit code in network traffic via a virtualized sandbox (see Figure 7). Their success is severely limited by session-based network traffic capture as well as by the increasingly sophisticated evasion techniques of exploit code, compounded by the fact that there are a huge number of exploitation vectors resulting from different software versions and traffic protocols. Moreover, social engineering-based attacks that exploit human trust and judgment often completely sidestep sandbox detection. As a result, these products are changing course to look for attack code in .exe files as well. As indicated previously, these files are often obfuscated and therefore slipping past inline detection.

Figure 7: Current Solutions

Cyphort Kill Chain Analytics

The Cyphort approach understands the entire threat kill chain. Based on the need for comprehensive visibility, Cyphort has built sophisticated collection and analytics engines (see Figure 8). The Collectors inspect traffic data and Cyphort Core analyzes suspicious traffic using correlation intelligence to identify the relationships between exploitation, installation, command and control, and execution phases in the kill chain, from both code structure and code behavior perspectives. This enables the following Cyphort advantages:

- **Cyphort recognizes Malware** regardless of whether it’s delivered via a vulnerability exploit or social engineering. Cyphort’s architectural flexibility allows it to focus on finding the malware payload code, rather than the exploit code. The malware payload is where the threat is most vulnerable and provides the best opportunity for detection.

- **Cyphort finds and extracts malware** even if it is encrypted or embedded in other files. Once Cyphort suspects that a network object contains malware payload code, it traces the code back to the root of the exploit code to help extract the malware via decryption, de-obfuscation, etc.

- **Cyphort determines the severity of each threat** reliably, and provides actionable intelligence for detected malware and infections. Cyphort runs the malware payload code in multiple behavioral analysis “cookers” in the Cyphort Core to detail the expected behavior of each attack.
Cyphort determines the likelihood of a threat to succeed in an enterprise’s specific environment. Cyphort tracks a threat from initial exploit through its command and control phase to fully identify if it successfully installed malware on a targeted host.

**Actionable Threat Intelligence**

Figure 9 shows how Cyphort’s supplemental security data can help deliver relevant and actionable threat intelligence. The concrete risk of an attack unfolding in an enterprise environment depends on the security posture of the target machines. The data helps address the following questions. Did the deployed anti-virus block the threat already? Did the last CVE vulnerability scan reveal a relevant un-patched vulnerability? What applications are running on the target, and what OS is installed? What are the assets on the target or what privileges does the target have to critical assets stored elsewhere in the corporate network?

Additionally, the Cyphort platform automatically incorporates third-party security and asset data (SIEM) and correlates that data with its own threat detection and modeling capability to provide contextual relevance for each threat, which, in turn, allows for fast priority and risk assessment without expensive escalation for each and every detected threat.
Protecting Ongoing Threats

The final and arguably the most important step in the Cyphort solution is mitigation of ongoing attacks and proactive protection against evolving threats. To that end, in environments that have already deployed a variety of security controls, Cyphort’s actionable threat intelligence (See Figure 10) empowers those controls by feeding them change requests. The Cyphort change requests are calculated to block network traffic from attacker-controlled, command and control sites — based on IP addresses for firewall changes, or based on domains and URLs for Secure Web Gateway changes.

Traffic can be blocked from already-infected client machines for isolation, or requests can be made to block downloads of the malicious code in the future based on “on-the-fly” generated signatures for IPS control changes.

Figure 10: Actionable Intelligence
Conclusion

Advanced malware threats are fundamentally different from the threats of yesterday. The tools required for detecting and mitigating these threats must be equally different or more evolved and sophisticated. Despite all the marketing hype, most solutions available in the marketplace today provide only marginal improvements over the security solutions you may already have in place. Typically expensive, these solutions are often tied to the architecture and detection methods of older threats and networks. Additionally, many of these solutions rely on a single-presence architecture and single-method approach, single-event and single-signal detection methods, and are therefore limited in their ability to comprehensively view and handle advanced threats across all stages of the attack cycle.

Cyphort provides a solution that is built from scratch specifically to defend against today’s advanced threats and polymorphic attacks. In fact, Cyphort empowers customers to defend themselves from the threats that matter most. The Cyphort advanced threat solution goes beyond malware detection to reveal the true intent of the attack and the risk to your organization with prioritized and expedited remediation.

Cyphort’s distributed architecture, combined with hierarchical machine learning as well as the big data analysis capabilities of the Cyphort Core Analysis Engine, ensures that no threats go undetected. With Cyphort, enterprise and cloud networks are protected and remain open for business.

The Cyphort Advanced Threat Defense Platform offers the following benefits:

1. Provides coverage across your entire enterprise attack surface, and is not limited to ‘key’ locations.
2. Detects most dangerous, armored and targeted threats. Our multi-method sandboxing and multi-platform threat detection coupled with machine learning and a robust correlation engine enables your security teams to quickly and accurately determine the existence and severity of an advanced targeted attack.
3. Enables context-based prioritized, actionable intelligence. We help enterprises like yours cut through the avalanche of security data to get to the threats that matter and respond with velocity. We understand that detecting already compromised systems is just as important as detecting previously unseen malware.
4. Results in a lower cost of ownership solution and lower opex. With everything automated, we help reduce resolution time by better understanding threat intent, stage, targets, and adversaries. Enterprises will know exactly how to mitigate risk using existing perimeter security controls, and cleanup only truly infected devices. And our software-based approach simplifies deployment by offering the flexibility enterprises require. Our solution can be installed on general-purpose hardware, virtual machines, and cloud environments. Our ‘right-size’ licensing makes it a practical solution for deploying across the enterprise, even the smallest of branch offices.
About Cyphort:

Founded in 2011 by a team of security experts, Cyphort advanced threat defense goes beyond malware detection to reveal the true intent of the attack and the risk to your organization with prioritized and expedited remediation. Our software-based approach combines best-in-class malware detection with knowledge of threat capabilities and your organizational context to cut through the avalanche of security data to get at the threats that matter and respond with velocity, in hours not days.

We empower enterprises with the three C’s of security — reduced resolution time and cost for easy deployment across your entire network, virtual and cloud infrastructure; comprehensive coverage via a distributed software model; and a context-based approach to Advanced Persistent Threats (APTs).