MeriTalk
Improving the Outcomes of Government IT

NETWORK SECURITY:
GOVERNMENT'S LATEST CYBER FRONTIER

ciena

LUMEN

As government agencies navigate network environments expanding into uncharted territories in the telework age, new threat actors are finding ways to infiltrate and exploit the federal enterprise. Known vulnerabilities and open source information become easy targets with the potential to take down an entire agency ecosystem.

Federal agencies have implemented safeguards to remain secure against attempted attacks, but network responsibilities stretch beyond that baseline. Agencies are navigating a new environment in which they must build a secure, trusted network infrastructure that is responsive to mission demand. The network must be able to scale and adapt to changing needs—especially in the new telework-heavy environment as the COVID-19 pandemic continues.

Within this nascent architecture, the same cybersecurity challenges persist in agency networks, exacerbated by the crisis. The modern threat landscape involves data leaks, introduction of unknown or authorized devices, unauthorized expansion of network infrastructure, denial of service, and attacks on trusted infrastructure. Attacks take advantage of increased strain on networks as government sites scale to accommodate heavy traffic and federal agencies become a target to steal research and development insights.

The tactics used by malicious cyber actors to attack the federal government are not new. Threat entities frequently use known vulnerabilities to enter a network and distribute malware or breach data. Patching security gaps in the network infrastructure is a never-ending challenge at the federal level that only a holistic approach to network security can solve. However, detecting a threat is not effective if agencies have not built and cannot operate a trusted and safe infrastructure.

Establishing a secure network

As agencies work to build a holistic network security solution, five components of a secure network are essential to keeping the enterprise responsive to mission demand: Availability, confidentiality, trust and integrity, resilience, and resistance are critical to establishing a secure network.

Availability ensures that the static network infrastructure can respond and meet demand. To make sure that data is not exposed to unauthorized actors, confidentiality keeps the data protected while in transit over the

```
_mod = modifier_ob.modifiers.new("
mirror object to mirror_ob
_mod.mirror_object = mirror_ob
operation == "MIRROR_X":
_mod.use_x = True
_mod.use_y = False
_mod.use_z = False
operation == "MIRROR_Y":
_mod.use_x = False
_mod.use_y = True
_mod.use_z = False
operation == "MIRROR_Z":
_mod.use_x = False
_mod.use_y = False
_mod.use_z = True

ion at the end -add back the desel
ob.select= 1
ob.select=1
t.scene.objects.active = modifier_ob
elected" + str(modifier_ob)) # modif
_ob.select = 0
.context.selected_objects[0]
objects[one.name].select = 1

("please select exactly two objects,

OPERATOR CLASSES ------------------

s.Operator):
X mirror to the selected object"""
ct.mirror_mirror_x"
mirror X"

ext):
ive_object is not None
```

network from one source to another. The third component, trust and integrity of the infrastructure, verifies that the network is operating in compliance with agency requirements and operating as expected.

Resilience and resistance—the last two components of a secure network—are closely tied together. When an outage occurs, a resilient network quickly reconstitutes the downed network connections. Resistance describes the infrastructure's ability to keep adversaries at bay when they try to attack. The network must be built securely from both a software and hardware perspective at every step of the supply chain to truly be resistant.

In an effort to secure the entire federal enterprise, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) lead the Trusted Internet Connections (TIC) and Continuous Diagnostics and Mitigation (CDM) network efforts. While each agency has its own network security plan in place, these efforts set government-wide standards for resilience and resistance.

The TIC initiative works to reduce the federal attack surface by monitoring and controlling network connections. During the mass shift to telework amid the COVID-19 pandemic, leaders of the TIC program released interim guidance to manage the unprecedented remote environment,[1] in addition to version 3.0 of its guidance tailored to modern network environments.[2] Through CDM, CISA is automating how agencies monitor and manage cyber vulnerabilities. Dashboards provide real-time analysis across the federal enterprise to keep networks resilient and resistant.

Early in the COVID-19 pandemic, the Departments of Health and Human Services and Defense both reported an increased attack surface area.[3] CISA's telework guidance works to get ahead of new vulnerabilities caused by the changing network architecture, but attacks persist.

These federal policies cannot stop one of government's biggest network vulnerabilities: its own workforce. Without a secure network architecture, phishing and malware can slip through undetected when an unsuspecting employee clicks a dangerous link that compromises the system. Federal agencies like the Department of Education have implemented new measures, including realistic e-mail phishing tests, to teach the workforce what to avoid.[4] Another way of educating the workforce is to enhance required annual training with tailored security content based on worker roles. For example, developers should receive application security training, and network operators are introduced to network-based attack methodologies and TTPS.

Looking ahead, public and private sector leaders have both predicted that the workplace environment will never go back to the way it was. Telework has proven itself as a productivity enabler with workforce convenience, but network vulnerabilities will continue undermining agency cybersecurity without an available, confidential, trustworthy, resilient, and resistant network in place.

[1] https://www.meritalk.com/articles/cisa-releases-interim-tic-3-0-guidance-for-covid-19-telework-surge/
[2] https://www.meritalk.com/articles/cisa-finalizes-tic-3-0-core-guidance-documentation/
[3] https://www.meritalk.com/articles/hhs-dod-battle-increased-cyberthreat-attack-surface-during-covid-outbreak/
[4] https://www.meritalk.com/articles/spearphish-testing-paying-off-at-education-department/

Agencies are not overcoming this new normal alone. Industry partnerships and solutions—like the services offered by Ciena and Lumen—can guide the government through establishing a secure network.

Ciena and Lumen capabilities

Building a secure network solution depends on strong partnerships that can keep agency architecture secure at every step along the supply chain. Not only must the software and hardware solutions be built with security in mind, but the network must be managed by a trusted source.

Lumen provides agencies with the foundation to build a secure network that can readily adapt to change. The architecture is based on a trusted hardware provider that secures the network foundation. TAs the network hardware generates telemetry, the operations component enhances the raw data with analytics and intelligence to make crucial security decisions.

Ciena provides the comprehensive solution of the hardware and software, and Lumen's expertise on the platform leverages the intelligence and analytics together in one place. This foundation allows Lumen and Ciena to deploy, operate, and manage the solution. This partnership is key to securing customer locations, and the two companies work together to provide agencies with the foundation for a secure environment.

Conclusion

Federal agencies are in the midst of an overwhelming network security challenge. New landscapes, emerging threats, and a strained architecture can all leave agencies vulnerable to persistent threat actors. By establishing an available, confidential, trustworthy, resilient, and resistant network architecture, agencies can cut their vulnerabilities and mitigate intrusions as they occur.

However, the government cannot build this network by itself. Industry partnerships can provide the enterprise with the infrastructure and analytics necessary to keep them secure. By working together on every step of the network timeline, Ciena and Lumen are the key to safeguarding federal networks by providing the foundational architecture of a secure environment. For more information please visit: www.ciena.com/government and www.lumen.com/public-sector.