IDC
Analyze the Future

IDC ANALYST CONNECTION

Robert Westervelt
Research Manager, Security Program

Nolan Greene
Research Analyst, Network Infrastructure Program

The Benefits of Network Visibility in Optimizing Security

April 2015

Having a secure network infrastructure that can prevent and mitigate data breaches is important to ensuring smooth business operations. When networks are not adequately secured and fall prey to a breach, organizations might find it difficult or, in some cases, impossible to fully recover from the financial and brand-related impacts. Many high-profile data breaches stem from configuration issues and weaknesses introduced by the growing complexity of corporate networks. Organizations need to gain a clear understanding of their network environment so that they will be agile enough to address potential issues before their business becomes the target of an attacker and a costly breach.

The following questions were posed by Gigamon to Robert Westervelt, research manager for IDC's Security program, and Nolan Greene, research analyst for IDC's Network Infrastructure program, on behalf of Gigamon's customers.

Q. How does pervasive visibility impact network security?

A. It is essential for network security specialists to have visibility into all the devices that are connected to the corporate network and, perhaps more importantly, the devices that are exposed to the Internet. It's a fundamental security best practice to regularly monitor the network for new devices attempting to connect to corporate resources. However, all too often, limited resources and increasingly complex corporate networks provide hackers and criminals with much-needed camouflage, shielding their malicious activity behind layers of obfuscation.

Part of the reason for this growing complexity is a trend that IDC calls the "3rd Platform." This is the latest paradigm of computing that sheds the client/server framework for an IT ecosystem built on cloud, mobility, virtualization, social technologies, and big data. IDC believes that visibility is a necessary part of an organization's plans to enforce corporate security policies while adding more robust videoconferencing and collaboration capabilities that can handle the proliferation of mobile devices and the continued growth of the Internet of Things (IoT).

Q. What are the benefits of increasing network visibility?

A. In all areas of network operations and management, including security, increased end-to-end visibility of users, nodes, virtual servers, and endpoints is a growing and welcome trend. There are many benefits, such as the elimination of blind spots. Perhaps the most singular benefit of visibility using network traffic is the ability to make rapid decisions in real time in response to threats before they have time to affect the entire infrastructure. In other words, the more you can see, the more you can secure your applications.

The two most tangible benefits and business drivers are maintaining the availability of critical applications and reducing the threat envelope in security architectures. From a security perspective, increased visibility can also provide the network security team with enough information to identify a problem before it results in a costly service disruption or data breach. Having that visibility can also help identify device usage patterns that can be used to improve network performance and eliminate underutilized devices and systems that expand the attack surface for hackers and criminals. Business drivers also include finding ways to boost employee productivity by shifting network resources to locations that need them most and eliminating bandwidth hogs that drain revenue. Increasing visibility also helps avoid having to drop security devices throughout the organization, thereby creating a sprawl of security appliances. This can help drive down costs.

The use of a visibility fabric approach can boost response times by allowing network teams to access and modify network traffic with greater flexibility. The approach uses a unified management model that enables rapid visibility and response as well as an open architecture framework to extend options to add new solutions or maintain existing tools. It's worth emphasizing that the benefit of a "single pane of glass" management approach is also enabled by a network visibility fabric. As network security grows more complex and networking and security teams become leaner, having one platform as the foundation for threat detection, management, and remediation becomes more critical. Finally, a visibility fabric can help eliminate issues associated with oversubscription and scale. As applications and networks grow, the amount of traffic can quickly exceed the capabilities of security devices and related management and reporting tools. IT no longer has to constantly rip, replace, and reconfigure security tools; rather, IT now can use the intelligence and programmability to allocate the right tools to the right traffic at the right time.

Q. How do I employ a visibility fabric in my overall security architecture?

A. An assessment of current infrastructure and the underlying policy model is paramount to beginning any project. Organizations must understand the physical and virtual assets in place, as well as any infrastructure serving remote offices. In conducting thorough assessments, organizations have been known to find abandoned database servers and other devices that may not have been previously documented. Once all infrastructure and connecting systems are well documented, organizations can gain a better understanding of current and future bandwidth needs.

Security products are increasingly burdened with too many connections, resulting in significant performance impacts. A typical response to this situation is to turn off important functions such as encrypted traffic inspection. Turning off security features not only results in poor security visibility but also prevents organizations from getting the true value out of their security investment. A visibility fabric can help organizations fully leverage existing investments and improve interconnectedness so that network analysts can respond with agility to multiple issues when something goes wrong.

Q. What are the differences between intelligent fabric and TAP/aggregation solutions?

A. Typical TAP/aggregation solutions act as packet brokers that process traversing traffic while providing source identification and ensuring effective analysis by associated monitoring tools. Organizations can choose between passive and active TAPs. The TAP/aggregation solution is valuable for monitoring live traffic but can be more costly because of the need for higher processing power. Scalability can also be an issue. Such aggregators also have limited ability to weed out unneeded traffic, and they provide limited assistance in offloading monitoring tools. These solutions cannot be placed in line with the network because of their limited failover capabilities. Over time, traffic growth and increased port usage can result in reduced visibility because the aggregators simply can't keep up. This results in degradation of the monitoring solutions in place.

Intelligent visibility fabrics are well suited for high-speed links and don't require redundant tapping points or SPAN ports, providing a layer for organizations that need a higher-density solution. The fabrics are intelligent and have the ability to filter and condition traffic based on the different requirements of monitoring and security tools. They can also handle high-density locations and hybrid deployments. Intelligent fabric solutions typically offer strong provisioning and management platforms and can be more adaptable to infrastructure changes or the addition of new capabilities. Network visibility fabrics include other intelligent features such as preventing duplication of effort — for example, relieving tool-processing resources when packets are gathered from multiple collection points along one path. These fabrics accomplish this by forwarding each packet only once and by removing packet duplication caused by inter-VLAN communication or incorrect switch configurations. Best-in-class visibility fabrics also have other advanced functionality, including content-based inspection. These capabilities are essential to delivering the right traffic to the right security device.

Q. What do I need to consider when deploying a visibility solution?

A. First, consider whether the network requires a centralized monitoring solution at its core or is decentralized such that analysis can be performed at the aggregation points. Conduct an analysis of the benefits of a distributed or centralized monitoring architecture. System management associated with service providers or big data projects typically requires a distributed architecture. Datacenter models are often centralized. The centralized approach limits performance issues and is likely to be more economical. This knowledge, along with determining your current and future needs when constructing a visibility fabric, will help create a less complicated architecture. Aggregation nodes come in different flavors to address networks with low-utilization links or high-utilization networks that require sophisticated flow mapping filters. Separate fabric nodes are available for deployments in regionally distributed sites or for a densely concentrated location where multiple ports are required. Organizations that require visibility into virtual machine traffic can consider virtualization-specific nodes that can tunnel traffic to an aggregation point.

As with any solution added within a network infrastructure, an understanding of your network topology and where a visibility solution would fit is a key consideration. Some important decision points are:

- Where do primary data sources reside on the network? Does data come directly from the edge router or from the spine or leaf? Is it coming from edge aggregation or the core?
- Do you understand the locations of blind spots on the network? Often there are lapses in visibility as it relates to virtual network assets and the traffic they generate. How is traffic in the virtual infrastructure protected from malicious actors?

- What types of traffic do security appliances and applications need to consume? Depending on the type of traffic, security appliances may need traffic analysis tools or raw data feeds.
- Do security tools operate in line with the network or out of band?
- How prevalent is the use of advanced encapsulations such as VxLAN or encryption mechanisms such as SSL/TLS? Is the security infrastructure capable of addressing both?
- Can traffic be "compressed" into metadata using formats like NetFlow or IPFIX to capture important flow characteristics without relying on a sampling mechanism to get a macro-level view for forensics?

IDC believes that the infrastructure complexity fueled by the 3rd Platform will prompt a rapid increase in attention concerning the quality and coverage of visibility to secure such an infrastructure. Lacking this, organizations may struggle to handle diverse types of traffic flows and expose themselves to blind spots that allow malicious actors to launch stealth attacks. This challenge will encourage organizations to gain visibility into remote, distributed environments or isolated sections of the network through network intelligence.

ABOUT THE ANALYSTS

Robert Westervelt is a research manager in IDC's Security Products group. Prior to joining IDC, Rob was senior editor at The Channel Company where he led the information security news coverage, reporting on threats, vulnerabilities, and technology trends impacting the security market for CRN. He has published hundreds of online articles about networking and endpoint security technologies and for security consultants, managed security services providers, systems integrators, and resellers.

Nolan Greene is a research analyst with IDC's Network Infrastructure group covering Enterprise Networks. In this role, he is responsible for market and technology trends, forecasts, and competitive analysis in the Ethernet switching, routing, wireless LAN, and adjacent networking markets. While contributing to quarterly and yearly forecast and market share updates, he also assists in survey design and end-user interviews and contributes to custom projects for IDC's Consulting and Custom Solutions practices.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com