Whitepaper

Addressing the Threat Within: Rethinking Network Security Deployment

Introduction

Cyber security breaches are happening at an industrial scale. The unabated volume of cyber breaches along with the scale and magnitude of the breaches is forcing the entire industry to re-think how cyber security gets deployed, managed and addressed. At the heart of this change is a fundamental shift in the assumptions and the model under which cyber security has been operating.

The traditional model was one that operated under simple assumptions. Those assumptions led to deployment models which in todays' world of cyber security have been proven to be woefully inadequate at addressing malware and cyber breaches. Some of these are outlined below:

- **Perimeter Based Security:** The traditional cyber security trust model was based on simplistic assumptions of creating a perimeter and ensuring that what was outside the perimeter was unsafe and what was inside was considered secure. That perimeter security typically consisted of a firewall at the internet edge and endpoint security software such as an anti-virus solution, at the user end. However, most of the perimeter firewalls and endpoint security software solutions leverage rules and signatures to identify malware. In today's world, many of the cyber breaches exploit zero-day vulnerabilities. These are vulnerabilities that have been detected but for which no patches exist in various pieces of software or for which no signature or rule exists as yet. Consequently it is increasingly difficult for traditional perimeter-based solutions to prevent malware and threats from breaking in.
- **Simple Trust Model:** The traditional cyber security trust model was based on a simple trust model of employees being trusted and everyone else being not trusted. However, in today's world where employees are using personal computing devices, such as smart phones for business needs, or where the work force consists of employees, consultants, contractors, and vendors, all of whom access an enterprise's network and IT resources, that simple trust model breaks down and the source of a threat could just as easily be an employee or contract employee. Additionally, the traditional trust model also incorporated the notion of IT-owned assets that were considered trusted as they had the right build of software and anti-virus, among others. However, today employees use not just IT-owned assets but personal assets such as personal laptops, tablets, and smart phones for business productivity. In other words Bring Your Own Device (BYOD) is increasing productivity, but breaking down the simple trust model assumptions.
- **Static Environment:** Traditionally, security appliances were deployed at fixed locations. This included firewalls, intrusion detection/prevention systems (IDS/IPS) and other malware detection and prevention systems. Typically these would assume a fixed perimeter or a set of fixed "choke" points at which traffic was expected to traverse and consequently be monitored for threats. However, with the mobility of users, devices and applications the predictability of traffic patterns has diminished. Additionally the adoption of the cloud has extended the edge and perimeter boundaries with the ability to dynamically burst capacity into the cloud on-demand. This is making the workplace a far more dynamic environment with far less predictability on where the boundaries and choke points lie. Consequently, the ability to consistently and comprehensively identify all threats based on the static deployment of security appliances at fixed locations has been severely impaired.

Despite the breakdown in some of the traditional assumptions outlined above, a lot of enterprise security architectures still rely on them for preventing network breach. Additionally, the very nature of cyber threats has also evolved significantly over time. In the past, once a worm or virus breached into a network it would propagate quickly and do as much damage as possible in as short a time as possible. This made it possible to detect worms and viruses more quickly due to the footprint they left in the wake of their disruption. Today's threats have evolved to become far stealthier, more sophisticated and destructive at an industrial scale. Many of them are grouped under an umbrella called Advanced Persistent Threats (APT). These APTs are the source of many of the recent large scale breaches. They tend to employ a variety of sophisticated methods to compromise the network and take up residence there for long periods of time, hence the name: Advanced Persistent Threat.

Anatomy of an Advanced Persistent Threat

Many of today's large scale breaches take place over multiple stages and over extended periods of time ranging from weeks to months. Some of these stages are outlined below:

1. **Reconnaissance:** During this stage, the threat perpetrator or threat actor typically spends time understanding the various online activities of possible targets and trying to identify a way to inject malware based on those activities. For example, the actor would observe what bank websites, or what social networks a user browses, what interest groups a user subscribes to, and other online habits. Based on this a profile for possible targets is built.
2. **Initial breach:** This is the phase where the user or target is initially compromised. Typically based on a user's activities and profile, an email or a blog post is formulated that invites the user to click on a link. Once the user clicks the link, the user is re-directed to a website where a zero-day vulnerability is downloaded onto the user's system. This is typically referred to as a phishing attack. Other such attacks like drive-by downloads are commonplace as well. Their job is to simply inject a piece of malware onto the user's system. In many cases that malware footprint is quite small and really intended to create a backdoor communication channel.
3. **Backdoor access:** Once the user's system has been compromised via the initial malware download, that malware then explores possible communication backdoors that can pass through firewalls, with the intention of opening up a communication channel with a command and control center that could be located anywhere in the world. Once that communication channel is established, additional malware and/or instructions are downloaded.
4. **Lateral movement:** The malware then starts probing and propagating internally by finding other systems that have vulnerabilities. However, this is done in a very stealthy way by disguising the malware's activity and by minimizing the footprint of activity, methodically. This activity can take weeks to months. In other words the lateral movement of the malware is very low and slow. During this phase, additional backdoors may also be opened in the event that the initial backdoor is detected and closed.
5. **Data gathering:** Once the malware spreads and finds access to critical resources across the infrastructure, it begins the process of identifying critical data resources to exfiltrate or recording data for the purposes of exfiltration.
6. **Exfiltration:** The gathered data is then exfiltrated in a mass way through the various backdoors. At this point the organization's information is severely compromised. The threat actor may request ransom, expose classified or confidential data, or sell the information at auction.

In many cases the organization stays compromised after the exfiltration, making it susceptible to continuous attacks and breaches. In fact, even after a breach is detected and many of the compromised systems are cleansed, in many cases, due the extensive nature of the breach, some systems continue to remain compromised and undetected. These compromised systems may then be made available through sites offering malware-as-a-service where individuals or groups can purchase these infected assets. Malware-as-a-service has grown into a big industry giving individuals and organizations easy and cheap means to leverage compromised systems to mount DDoS attacks for example.

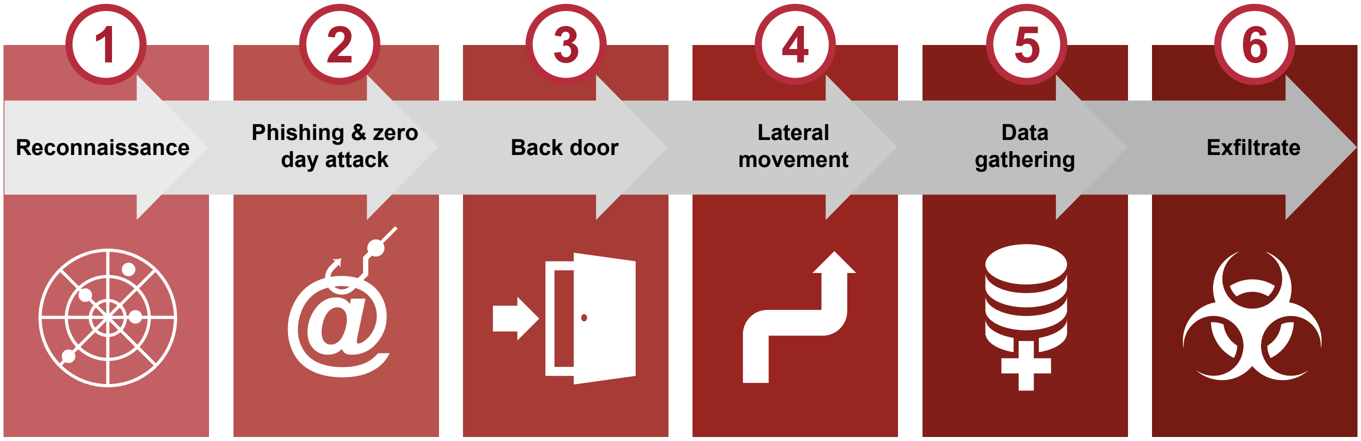

Figure 1: Anatomy of an advanced persistent threat

In a recent study[1] that evaluated 1,200 enterprises across 63 countries, it was found that 97% of the organizations in the study were breached during the test period. Of those organizations, 75% had active command and control activity. In another study[2] it was found that the mean number of days from initial intrusion to detection of the breach was 134 days indicating that many organizations can stay breached without knowing it for months.

This all points to a need to rethink how security is modeled. Enterprises can no longer act on the assumption that they can keep threats out. Instead organizations should increase focus on detection of breached systems and containment of malware. Identifying compromised systems has become increasingly difficult given current trends in IT.

IT Trends Impacting Security

Changing Workforce and BYOD

There are several IT trends that adversely impact the ability to address security from within. As mentioned earlier, the very nature of the workforce has changed with employees, consultants, and contractors all being treated as part of an enterprise's workforce. This has made it harder for IT to enforce controls based on roles. BYOD and the consumerization of IT has significantly loosened the strict controls that IT had on the security posture of computers, laptops, mobile phones and other devices that the workforce uses for productivity.

Increase of East-West Traffic

Another major shift is in the data center where traffic patterns are shifting to an east-west direction as a result of servers and Virtual Machines (VMs) talking to each other and to database systems, storage systems and other applications all within the data center. East-west traffic typically never hits the core of the network where it can have the benefit of security inspection like IPS/IDS deployed to detect malware or threats within traffic. Further, the volume of east-west traffic is quickly becoming a much larger percentage relative to north-south traffic that is traffic flowing to and from the Internet. This makes it easier for a piece of malware that may have breached an older or unpatched server to spread laterally within the data center undetected by security measures meant to intercept and inspect north-south traffic (see Figure 2).

As an example, Facebook runs 1 million map-reduce jobs per day.[3] This results in significant network traffic that stays within the data center. While most enterprises would not approach this level of scale, the growing use of big-data solutions by many large and mid-size enterprises is a driving force in this shift in traffic patterns within data centers. As another example, the adoption of VDI (Virtual Desktop Infrastructure) by several enterprises has moved the desktop into the data center. Consequently client-server traffic which traditionally used to be north-south traffic and that traversed through the core of the network and through well-defined choke points, has now become east-west traffic between the virtual desktop instances and the applications, all of which are hosted within the data center. All of this traffic is flying under the radar of security appliances that do not have access to this network traffic.

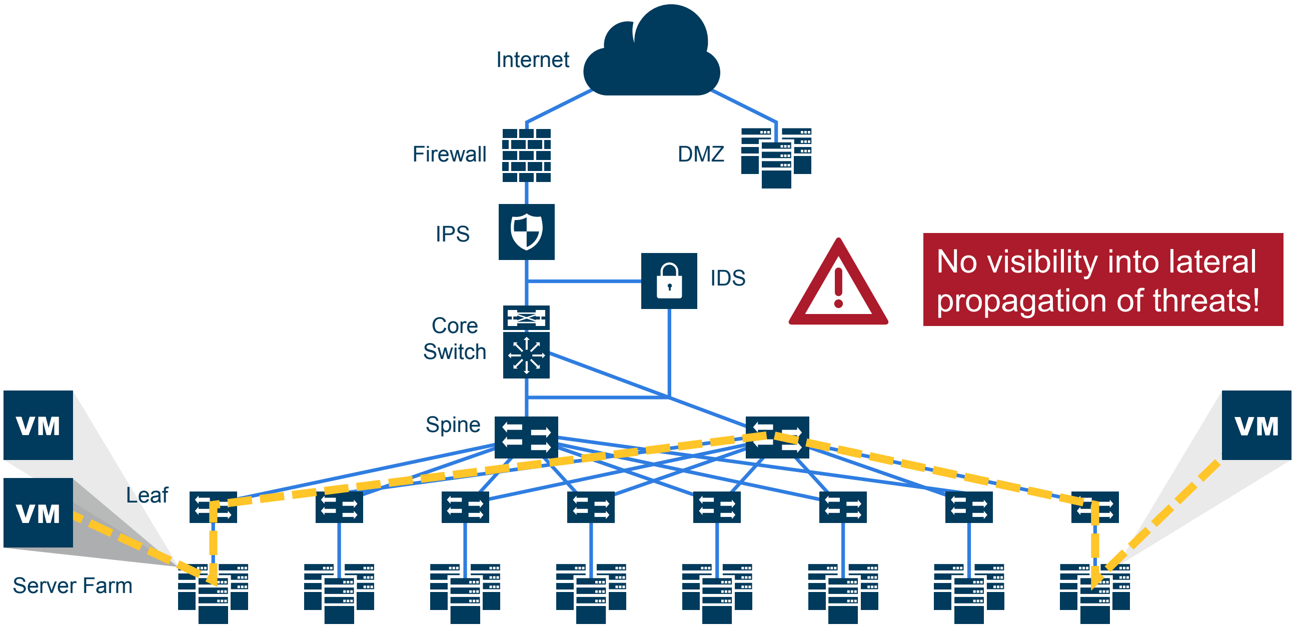

Figure 2: East-west traffic within data centers

[1] FireEye. 2015. Maginot revisited: More Real-World Results from Real-World Tests. https://www2.fireeye.com/WEB-2015RPTMaginotRevisited.html

[2] Trustwave. 2014. Global Security Report. https://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf

[3] Wiener, Janet and Bronson, Nathan. "Facebook's Top Open Data Problems." Web blog post. research.facebook.com, Sept. 2014. https://research.facebook.com/blog/1522692927972019/facebook-s-top-open-data-problems/

Mobility

Mobility further compounds the challenge of securing today's networks. Users, devices, and applications are all mobile today. For example, an application packaged as a virtual machine can be moved at the click of a mouse or perhaps even in a completely automated way between racks, rows, pods, or even across data centers. And this can happen without the knowledge of the security team. A security appliance such as an IDS or IPS that is connected directly into a link within a data center and focused on inspecting application traffic may be rendered ineffective when the application itself moves to a different location unbeknownst to the security team. In other words location is now becoming less relevant when deploying security solutions. This is true even in the campus edge where users and devices are mobile.

Growing Use of Encryption

Finally, there is a growing use of encryption technologies such as SSL within enterprises. While encrypting data in motion offers security from prying eyes the secure communications channel it creates can also be used by malware to masquerade under the privacy umbrella. Many security appliances are blind to encrypted traffic and consequently the use of encryption by malware is on the rise. Where security appliances are able to inspect SSL encrypted traffic, their performance takes a significant hit due to the computationally intensive nature of SSL decryption. A Gartner report[4] has predicted that by 2017 more than 50% of network attacks will use encrypted traffic to bypass controls.

The combination of these factors, i.e. the sophisticated and evolved nature of threats, the changes in network traffic patterns, mobility, the growing use of SSL and encryption technologies by malware, and the use of an outdated trust model to design security architecture, is creating an environment that is leading to at-will breaches.

Addressing the Challenge

In order to better address this growing challenge, the fundamental trust assumptions around cyber security have to be revisited. Modern security strategies have to be forged on the assumption that breaches are inevitable. In other words, there has to be a growing emphasis on detection and containment of breaches from within, in addition to prevention of breaches. Since the network is the primary medium that bridges the physical, virtual and cloud environments, network traffic is becoming increasingly critically important for its role in providing the window to the enterprise for malware and threats. Many security vendors are doing just this, by analyzing network traffic for threats, anomalies, and lateral movement of malware. However, no matter how sophisticated these security solutions become, they are only as good as the network traffic they see.

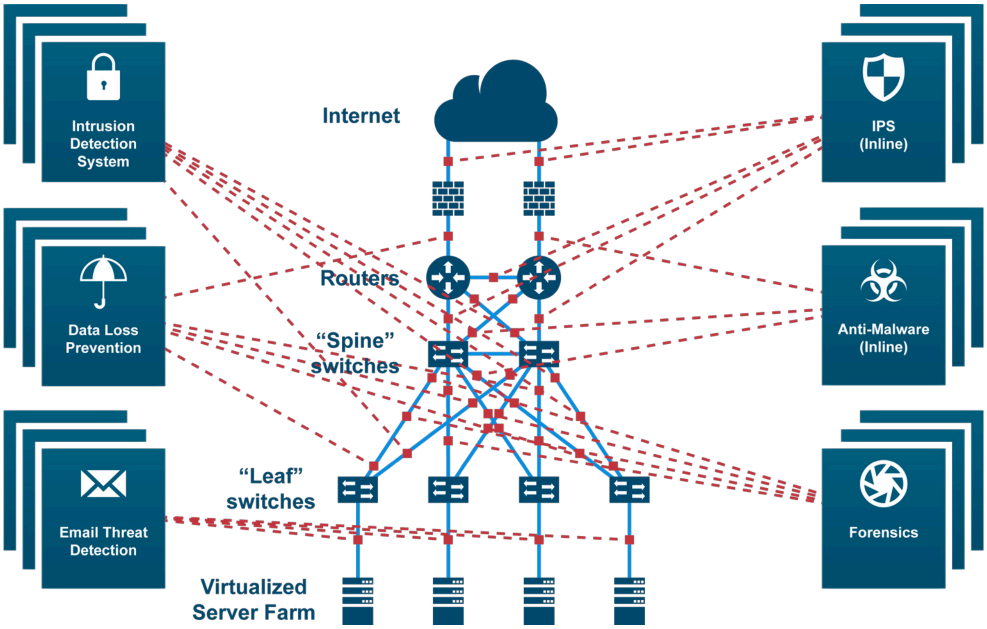

Figure 3: An ad-hoc and unstructured approach to security deployment

[4] FD'Hoinne, Jeremy and Hils, Adam. 'Security Leaders Must Address Threats From Rising SSL Traffic'. Gartner Report, 9 Dec 2013.

Legacy Approach to Looking Within

The legacy approach to doing this was to connect security appliances directly into the network through a network TAP or to a mirror/SPAN port on a network switch/router. Providing greater access to network traffic meant deploying significantly more network security appliances at more places in the network. However, the multi-dimensional nature of security lends itself to use of a variety of different types of network security solutions in order to increase the coverage envelope. This creates several challenges in the deployment model for these security solutions (see Figure 3). Some of these include:

- Contention across the different security appliances for access to traffic from the same points in the network. In other words, directly connecting an appliance to a network TAP or a mirror/SPAN port allows just one appliance to get access to that traffic.
- Mismatch between the processing capability of the security appliances and the volume of traffic that the security appliance needs to process.
- Blind spots and inconsistent view of traffic. Security appliances that are connected into specific points of the network may not see traffic from other parts of the network or from users or applications that have moved to other parts of the network.
- Increase in the number of false positives. More security appliances mean more false positives for those security applications prone to them.
- Rapidly increasing cost as security tools proliferate across the network increasing management complexity and cost.
- Network disruption as deployments move from an out-of-band monitor mode, to an inline protection mode.

A Security Delivery Platform as a New Model for Security Deployments

As the industry coalesces on increasingly looking within the network for malware, the focus has been on the growing sophistication of the security solutions. There has not been much thought around the deployment architecture for such solutions, which leads to several of the challenges identified previously. This is an area that has been largely under-served and yet is fundamental to looking within the network for malware and breaches. In order to address the above challenges, a structured platform-based approach is required that delivers traffic visibility for a multitude of security appliances in a scalable, pervasive, and cost effective manner. The solution should encompass the following components:

- Deliver traffic visibility from physical and virtual environments consistently even when users, devices, and applications are moving around.
- Take out the guesswork on where to place security solutions i.e. eliminate the dependence on identifying static choke points within the network especially in today's dynamic environments characterized by user/device/application mobility.
- Provide a solution to decrypt encrypted communications so that security tools can detect malware that leverages encrypted communication channels, while at the same time ensuring that sensitive information is not compromised.
- Provide the ability to deliver just the relevant traffic streams to the specific types of security appliances. For example, an email security solution need not see YouTube traffic. Sending only relevant traffic allows the security solutions to function more effectively and waste less bandwidth and resources processing irrelevant information.

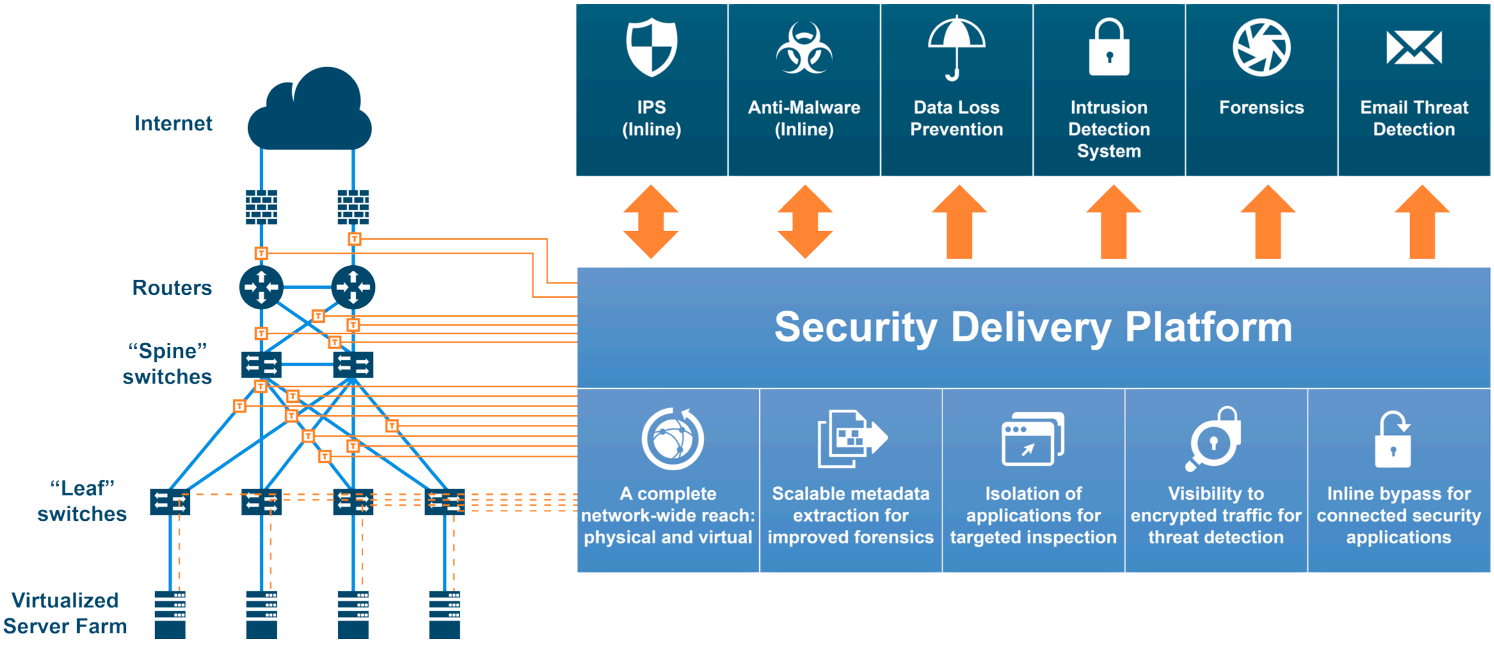
IPS (Inline)
Anti-Malware (Inline)
Data Loss Prevention
Intrusion Detection System
Forensics
Email Threat Detection
Internet
Routers
"Spine" switches
"Leaf" switches
Virtualized Server Farm
Security Delivery Platform
A complete network-wide reach: physical and virtual
Scalable metadata extraction for improved forensics
Isolation of applications for targeted inspection
Visibility to encrypted traffic for threat detection
Inline bypass for connected security applications

Figure 4: A Security Delivery Platform: Key components

- Generate detailed flow and session intelligence based on actual traffic not just a sample of the traffic.
- Support inline and out-of-band network security deployments from the same platform, while providing the ability to load balance both inline and out-of-band security appliances as well as provide the ability to bypass inline security appliances in the event of failure.

A Security Delivery Platform that addresses the above considerations provides a powerful solution for deploying a diverse set of security solutions, as well as scaling each security solution beyond traditional deployments. Such a platform would deliver visibility into the lateral movement of malware, accelerate the detection of exfiltration activity, and could significantly reduce the overhead, complexity and costs associated with such security deployments (see Figure 4). In today's world of industrialized and well-organized cyber threats, it is no longer sufficient to focus on the security applications exclusively. Focusing on how those solutions get deployed and how they get consistent access to relevant data is a critical piece of the solution. A Security Delivery Platform in this sense is a foundational building block of any cyber security strategy.

GigaSECURE as a Security Delivery Platform

GigaSECURE® is Gigamon's offering of a Security Delivery Platform. The GigaSECURE platform connects into the network, across physical and virtual infrastructures, and delivers traffic to all of the applications that require it. Security appliances simply connect into the GigaSECURE platform at whatever interface speeds they are capable of connecting and consequently receive a high-fidelity and relevant traffic stream from across the network infrastructure. Flow meta-data extraction from network traffic is also done within GigaSECURE and flow records can be exported to various security tools for analysis. See Figure 5.

GigaSECURE supports a variety of security solutions that can sit out-of-band to the production network, for detection of malware and the lateral movement of malware, detection of exfiltration activity, post incident forensics, as well as other security initiatives. Additionally, it also serves as a platform for deployment of a diverse set of security solutions that need to sit inline with the network traffic. Inline security solutions typically provide the ability to take preventive measures in real time on detection of threats, malware or anomalous behavior. GigaSECURE can support both inline and out-of-band deployments in parallel. When supporting inline security deployments, GigaSECURE provides full failure protection and load distribution capabilities across a variety of inline deployment modes.

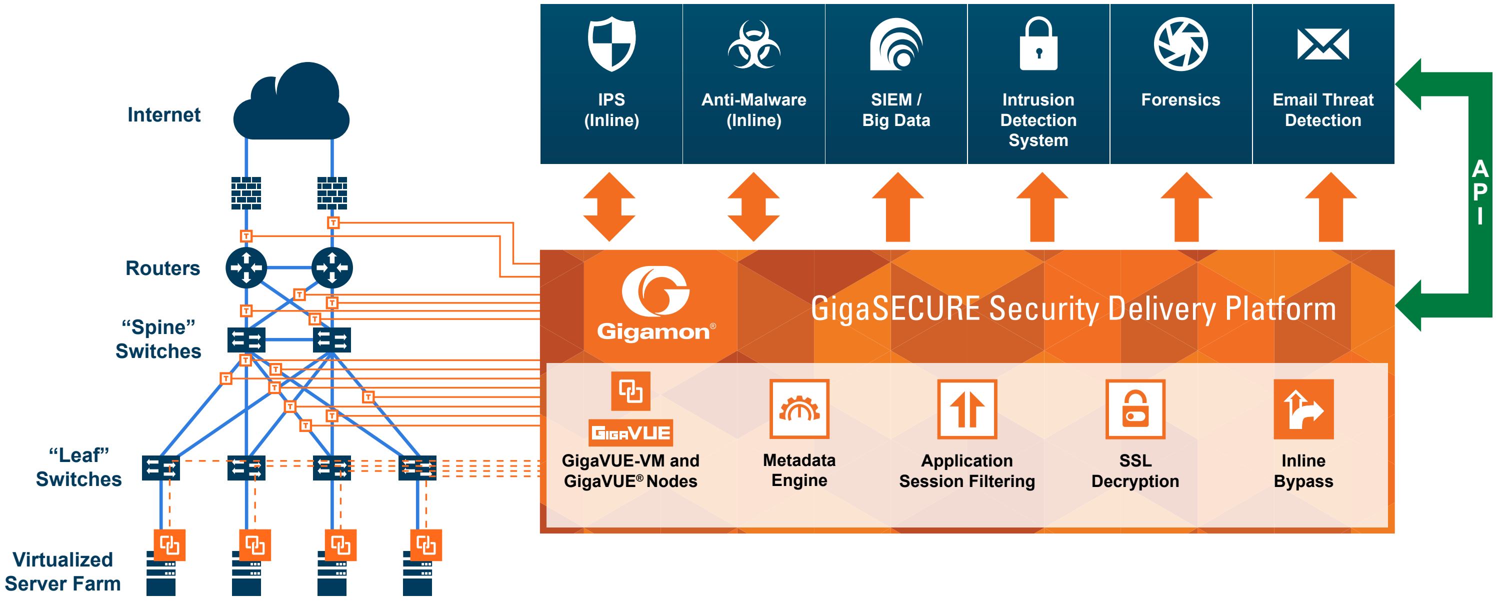

Figure 5: GigaSECURE Security Delivery Platform

Components of the Platform

GigaSECURE consists of visibility nodes, GigaVUE OS™ software with patented Flow Mapping® technology, traffic intelligence functions powered by GigaSMART® and a centralized fabric controller (GigaVUE-FM). These are described below.

- **Virtualized visibility nodes:** GigaVUE-VM is a virtualized node that provides the ability to deliver traffic visibility into virtualized workloads. The GigaVUE-VM solution provides the ability to track virtual machines as they move from server to server, and enforce Follow-the-VM policies to ensure that application traffic is always sent to the security tools even as the VMs move.
- **Scale-out, cost-effective visibility nodes:** The GigaVUE TA Series of visibility nodes, along with the GigaVUE-OS in conjunction with whitebox Ethernet switches, provide a cost-effective way to provide scale-out traffic visibility. These nodes through the power of Flow Mapping® technology provide sophisticated aggregation, filtering, and replication capabilities at a cost-effective price point enabling a deployment model where traffic from across the infrastructure can be channeled back to selective security appliances.

  The combination of the GigaVUE-VM and the GigaVUE TA Series enables visibility into east-west traffic and visibility across the internal campus and data center networks. They also address the issues of mobility and provide a consistent source of high-fidelity traffic to security appliances which now have the ability to monitor the lateral propagation of threats and look pervasively inside the infrastructure.
- **Traffic Intelligence functions powered by GigaSMART:** While the GigaVUE-VM and GigaVUE TA Series products enable security appliances to get highly relevant traffic feeds from across the infrastructure in a cost-effective scale-out manner, the GigaVUE H Series platforms powered with GigaSMART technology provide the ability to act on those traffic streams and perform a series of functions that serve to offload and optimize a variety of security solutions. Some of the advanced GigaSMART functions that can be availed by security solutions include:
  - **High performance NetFlow (IPFIX) and metadata generation:** IPFIX is a powerful standards-based technology that is gaining momentum in the network security space for forensics, trend analysis, and anomaly detection. IPFIX looks at raw network packets and derives sophisticated flow-based meta-data such as records of conversations between endpoints, duration of conversations, channels of communication, etc. GigaSECURE centralizes the function of generating these flow records so that this can be done consistently across heterogeneous and disparate infrastructure. The flow records can be served up to a variety of security solutions that analyze flow metadata. The flow meta-data generation is done at very high throughput so as to generate high-fidelity records that are essential for good security analytics. The solution also enables custom templates to be defined so that the information that can be gleaned from the traffic can be highly tailored to the specific deployment environment.
  - **SSL decryption:** As the volume of malware that leverages encrypted communication channels increases, the need to peek into those encrypted channels of communication increases. Decrypting those encrypted channels of communication is best done within the GigaSECURE Security Delivery Platform so that this is done once, at very high performance thereby eliminating this blind spot simultaneously for multiple security appliances that do not have the ability to deal with encrypted communications. For those security appliances that do have the ability to do this, it offloads a computationally intensive task from being repetitively done in each such security appliance.
  - **Application session filtering:** Many security solutions do not need to look at entire flows that are either trusted or that they have no ability to process. With the Application Session Filtering capability, the GigaSECURE Security Delivery Platform has the ability to look deep into the packet at the application layer, identify application flows based on any arbitrary pattern within the packets, and steer entire sessions (i.e. all packets belonging to that session even if subsequent or preceding packets for that session do not match that pattern) to a specific security solution, or to discard the entire session. This powerful capability allows precise control of what types of traffic data are sent to security tools based on L4-L7 and more sophisticated content matching, thereby ensuring that security solutions are focused on working off network traffic that is most relevant to them while simultaneously offloading those appliances from having to process large volumes of irrelevant data. The identification of what is relevant and what is not can be customized to each security appliance.
- **Inline protection and load balancing:** Many security appliances work inline with the network traffic to prevent malware and malicious activities in real time. Many other security appliances work in an out-of-band mode for detection and incident generation purposes. The GigaSECURE Security Delivery Platform provides a common platform to serve traffic feeds to both inline and out-of-band security deployments. When serving inline security deployments, the GigaSECURE platform provides the ability to load balance traffic across multiple inline security solutions, as well as the ability to daisy chain different inline security appliances, each providing different levels of protection. Traffic can be distributed to the security appliances based on a variety of criteria, while ensuring that forward and reverse traffic for a given flow always go to the same security appliance. The platform also provides resiliency and protection in the event that any of the inline security appliances experiences a failure, both in

load-balanced mode as well as when inline appliances are daisy chained thereby ensuring that network traffic forwarding does not get disrupted in the event of a failure. Security appliances can also seamlessly be moved from out-of-band mode to inline mode and vice versa with no disruption to the network. This is a powerful capability of the platform that unifies and simplifies the deployment of a variety of inline and out-of-band security solutions while addressing resiliency and failure scenarios very effectively.

- **Centralized Fabric Controller (GigaVUE-FM):** GigaVUE-FM serves as the centralized controller that provides the ability to unify the different components of the GigaSECURE Security Delivery Platform. It serves as a centralized policy definition point for the virtualized and physical visibility nodes. GigaVUE-FM exposes a set of northbound APIs that allow security solutions to fine-tune in near real time the traffic feeds that they are receiving so as to be able to adjust their visibility into the network and IT infrastructure based on what real-time anomalies, threats and conditions they are seeing. In other words, the APIs enable a degree of automation that allows security tools to control the traffic feeds they receive from the Security Delivery Platform based on the dynamic conditions they see in real time or near real time.

GigaSECURE Security Delivery Platform addresses the under-served, yet much needed requirement of a scalable and cost-effective platform that simultaneously expands the reach of multiple security appliances while addressing the challenges of eliminating contention, helping to reduce cost, and simplifying deployment architectures. The approach significantly improves the coverage model for network security thereby providing better visibility into internal threats and lateral threat propagation.

Benefits

There are several benefits to taking such an architectural- and platform-oriented approach for security deployments. The solution:

- Provides immediate and pervasive insight into network traffic within an enterprise and with it visibility into all lateral movement by malware.
- Delivers traffic to the security appliances, eliminating the guesswork on where to place security appliances for getting relevant traffic feeds.
- Enables upgrades, changes, or moves from out-of-band to inline without impacting the network security solutions.
- Reduces false positives significantly due to consolidation of multiple security solutions to a smaller set that is centralized and leverages the Security Delivery Platform.
- Eliminates blind spots associated with mobility as well as encryption.
- Provides a consistent source of packet and flow data for all security appliances.
- Eliminates contention for traffic—relevant traffic is replicated and delivered to all security solutions.
- Improves efficacy of security solutions by elimination of irrelevant traffic feeds to those solutions.

Summary

The changing cyber security threat conditions are driving a need for a fundamental shift in the trust model for security. As organizations accept the inevitability of network breaches, their focus is shifting to security architectures for detecting malware and threats within the organization, and responding to mitigate risk. Doing this requires far deeper insight and far greater coverage across the infrastructure than traditionally feasible and consequently a new model for deploying security solutions. This model must address pervasive reach to the network, exploding traffic volumes and contention for the traffic by multiple tools. A structured and architectural approach to pervasive network visibility gives security solutions access while enabling them to scale cost effectively. The benefits of increased security and cost effectiveness are making the Security Delivery Platform consequently a foundational building block to deploying security solutions. GigaSECURE is a Security Delivery Platform from Gigamon, an industry first combination of compute, as well as packet filtering capabilities that is the way forward for security services delivery in networks being equipped to detect and respond.

Join us along with our Ecosytem Partners to turn the tables on cyber criminals at wefightsmart.com

bivio networks · Check Point Software Technologies Ltd. · Damballa · FireEye · Fortinet · lastline · Lumeta Network Situational Awareness · plixer · RSA
Blue Coat · Cisco Developer Registered · dataphy · FlowTraq · Hewlett Packard Enterprise · LightCyber · ManagedMethods · pindrop security · savvius
ca technologies · Cyphort · ExtraHop · ForeScout · Imperva · LogRhythm The Security Intelligence Company · niara · Reservoir Labs · tenable network security

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