MeriTalk
Improving the Outcomes of Government IT

ciena

Protect the Network from the Edge to the Fiber

How network as a sensor helps agencies improve security and resiliency

A state actor hijacks a defense unit's network traffic using Border Gateway Protocol (BGP), the routing protocol for the internet. As a result, that traffic starts flowing through North Korea.

Or, an agency's network goes down and then comes back up, seemingly without incident. In reality, a bad actor changed the path of the fiber, directing it through a hub designed to exfiltrate data.

These scenarios are not hypothetical—they represent real consequences of breaches at the lowest network layers. But cybersecurity at Layers 0 through 3 is often an afterthought. If the network is available and performing well, temporary service interruptions can be chalked up as glitches that were resolved. That mindset can have serious consequences for national security, intellectual property, citizen data, and critical infrastructure.

Increasing numbers and severity of cyberattacks against governments and critical infrastructure providers have made a holistic approach to cybersecurity an imperative for federal agencies. Everything on the network must be visible, from endpoint devices down to the network fiber. Otherwise, comprehensive network management and defense is impossible. Then, security must be embedded into every layer in the network. If any layer is overlooked, attackers have a potential path into the network—and from there, into every other layer.

A comprehensive approach to network visibility and security requires a new way of thinking. As networks continue to rapidly grow in capacity, complexity, and flexibility, the historical approach of bolting on sensors for visibility does not scale in terms of cost or labor. And bolted-on equipment does not always evolve with the network.

Today, however, agencies can leverage the network itself as an always-on, always-aware sensor, from which agencies can capture and analyze rich telemetry to gain broad and deep visibility into all activity on the network.

With built-in sensor capabilities, the network can grow and provide the visibility necessary to support future mission capabilities securely. Network-as-a-sensor capabilities enable agencies to obtain a real-time picture of how data is flowing across the network and analyze that data to identify:

- Changes in the network that cause problems such as latency, jitter, or dropped packets
- The best path through a network to ensure resilient service, even in the event of a cyberattack
- The root cause of a problem, such as inadequate network capacity or a cyberattack
- Poorly performing equipment, so it can be replaced before it fails

Discussions of network security and resiliency often revolve around firewalls, intrusion prevention systems, network access control, and network threat mitigation and anomaly detection—typically operating at the network and transport Layers (Layers 3 and 4). But today, agencies can go deeper—to Layers 0, 1, and 2 of the network—to bolster their network security even more.

Protection at the lowest layers of the network enables agencies to be more reactive to threats and failures. Agencies can detect problems that they normally would not be looking for because they lacked the capability.

Ciena provides a real-time view of the lowest layers of the network

Ciena's unique programmable infrastructure is designed from the modem up to generate unparalleled, rich optical telemetry. With this telemetry, agencies gain greater awareness of network activity, which informs decision-making and response.

Ciena's network-as-a-sensor capabilities utilize coherent optical modems at the lower layers of the network to gain visibility into a wide range of factors, including:

- The type of fiber, as well as any stress on it
- The distance a signal has traveled
- The exact location of a break in the fiber
- Changes in the fiber type or characteristics
- Manipulation of aggregate data flows

The information helps agencies quickly respond to problems—which might be simple equipment failure or a sign of nefarious action. Coupled with Ciena's wire-speed optical encryption solution, which encrypts all traffic before it enters the fiber, agencies have additional assurance that bad actors will not gain access to any information.

Moving up the network stack, Ciena monitors for data flow changes and informs on endpoint inventory and the associated risks or threats to each one. Ciena's Adaptive IP™ Apps at Layer 3, for example, record the IP protocols that routers are exchanging and save the data for analysis. As a result, agencies get a real-time picture of how data is flowing across the network, and can conduct network forensics to determine the cause of a problem, such as jitter or dropped packets.

When agencies introduce new services, Ciena enables them to create "birth certificates" that provide a baseline of performance characteristics on day one. From there, agencies can monitor for deviations over time.

Network as a sensor enables the Adaptive Network™, which responds to changing requirements

Ciena's programmable infrastructure is the backbone of network as a sensor and a key component of the Adaptive Network, a dynamic infrastructure that is designed to respond to changing agency requirements.

The Adaptive Network creates a communications loop that relays information from network elements, instrumentation, users, and applications to a software layer for review, analysis, and action.

The Adaptive Network comprises three layers:

- Programmable Infrastructure: the network's physical and virtual elements, as well as the telemetry gathered from them. The programmable infrastructure layer is highly intelligent and interprets data so the network can make decisions—whether that means routing traffic around a circuit that is down or investigating and correcting an issue with latency or lower-than-expected capacity on a specific link.

- Analytics and Intelligence: analysis of network performance data generated by the programmable infrastructure. Artificial intelligence (AI) provides the ability to predict potential network problems and anticipate trends more accurately by turning mountains of data into actionable insights.

- Software Control and Automation: automation of network tasks, such as loading access controllers and provisioning routers. This can eliminate human errors and keep the network running at peak performance.

Network as a sensor and the Adaptive Network can help agencies significantly improve their cybersecurity posture. Ciena works in partnership with agencies to define network requirements and tailor solutions that are unique to each environment.

To learn more, please visit: www.ciena.com/government