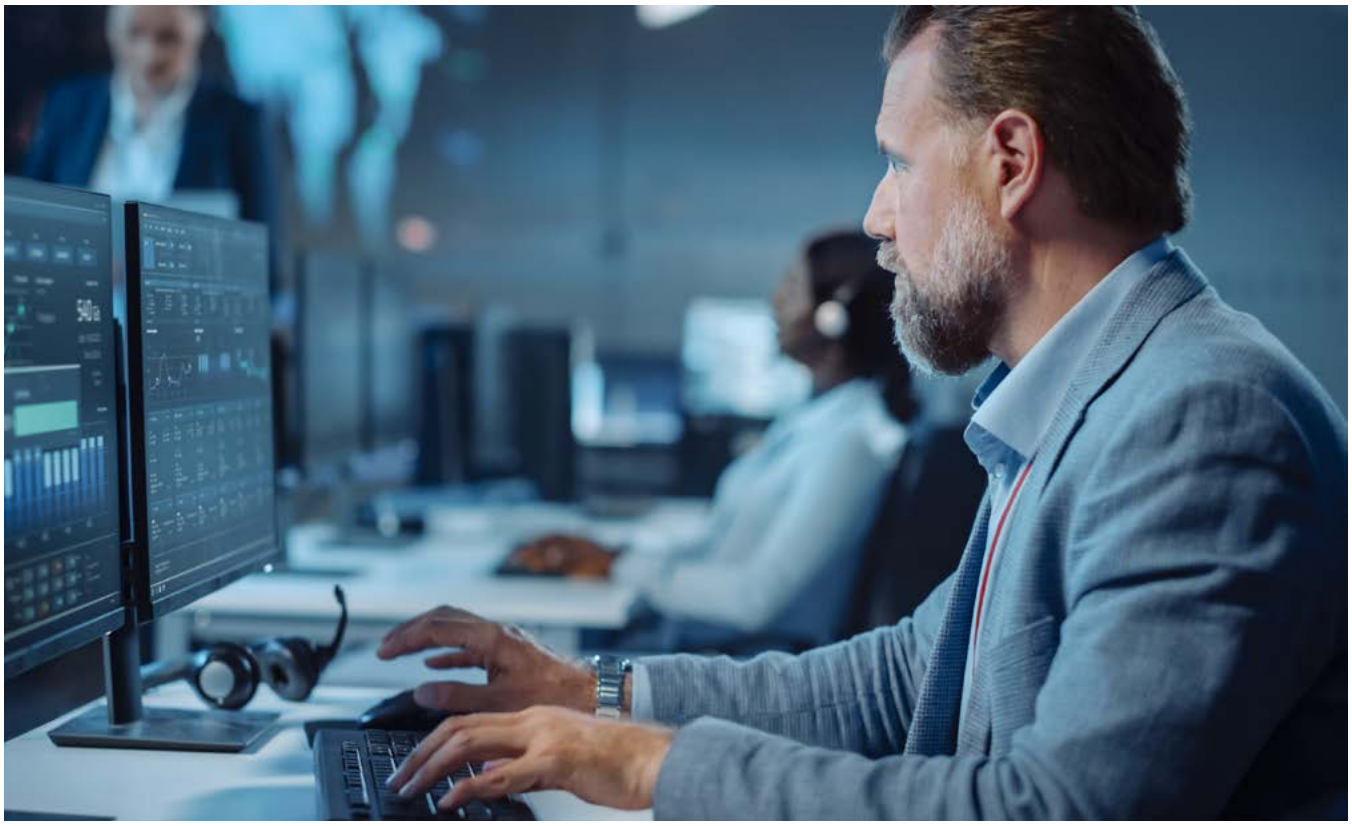
leidos

How to Secure Systems Without Limiting Innovation

A ROBUST CYBERSECURITY POSTURE LAYERS CUTTING-EDGE TOOLS TO PROTECT DATA AT EVERY STAGE.



Thanks to a continuously expanding Internet of Things (IoT), connected devices are everywhere in the federal government, producing and processing data that drives progress. But greater connectivity also means larger attack surfaces and more security vulnerabilities. As the Cybersecurity & Infrastructure Security Agency (CISA) directs federal leaders to protect and reduce attack surfaces, agencies need software and systems that are intrinsically secure, resilient, cost-effective and support post-quantum cryptography initiatives.

"Our systems are becoming more complex, and with that our supply chains are becoming more complex," says Raymond Richards, Director of Software at Leidos Dynetics Group. "We can't write every line of code from scratch when we build complex systems, so we have to use pre-existing software. It can be difficult to understand the provenance of all the software we integrate."

Meanwhile, adversaries ranging from independent actors to nation states are honing their attacks using extensive resources — in expertise and cash. To counter these persistent threats, the Leidos Secure framework supports a proactive approach to security integration by default and design. While Leidos Secure Software protects the software development supply chain through rigorous software bills of materials and an everything-as-code strategy, Leidos Secure Systems initiatives safeguard systems and the data moving throughout them by detecting and thwarting adversarial activity.

Software is "the most important building material of the 21st century," Richards says, and building secure software is vital to protecting the heart of software — the data. Once these building blocks are connected into systems, it becomes equally vital to secure the entire system as the sum of its parts, in addition to each piece.

Protecting data at every stage

Leidos' research and development encompasses systems from all parts of the spectrum, including embedded cyber physical systems, novel cloud security and post-quantum cryptography (PQC) solutions, with an eye toward building in cyber resiliency.

"Resiliency" is a key word to frame the protection of systems and data flow against cyber attacks. Resilient systems must have failsafes that enable them to provide the intended outcomes despite adverse events. Such fault tolerance has been built into

electrical and mechanical systems for many years. During a power failure, for example, a generator will run backup power to prevent a complete blackout. Leidos is working toward designing a similar type of resilience with enhanced cybersecurity measures to protect data and ensure intended functionality of operation for cyber systems.

"Take power substations. A lot of the systems were originally built in the time of phone operators, and now we're equipping them with WiFi. There's data flow and transmission that needs to be protected, and if a power grid fails, whole communities are vulnerable," says Rachael Williams, Principal Investigator of Leidos Secure Systems. "We're taking a defense-in-depth approach to monitoring these systems, to make sure that they haven't gone off the rails or are doing something out of scope or have been compromised in some way."

To implement these failsafes, "we are generating novel ways of detecting variance, or that the execution of the software is headed on a path that will not provide the intended outcome," Richards says, "and using advanced techniques, such as AI, to identify nefarious activities and respond to them."

Their current focuses cover three areas: runtime monitoring of systems, enhancing privacy of data in use for edge-to-cloud computation and building resiliency against quantum computing.

Runtime monitoring: In the increasingly interconnected world, Leidos is reaching into industrial operational technology (OT) edge devices and embedded systems for active, runtime monitoring of operations. Leidos Secure Systems is building a distributed trust solution for embedded systems to check both integrity of software, with secure boot procedures, and authenticity of devices using hard-to-crack attestation secrets. With devices secure in a known trusted state, Leidos is also developing active monitoring of data transmissions flowing from devices for OT mission critical systems to detect anomalous activity and unintended behaviors.

Enhancing privacy: Enabling people to leverage edge-to-cloud for collaboration and more advanced computational work by developing privacy-preserving computation is a key goal for Leidos Secure Systems. Privacy enhancing technologies (PETs) are technologies that seek to protect privacy and confidentiality of data in use — whether across groups collaborating on an AI/ML model in a decentralized way, or for individuals seeking to model sensitive, private data using cloud technologies. Leidos is building out taxonomies and example uses of PETs, including fully homomorphic encryption (FHE) with AWS, Federated Learning, Trusted Execution Environments and Zero Knowledge Proofs for near real-time inferencing.

Quantum resiliency: The advancement of quantum computing poses significant threats to our most widely used current encryption methods, making it more difficult to protect the integrity of data in transit. In Leidos' PQC solution for secure network access, "there are multiple dynamic channels and different types of quantum-resilient encryption enabled," Williams says, "so that you can handle when things go wrong, and even reroll your cryptographic keys on the fly." Leidos is building out capabilities that are encryption-agnostic and crypto-agile for more robust security in data transmission.

Ultimately, as robust as each of these research areas might be on its own, they're even stronger when grouped together to create a layered, defense-in-depth strategy — attestation paired with integrity checking on devices, and dynamic channels of quantum-resilient encryption techniques, for example. Richards notes that airliners rely on three autopilots, leveraging redundancy to reduce the risk of disaster. Similarly, "we have a vision for designing in security, designing in redundancy using design patterns to support resiliency," Richards says. Layering these defenses within solutions on top of other complementary tools further bolsters the security of the data, no matter what state it's

"We are generating novel ways of detecting variance, or that the execution of the software is headed on a path that will not provide the intended outcome, and using advanced techniques, such as AI, to identify nefarious activities and respond to them."

- Raymond Richards, Director of Software, Leidos Dynetics Group

> "It benefits us to equip ourselves with these more technologically advanced, though less secure, technologies and devices, so we really need to level up our security, not pull back or limit ourselves."
>
> **- Rachael Williams, Principal Investigator, Leidos Secure Systems**

in. Toward that end, "we were excited to see the National Cyber Strategy Implementation Plan, and after years of research, we have practical solutions to address the challenge of cyber resilience," Williams says.

A customized approach

Acquiring solutions based on cutting-edge industry research may feel out of reach for government technologists working within budget constraints. But Richards says the goal is to make cyberattacks expensive for adversaries, not agencies.

"We want the cost calculus for cyber adversaries to be something they have to consider — that they can't just hire every-day cyber actors, they have to apply additional resources," Richards says. "At the same time, we don't want to make the cost of ownership of these systems for the U.S. go up in a commensurate way."

To keep that total cost of ownership from skyrocketing, Leidos works to build solutions that meet customers where they are. Rather than designing an entirely new system from the ground up, for example, the team can take a vendor-agnostic approach to implementing newly developed protections in existing systems, with current and future cybersecurity requirements top of mind.

Keeping pace with innovation

Advancements in software and systems, from the cloud revolution to emerging applications of quantum computing and artificial intelligence, enable incredible achievements in the federal space. But as these technologies advance the realm of what is achievable, they also strengthen the powers of our adversaries. The more computational power we unlock with quantum computing, and the more digitally connected our small handheld and embedded devices are, the more cybersecurity vulnerabilities emerge as threat surfaces grow with the complexity of systems. Agencies must be equipped to protect attack vectors with more advanced technology, rather than limit innovation to maintain security.

"With the cloud and OT, it benefits us to equip ourselves with these more technologically advanced, though less secure, technologies and devices," Williams says. "So we really need to level up our security, not pull back or limit ourselves. There are reasons we've made these great advancements. We need to understand what kind of communication is occurring and what data transfer is going on to really understand the systems people are using and then build out solutions to use them securely."

Security doesn't need to inhibit progress. Maximizing the security of new technologies without limiting their potential is a difficult balance, and it's one Leidos is tackling head on. Richards likens the field of cybersecurity to the Red Queen's race in Alice in Wonderland: "It takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!"

Learn more about how Leidos is leveraging advanced techniques to secure systems without compromise.

23-Leidos-0919-26928