Make the Quantum Leap from Reactivity to Proactivity

The Government CDO Challenge — Turning Data Into Actionable Insights

Today's government networks require innovation to generate useful and actionable insights. This means digital transformation and forward thinking. It's about making the quantum leap from reactivity to proactivity. Government agencies and Chief Data Officers (CDOs) cannot afford to be reactive. Cyber criminals, adversarial nation states, international pandemics, global economic problems, and calls for transparency are just some of the external drivers demanding faster, more proactive responses.

So, how do government agencies truly achieve this proactive digital transformation? Here are three overarching strategic suggestions that will produce tangible results.

- Place an emphasis on network monitoring to create a visibility architecture
- Consistently validate how your network and equipment are actually performing
- Ensure your infrastructure is agile enough to support the speed of business

First and foremost, the network is changing. Users are more sensitive to network issues and digital business models need to move from predictive to prescriptive analytics. Visibility has to be an integral part of the network. It will improve network security, optimize network and application performance, and reduce troubleshooting efforts. Fundamentally, visibility enables you to collect data when you want, how you want, using taps and network packet brokers (NPBs). Consider this, how well do you monitor user experience today and how much value do you derive from agency data? Visibility drives these actions.

A second activity is to continually test and analyze your architecture. You can't improve what you don't measure. This means validating the security, performance, and stability of your design by using real-world traffic profiles, loads and threat vectors. After that, collect critical information on how your systems will react once deployed so you can emphasize quality of experience and measure internal and external SLAs (especially for cloud networks). Not only will testing save you time and costs, it will prevent surprises.

Lastly, your infrastructure needs to be agile enough to support the speed of business — whatever users, adversaries, and global pandemics throw at it. Agility comes through technology and process modernization. Benefits of government agency modernization are numerous and include: lower cost and greater efficiency of complex tasks, strategic advantages from leveraging the latest technology, elimination of vulnerabilities inherent to legacy systems, and agency future-proofing by planning for technology advances.

Six Areas Where Network Modernization Can Make A Big Impact

Here are six key tactical actions that your NetOps team should consider to modernize your government agency network and make the agency more proactive:

1. **Position yourself to collect data when you want, how you want.** Surgical precision is required to provide visibility into your network and how it actually behaves. NPB's and taps give you that power. Once this equipment is in place, you can change equipment without affecting the network.
2. **Turn the data you collect into actionable information.** Properly designed visibility architectures deliver the critical intelligence needed to boost network security protection, reduce troubleshooting costs, create architecture efficiencies, and extend the life and utility of monitoring tools. For instance, context aware data processing can be used to expose indicators of compromise, provide geolocation of attack vectors, and combat encrypted threats.
3. **Modify your infrastructure so that it is agile enough to support the speed of business.** This includes upgrading your monitoring processes to the 21st century. While Change Boards are a necessary oversight function, you need to be able to add/remove security and monitoring tools without change board approvals to address network problems and security threats as they arise. This saves most IT departments hours, days, even weeks of time, reducing mean time to repair (MTTR) by up to 80%.
4. **Optimize your network for telecommuting.** In the modern era of pandemics, your workforce needs the flexibility to work remotely. Therefore, IT personnel must optimize the network by making sure it can handle remote worker load. This means pre-testing your solution at full load to ensure that it works as designed — with no surprises.
5. **Deploy new technologies, like application intelligence.** Application intelligence provides contextual data information that allows businesses to prevent many network problems and significantly reduce the impact of network problems that do occur. This includes usage forecasting and trend analysis that can reduce costs, especially for service outages.
6. **Continue to embrace commercial off the shelf solutions (COTS) to decrease deployment times and costs.** Custom solutions are expensive and take a long time to develop. In contrast, COTS solutions have a quicker time to market and costs are spread across multiple customers.

To implement use cases relevant to government agencies, Keysight offers a wide range of monitoring solutions. This includes taps, network packet brokers, application intelligence, and performance monitoring. Reach out to Keysight and they can show you how to modernize your network and make the quantum leap from reactivity to proactivity.

Learn more at: www.getnetworkvisibility.com

Keysight sponsors GetNetworkVisibility.com, a thought leadership website dedicated to the importance of packet-based visibility to power security, performance, and network monitoring tools. For more information, contact us at:

KEYSIGHT

www.getnetworkvisibility.com/contact-us/