WHITE PAPER

Five Ways Application Intelligence Will Supercharge Your Monitoring Tools

The Right Application Information Is Critical

Constantly changing network security threats, an emphasis on customer quality of experience, and a greater need to measure internal and external SLA's (especially for cloud networks) have become increasingly important topics for IT. These three requirements are forcing IT to acquire an even better insight and understanding of the network to maximize its performance. To accomplish this, IT has begun turning to application intelligence to provide the insight needed.

Properly designed visibility architectures deliver the critical intelligence needed to boost network security protection, reduce troubleshooting costs, create more efficiencies, and extend the life and utility of monitoring tools. For instance, early detection of breaches using application data reduces the loss of personally identifiable information (PII) and reduces breach costs. Specifically, context-aware data processing can be used to expose indicators of compromise, provide geolocation of attack vectors, and combat secure sockets layer (SSL) encrypted threats. Efficiencies can also be created by filtering data at the application level to remove unnecessary data clutter at the tool interface to control costs.

Visibility architectures deliver the critical intelligence needed to boost network security protection, reduce trouble-shooting costs, create more efficiencies, and extend the life and utility of monitoring tools.

KEYSIGHT TECHNOLOGIES

Top Five Benefits of Application Intelligence

To gain the maximum value from your network and control both network and tool costs, context-aware data processing allows you to enhance the following five network activities:

- Expose indicators of compromise (IOC)
- Perform proactive troubleshooting activities
- Conduct application filtering for security and monitoring tools
- Provide SSL decryption
- Enhance regulatory compliance

These five capabilities can deliver significant value to any IT department by making the network (and applications running on it) more secure, stronger, and more resilient.

According to the 2016 Verizon Data Breach Investigation Report, most victimized companies don't discover security breaches themselves. Approximately 75% have to be informed by law enforcement and 3rd parties (customers, supplier, business partners, etc.) that they have been breached.

Exposing Indicators of Compromise

The main purpose of investigating indicators of compromise for security attacks is so that you can discover and remediate breaches faster. Security breaches almost always leave behind some indication of the intrusion, whether it is malware, suspicious activity, some sign of other exploit, or the IP addresses of the malware controller. Despite this, according to the 2016 Verizon Data Breach Investigation Report, most victimized companies do not discover security breaches themselves. Approximately 75% have to be informed by law enforcement and 3rd parties (customers, suppliers, business partners, etc.) that they have been breached. In other words, the company had no idea the breach had happened. To make matters worse, the average time for the breach detection was 168 days, according to the 2016 Trustwave Global Security Report. What if you could reduce the 168 day average to 168 seconds?

To thwart security attacks, you need the ability to detect application signatures and monitor your network so that you know what is, and what is not, happening on your network. This allows you to see rogue applications running on your network along with visible footprints that hackers leave as they travel through your systems and networks. The key is to look at a macroscopic, or application view, of the network for IOC.

For instance, suppose there is a foreign actor in Eastern Europe (or other area of the world) that has gained access to your network. Using application data and geo-location information, you would easily be able to see that someone in Eastern Europe is transferring files off of the network from an FTP server in Dallas, Texas back to an address in Eastern Europe. Is this an issue? It depends upon whether you have authorized users in that location or not. Due to IOC, you now know that the activity is happening. The rest is up to you.

Other examples of IOC could include the following:

- You are seeing that the DNS text field is being populated with information, indicating malware is moving data out of your network
- There are more DNS/HTTP requests than normal
- There are multiple versions of a specific browser type in use by the same individual

These are just some of the indicators of compromise that you could find. There could be numerous other areas to investigate on your network.

85% of network mean time to repair (MTTR) is the time taken to identify that there is in fact, an issue. Even worse, the MTTR clock starts ticking whether IT knows there is an issue or not.

Performing Proactive Troubleshooting

One key component of problem resolution is problem identification. Zeus Kerravala, Principal Analyst at ZK Research asserts that, "Problem identification is IT's biggest challenge." He explains that 85% of the mean time to repair (MTTR) is the time taken to identify that there is in fact, an issue. Even worse, the MTTR clock starts ticking whether IT knows there is an issue or not.

A second component of problem resolution is identifying the location of the problem(s). It is one thing to try to find the needle in the haystack. But which haystack should you even be looking at (network equipment, network applications, virtual data center, cloud provider, user/customer premises equipment, etc.)? The right choice here can save you hours, or even many days, worth of time. The wrong choice can have devastating effects for the company and your career.

A visibility architecture that uses context-aware data processing information can be used to capture critical information needed for the whole troubleshooting process. Geolocation capability can be used to help quickly locate geographic outages and potentially narrow troubleshooting efforts to specific vendors that may be causing network disruptions. This reduces troubleshooting costs and improves customer quality of experience.

The use of metadata not only makes traditional troubleshooting efforts better but it allows IT to become proactive. Proactive troubleshooting is the Holy Grail for network administrators—to prevent a network problem from happening, or at least remediate it before anyone notices it. The metadata can also be combined with trending and bandwidth consumption to anticipate problems before they actually happen and affect the network.

Proper application filtering can increase IDS security tool efficiency by 35% or more.

Maximize Network Security and Tool Efficiency with Application Filtering

A third powerful use case for application intelligence is to use application filtering to improve security and monitoring tool efficiencies. It is not just about using the right tool

for the right job. Delivering the right information is just as critical because garbage in results in garbage out. For instance, by screening application data before it is sent to an intrusion detection system (IDS), information that does not require screening (e.g. voice and video) can be routed downstream and bypass IDS inspection. Eliminating inspection of this low-risk data can make your IDS solution up to 35% more efficient.

However, for application data to deliver true savings, the solution must be as intelligent as possible. It does no good to create a solution that saves 35% more time only to have to add 150% more time in creating application signatures and defining filtering rules. The math only works if the solution already has several hundred application definitions pre-defined.

In addition to the application definition, the solution needs to distinguish application sub-functionality as well. For example, some SIP-based voice quality monitoring solutions need to understand whether the voice source was a traditional voice call or a digitally generated (voice over IP using a computer) call. The SIP protocol has a codec field that indicates the voice source. Application context-aware data processing can be used to read the codec field and pass that information along so that a copy of the traffic is routed to the right type of voice quality tool for proper analysis.

Information granularity like this reduces application troubleshooting costs and allows you to optimize customer quality of experience by providing the all-important details. It is one thing to know that something is happening, it is another to know why. The details also allow you to access empirical data to identify bandwidth usage, trending, and growth needs to be proactive in managing their resources and forecast expansions.

SSL Decryption

Cost-effective SSL decryption capability has become another important activity for IT. According to a Blue Coat infographic, half of all network security attacks in 2017 will use encrypted traffic to bypass controls.[1] Line rate packet broker-based SSL decryption delivers better visibility into these hidden security threats and reduces security tool CPU overloading due to SSL decryption functionality.

While separate SSL decryption tools are available and useful, SSL decryption that is integrated into the visibility solution allows for an easy and cost effective way to examine monitoring data. For example, this capability can be used to decrypt SMTP mail traffic and hand it off to an antiviral tool for virus/malware inspection. Other data could be decrypted and sent off to a data loss prevention (DLP) device for deeper inspection.

[1] Blue Coat. June 8, 2014. Accessed September 30, 2016. https://www.slideshare.net/BlueCoat/infographic-stopattackshidingunderthecoverofsslencryption

Another use case is to deploy SSL decryption capabilities to examine what kind of encryption is in use on the network and how effective it is. For instance, are older, weaker encryption algorithms being used or are stronger, more powerful, algorithms that can fend off modern security threats in use? Encryption metadata from context-aware data processing can be used to find the weaker encryption algorithms.

SSL decryption capabilities can also be combined with other features like data masking to enable logging and troubleshooting to improve regulatory compliance. Once the data is unencrypted, the sensitive clear text data is masked and then sent to troubleshooting tools for analysis.

Application monitoring lets you know that employees may be using services like Drop Box to transfer company files and bypass your security policies.

Enhancing Regulatory Compliance

A fifth fundamental concern is around regulatory compliance. This has been top of mind for enterprises for several years now. All companies are looking for ways to strengthen compliance, reduce costs, minimize security risks, and eliminate potential compliance fines. Application data can provide many benefits in this area as well. This includes monitoring application usage, data masking, data searching, and even data validation.

One example is to use context-aware data processing to monitor cloud application usage. For instance, application monitoring lets you know that employees may be using services like Drop Box to transfer company files and bypass your security policies. Once an employee is no longer employed by the company, they could still have access to those files since IT cannot restrict the privileges to off-network storage devices.

Another example is where employees may be using other, non-company standard, email services (like web-based mail services) to access and download files. This use case usually involves accessing media that does not go through anti-virus/malware inspection and can therefore pose a security threat to the corporate network, especially regarding file downloads.

A third example is data masking. Critical data, like credit card numbers, social security numbers, etc. can be masked before it reaches monitoring tools. This ensures that various regulatory compliance requirements are met.

A fourth example is data search capability to look for key words, phrases, or numbers. Regex search strings can be created for phone numbers, credit card numbers used in transactions, social security numbers, emails from certain IP addresses, or names. This feature allows critical data to be filled out and sent to a DLP for further analysis. The data could also be sent to other purpose built tools, like a tool that uses credit card data and the Luhn checksum algorithm to validate if the provided 16 digit credit card numbers are actually valid.

Simplicity Is Key

The plethora of separate and special purpose tools on the market create a lot of complexity for most network monitoring architectures. Reducing monitoring complexity has a direct effect on operational expenditures. To overcome this, IT needs to be able to return to the days when network monitoring was simple. The best way to do this is to use a visibility architecture that has a feature set capable of delivering the Top 5 benefits mentioned previously within one integrated solution. Examples include built-in features like: data masking, SSL decryption, packet captures, packet or NetFlow data, etc.

This level of integration is paramount. For instance, if a vendor cannot support using data masking concurrently with NetFlow in the same module, then you will incur extra configuration time and costs for that type of solution. All of the features need to be able to run at line rate as well. Security threats do not wait, neither should your NPBs.

The solution also needs to be intuitive to configure. Which would you prefer, drag and drop capability for filter creation or to be given a command line interface (CLI) and a “cookbook” so you can write your own applications with all of the extra time you have? A drag and drop user interface (UI) that allows an administrator to create and modify application level filters can be five to ten times (or even more) faster than a CLI (used for writing Regular Expressions) and a cookbook with page long examples of commands that an admin will need to write.

Simplicity means having a vendor that uses a team to continually create new application signatures so you do not have to. This saves you time, money, reduces complexity, and improves application signature accuracy. This is the kind of resource that is easy to leverage, not a “cookbook” of formulas that you need to write, code, and validate on your own.

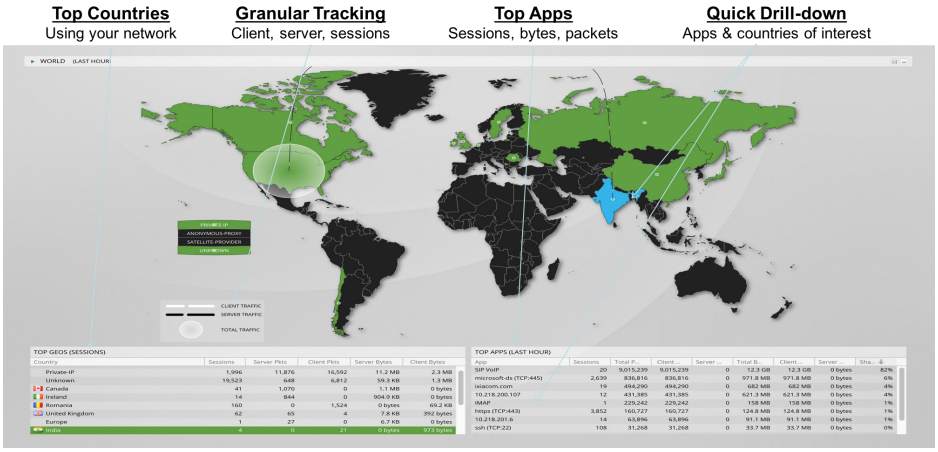

Figure 1. Application Intelligence Example

A drag and drop user interface that allows an administrator to create and modify application level filters can be 5–10 times (or even more) faster than a command line interface (used for writing regular expressions) and a cookbook with page long examples of commands the admin will need to write.

Conclusion

A properly constructed visibility architecture enables context-aware data processing to make your application monitoring tactics stronger against cyber threats and faster in mitigating device and application failures. The application intelligence created delivers a faster mean time to repair that directly equates to monetary savings.

When incorporated into a visibility architecture, context-aware data processing can provide the following benefits:

- A stronger, more resilient security architecture
- Faster mean time to repair
- Decreased costs for breaches and network failures
- Better support for regulatory compliance
- Better efficiency for monitoring tools

Learn how you can easily start eliminating visibility and security blind spots and use application intelligence to supercharge your security and monitoring tools with Ixia's IxVision visibility architecture at https://www.ixiacom.com/solutions/out-band-monitoring.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES