GameChanger NETWORK VISIBILITY FOR COMPLEX NETWORKS

New Challenges Raise Stakes for Network Visibility

A holistic approach is better suited toward today's complex networks.

Government networks looked drastically different ten years ago than they do today. Ten years ago, virtualization was just taking hold. Other advances, like cloud infrastructure, pervasive mobility, the use of sensors and digital government, were just getting started. These changes have created more network traffic, more complexity, and more blind spots.

All these advances mean multiple network connections. To remain productive and secure, agencies need consistent and thorough visibility into all these connections. Yet today, many organizations don't have the visibility they need. A 2016 survey from SANS, for example, found only 16 percent of respondents consider their network visibility infrastructure mature.[1]

There are several ways to increase network visibility. At the very least, revisit existing policies and tools with an eye toward plugging the gaps, says Dan Conde, analyst at Enterprise Strategy Group. He recommends a more holistic, platform approach. Most organizations have dozens of point solutions for network management and monitoring, but are missing important tools to improve network visibility. By separately managing each tool, it's easy for connections to fall through the gaps.

Instead, base your network visibility capabilities on a strong platform such as NetFlow or SFlow. A strong platform will help external solutions such as intrusion detection systems and firewalls plug in via APIs. These platforms usually have easy-to-use, configurable management consoles and ensure all tools work together to provide the requisite visibility.

NETWORK VISIBILITY: THE CORNERSTONE OF EFFECTIVE CYBERSECURITY

Cybersecurity remains a top priority for government agencies. In 2016 alone, the White House announced its intentions to implement the Cybersecurity National Action Plan. Among other things, this would create the position of Federal Chief Information Security Officer. The White House also has allocated more than $19 billion for cybersecurity in the FY 2017 budget—that's more than a 35 percent increase from FY 2016.

Part of that funding is allocated for agencies to retire and replace legacy IT systems with more modern, effective technology. That's a golden opportunity to switch from traditional endpoint cybersecurity tools to new solutions that address today's complex networks.

While legacy cybersecurity tools still have value, they often don't provide the comprehensive visibility required for tight security control. The rise of virtualization, cloud storage and services, and other 21st century technologies have created blind spots that prevent full visibility. This makes it increasingly difficult to identify and prevent malicious activities.

According to ESG's Network Security Monitoring Trends Report, about one-third of organizations report blind spots are one of the top challenges related to network security monitoring. Limited visibility makes it harder to monitor network flow to detect breaches or attempted breaches, both on traditional and WiFi networks.

To ensure full visibility, experts recommend tools that can:

- Monitor both north-south and east-west traffic
- Continuously monitor, analyze, categorize, separate and store all relevant activity
- Use multiple data sources to provide a full view of security incidents over time as they evolve and move through networks
- See the type, operating system, compliance status, connection method and geographic location for every connected device
- Use intelligent packet capture
- Set policy and behavior thresholds
- Employ security analytics

Shutterstock.com

[1] https://www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047

IMPROVE CYBERSECURITY WITH NETWORK VISIBILITY

GameChanger NETWORK VISIBILITY FOR COMPLEX NETWORKS

The Challenge of Insider Threats

Some of the greatest network threats come from within an agency.

The idea of government employees or contractors accessing sensitive data or deliberately halting network operations may seem unbelievable. But it happens—and it happens quite frequently. A 2015 report from Meritalk[2] found 45 percent of agencies experienced insider threats and almost 30 percent lost data as a result of those incidents. Of course, not all those incidents are deliberate. Some happen simply because users fail to follow approved policies, leading to breaches like using unsecured connections and clicking on malicious links.

Recent years have seen an explosion of technologies like cloud, mobility and sensors, along with the push toward digital government and virtualization. These advances make these threats and potential breaches even more difficult to pinpoint. Internal network visibility

Shutterstock.com

is critical, yet the Meritalk study found nearly half of agencies can't tell how or if a document has been inappropriately shared and about one-third can't tell what data has been lost.

The key, says Jim Duffy, senior networking analyst at 451 Research, is to develop and enforce policies to determine who is on the network, who is allowed to be on the network, what devices are allowed on the network, and specific role-based access for users and groups of users.

"The IT department has to be able to notice if someone is trying to get into an area of the network they aren't authorized to get into, or that packets coming from a certain destination are trying to infiltrate a specific IT device like a server or another switch, or that somebody has brought in a rogue program and is trying to introduce it onto the network," says Duffy.

Network monitoring tools—especially those providing lateral (east-west) visibility and behavioral anomaly detection—are critical to protecting the network within the perimeter. For insider threat detection and prevention, these capabilities are as important as others required for network visibility outside the perimeter.

ADVANCES IN NETWORK VISIBILITY TECHNOLOGIES

CHANGING PRIORITIES AND TECHNOLOGIES have made full network visibility more difficult than ever before. Here are four areas in which the tools and processes have advanced significantly.

Improved Packet Capture, Store and Analysis: Imagine your network was breached 20 minutes ago. Wouldn't it be useful if you could go back in time 20 minutes to examine what happened, find the root cause, fix the problem, and better prepare for the next event? Today's packet capture tools can do just that. Think of these tools as a "network visibility DVR." They can capture and analyze network traffic, and provide valuable statistics and other information to help you drill down to find root cause of events.

Better Network Instrumentation: The types of instrumentation organizations use to monitor network state, performance, traffic, usage and devices on the network varies dramatically. It typically includes some combination of agents and probes. Recent advances in instrumentation now help you monitor virtual environments much like physical environments. This is especially useful for workloads in the cloud—something that has been virtually impossible until recently.

More Robust Packet Brokers: Today's network packet brokers—basically watchdogs that distribute the right data to the right tools—are evolving to address today's issues, such as virtualization, increases in network speed, and the bi-directional information flow. Modern packet brokers can also eliminate redundant data while retaining original data packets; perform deep packet inspection, SSL decryption and data masking.

Streaming Analytics: Like big data analytics, these solutions analyze large amounts of information from multiple sources—and they do so in real time. They can monitor live network traffic as it flows. In some cases, they can also replace—or at least augment—SNMP polling. With the ability to monitor network traffic in real time, streaming analytics can serve as the basis for real-time analysis and action.

[2] https://www.meritalk.com/insidejob

GameChanger NETWORK VISIBILITY FOR COMPLEX NETWORKS

Manage Advanced Threats in a World of Pervasive Encryption

Techniques such as pervasive encryption provide additional network monitoring challenges.

Pervasive encryption is the concept of encrypting as much network traffic as possible. This is widely considered the Gold Standard of security in 2017. That's particularly true in the federal government arena, which encrypts as much as 90 percent of its network traffic.

While this practice clearly improves security, there are real challenges to "going dark," as the practice of pervasive encryption is often called. One of the biggest issues is dealing with the loss of the network traffic visibility necessary to fully protect agency data and networks. For example, the FBI has repeatedly voiced concerns about how law enforcement is sometimes less effective because it can't interpret fully encrypted traffic.

Besides the lack of visibility, pervasive encryption is causing more organizations to remain unaware of persistent and embedded cyber-attacks over long periods of time. One thing often thing leads to another. An innocuous event leads to someone discovering something "odd," which leads to another layer of security concern. By the time an Incident Response team is involved, the situation is completely out of hand.

"Today's reality really requires agencies to take a second look at whether their visibility is being impacted," says Andrew Benhase, Principal Architect with Cisco Systems. "Such a high percentage of traffic encryption today can render some network security technologies less relevant in terms of traditional threat identification."

NEW WAYS TO EXAMINE TRAFFIC

What all this means is that agencies and other organizations need new ways to analyze network traffic to maintain or increase their security posture. For example, the behavior pattern within the network is more important than ever before. It can provide more detailed information about the flow of information within the network, even though the information is actually encrypted.

With the right technology, IT staff can analyze the packet metadata, or the information collected from the network about what is happening within the network. For example, an agency can use technologies such as NetFlow or IPFIX to collect data from every network component and send it in as information about actual network traffic to be analyzed.

The intelligence of some of today's most advanced solutions can also analyze the IP address attached to the header of each packet and increase tie that into security data being stored elsewhere. Correlating that IP address to a wealth of information within the network can yield critical data, such as usernames, employee names, physical locations of devices, time of login, machine type, posture of the machine and detailed directory information.

> "TODAY'S REALITY REALLY REQUIRES AGENCIES TO TAKE A SECOND LOOK AT WHETHER THEIR VISIBILITY IS BEING IMPACTED."
>
> —ANDREW BENHASE, PRINCIPAL ARCHITECT, CISCO SYSTEMS

These capabilities when combined can result in valuable network security information for the analyst. And when combined, this can translate into a security-relevant threat overlay for the entire Enterprise network. More importantly, it provides agencies with an immediate operational understanding of their network—in other words, a very real cyber-situational awareness.

"The ability to fuse this information together is critical to cybersecurity today," says Benhase. "Without it, you are in effect staring at a 12-inch black and white CRT in the 1950's instead of watching a 65-inch 4K resolution screen mounted on the wall."

FIND THE RIGHT PARTNERS TO ENSURE DEFENSE IN DEPTH

Improving cybersecurity these days clearly requires a new approach. That approach must combine traditional cyber technologies like deep packet inspection and next-generation firewalls with newer innovations to help gain dimensional depth against the challenges of an ever increasing world of pervasive encryption.

Bringing these security technologies together into a comprehensive Defense in Depth strategy is best achieved by partnering with experienced information security companies—especially those with specific government expertise. With the right partners, agencies can ensure they're using the most advanced, effective, cohesive solution possible.
