3 Data Security Safeguards for Performance Monitoring Tools

Is your Network Performance Monitoring and Diagnostics (NPMD) solution a target for attackers? With increasingly creative exploits, it is important to stay ahead of the curve when it comes to data protection. NPMD tools that do not keep pace can leave your information vulnerable.

Overview

With data breaches making headlines almost daily it is critical to ensure adequate security for the data traversing your network. One area that can often be neglected is the protection of information collected and stored by your NPMD solution. Effective performance monitoring and troubleshooting of mission critical services can be accomplished while protecting sensitive customer and company intellectual property by using the latest encryption standards and adhering to the following three-point strategy:

- Protect data in motion
- Secure information when stored at rest
- Provide strong Authentication, Authorization, and Accounting (AAA) capabilities

Risks and Trends

In recent years, hacks have targeted different points on the network by locating vulnerabilities. These "cracks in the wall" have allowed smart criminals to not only obtain millions of users' personal data and opened them up to identity theft, it has also impacted the enterprise by devaluing companies and limiting organizational ability to conduct business.

The constantly growing frequency and severity of attacks against organizations, businesses, and government entities highlight the reality that critical company and customer information is vulnerable anytime and everywhere. It can occur when in motion on the network, while stored at rest, and if user IDs or passwords have been compromised.

The best NPMD solutions are capable of capturing terabytes of traffic for later network forensic analysis. This is ideal for fast troubleshooting but without strong protections in place, it can also become a target for malefactors, leaving important customer or company data vulnerable to attacks.

Not all NPMD solutions are created equal, so it's important to ask tough questions to accurately assess your current performance monitoring vulnerabilities to hackers.

Data in Motion Protection

NPMD data is frequently transmitted between individual components and also to a client (e.g. laptop) when a user is connected for monitoring performance or troubleshooting. To protect sensitive data during these communications, most NPMD offerings utilize at least SSL encryption with more up-to-date solutions supporting TLS encryption. The very best will leverage the most secure TLS v1.2, including attempting to negotiate with this robust protocol when connecting to a client.

Data at Rest Encryption

Packet capture appliances installed as part of a full-featured NPMD platform can speed troubleshooting and protect the integrity of the network. However, beyond offering important data that will frequently resolve service anomalies, packet payload can also contain highly sensitive information. From credit card information to corporate financial documentation, unauthorized access to sensitive data can be highly damaging to the organization. This makes these devices potential targets to hackers or malefactors.

The best defense is to ensure any data at rest within an NPMD solution is encrypted. The difficulty is the strongest encryption techniques, such AES-256 used by many governments and recommended by the National Institute of Standards and Technology (NIST) demand significant processor power to both decrypt and encrypt the data. At the data rates of modern networks, many NPMD packet capture appliances simply cannot keep up. The result is some packets cannot be successfully stored and must be discarded. This often results in, troubleshooting and performance monitoring blind spots.

IMPORTANT:

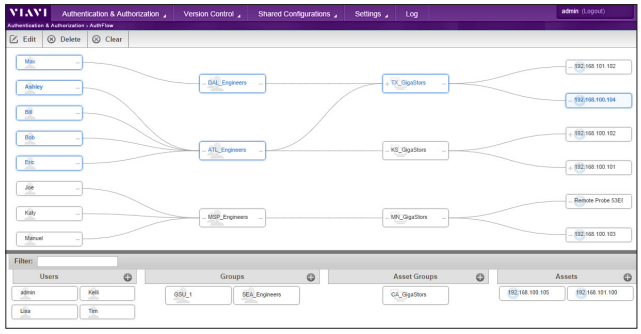
Not all solutions are purpose-built to keep up with line rate while managing 256-bit encryption. Determine whether increased security comes with any performance impact.

Robust AAA Peace of Mind

Modern IT operations demand a strong resource-wide security strategy to protect critical assets and intellectual property. Once in place, the last thing you need is an NPMD solution that compromises this process.

Centralized and easy-to-use management of Authentication, Authorization, and Accounting (AAA) and the ability to tie into services like Active Directory, RADIUS or TACACS+ is a must-have for every NPMD solution. Similar to any other network connected device, risks such as security breaches, former employee access, or contractor's forgotten login credentials are a threat vector for NPMD products as well. Likewise, the capability to enforce policies associated with password length and complexity already established in-house are all important security factors to consider as you deploy a performance monitoring platform.

Once a user has been authenticated and authorized the importance of accounting and access moves front and center. Given the considerable amounts of potentially sensitive data and information captured within most NPMD solutions, monitoring each user's activity via ongoing auditing is crucial while restricting access to need-to-know only for payload data is a best practice. Look for NPMD solutions that offer simple and easy-to-use methods to achieve this with just a couple of mouse clicks.



By choosing an NPMD solution that supports the implementation of the three-point security strategy outlined above, you can protect sensitive customer and company data while accomplishing optimal service monitoring and fast troubleshooting when anomalies occur.

Comprehensive, Secure NPMD

The Observer® Platform is a fully integrated NPMD solution, purpose-built to support the highest level of network security.

Its features include:

- TLS-based 256-bit encryption for data in motion and data at rest
- Power to keep up with line-rate during encryption
- Web-based interface for reduced learning curve, maximum ease of use
- Centralized management of AAA

VIAVI

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the Viavi office nearest you, visit viavisolutions.com/contacts.

isyourpmsolutiontarget-wp-ec-ae
00000000 000 0017