Modernizing defense networks:
The push for future-proof security solutions

Unprecedented threats to DOD network security from a wide range of adversaries underscore the need for modernized solutions to protect mission-critical operations and sensitive data today and in the future.

The 2023 Department of Defense (DOD) Cyber Strategy revealed DOD agencies are facing unprecedented threats to network security that put the integrity and effectiveness of its operations at risk. From "script kiddies" to adversarial nation states, bad actors of all sophistication levels aim to breach DOD systems to steal sensitive information, disrupt communications and compromise mission-critical operations. These attacks can exploit weaknesses in outdated or improperly configured systems, leading to unauthorized access and potential data breaches that can have severe implications for national security.

"When you're running a mission-critical network, you become a magnet for adversaries," said Jim Westdorp, chief technologist for Ciena. "The DOD by its very nature has a big target painted on its back, attracting attacks from a broad spectrum of adversaries."

To keep up with the ever evolving, broad scope of their attack surface, DOD agencies are investing in modernized solutions that secure not only against current threats but also against future ones, building more resilient and reliable networks that can support mission-critical infrastructure and protect the most sensitive and classified data.

Future-proofing networks to stay ahead

Agencies understand the digital transformation journey is long and winding, necessitating tens of millions of dollars and years of overhauling legacy systems. But when national security hinges on an agency's ability to adapt and respond to emerging threats like quantum computing, modern, secure solutions are no longer a luxury—they're imperative.

"If you have a cyber event and someone compromises the network, particularly the low level where there's so much information flowing across the network, it's not about the money anymore at that point," Westdorp said. "Not only would it be even more expensive to mop up after, but in the case of the DOD, an attack could be detrimental for our service members who are at the pointy end of the spear."

According to the Defense Industrial Base 2024 Cybersecurity Strategy, agencies should invest in secure network solutions that protect critical infrastructure today, while also being able to scale and defend against any threats that may come about in the next 10 years.

For instance, one significant threat to current cybersecurity measures is the potential development of quantum computers capable of breaking existing public key infrastructure encryption methods. While such a quantum computer doesn't exist yet, Westdorp considers it a foreseeable future threat. This is concerning because an adversary could store encrypted data today and decrypt it later when quantum computers become available.

> **"If you have a cyber event and someone compromises the network, particularly the low level where there's so much information flowing across the network, it's not about the money anymore at that point."**
>
> Jim Westdorp, Chief Technologist, Ciena

As a way to prepare for the future of quantum threats, security agencies like National Institute of Standards and Technology (NIST) and National Security Agency (NSA) are developing new quantum-resistant algorithms designed to withstand attacks by quantum computers.

"NIST and the NSA have been working on new sets of ciphers to address the key distribution problem," Westdorp said. While these standards are still in the finalization stages, companies like Ciena are planning ahead.

"We have built the capability to incorporate those new standards into our next-generation encryption engine so that once there is a standard, we can program our hardware to comply," Westdorp said.

Beyond algorithmic advancements, Westdorp said quantum key distribution (QKD) offers a highly secure method for key exchange. QKD leverages the principles of quantum mechanics to ensure that any interception attempt on key distribution is detectable, preventing adversaries from eavesdropping unseen.

For example, if a general were to send a command to a warfighter at the edge, and an adversary intercepted the key exchange, the quantum states would alter, revealing the eavesdropper's presence and prompting the parties to abort the transmission.

Given that defense networks form the backbone of national security infrastructure, the use of QKD can significantly enhance the protection of critical systems, ensuring that military communications, strategic plans and sensitive data remain secure from sophisticated cyberattacks in the future.

Ciena's secure-by-design approach

As the cyber threat landscape continues to evolve, staying ahead requires continuous innovation and adaptability. Defense agencies must engage with technology providers who understand the latest advancements and integrate them into their networks. For Westdorp, this means teaming up with partners who build products with security top of mind.

"Just as important as feature functionality is how you designed that product in the first place," said Westdorp. "It's not just about having the right features, it's about how you design and develop the product to be secure from the ground up."

According to Westdorp, Ciena takes a "secure-by-design" approach to ensure that when an agency implements a product in the network and uses it normally, it's designed to be safe and compliant with federal security requirements.

Waveserver, Ciena's high-capacity data distribution node, was designed with not only current threats in mind, but also future threats like advanced quantum computers. Designed with an encryption engine built into each modem, Waveserver uses an innovative optical encryption approach to provide quantum-resistance straight out of the box.

The implementation combines standards-compliant algorithms and a locally provisioned pre-shared key (PSK) cryptographically, to enable a solution that provides new AES encryption keys every second and protects against quantum computer attacks on today's key exchange algorithms. Waveserver can also interface with QKD devices, positioning users to be able to combat quantum threats as they evolve.

"Waveserver will support up to 1.6 terabits per wave and includes real-time encryption engines capable of handling today's encryption standards, as well as being upgradeable for future quantum-resistant algorithms," Westdorp explained.

> **"It's not just about having the right features, it's about how you design and develop the product to be secure from the ground up."**
>
> Jim Westdorp, Chief Technologist, Ciena

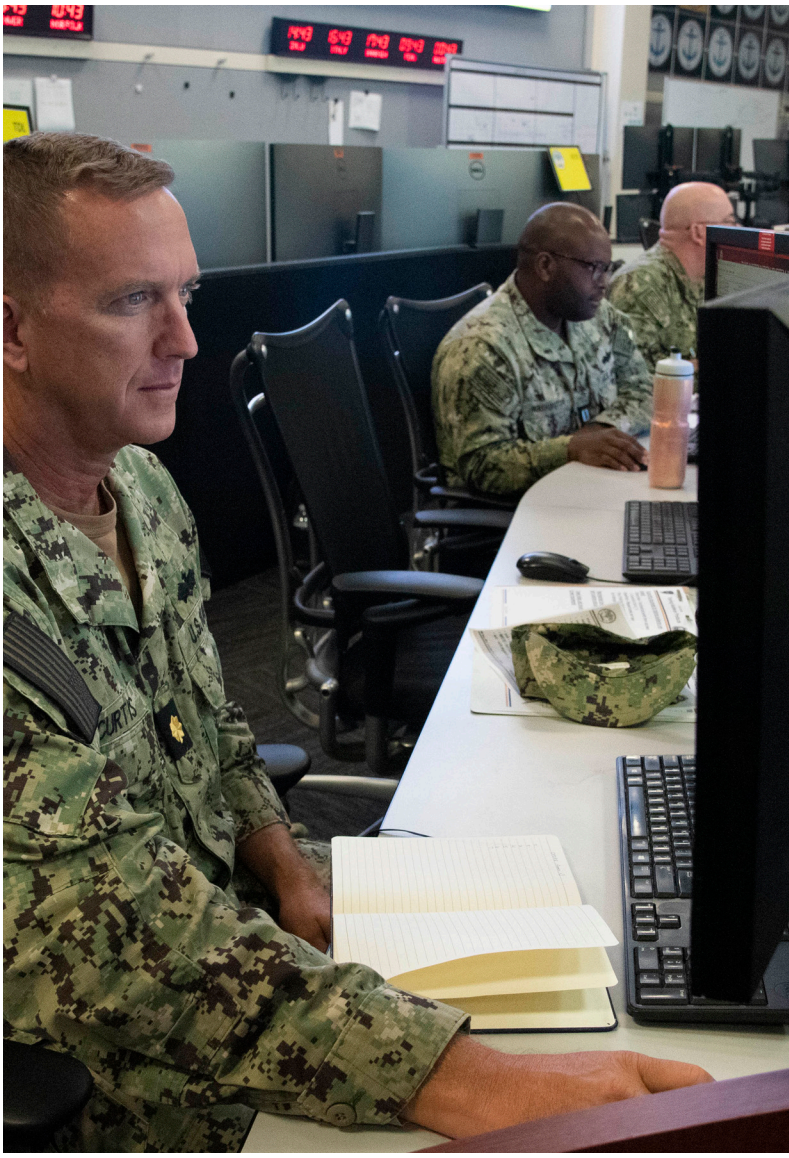
Especially for networks used by the DOD and the intelligence community, this comprehensive encryption capability is crucial to securing high-capacity transport and data center interconnect applications. Additionally, defense agencies can feel confident in the security of their networks as Ciena's encryption products are built to comply with NIST, FIPS 140-3 and Common Criteria. Westdorp considers that mandatory for deployment in defense networks that handle highly confidential and mission-critical data at all times.

"These critical networks are used in support of the DOD and the warfighter mission, so if an adversary is going to attack something, they're going to go after the network, which is a force multiplier for the services," Westdorp said. "If a product doesn't meet these security standards, then it's not really suitable for the mission."

For defense agencies, network security is not just a technical challenge but a mission-critical imperative. With partners like Ciena, they can leverage cutting-edge technologies to protect against current and future threats, ensuring their communications remain secure and their missions successful.

"The real issue we're concerning ourselves with is the protection of our service members and national security," Westdorp said. "The stakes couldn't be higher."

Learn more about Ciena's portfolio of secure communications solutions.



> **"The real issue we're concerning ourselves with is the protection of our service members and national security. The stakes couldn't be higher."**
>
> Jim Westdorp, Chief Technologist, Ciena