APPLICATION NOTE

Quick Tips to Improve Network Compliance

Corporate compliance ambiguity is fostering a major source of uncertainty for the IT personnel who are responsible for creating regulatory compliance solutions. Research conducted by the North Carolina State University and Protiviti shows that concerns over regulatory change and heightened regulatory scrutiny continues to be one of the top business risks. The Executive Perspectives on Top Risks for 2018 Report shows that 59 percent of respondents rated this particular topic as a "significant impact" risk to their organization.

One foundational solution is to create a visibility architecture that can lower this risk by capturing better compliance data to create improved audit trails. This includes:

- Optimizing data flows for current regulatory compliance initiatives
- Helping to discover rogue IT (unauthorized applications and devices) to avoid policy and compliance issues
- Detecting signs of off-network storage and unapproved web-based email solutions which allows IT to enforce its policies better

A visibility architecture is an end-to-end infrastructure which delivers network, application, and security visibility. This visibility allows you to optimize your network data capture, data privacy, and compliance verification techniques.

Devices like network packet brokers (NPBs) allow you to mask sensitive data, perform packet slicing, implement lawful intercept, and discover rogue IT. Purpose-built compliance solutions use data filtered by NPBs to perform activities better and allow IT to demonstrate their regulatory compliance in an easy manner.

Overview

This brief reviews techniques to improve regulatory compliance issues.

Additional Resources:

- How to improve network compliance Podcast
- Best practices for network monitoring

KEYSIGHT TECHNOLOGIES

A visibility architecture starts with data access. At this point, you will want to insert taps into the network between the network data flow and your monitoring tools (or NPB) to improve monitoring data quality and time to data acquisition.

The second layer is the monitoring data manipulation layer. This is where you will want to deploy NPBs between those taps and the security and monitoring tools to optimize the data sent to the tools. Once the NPB is installed, you can perform out-of-band data filtering, deduplication, packet slicing, header stripping, and many other functions to refine the data before it is sent to your monitoring and compliance solutions.

The third layer of a visibility architecture consists of the monitoring and compliance devices. Data from NPBs can also be fed to purpose-built compliance solutions and logging tools to support the demonstration of regulatory and endpoint compliance to auditors. Examples include logging devices (e.g. LogRhythm), compliance managers, endpoint management solutions, etc. The data being fed to these tools can be either lightly filtered or heavily filtered based upon detailed Layer 2 – 4 and/or Layer 7 parameters. It all depends upon what you need.

Data from network packet brokers can also be fed to purpose-built compliance solutions and logging tools to support the demonstration of regulatory and endpoint compliance to auditors.

Once you have your visibility architecture in place, there are several possible ways to optimize your compliance workflows. Here are some examples:

- Provide masking of sensitive data. This includes data masking for one or more digits so that security and monitoring tools downstream do not receive clear text data.
- Remove the data packet payload with packet trimming. When packet header information is all you need, packet slicing allows you to eliminate the propagation of unnecessary and dangerous data within the payload of the packet.
- Perform lawful intercept of data from specified IP addresses and VLANs. This provides an easy way to capture and forward data requested by court orders and government laws (like the Turkish 5651 law that requires the logging of financial data).
- Create regular expression (REGEX) search strings using application intelligence to enable better searches for specific data.
- Discover rogue IT (unauthorized applications and devices), which helps avoid policy and compliance issues. Unknown applications can be identified so that IT can ascertain how and where those applications are being used.
- Enforce IT policies, like detecting off-network storage and unapproved web-based email solutions. This allows IT to identify data which could be a potential security/compliance risk. For instance, a former employee could have stored a file to an off-network data storage and then could retrieve that file after leaving the company and no one would know about it.

Visibility Architecture Solutions from Keysight

In the end, any regulatory compliance strategy is only as good as the quality of data that is being fed to the tools. The most important part of your regulatory compliance plan will be the architecture, as this piece will determine what, if any, policies and procedures are being adhered to.

Keysight's network visibility solution involves using network packet brokers in conjunction with application filtering and taps. Learn more about Keysight's **Taps, Network Packet Brokers, AppStack,** and **Hawkeye** technology along with the solutions that our technical partners offer.

The most important part of your regulatory compliance plan will be the architecture, as this piece will determine what, if any, policies and procedures are being adhered to.

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