CASE STUDY

SECURE, EFFICIENT, RELIABLE, AND RESILIENT MILITARY COMMUNICATIONS

Best-In-Class Application Threat Intelligence Protects Email And Office 365tm On Cloud

This federal agency has a critical and sensitive mission: they are responsible for implementing the defense policy established by the government across multiple lines of armed services. The organization is chartered with protection of the country at home and abroad, working with allies and partners wherever possible.

Their aim is to ensure the armed forces have the training, equipment and support necessary for their work, all within a prescribed budget. Responsible for mounting a cyber-defense across all military organizations in the country, they worked with Keysight to target specific application traffic, conversation endpoints and bandwidth consumed. This metadata had to be forwarded to security “sensors” for long term storage and analysis.

In addition, like many organizations today, they were concerned about possible security threats contained in emails going to and from their defense partners. Through their Service Provider, they sought a “Gateway Service” to monitor and protect these communications.

Finally, the agency wanted visibility into encrypted traffic and applications that were being run over non-standard ports where attackers were attempting to evade security countermeasures. An example of this is SSH running over the port used by SSL. Secure, efficient, reliable and resilient communications were needed.

The agency wanted visibility into encrypted traffic and applications that were being run over non-standard ports where attackers attempted to evade security countermeasures

Company:

National Defense Agency
Chartered with protection of a country, including cyber-defense across all military organizations within the country

Key issues:

- This federal agency sought heightened security on communications external and internal to the agency and their defense partners.
- The customer wanted a “Gateway Service” providing inline security between the agency and emails to/ from external partners
- They sought to specifically monitor traffic over “non-standard” ports, alerting them to possible security threats
- With multiple Data Loss Prevention (DLP) tools and Intrusion Prevention and Detection (IPS/IDS) vendors, they needed a network packet broker and solution that scaled across all platforms

Solutions:

- (3) Network Packet Brokers (NPB) with AppStack featuring IxFlow™
- Subsequently, added (2) more NPBs with AppStack.

Results:

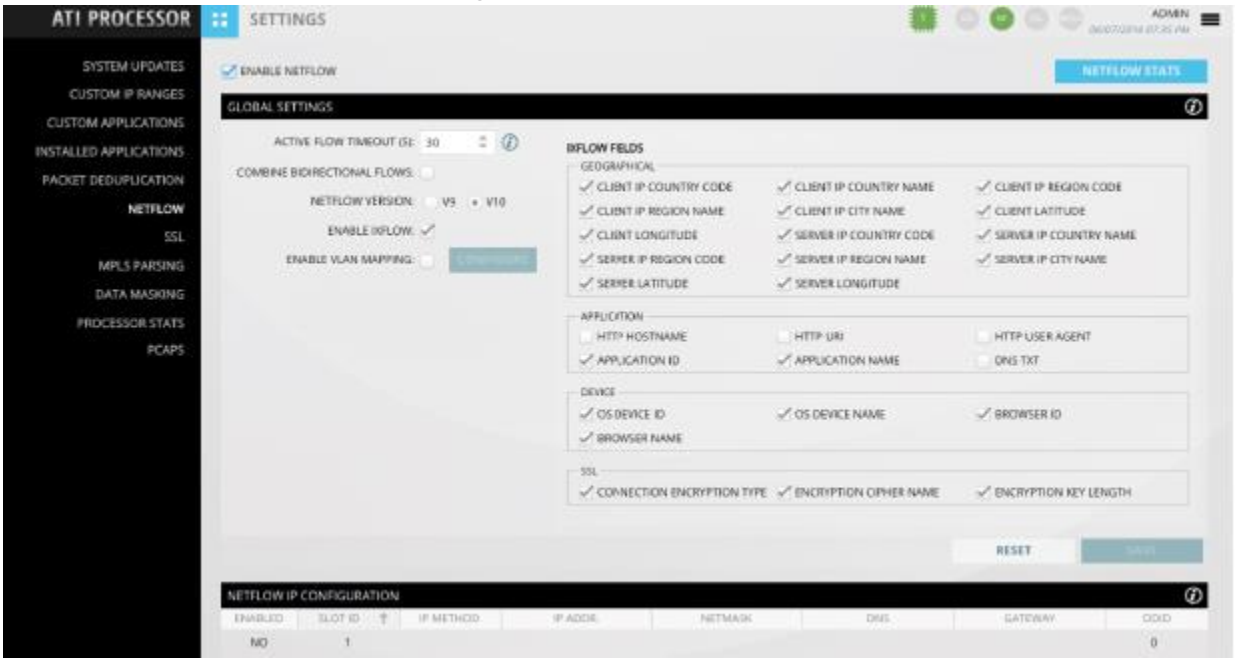
- Secure, efficient, reliable and resilient military communications
- No training time required
- Email with external defense partners and Office 365, hosted on the Cloud, was secured.

KEYSIGHT TECHNOLOGIES

Keysight's AppStack Delivers Actionable, Application-Level Insight For Agency Use

The agency's Service Provider approached the Keysight team with an explanation of these issues, addressed directly by the advanced intelligence and visibility offered by Keysight's NTO 6212, the AppStack platform. Keysight's AppStack scales across multiple vendor products, filtering network traffic to provide rich data on application behavior and the location of users to a variety of tools used by the agency, including data loss prevention tools, malware prevention and threat detection. It easily identifies unknown network applications, mitigates security threats, and identifies trends in application usage.

Keysight's ATI processor provides rich intelligence with 27 filters for NetFlow data



Inline Solution For Secure Email Communications

One of the first areas the customer wanted to address was email going from military units to defense partners. With AppStack, they could filter outgoing email traffic through what they called a "Gateway Service" passing data inline to threat detection boxes and data loss prevention tools for inspection and monitoring.

They also had visibility of applications that were being run over non-standard ports, indicating if people were trying to spoof their way in, evading security processes.

After viewing a demo of AppStack, the Service Provider ran penetration tests on the platform, ascertaining the solution did not allow for backdoors or new insecurities.

No other vendor evaluations were conducted. The Service Provider reported to the team there were no other Metadata solutions available that met the agency's stringent requirements, nor could they match the depth of insight offered by AppStack.

Intuitive GUI Required Zero Training Or Professional Services

After demonstrating the AppStack's user-friendly GUI to the Service Provider, neither training or Professional Services were required to launch the service. The agency has since expanded the Keysight packet broker solution, adding two additional units to include filtering and visibility for their Office 365 applications housed on the cloud.

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