Whitepaper

Disrupt the Machine-to-Human Fight with a New Defender Lifecycle Model in Security Operations

A Defender Lifecycle Model Shifts Control and Advantage Away from the Attacker

Synopsis: Traditional security strategies focused on prevention are no longer sufficient to defend against the increasing speed, volume and polymorphic nature of today's cyber threats. Instead, organizations must embrace a new Defender Lifecycle Model, which shifts control and advantage from the attacker back to the defender by integrating machine learning, artificial intelligence (AI) and security workflow automation with a foundation of pervasive coverage.

Breaches Are Inevitable. The Question Is, Why?

There's no such thing as absolute security. Facing more determined hackers with increasingly sophisticated methods, organizations must accept the fact that they are vulnerable and open to an attack at any moment. Data breaches will happen.

Why has this become a fact of life? While several scenarios contribute to the inevitability of breaches, two primary factors stand out:

- **The speed of data.** With the speed at which data travels today, real-time security against unknown threats is a near impossibility. Consider, for example, 100 Gigabit Ethernet links. The time between data packets traversing these networks is 6.7 nanoseconds — in other words 6.7 billionths of a second. That speed surpasses our ability to perform any meaningful or intelligent application security, threat detection or inspection. As a result, unknown threats will break through organizations' defenses and propagate across their infrastructures.
- **Democratization of malware.** Today, sophisticated malware, Command and Control (C&C) infrastructures and phishing campaigns are all available for rent or purchase on the dark web. Consequently, the capacity to compromise the human element through social engineering, leverage large-scale botnets or use any number of other cyber-attack techniques is no longer limited to elite, sophisticated hackers or nation states. Rather, they are all available to the general public.

Defenders are overwhelmed by trying to manage and mitigate the increasing volume and variety of incidents — an issue further compounded by the fact that organizations continue to use mostly manual workflows to address incidents. This often leads to them falling a step, if not several, behind attackers who are launching intensive, sustained attacks using droves of automated bots. In effect, this becomes a machine-to-human fight where organizations are severely disadvantaged due to a shortage of skilled manpower and resources.

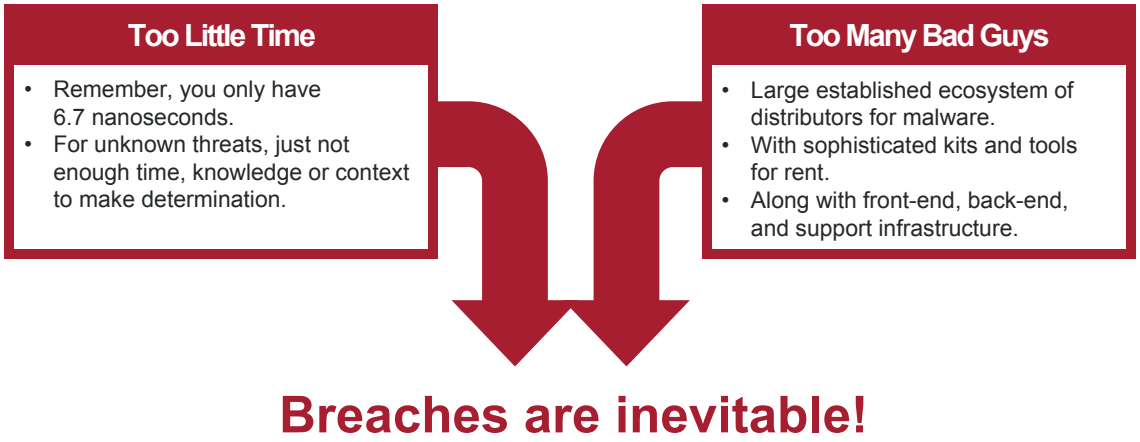

Figure 1: Real-Time Threat Prevention May Not Be Possible, Particularly for Unknown Threats

A Paradigm Shift: Building Immunity vs. Patching with Bandages

Too often, organizations fall prey to the misperception that the quality of security is measured by the quantity of security tools. In other words, the more tools they have, the more secure they are.

Unfortunately, plugging security products into portions of an infrastructure is akin to patching injured portions of the skin with bandages, which provides minimal coverage, offers limited protection and cannot constrain exposure to airborne, waterborne or other forms of communicable diseases. What's more, they can also only be applied after an injury and not used to help predict or prevent one.

This current security model is lacking. To defend against the increasing speed, volume and polymorphic nature of today's cyber threats, organizations need a new Defender Lifecycle Model, whereby they act under the assumption that they will be breached. They need to build network security from the perspective of developing immunity rather than trying to patch after an incident.

A Defender Lifecycle Model:

1. Works from within as well as across your entire infrastructure — whether physical, virtual or cloud networks.
2. Continuously learns, adapts and remembers.
3. Responds and takes action quickly.

In effect, a Defender Lifecycle Model provides the opportunity to level the playing field and move the advantage and control from the attacker back to the defender by integrating machine learning and AI-based technologies, as well as automating security workflows. It changes the dynamic by making this a machine-to-machine fight rather than perpetuating the attacker advantage in a machine-to-human scenario. With this new model, you can map out the role of various security products, gain a better understanding of your overall security readiness and gaps and ultimately, strengthen your overall security risk posture and efficiencies.

Foundation of a Defender Lifecycle Model

In expanding beyond the attack kill chain, this new Defender Lifecycle Model focuses on a foundation layer and four key pillars — prevention, detection, prediction and containment — that work together in an automated, cyclical continuum.

Pillar 1: Prevention, Making It Harder to Break Through the Perimeter

Good hygiene is the key to prevention; the precursor to a healthy security approach. Derived from "traditional" preventative measures such as department and perimeter firewalls, identity and access control, network segmentation and asset isolation, good hygiene creates an environment that makes it harder for adversaries to break into an organization as well as to propagate and spread within an organization. In other words, it forces them to take unnatural steps to carry out their activities and in doing so, makes it easier to detect their presence.

In early security models, this pillar served as the entire security "prevention" pillar. Today, while still crucial, it is only the first step toward building a more robust Defender Lifecycle Model.

Pillar 2: Detection, Building Context with Big Data and Machine Learning

Good hygiene feeds into the second pillar of a Defender Lifecycle Model: detection. By forcing adversaries to take unnatural steps, you can more easily surface anomalies in behavior.

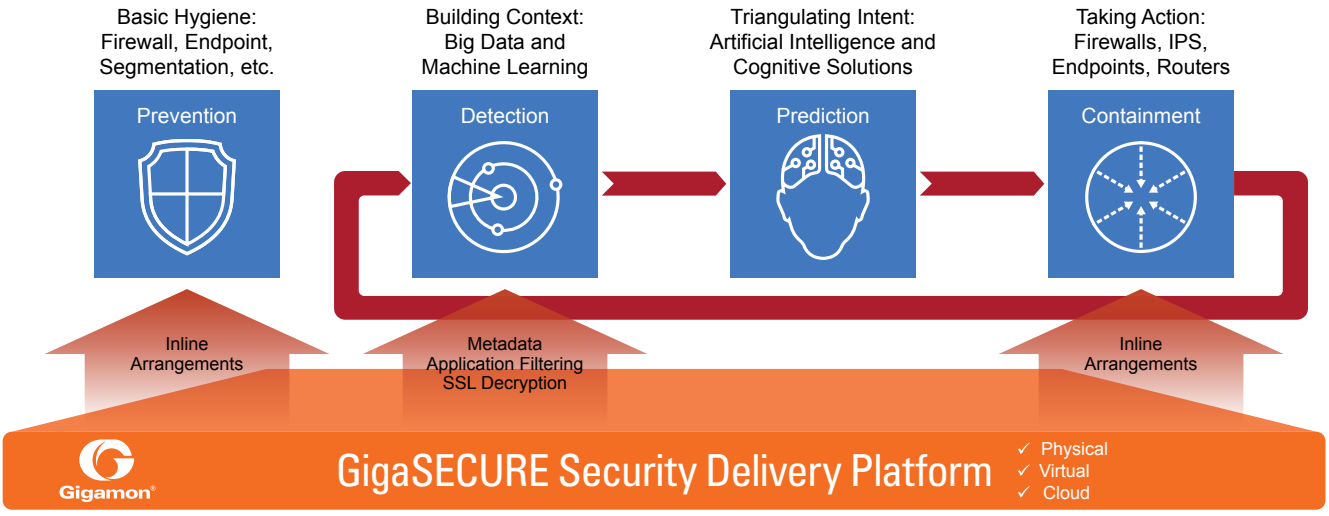

Figure 2: A New Security Model: The Defender Lifecycle

Anomalies are variances relative to normal behavior and therefore, detecting them requires the establishment of a baseline of normal behavior. The key is establishing context and becoming familiar with everyday network behavior to determine and understand what normal looks like. Once you've established that baseline, you can triangulate user activity against it — as well as against known bad behavior — to detect abnormalities within systems. This is the basis of many machine learning technologies today — they learn, they remember and adapt to changing user, device and application behavior and they detect deviations from that behavior.

Pillar 3: Prediction, Triangulating Intent with Artificial Intelligence

Identifying anomalies allows you to build the next phase of a Defender Lifecycle Model: prediction. Prediction is key to understanding intent, for example, what the bad actor is intending to do or has already done. Identifying a single anomaly does not mean much, nor does it provide context of the entire threat behavior. You need to understand the intent of the bad behavior. This is where artificial intelligence and cognitive solutions come into play.

Since many of the malware and C&C threats are essentially "existing" frameworks that have been rented or purchased, it follows that subsequent actions in the attack cycle may mimic behaviors that have been learned or seen in the past, albeit morphed or disguised. AI-based solutions attempt to uncover patterns in the face of polymorphism and guise to predict intent, to surface underlying patterns of behavior and to generate a set of actions that lead to the next stage in the defender lifecycle: containment.

Pillar 4: Containment, Taking Action

Once you've uncovered intent, you can take action to contain, remediate or even allow contained detonation of the threat so as to better understand the intent.

Detection and prediction are powerful pillars, but without containment, you cannot gain control and mitigate bad behavior in a rapid manner that minimizes cost and risk. Today, the threat containment process is manual and time intensive, requiring coordination across multiple groups and actions across endpoints, routers and switches, firewalls and IPSs. Ownership and change management for many of these steps rest within different departments of an organization, and each requires a different set of procedures, skills and review processes. This must change. Organizations need to hasten containment through streamlined processes, minimized touch points and the development and deployment of automation and security workflow orchestration solutions.

The New Foundation Layer: Pervasive Visibility, the Basis of a Defender Lifecycle Model

Pervasive visibility into data moving across physical, virtual and cloud environments is the foundation of a Defender Lifecycle Model. Without it, detection, prediction and containment solutions will be patchy at best and could essentially defeat the objective of building out a Defender Lifecycle Model. The best way to deliver the necessary and complete level of visibility is through a Security Delivery Platform.

A Security Delivery Platform helps ensure coverage across your entire infrastructure and the data that traverses it. It allows for the delivery of diverse and sophisticated security services that can learn, detect, predict and contain threats throughout the lifecycle. A Security Delivery Platform provides essential services to the four pillars of a Defender Lifecycle Model, strengthening them, increasing their efficacy and helping to constrain the costs of building out, maintaining and optimizing the model.

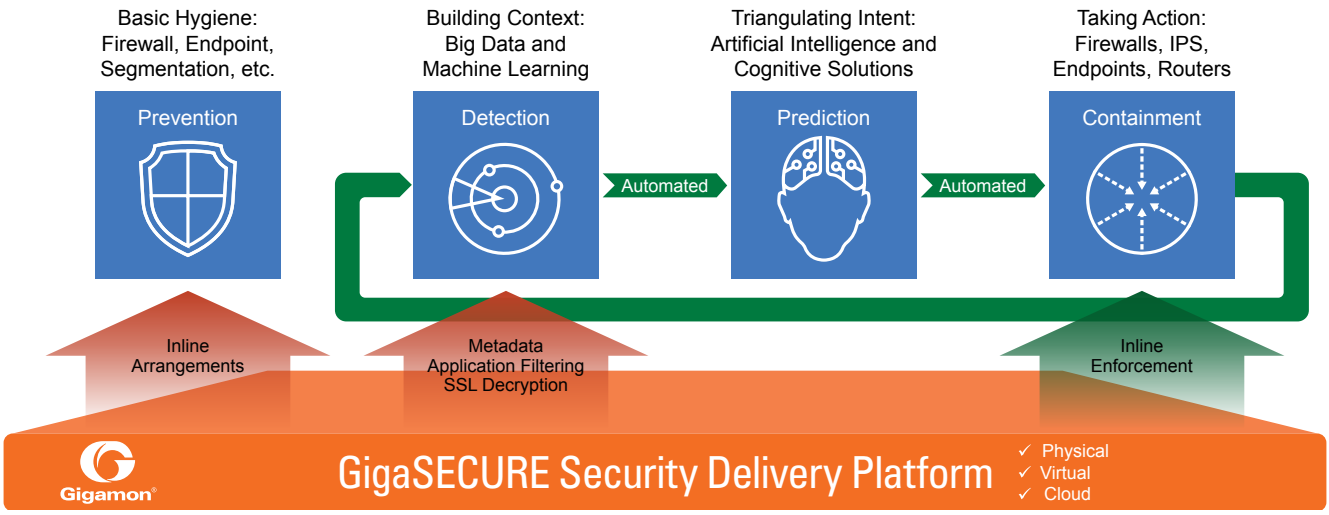

Figure 3: A New Security Model: The Defender Lifecycle

How a Security Delivery Platform Works: Key Services

A Security Delivery Platform provides several key services that support each pillar of the new Defender Lifecycle Model.

Pillar 1: Prevention

A Security Delivery Platform supports flexible in-line deployments for various security solutions such as firewalls and IPSs. While supporting resiliency and failover, it enables load balancing of traffic across security applications, daisy chaining of security tools and the distribution of relevant traffic to appropriate security appliances. Moreover, with its SSL/TLS decryption functionality, it can deliver visibility into encrypted channels of communication across in-line and out-of-band security solutions.

With a Security Delivery Platform, you can seamlessly move security solutions either in-line or out of band without impacting the network. You can also simplify workflows, reduce friction between security and network departments and facilitate the introduction of new solutions with minimal impact. Together, these capabilities contribute to good security hygiene.

Pillars 2 and 3: Detection and Prediction

Detection and prediction are predicated on the ability to access the right information. Today, the network has become the medium of choice to extract information. In fact, it is the only medium that connects users, devices and applications in all environments — physical, virtual and cloud — thus making it the single most content-rich source of information. From network traffic, you can glean information about application behaviors, end-point and user behavior and data access patterns.

Attempts to spread malware laterally across an organization, perform any adversarial Command and Control activity or exfiltrate data typically occur over the network. Consequently, if harvested correctly — which a Security Delivery Platform is designed to do — network traffic can become the source of truth and the "gold standard" of information for forensic activity. A Security Delivery Platform can conveniently harvest information from the network and feed it into machine learning and AI-based technologies to help ensure that they are working from accurate data sets and with time-relevant information.

With a Security Delivery Platform, you can gain access to:

- Application-specific and broad streams of network traffic data.
- Network packet data from/to entities of interest.
- Decrypted traffic based on SSL/TLS sessions.
- Metadata extracted from encrypted streams of communication, which becomes especially critical as the industry moves toward embracing encryption as the norm.
- Metadata extracted from network traffic data including items such as DNS information, and SSL certificate information.

By enabling this level of visibility and working directly with network traffic or data in motion, a Security Delivery Platform can significantly reduce cross-departmental challenges of extracting relevant data, as well as processing overhead on various security solutions and appliances such as domain controllers and routers. Your security tools are no longer grappling with an overload of data or working on incomplete data sets and instead, can focus on what they were specifically designed to do.

Pillar 4: Containment and Action

A Security Delivery Platform plays a critical role in helping to ensure that the right security solutions can take the right actions at the right time. Fittingly, the services delivered by the tools in the prevention pillar also support the containment pillar where the active security devices are the same. Typically, these devices include firewalls, IPSs, routers and switches.

Key Security Delivery Platform services that support containment and action include:

- The ability to deploy security solutions in-line with network traffic without risk of taking down the network should failure occur.
- Scalability of in-line tools through sophisticated, session-aware load-balancing capabilities.
- Decryption of traffic where necessary.
- Filtering in or out the right traffic to help ensure that firewalls, IPSs, routers and switches see the traffic they are programmed to act on.

Speeding up the Defender Lifecycle Model with Automation and Orchestration to Close the Loop

A Defender Lifecycle Model is clearly becoming a necessity in security operations. However, it is not a silver bullet against threats. Even with a solid model, you may find yourself a step behind your adversaries. The reason lies within the continuous loop from detection to prediction to containment and back again to detection. You must be agile and quick to respond to incidents — and unremitting in reassessing your situational awareness to uncover any additional or new anomalous activity.

Security operations are typically constrained by organizational processes, siloed product deployments, manual and time-intensive tasks and an acute shortage of security professionals. Any efforts to build a continuous and adaptable security approach must address these inefficiencies and remove human touchpoints wherever possible. This is why automation and orchestration become integral aspects of the new model.

While aspects of machine learning and AI are becoming more automated to address the needs in pillars 2 and 3, the containment pillar remains a significant bottleneck as highly manual, laborious and time-consuming processes continue to be the norm. For example, devices designed and designated to take action may be owned by different departments within an enterprise's IT structure — a situation that can lead to tedious and error-prone change management and delays.

In order to automate and orchestrate a set of actions, you must address a few requirements and develop a plan to:

1. **Ensure security solutions are positioned in all the right places.**
   To take actions, security solutions need to be in the right places so they can act on the right traffic. Programming a rule in a router makes no sense if, for example, a piece of malware is attempting to remotely connect into a server that is not on the segment connected to the router. The first criteria to enabling proper orchestration and automation is to make sure that any device taking action is in all the right places.
2. **Have a consistent and uniform set of APIs.**
   Having a simple, consistent set of APIs for automation and orchestration is a key requirement for hastening a Defender Lifecycle Model response. The challenge today is not a lack of APIs, but rather a proliferation of them. Since organizations use different security solutions from different vendors — all with their own unique APIs — the task of orchestration and automation becomes extremely complex and problematic. What's more, that does not even include the Herculean task organizations face in trying to keep up with API changes from all vendors. The industry needs to move toward a reduced and consistent set of APIs that orchestration solutions can use to simplify automation.
3. **Enable the right set of actions.**
   To name a few, the right set of actions includes redirecting traffic to a sandbox, blocking certain types of traffic and capturing a full conversation to a recording device.

A Security Delivery Platform provides an opportunity to address many of these considerations and speed up the cycle from detection to prediction to action and back again.

- **A Security Delivery Platform is in the right places.**
  In many cases, a Security Delivery Platform is a front end for firewalls, IPSs and other in-line network appliances. As such, it is in many of the right places — or, in some deployments, a superset of the right places within which these solutions find themselves.
- **A Security Delivery Platform has a consistent, uniform set of APIs.**
  When used to manage and control traffic flows both within the network as well as to various, connected security solutions, a Security Delivery Platform exposes a set of APIs that provide you with a simple consistent way to automate — rather than forcing you to contend with the complexities of API explosion and overload. In essence, the APIs exposed by a Security Delivery Platform become a de facto communications bus or conduit for all connected security tools and significantly reduce the API explosion problem.
- **A Security Delivery Platform can trigger the right set of actions.**
  When coupled with the platform's ability to take certain actions in-line with the network, the problem of orchestration and automation becomes a far simpler exercise, which enables you to truly embrace security automation and address many of the challenges associated with accelerating the system's response.

Reclaiming the Defender Advantage

It's clear that organizations increasingly find themselves at an inherent disadvantage when dealing with cyber threats as attackers continue to hold the lead by inundating them in volume, diversity and sophistication of attacks, and stretching their ability to respond.

It's time for a reversal and restoration of the advantage back to the defender. As the industry and governments rethink approaches to cybersecurity, we need to consider a new model that:

- Maps out the defender lifecycle and models itself similarly to the human immune system. Such a model can apply machine learning and AI-based technologies to the defender's advantage.
- When coupled with security workflow automation and orchestration for rapid response, the defender lifecycle provides an opportunity to disrupt the machine-to-human fight and make it a more defendable machine-to-machine battle.

With a Defender Lifecycle Model, you can prevent, detect, predict, contain and take action to thwart bad actors and threats quickly and decisively, and also reduce cost and complexity, mitigate security risks and improve business decision making. For more information visit **www.gigamon.com/gigasecure**

2042-01 07/17

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com