WHITE PAPER

ixia

The Real Secret to Securing Your Network

915-6639-01 Rev. A, October 2014

Table of Contents

Executive Summary

Concerns over network security continue to persist year after year. Everyone is waiting for the perfect security product that will stop intruders in their tracks. However, this won't ever happen because the approach is fundamentally flawed. Security isn't something you purchase, it's something you need to do – everyday.

This paper covers the fundamental mind shift that must happen for CISO's and their teams. Once that shift occurs, a security and visibility architecture can be put into place that provides three valuable assets to mitigate security threats: better data to analyze security threats, better operational response capabilities against attacks, and the application of consistent monitoring and security policies.

Further details are included on different deployment scenarios, such as:

- In-line and out-of-band security tool placement
- Deployments for traditional physical networks
- Deployments for virtual environments (like virtualized data centers).

In addition, solution details are also provided for typical visibility architectures and how the architectures will support your security policies.

Network security continues to be a hot topic in the market place, and for good reason. Security attacks are not a question of "if" but "when."

The Golden Key to Network Security

Network security continues to be a hot topic in the market place, and for good reason. Security attacks are not a question of "if" but "when." Verizon's 2014 Data Breach Investigations Report (DBIR) indicated that there were 63,437 reported security incidents in 2013. That's a lot of potential damage. According to Verizon, an "incident" is defined as "a security event that compromises the integrity, confidentiality, or availability of an information asset." An incident is also different from a "breach," which Verizon defines as "an incident that results in the disclosure or potential exposure of data."

There were 1,367 confirmed breaches reported last year.

These numbers are only the reported incidents, and are not the number of actual attacks that were attempted. That number is unknown, but is undoubtedly considerably higher. With these kinds of annual data points for security threats, you would think that business leaders for all company networks would have completely secured their networks by now, but (obviously) the reality is that many business executives still don't want to accept that a security attack could happen to them – even though it's happening to many others.

Some of the high profile recent attacks include: Facebook, Twitter, Apple, Microsoft, Target, Neiman Marcus, Michaels, Sprouts, Basha's, Adobe, Home Depot, Jimmy John's Restaurants – the list goes on. While the businesses in this list got a wake-up call to seriously address security, it doesn't change the fact that damage was done and valuable information has already been taken/exposed. In the case of Target, after the break-in the CEO and CIO were let go due to the publicity damage inflicted upon Target's reputation and the resulting financial damage due to customer churn.

So, what's the confidence level in your current network security? Whether you know it or not, your network is probably exposed. For instance, the data in the Verizon 2014 DBIR suggested that over 25% of incidences may be caused by one-off errors – like the accidental publishing of sensitive information on the company or government website.

For example, the State of Texas accidentally published confidential employee social security numbers by mistake in 2011.

As another example, Forrester Research analyzed the 2010 version of the Verizon DBIR and found that most organizations don't properly monitor their networks for evidence of security incidents. Forrester found that in 86% of the breaches, the victims had evidence of the incursion in their log files, even though many didn't know it. See the Forrester Research report "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" from February 1, 2011 for more information.

The key concept is that security isn't something you purchase, it's something you need to do – preferably on an everyday basis. There is no perfect security product that can stop intruders in their tracks. It needs to be a concerted process of best practices that are put into place and maintained. The first step is to put a visibility architecture in place that supports your security plan.

The key concept is that security isn't something you purchase, it's something you need to do – preferably on an everyday basis.

A visibility architecture is essentially a cost-effective design that provides access to network traffic, intelligently filters data, sends the groomed data to analysis tools, and then delivers information as output from the monitoring tools so that IT can make informed decisions about problem resolution and network improvements. With the proper visibility architecture in place, you'll be able to see what is (and what is not) happening on your network. Simply put, you can't monitor what you can't measure and you can't make accurate corrections without accurate monitoring data.

Once a joint security and visibility architecture is in place, it will provide three valuable attributes to mitigate your security threats:

- Better data to analyze security threats
- Better operational response capabilities to attacks
- The ability to apply a set of consistent policies across your network

These three capabilities are the "golden key" to help you secure your network. Implementation of one or two capabilities may help, but it's the whole trifecta that will deliver the benefits that can safeguard your intellectual property and prevent exfiltration of critical company data.

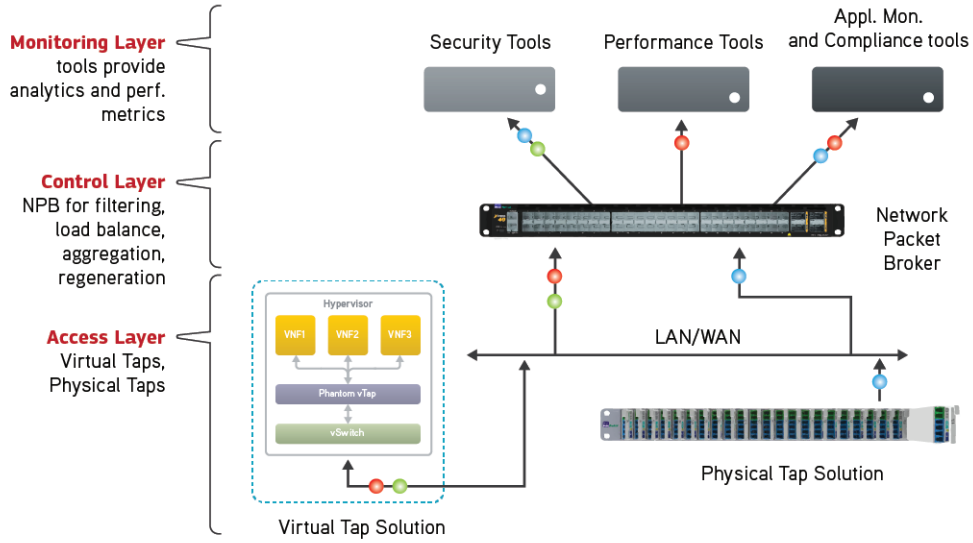
Common deployment scenarios that increase security visibility in the network

As a first step to designing your joint visibility and security architecture, you'll need to understand your specific goals ahead of time so that you can get the design correct.

As a first step to designing your joint visibility and security architecture, you'll need to understand your specific goals ahead of time so that you can get the design correct. For instance, are you trying to monitor and secure your physical network, virtual network, or both? In addition, do you plan on inserting your security tools in-line, out-of-band, or both? The answers to these two sets of questions will dictate the basic design of your visibility architecture along with how and where your network monitoring points need to be located.

In the first scenario, the question of monitoring for a physical or virtual environment is important because the two network environments have different monitoring points and different equipment requirements. While a network tap would be the universal type of network access point, the type of tap used in a virtual environment is different from a tap for the physical network. Where you insert the tap also dictates the amount of relevant (i.e., quality of) data that you can collect.

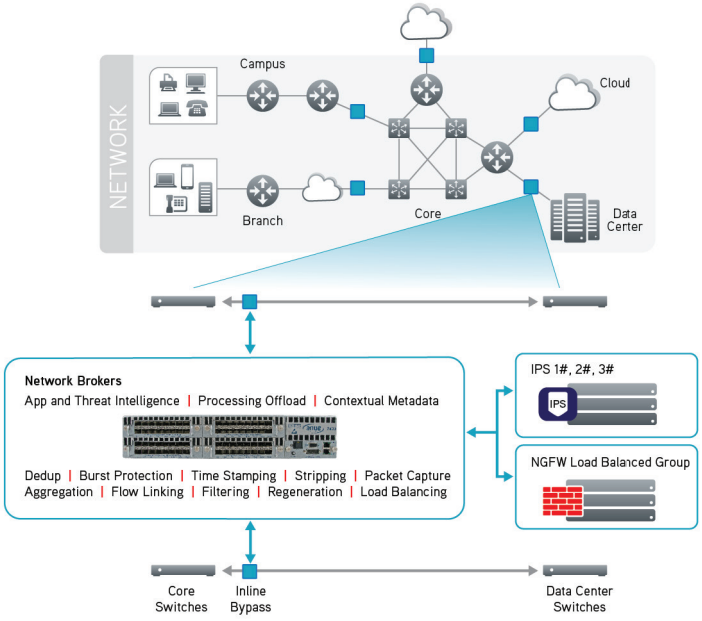
This is definitely a point that needs further clarification. Just as the virtual and physical portions of your network are different and have different hardware, software, rack space, and power requirements, so is how you go about monitoring them (at least in the access layer). This is shown in the following diagram.



You need the right tap for the right job but after that, a common set of network packet brokers and monitoring tools can be used. In fact, a common set of network packet brokers and monitoring tools SHOULD be used so that the monitoring tools can analyze the same type of information across the whole network to get as accurate a picture as possible.

In the second scenario, how you insert your security tools into the network will dictate what you can do with them. For instance, if you use an in-line scenario, then you can intercept external attacks and kill them right away or divert them to a honey pot for further analysis (i.e. threat origin, attack vector they are using against your network, objective of the attack, etc.). If you don't plan to respond to security threats in real-time, then an out-of-band solution may be better for you as it typically requires less cost and is less complex. Let's dive into these implementations a little further.

In-line network visibility is all about enabling real-time vigilance. This methodology is designed for proactive threat prevention. How can you detect a threat in real-time? What can you do once you discover a threat? How can you ensure regulatory compliance requirements have continued to be met? These are the relevant questions to ask.



Once you install a bypass tap, which is a specialized "high-availability" tap, you have the ability to see all of the traffic coming into the different segments of your network. Not only does this allow you to see data, but if you install other equipment like a network packet broker (NPB) and connect it to the bypass tap, you can use the NPB filter to groom and divert data to intrusion detection and prevention (IDS, IPS) equipment, honey pots, etc.

Examples of typical in-line security tools include the following:

- Intrusion prevention systems (IPS)
- Firewalls and next-generation firewalls (NGFWs)
- Data loss prevention (DLP) systems
- Unified threat management (UTM) systems
- SSL decryptors
- Web application firewalls (WAF)

Out-of-band visibility solutions are designed for routine analysis of the network security. This methodology is useful for delivering key information to your security tools for detailed threat analysis (especially for advanced persistent threats) with SIEMs, forensic tools, data recording, malware analysis, and packet captures. In this scenario, either a standard tap or virtual tap is used to provide the network access for the packet broker and security tools.

Examples of typical out-of-band security tools include the following:

- Security Information and Event Management (SIEM) systems
- Behavior analysis systems
- Forensic tools
- Data recording
- Malware analysis tools
- Log management systems
- Packet capture tools

Implementing a visibility architecture solution

A visibility architecture allows you to reinforce your security architecture by providing three important functions:

- Ability to access the proper data to analyze anomalies and trends across your network
- Capability to respond to threats in real-time through manual intervention and/or automation
- Ability to harness application intelligence to deliver real-time vigilance

These three functions can be mapped to the three Golden Key benefits discussed earlier, creating a combined visibility and security architecture. As a reminder, the three Golden Key benefits are:

- Better data to analyze security threats
- Better operational response capabilities to attacks
- The ability to apply a set of consistent policies across your network

Let's discuss how the visibility architecture security functions provide Golden Key benefits.

Better data to analyze security threats

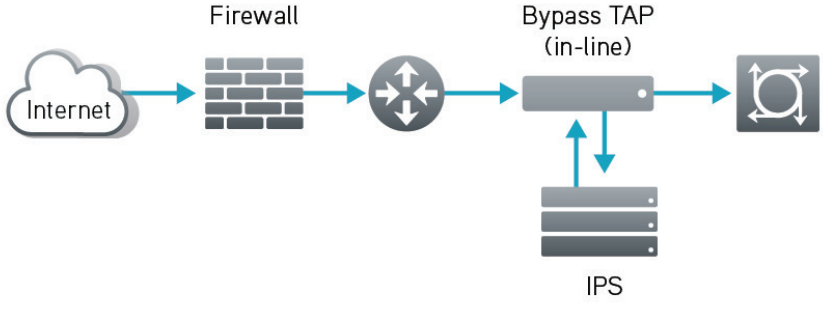
The first step to acquiring better data for analysis starts with the type of access point.

The first step to acquiring better data for analysis starts with the type of access point. As mentioned previously, taps are the fundamental network access points. While SPAN ports could be an alternative to taps, those have been shown to have very negative characteristics: summarized data instead of actual data packets and time delays for the forwarded data (which make it difficult to get accurate performance information).

The type of tap you need depends upon your security and visibility goals. In general, there will be three categories of taps to choose from:

1. Bypass tap – typically used for in-line solutions
2. Standard tap – used for general access and out-of-band solutions
3. Virtual tap – used in virtualized networks (cloud, virtualized data centers, etc.)

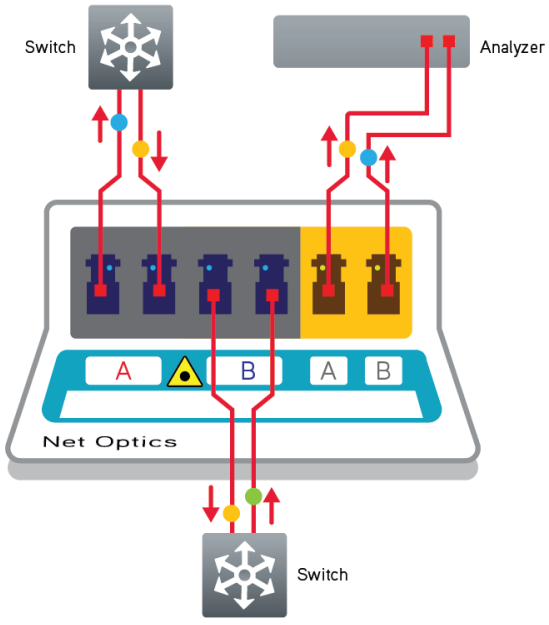
Depending upon your needs, one of these three types of taps should give you the access you need to the proper data. In the case of the bypass tap, it's placed in-line in the network for threat prevention. So, it should be placed after the firewall but before any equipment. The advantage of this location is that should a threat make it past the firewall, that threat can be immediately diverted or stopped before it has a chance to compromise the network. This is detailed in the following figure.



Because of its location in the network, the bypass tap has specific requirements placed upon it that include the following:

- It cannot take the network down so it must have integrated fail-over capability with negligible delay
- It cannot slow or block application traffic
- It must have high-availability and heartbeat technology to detect if connected tools go down so the fail-over capability can be initiated
- It must scale with network demands

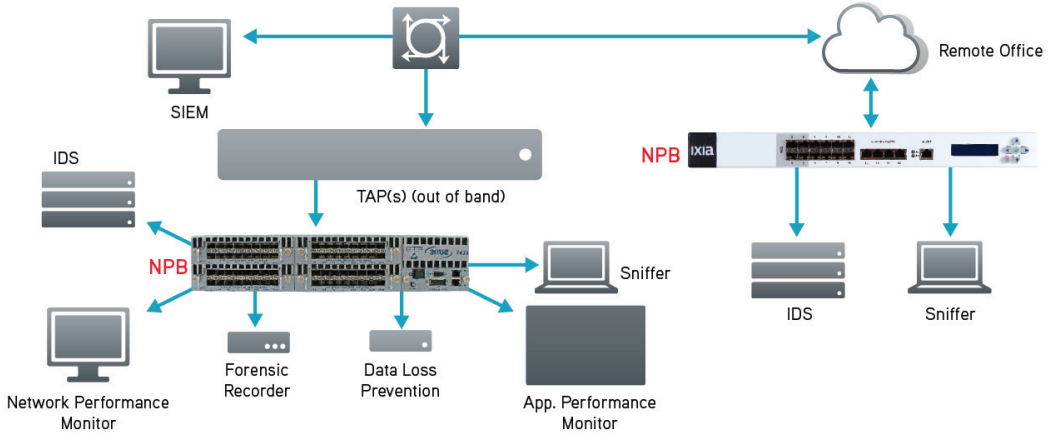
The bypass tap then provides the access for real-time traffic analysis as well as the ability to respond to threats with real-time actions, like data diversion.



Standard taps are similar to the bypass tap except that they don't have the fail-over requirements, since they typically sit out-of-band. This is reflected in the adjacent diagram.

Standard taps are the most common tap deployed and are available with copper or fiber interfaces. They are the workhorses that provide access and can be located anywhere across the network as needed. As the data packets come in, a copy is made of them. The original data is sent back out to the network while the copy is forwarded on to another device – typically a network packet broker, but a monitoring tool could be directly connected to the tap as well.

Enterprises have been using tap solutions for network traffic access for many years. Traffic capture, analysis, replay, and logging are now part of every well-managed network environment. This is illustrated in the following diagram.



While inter-VM traffic was optimized to speed up connections and minimize network use on the physical core network switches, such optimization has made traffic invisible to physical tools, which are unable to extend easily into the virtual environments. In addition, next-generation data centers use virtualization technology to deploy private/public cloud environments on a single physical server or across a clustered group of servers, local and remote. Traditional taps cannot see the traffic between VMs that reside on the same hypervisor (east-west traffic), nor can they "follow" VMs as they are migrated from one host to another.

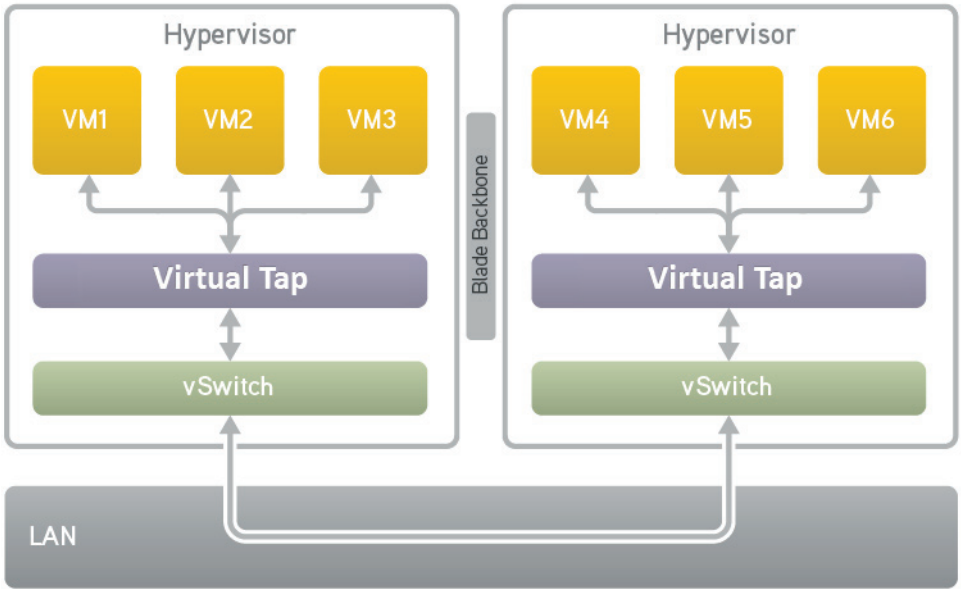
Visibility is further reduced by the complexity of blade servers that have each blade running multiple VMs on a hypervisor. Traffic running on blade servers shares a common backplane and creates a network blind spot, since the physical network and its attached tools are unable to see traffic above the virtual switch layer or the blade chassis network modules.

Virtual taps are specifically designed to enable protection for the virtualized data center. They are similar to standard taps in that they forward packets to network packet brokers and monitoring tools. The difference between the two types of taps is that the virtual tap is pure software.

Since the virtual tap is designed as a hypervisor plug-in, it can be installed in the necessary areas of a virtual environment to capture inter- and intra-VM traffic. This design allows it to provide access above the internal virtual switch layer within the hypervisor.

The deployment of virtual taps can be used for more than providing security data to existing security monitoring tools but can also help thwart the spread of malware by sending periodic data to malware detection systems to prevent the spread of unnoticed malware among VMs.

After the access layer, there is the control layer where the collected data can be manipulated; extraneous data can be filtered out, duplicate data eliminated, and sensitive data (like credit card data) can be removed before the data is forwarded to the monitoring tools.



Packet brokers are the primary component of the control layer and are the second step to acquiring better data.

Packet brokers are the primary component of the control layer and are the second step to acquiring better data. They will add immediate value to your security analysis process. Typically, they are located after the tap in either in-line or out-of-band configurations, as dictated by the visibility architecture design. These components have the granular filtering mechanisms required to perform the necessary filtering, and quickly isolate anomalous data for security tools. Instead of the tool being flooded with millions of packets, only the relevant data needs to be sent to the tools if a packet broker is used. This naturally contributes to higher efficiencies and faster time to resolution for both anomalies and outages.

Depending upon how the packet broker is deployed, there are different feature sets required. In an in-line situation, fail-over and redundancy will be one of the key features. This not only applies to the NPB itself but also to the ability to support fail-over scenarios for the tools that are connected to the NPB as well.

Important in-line NPB features include:

- Graceful load balancing fail-over mechanisms that do not disrupt existing sessions of available IPS appliances
- Load balance across mix of 1 GE and 10 GE appliances

- Automatic N+1 high availability load balancing
- Maintenance mode to allow convenient servicing of connected appliances in the load balanced group
- Ability to monitor multiple links in-line by load balancing across multiple IPS appliances
- Heart beat built in to network packet broker to detect and protect "brown out" failures
- In-line filtering of traffic sent to IPS appliances to remove unneeded traffic
- Complete high availability solution with multiple NPBs in active/active or active passive mode
- Full support of out-of-band and in-line operation

For out-of-band solutions, the NPB features focus much more on data stream manipulation and load balancing for tools to maximize the ROI for your monitoring efforts. In this deployment scenario, the list of relevant out-of-band NPB features include:

- Packet capturing
- Data filtering
- Load balancing
- Aggregation
- De-duplication
- Packet slicing
- Time stamping and port tagging

Better operational response capabilities

Once you have the necessary data, it needs to be properly analyzed. This is where a visibility architecture and security architecture must be well integrated. On-demand security tools should be connected and integrated into the packet broker programming so that predefined and on the fly filters can send appropriate anomaly data out the correct ports to a variety of waiting security tools.

A key feature of network packet brokers in this area is the ability to use web-based APIs for communication with network management and orchestration systems. This feature allows you to integrate an NPB with your data center automation initiative to implement near real-time changes in your visibility network to deliver data to your security tools. For example, if your SIEM detect that there is an incident taking place, it can direct the NPB to capture a certain set of packets on a certain link and then forward those packets to a specific security analysis tool for proper analysis. All of this would take place without any manual intervention with the NPB (assuming the NPB has the proper connections in place).

Role-based access is another NPB feature that can be very useful. This feature allows you to place users into different access groups so that privileges for the creation/modification of data filters, as well as other functions, can be segmented as needed. For instance, role-based access allows internal groups/individuals to set filter customization and linkages to their respective tools (like provisioning systems, SIEM tools, etc.) without having to worry about another group affecting their access or automation linkages to the packet broker. This provides further confidence that the packet broker capability will perform as needed, when needed.

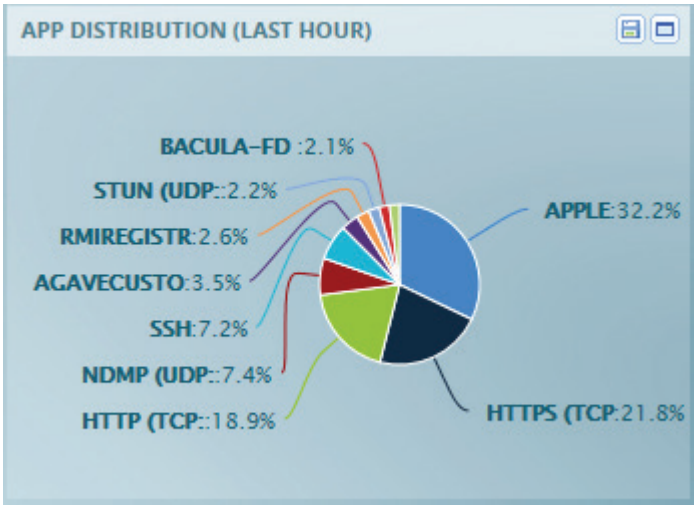
A key feature of network packet brokers in this area is the ability to use web-based APIs for communication with network management and orchestration systems.

Removing dependencies on other groups can have dramatic business consequences. Service and equipment turn up time can be decreased from hours/days to minutes. Some enterprises have also tried implementing internal SLA's to speed up intergroup dependencies. Automation and role-based permissions helps to sidestep this whole SLA conversation and make life easier within the IT department.

Depending upon your NPB choice, application intelligence is an extended functionality that is included and allows you to go beyond layer 2 through 4 (of the OSI model) packet filtering. With application intelligence, you can reach all the way into layer 7 (the application layer) of the packet data. The benefit here is that rich data on the behavior and location of users and applications can be created and exported in any format needed – raw packets, filtered packets, or NetFlow information. IT teams can identify hidden network applications, mitigate network security threats from rogue applications and user types, and reduce network outages and/or improve network performance due to application data information.

A core feature of application intelligence is the ability to quickly identify ALL applications on a network.

In short, application intelligence is basically the real-time visualization of application level data. This includes the dynamic identification of known and unknown applications on the network, application traffic and bandwidth use, detailed breakdowns of applications in use by application type, and geo-locations of users and devices while accessing applications. The filtered application information is typically sent on to 3rd party monitoring tools (e.g., Plixer, Splunk, etc.) as NetFlow information but could also be consumed through a direct user interface in the NPB. The benefit to sending the information to 3rd party monitoring tools is that it often gives them more granular, detailed application data than they would have otherwise to improve their efficiency.

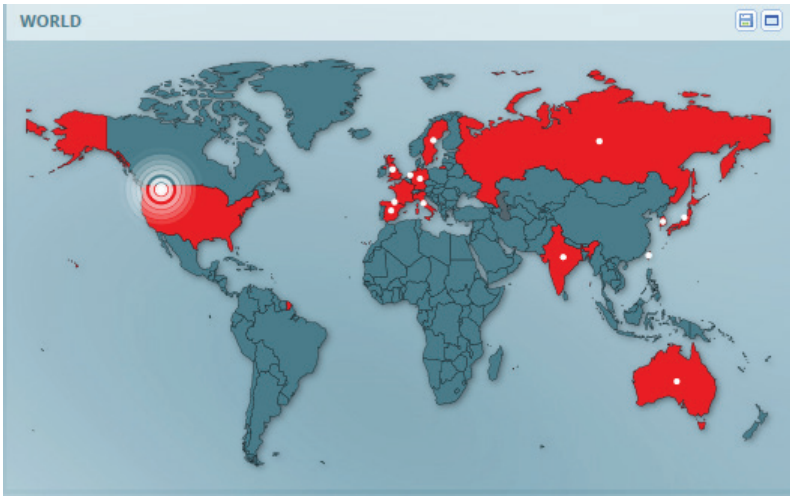


The application intelligence effectively allows you to create an early warning system for real-time vigilance. In the context of improving network security, application intelligence can provide the following benefits:

- Identify suspicious/unknown applications on the network
- Identify suspicious behavior by correlating connections with geography and known bad sites
- Audit for security policy infractions, including use of prohibited applications

A core feature of application intelligence is the ability to quickly identify ALL applications on a network. This allows you to know exactly what is/ is not running on your network. The feature is often an eye opener for IT teams as they are usually surprised to find out that there are actually applications on their network they knew nothing about. Another key feature is that all applications are identified by a signature. If the application is unknown, a signature can be developed to record its existence. These unknown application signatures should be the first step as part of IT threat detection procedures so that you can identify any hidden/unknown network applications and user types.

A second feature of application intelligence is the ability to visualize the application traffic on a world map for a quick view of traffic sources and destinations. This allows you to isolate specific application activity by granular geography (country, region, and even neighborhood). User information can then be correlated with this information to further identify and locate rogue traffic. For instance, maybe there is a user in North Korea that is hitting an FTP server in Dallas, TX and transferring files off network. If you have no authorized users in North Korea, this should be treated as highly suspicious. At this point, you can then implement your standard security protocols (e.g., kill the application session immediately, capture origin and destination information, capture file transfer information, etc.).



Another way to apply application intelligence is auditing your network policies and usage of those policies. For instance, maybe your official policy is for employees to use Outlook for email. All inbound email traffic is then passed through an anti-viral/malware scanner before any attachments are allowed entry into the network. With application intelligence, you would be able to tell if users are following this policy or whether some are using Google mail and downloading attachments directly through that service (bypassing your malware scanner). Not only would this be a violation of your policies, it presents a very real threat vector for malware to enter your network and commence its dirty work.

Another way to apply application intelligence is auditing your network policies and usage of those policies.

In the end, it's the difference between being alerted to a security breach after it happens or the ability to shut off rogue applications and user behaviors right as they happen. The choice is up to IT and how they want to deal with network security.

Application of consistent policies

The application of consistent monitoring policies is the third key essential benefit of a combined visibility and security architecture. You need to have a holistic approach to the network. If you have a fantastic plan for capturing and analyzing data, but it's only for half of the network, that doesn't help you much. While this might seem like a crazy comment, it's actually not. Many companies have a good strategy for their physical networks, but either overlook or don't know how to access the data on the virtualized portions of the networks. This is an extremely important blind spot in your network monitoring strategy, as up to 80% of virtualized data center traffic never makes it above the top of the rack – where the traditional monitoring points can access the data. Without proper access to this data (which requires the virtual tap mentioned earlier), you can have serious issues in your network that go unseen: hidden malware, performance problems, and regulatory compliance issues.

With the creation and application of a consistent monitoring policy, you will avoid the virtualization pitfall just mentioned as well many other future problems that typically arise when new equipment is added.

Conclusion

In an era where 43% of companies are experiencing data breaches on an annual basis (according to a recent Ponemon Institute study for 2013), network security is poised to become one of the most important business tools there is to protect intellectual property and corporate reputation. The Ponemon report also indicated that the cost of a breach is up 15% over 2013, and now averages $3.5 million per incident. This is another reason to reassess network security processes.

To counteract this security threat, businesses need a strategy that allows them to capture better security data, execute operational responses quickly and appropriately, and be able to implement consistent policies across their networks.

The mechanism to achieve these goals is fairly straight forward:

- Insert a visibility architecture into current your protection framework that can focus on the three monitoring layers – access, control, monitoring tool
- Integrate the visibility architecture with your security architecture so that you can proactively monitor virtual environments for security breaches and anomalies
- Implement and maintain consistent security/monitoring policies across the entire network to prevent blind spots and loopholes that can be exploited

In the end, the key point should involve a mindset change to understand that network security is something you will need to do on a daily basis.

To counteract this security threat, businesses need a strategy that allows them to capture better security data, execute operational responses quickly and appropriately, and be able to implement consistent policies across their networks.

ixia

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Ixia European Headquarters
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750
(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters
21 Serangoon North Avenue 5
#04-01
Singapore 554864

Sales +65.6332.0125
Fax +65.6332.0127

915-6639-01 Rev. A, October 2014