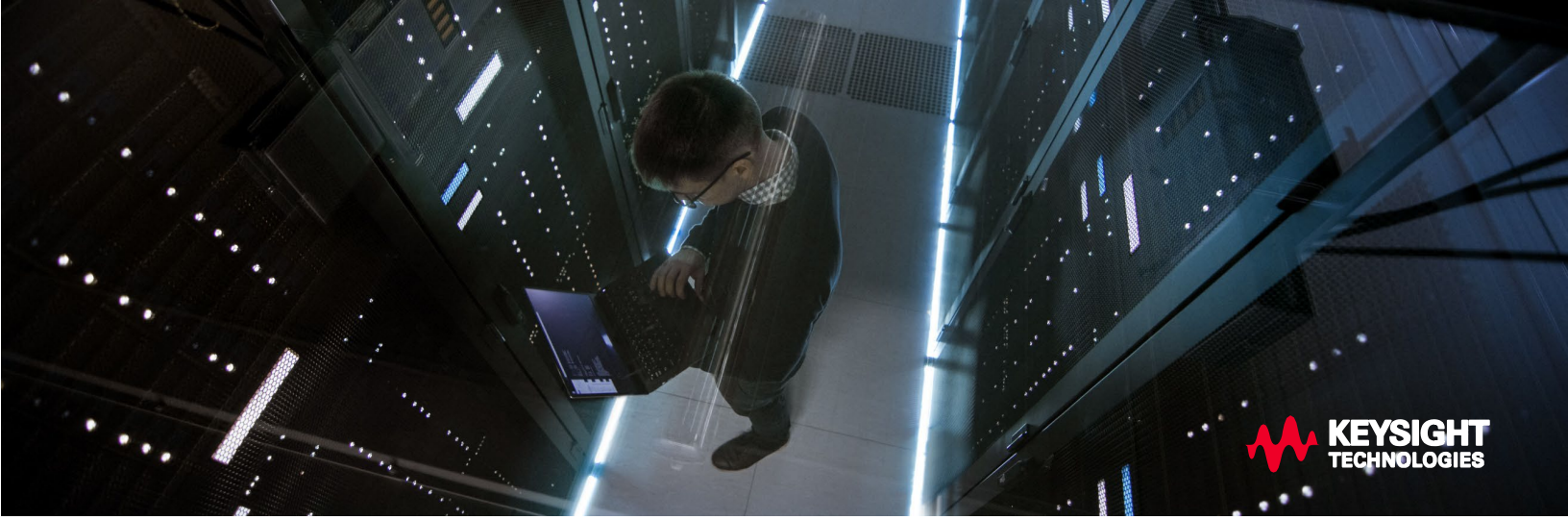

Data is the Lifeblood of Security Defenses

Missed Data Leads to Missed Security Threats

Government agencies are under constant attack from various types of bad actors. Missing just one piece of critical data can mean that your intrusion prevention system (IPS) misses a security threat and allows the threat to enter the network. However, there are clear technical activities that you can implement to minimize agency risk and the potential consequences of a breach.

Here is a short list of powerful solutions that a SecOps team can perform to fortify government networks:

- Deploy an inline security solution (consisting of a L2/L3 firewall, web-application firewall, IPS, and other equipment) that includes external bypass switches and network packet brokers (NPB).
- Activate SSL/TLS decryption (without slowing down your inline security solution) to find encrypted malware.
- Install threat intelligence solutions to fortify malware and ransomware blocking.
- Perform data filtering by application type to find indicators of compromise (IOC).
- Capture packet data to conduct deep packet inspection (DPI).
- Implement cyber resilience functions to ensure that the downtime and cost of a breach is minimized.

Cyber Security Solutions That Work

While there are many directions you take to implement those solutions, too many projects moving in too many directions may cause more harm than good. When it comes to cyber security, simplicity is best. Here are four fundamental actions to consider along with some example use cases per category.

1. Maximize service continuity and network uptime of security defenses with an external bypass switch
2. Optimize inline security deployments for maximum network security protection
    - Deploy inline NPBs with High Availability to strengthen inline security deployments
    - Enhance inline security solutions using load balancing and serial tool chaining
    - Perform SSL decryption to inspect packet data for malware threats using an external SSL decryption appliance or internal NPB decryption
3. Provide innovative security solutions to enhance threat identification activities
    - Use application filtering out-of-band to reduce load on DPI appliances (like DLPs and IDSs)
    - Create an early warning system for a compromised network using application intelligence
    - Spot suspicious activity based upon NetFlow and IPFIX protocol metadata information

- Spot suspicious IOC activity (command & control and ransomware) by filtering on application type and bandwidth usage correlated with geolocation to observe data flows across the network
- Create activity baselines to expose aberrant behavior
- Monitor communications to and from known compromised IP addresses using a threat intelligence probe

4. Strengthen defensive security measures to prevent breaches
   - Conduct data filtering to remove uninteresting information (cached traffic, backups, Windows updates, etc.)
   - Improve BYOD security by deploying assured identity management for mobile devices
   - Block malicious traffic from known bad IP addresses to exponentially reduce the strain on expensive application aware equipment
   - Automatically update known bad IP address access lists to reduce human efforts
   - Block the exfiltration of command & control traffic and data to known bad addresses
5. Deliver functionality that supports and enables cyber resilience by looking for faster attack diagnosis, faster testing of potential fixes, and faster network recovery

How to Fortify Your Network

To implement use cases relevant to government agencies, Keysight Technologies offers a wide range of security solutions including:

- Vision ONE network packet brokers (NPBs) with zero packet loss for full featured, non-blocking monitoring up to 100GE
- iBypass external bypass switches that increases your network reliability with superior fail-over and fail-back techniques
- Inline Vision ONE NPBs that support high availability to create improved security appliance survivability and self-healing architectures
- Integrated SSL/TLS decryption that removes the heavy decryption burden from your security tools while still exposing hidden security threats
- AppStack application intelligence feature for the Vision ONE that captures IOC and correlates that information with geolocation data to create an early warning solution
- ThreatARMOR threat intelligence gateways that stop incoming malware and outgoing data exfiltration with known bad IP addresses
- ThreatARMOR threat intelligence gateway solutions that can be used to isolate IP links to create an air gapping solution that also thwarts security threats
- A combination of features and other products that can create a resilient cyber security solution to remediate and mitigate the effects of a cyber-attack as fast as possible

Reach out to us and we will show you how to fortify your network against multiple threat vectors.

Learn more at: https://ixia.keysight.com/solutions/segments/government-solutions

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at:

https://ixia.keysight.com/contact/info