Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 12, Issue 5

Knowing is Half the Battle: Visibility is the Key to Security

By Roark Pollock

Enterprises are investing more than ever in security technology as a result of increased awareness of vulnerabilities, media coverage of attacks with financial impact, hacktivism, and the consumerization of IT. Most companies have made significant investments in network security technologies and tools over the past decade. It's an executive-level topic.

According to the Identity Theft Resource Center, breaches have grown almost 28% from 2013 to 2014, with further increases expected in 2015.

So, what is 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 have been caused by one-off errors—such as accidentally publishing sensitive information on the company or government website.

The estimated cost per breach is $12.7 million1. In the last five years, the number of successful attacks per company has increased 144 percent (according to their 2014 Global Report on the Cost of Cyber Crime) and the average time to find a breach was 170 days.

Intrusion prevention systems (IPS) using inline security are a great solution to security problems, but your networks need more. The key to limiting breaches and the damage they inflict is visibility.

Most security professionals focus on policy, training, tools, and technologies to address network security. However, security tools and technologies are only as good as the network data they receive for analysis. Mounting Governance, Risk Management and Compliance (GRC) requirements are intensifying the need for network visibility.

What they really need is a visibility architecture that routes the right data to each security tool to enable adaptive and dynamic monitoring.

Data sent to tools indiscriminately without network visibility, forces the tools to perform the filtering operation and consume significant tool capacity in the process. For example, if you have tap feeding a VoIP analyzer; they may be dumping a huge amount of data on the tool, when the VoIP analyzer only needs VoIP flows.

Network visibility resolves these issues and gets the right data to the right tool for analysis. Improved network visibility offers the ability do the following:

- Monitor inclusive of virtualized environments,
- Provide automated responses for adaptive monitoring,
- Improve incident remediation,
- Improve handling of sensitive data, and
- Provide granular access control so the entire monitoring process is tightly controlled.

Security Monitoring for Virtualized Environments

Security in virtual environments is as important as security is to IT. Data in the virtual environment has been difficult to acquire for analysis. Rather than forming two separate network monitoring camps, security professionals should be included in the virtualization process, particularly if an external Cloud provider is involved.

Traffic between virtual machines residing on the same physical host (Inter-VM or "east-west" traffic) traverses through virtual switching internal to the host. This traffic is switched locally and never gets to physical monitoring tools, creating a "blind spot" or a "black hole".

This blind spot renders monitoring tools incapable of providing a comprehensive, raw view of traffic because they cannot see the internal communications within the virtualized environment. The blind spot is a pitfall, leaving your network vulnerable.

Regulatory requirements do not go away in the case of virtualized environments. According to the Information Supplement to the PCI DSS Virtualization Guidelines published June 2011:

"Appropriate security controls should be identified and implemented in a virtualized environment that provide the same level and depth of security as can be achieved in a physical environment."

Much of the requisite security technology is not in the virtualized environment. In addition, security analysis done exclusively in the virtualized environment may not provide the holistic view you require to detect sophisticated attacks.

Automated Responses for Active, Adaptive, Proactive Monitoring

A network visibility architecture can quickly turn a passive monitoring infrastructure into an active, adaptive, and proactive visibility and security solution. Security professionals and network engineers can set pre-defined triggers in their performance and security monitoring tools to raise flags and address immediate threat issues.

With a well-integrated visibility solution, these performance and security monitoring tools can be set to immediately kick off a secondary set of capture, analysis and correlation, as well as inspection action sets based on the individual pre-defined triggers. These automated response actions make the overall integrated visibility infrastructure or architecture more powerful and useful than the combination of the individual components.

Examples of these automated responses based on pre-defined events or data triggers include, but are not be limited to:

- Automated security event responses that accelerate security anomaly remediation
    - This includes automated security actions such as directing questionable traffic flows to forensics recorders, IDS or DLP devices or honeypots.
- Automated network event responses that reduce root cause diagnosis to hours
    - This includes automated NPM and APM actions that direct traffic to forensics recorders for quick diagnosis.
- Automated sampling activities that reduce IT workload and increase effectiveness
    - This includes automating repetitive and routine tasks like capturing periodic snapshots for SLA and compliance sampling.
- Automatically mitigating tool outages or congestion that cut blind spots and maximize capacity
    - This includes the creation of tools thresholds and capacity load balancing that prevents over-subscription and possible failure impacts.

When used with SIEM tools, a visibility solution provides dynamic incident remediation.

Speeding Incident Remediation

When used with SIEM tools, a visibility solution provides dynamic incident remediation. It will automatically capture packets from security events identified by the SIEM, speeding root cause analysis, eliminating time-consuming manual steps, and simplifying compliance.

A visibility architecture's automation capability complements a SIEM's ability to detect, analyze, and respond to security threats. When SIEM tools detect an anomaly, it automatically sends the right traffic to a forensic recorder or other security probe. Incident remediation begins the instant an anomaly occurs with the benefit of having the required packet information.

Forensic recorders, malware protection systems, and data loss prevention appliances are only as useful as the data they receive. When you automate data center monitoring, the right traffic is sent to the right monitoring tool at the right time. Threats are resolved effectively and quickly with the right packet information, leveraging fully existing forensic recorder and security appliance investments.

Reducing the Security Risk of Sensitive Data

A key concern for security professionals is the sensitivity of data being monitored, typically for GRC or privacy reasons. Handling sensitive personal information (SPI) is an emerging issue.

With copies of packets generated and transported across the monitoring network for analysis purposes, another attack avenue is opened (even if the data never leaves the organization). Insider threats are real and can be very expensive.

Financial data, medical data, personnel data all fall under this category. For example, privacy may relate to employee and customer personal information. Data being transported across the network for the purpose of security and network analysis can introduce a point of attack.

Very often the security analysis tool does not require the data packet payload at all. It may require only the packet header, which is rich in information, such as the source of the packet, packet length and other data of analytical value. A visibility tool selectively strips the data packet payload before sending the data stream to security and network performance monitoring tools. As a result, sensitive data does not traverse the network, and tools that only analyze the packet header will not be exposed to sensitive data.

Further, visibility solutions can analyze the data packet payload for sensitive data strings and selectively mask only that specific data in the payload. Therefore, information such as personal identification numbers, credit card numbers, etc., can be selectively hidden from capture, analysis tools and users.

Granular Access Control

With a visibility architecture, you can pull together valuable information from the collective network, leading to a "keys to the kingdom" scenario. Fortunately, a visibility architecture provides an integrated approach to secure access to network data.

It can govern users who access the control panel, and which resources they can view or modify. Access to data can be controlled at multiple points, including network ports, tool ports, or data filters. Resources that are out of scope for an individual are locked within the control panel and are inaccessible to unauthorized users. It also provides group-level access control and integrates with TACACS+ users and groups.

Network visibility integrates into the existing network security management infrastructure and provides information to the network management system via SNMP. It also provides auditable and verifiable compliance documentation.

Granular access control enables security professionals to access exactly the data they need for analysis without requiring excessive access. Likewise, network engineers' access is restricted to the data required for their job function.

Granular access control enables security professionals to access exactly the data they need for analysis without requiring excessive access.

Conclusion

Monitoring technologies for security, compliance, and network performance are an IT responsibility that require an increasing amount of high-quality network data. Even the best security technologies in the world, given bad or incomplete data, will analyze the bad data and deliver incorrect and misleading analysis, thus compromising network security.

Leveraging a visibility architecture that works with your security implementations and delivers the data needed for security analysis tools to meet GRC and security requirements. A visibility architecture provides timely and accurate network data required by each tool to perform analysis, along with a host of additional benefits.

---

[1] Ponemon 2014 Cost of a Breach Study: Global Analysis