WHITE PAPER

Network as a Sensor

Network-as-a-sensor capabilities enhance cyber posture

The safety and security of our critical infrastructure has never been more important than it is today. Adversaries have advanced capabilities and are constantly targeting these systems; consequently, investments in cyber security are expected to top $17 billion in 2021. Still, continued investments in new solutions will not realize their full potential unless foundational capabilities are in place. For example, AI-based endpoint protection leaves gaps if there is not a full inventory of endpoints. The Zero Trust network paradigm is predicated on awareness of data flows and network infrastructure. Finally, although most attacks are at Layer 3 and above in the network, nation-state threats will also attack the lower layers of the network; having accurate telemetry and visibility at the lower levels validates the integrity of the physical layer in critical infrastructure. Failure to achieve fundamental awareness capabilities substantially weakens other cyber security investments.

For many years, The Center for Internet Security has published a prioritized list of security controls. Collectively known as the 'CIS Top 20'[1], it focuses on the most important areas in which to invest to build a defensible infrastructure. The first control is hardware inventory; the next five controls focus on software inventory, vulnerability management, configuration management, administrative control, and effective monitoring and analysis. Awareness is key in network management and defense; it is difficult, if not impossible, to manage and defend something that cannot be seen. The network is the backbone of service; it establishes and enables communications between everything else. A secure network should provide a critical eye to answer the top six CIS security controls. Without leveraging the network as an 'always-on, always-aware' sensor, potential security-relevant events are missed every day.

Ciena is focused on the development of a series of 'network-as-a-sensor' capabilities to augment and enhance other cybersecurity investments. The network is an undeniable, unalterable source of truth. Each frame, packet, and transaction exchanged between users must traverse the network and the network is 'aware' of this fact at some level. Every cyber event is dependent upon the network to enable the attack.

It is important to appropriately leverage key observables in the form of telemetry to better inform network and security operators. It is this network telemetry that is crucial to true awareness, decision-making, and response.

The challenge is providing appropriate telemetry from multiple layers of the network so that cyber events are actionable, and evidence/intelligence is obtained. Layer 0 and Layer 1 monitor for changes in the physical infrastructure: additions or modifications to the physical network infrastructure, as well as manipulation of aggregate data flows. Layers 2 and 3 monitor for higher-layer data flow changes and inform on end-point inventory and the associated risks/threats to each.

Ciena's unique programmable infrastructure is designed from the modem up to generate unparalleled and rich optical telemetry. This design—combined with tailored analytics and a decision engine to build a highly scalable, resilient, and resistant infrastructure—can be used in future offerings to inform analysts of critical security events. The potential to eliminate the introduction of malicious devices, stop lateral movement, and contain data exfiltration exists in the very fiber and network devices that make up the infrastructure today.

[1] https://www.cisecurity.org/controls/cis-controls-list/

Layer 0 and Layer 1 Wide Area Network (WAN) use case

Typically, when cyber risks are assessed in a network, the upper layers of the network get much of the attention as most of the attacks are focused on Layers 4 and above of the OSI stack. However, some of the most dangerous attacks are those on the lower layers where a compromise is capable of exposing the entirety of a network to an adversary.

Ciena is an experienced provider of network transport solutions for critical infrastructure. Ciena's class-leading coherent modems not only provide support for up to 800 Gb/s optical channels and 32 Tb/s of capacity per fiber but supply a rich set of telemetry from which the state of the physical network can be observed. Consider the possibilities now that the network can provide near real-time measurements of:

- Time domain reflectometry to determine fiber bends, stress, or break locations
- Fiber characteristics such as optical loss, distance, dispersion, and polarization state
- Link propagation metrics such as Bit Error Rate(BER), linear and non-linear noise

With Ciena-provided optical observables and a future enhanced analytics capability, it is possible to realize improved 'network fiber health' which dramatically augments existing fiber intrusion detection.

Layer 2 and Layer 3 edge use cases

The edge of a network is often exposed in areas that are difficult or impossible to physically secure. These locations present significant risk as they are in areas that adversaries are very likely to physically compromise and where equipment could be added to the network. These additions could be for longer periods of time or just long enough to drop off malicious payloads. The best defense in these areas relies on locked racks or closets and administrative controls on the devices including port security and tamper- proof cases. Determined adversaries are capable of very quickly bypassing these controls or simply accepting the risk of detection to deliver the payload, knowing their presence will likely go undetected given the short time they are on net. A successful defense against these kinds of attacks includes the ability to quickly detect their occurrence and be notified by an alarm in a way that is not ignored due to alert fatigue. Furthermore, the ability to respond to an attack in both recommended, manually configured, and automated ways is important.

Ciena's current offerings provide the building blocks to unlock future security solutions: example capabilities of such a system include the ability to detect, alert, and respond to various attacks as they occur or the ability to sense a change in a network security posture. The system could be positioned as an on-premise disconnected solution or as part of a holistic enterprise system that monitors the edge of the network in real time.

Future possibilities

- Profile existing fiber assets
- Machine learning and trending analysis of performance monitoring data
- Analyze data from fiber modems every 500 μsecs
- Analyze statistics from indications that a fiber is being tampered with
- Multi-vendor compatible—learn from data, not documentation

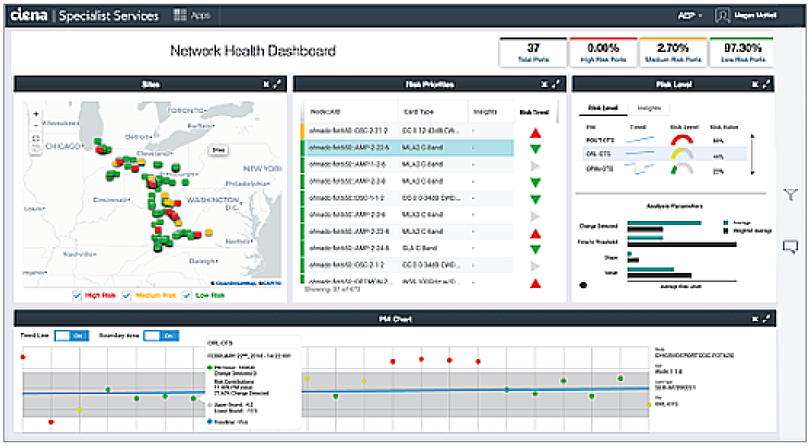
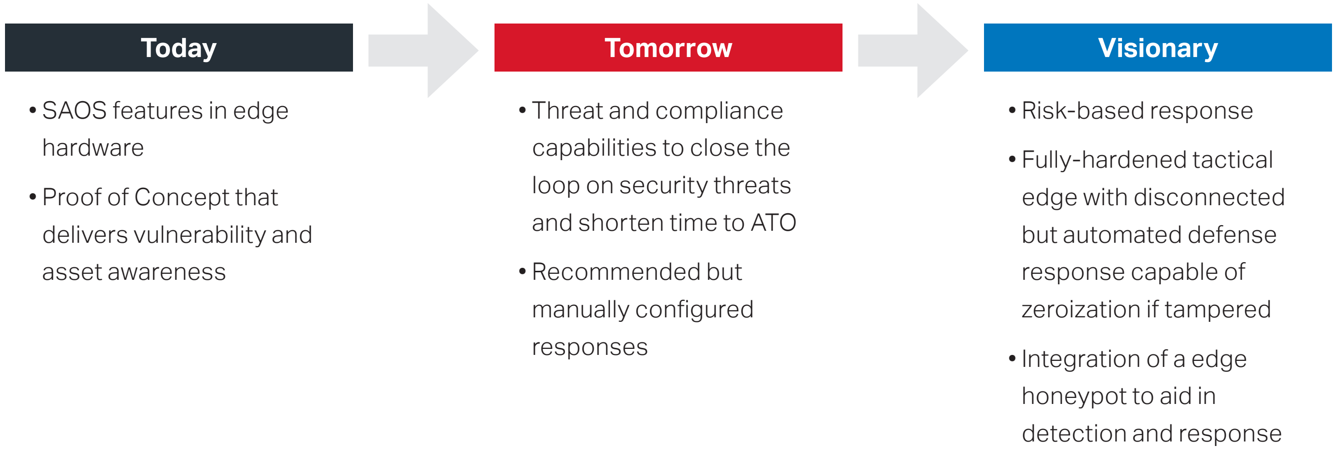


Figure 1. Existing network health application could be enhanced to include additional modem parameters



Today

- SAOS features in edge hardware
- Proof of Concept that delivers vulnerability and asset awareness

Tomorrow

- Threat and compliance capabilities to close the loop on security threats and shorten time to ATO
- Recommended but manually configured responses

Visionary

- Risk-based response
- Fully-hardened tactical edge with disconnected but automated defense response capable of zeroization if tampered
- Integration of a edge honeypot to aid in detection and response

Figure 2. Status of the edge security solution

Solutions for Government
Learn more →

Ciena’s newest release of SAOS along with tactical edge network elements supports immediate detection, storage, and alerting anytime a device attempts to connect to an open interface. These enhancements allow alerting to a future cloud based or on-premises solution that can trigger enumeration of the new device’s vulnerability, threat, and risk posture as well as recommend mitigation steps to control or eliminate the suspect device’s presence. This enables intelligent responses as determined by individual mission needs.

Summary

The capabilities of tomorrow and the visionary features described in this paper are advanced capabilities that Ciena is working on for future releases. Leveraging current Ciena analytics with these future capabilities have the potential to significantly improve the cyber posture of critical infrastructure with a combination of multi-layer and multi-vendor inventory capabilities, along with rich metrics that provide insight into the health of the communication link and the fiber infrastructure that it rides on. Ciena works in partnership with agencies to define network requirements and tailor a network-as-a-sensor solution to each unique environment.

As a supplier of equipment and services to government agencies Ciena takes a comprehensive approach toward maintaining the security and continuity of its supply chain.

? Was this content useful? Yes No