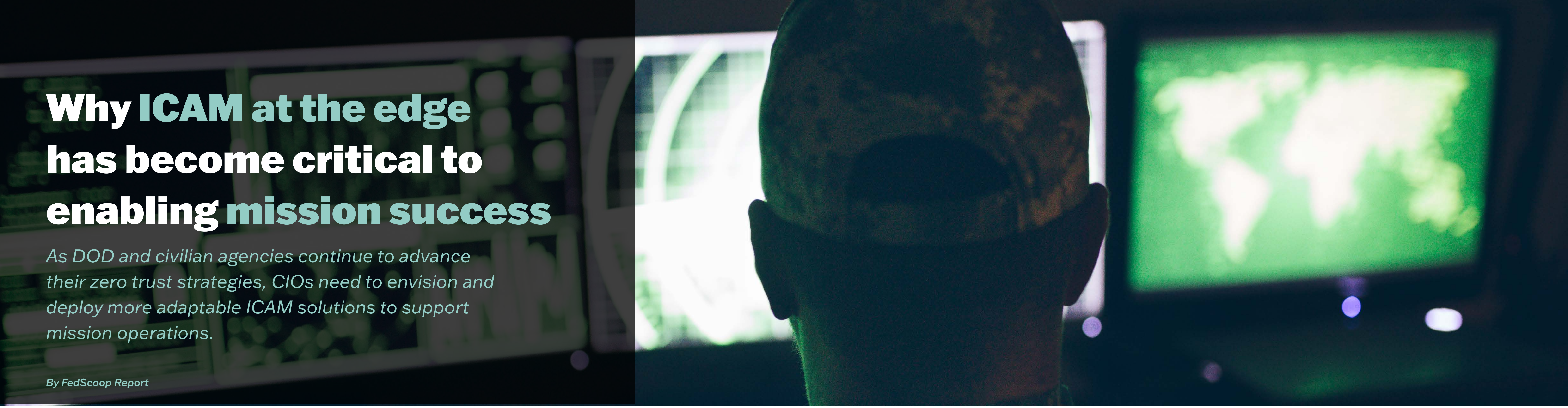


Why ICAM at the edge has become critical to enabling mission success

As DOD and civilian agencies continue to advance their zero trust strategies, CIOs need to envision and deploy more adaptable ICAM solutions to support mission operations.

By FedScoop Report

Whether circumstances involve military personnel working in remote regions with coalition partners; incident responders assisting in disaster or humanitarian efforts; or public safety officials responding to local emergencies — leaders on the ground increasingly face a common challenge: The need to share and validate the information with multiple organizations quickly and securely.

Sharing intelligence in those situations — when events are changing quickly and every minute counts — demands having the ability to manage information access privileges in real time "at the edge." Establishing that ability, however, can routinely come into conflict with enterprise-wide security safeguards and protocols — and in particular, the rules of engagement governing identity, credential and access management (ICAM).

"The reason ICAM is important to the CIOs of the world — and why it's different from just identity and access management," argues Dr. John Sahlin, director of cyber solutions of GDIT, "is that we're adding the vital element of other types of credentialing, taking into account things like telemetry information."

"We also need to take into account other elements of dynamic access management. ICAM really sets the core for a dynamic, adaptive security risk posture. It allows us to be resilient, and it allows us to be responsive to an emerging threat."

That's certainly true on the cybersecurity front. "As threats evolve — and they're evolving rapidly from all different directions — we need to evolve at least as fast as our adversaries in order to be successful. And the only way you can do that is by establishing a dynamic security posture," he said.

But it is equally true in today's broader IT environment, where the ability to dynamically authorize access to mission-critical information reliably and securely ensures data integrity has become essential.

ICAM for the enterprise

That's why ICAM is central to the federal government's zero-trust architecture strategy released in January. Among other objectives, agencies must modernize how they identify, authenticate and track users accessing information in real-time across their networks. ICAM deployments accomplish that through a combination of capabilities that enable and dynamically manage:

- Centralized authentication of users' identity
- Automated workflows for account requests and renewals
- Enterprise-level aggregation and audit of access rights
- Implementing policy decision points and policy enforcement points
- Safeguarding accounts and services with elevated access
- Multi-factor authentication

However, while enterprise-wide ICAM solutions — capable of managing governance, policy and enforcement controls across multiple domains — are critical to achieving zero-trust environments, they can also prove impractical or counter-productive to those carrying out their missions in remote or disconnected environments. Enterprise-grade ICAM policies and solutions aren't well suited when naval crewmen are operating aboard ships at sea or military personnel and first responders are on the move.

Consequently, as agencies continue to advance their zero-trust strategies, it's imperative that they envision and deploy more adaptable ICAM solutions that can support mission operations "at the edge" to ensure mission success, said Sahlin.

ICAM at the edge

"The difference between ICAM at the edge compared to enterprise ICAM is that it allows regionally specific policy decision-making, policy enforcement points, credentialing and access management decisions at a local level that may not make sense at the enterprise level," Sahlin explained. "You don't want to wait to have to go through all the enterprise procedures to make those things happen."

ICAM-at-the-edge solutions can give those in the field or at the edge secure and dynamic access privileges by federating ICAM solutions. That allows organizations to share identity and access information across an enterprise while providing localized controls essential to coordinating operations on the ground as situations and players change.

For instance, when first responders mount a disaster recovery or humanitarian assistance effort, "you need to rapidly add in mission partners — like local law enforcement, local fire department, non-governmental organizations like the Red Cross, or Doctors Without Borders. You don't necessarily want to add literally every police department in the country at an enterprise level in order for FEMA to execute its mission," Sahlin said.

Similarly, "some services or even units may not have the ability to wait for the DOD Enterprise to execute [credentialing for] every possible iteration of coalition partners, or foreign nations and interagency operations in order to execute the mission, because, at that point, you really don't have a mission-specific security posture."

Planning for enterprise + edge

Establishing an IT environment where ICAM functions appropriately across the enterprise — and at the edge — ultimately requires traditionally enterprise IT leaders also to think tactically, said Sahlin. That can be a challenge for some organizations.

IT leaders and engineers who grew up in an enterprise IT environment tend to think of big-iron data centers, extensive infrastructure and enterprise-level policies. However, enterprise-level rules may not apply or even be relevant at the tactical edge. To operate effectively in a disconnected world, users need solutions that have flexibility. When they don't, users inevitably will disconnect from the enterprise and improvise to accomplish the mission.

Thinking about ICAM at both the enterprise and tactical level, Sahlin said, is akin to fielding any brand name across the world. "The enterprise brand stays the same, but if you want to operate successfully in different parts of the world, you're going to have to allow for a very different experience that is representative of the local environment, culture and needs."

> *The difference between ICAM at the edge compared to enterprise ICAM is that it allows regionally specific policy decision-making, policy enforcement points, credentialing and access management decisions at a local level that may not make sense at the enterprise level,"*
>
> *-Dr. John Sahlin GDIT*

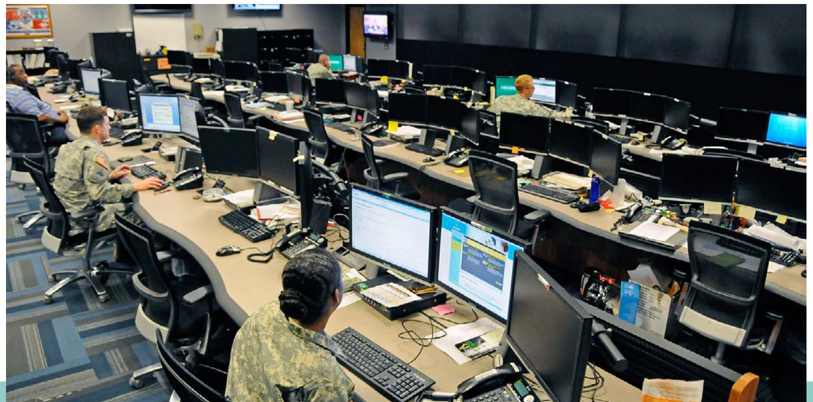
Translating that back to IT, he explained, "if I focus on the standards by which each individual component interfaces with another, then it becomes a lot easier for me to plug in and plug out different solutions, different data sets, and different hardware components."

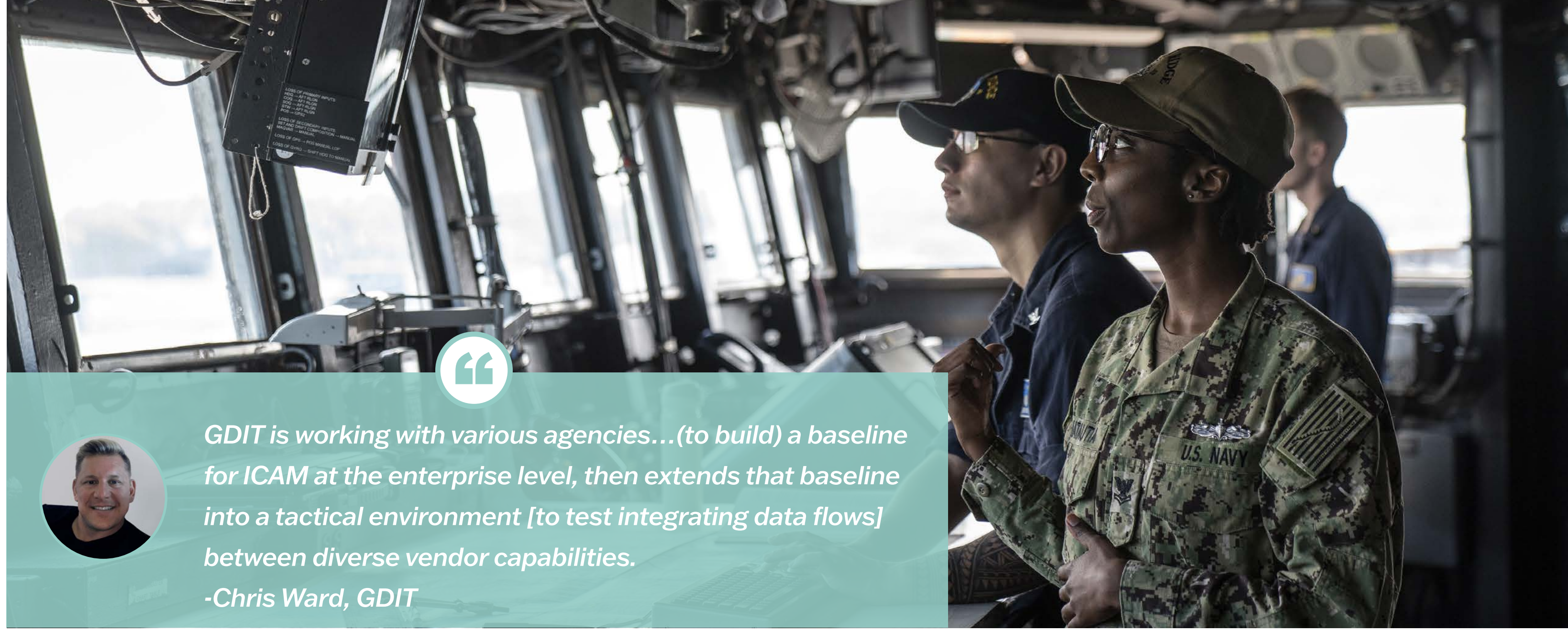
That doesn't mean giving mission partners veto power over what makes sense at the enterprise level, said Sahlin. But it does mean enabling them — helping them understand how those enterprise policies and technology rollouts work and how to make business decisions that make sense for their tactical environments.

Additionally, when thinking about the tactical edge, enterprise IT leaders need to understand the size and scope of operations they're supporting, putting themselves in their users' shoes. And they also need to understand mission partners' connectivity and data requirements.

At DOD, for instance, that could mean facilitating a Marine air-ground task force or a brigade, or it could also be smaller in scale, like sensors on vehicles. Differences in services and equipment and how they will interact with other entities are where the nexus between ICAM and zero trust becomes important to maintain adaptive access and risk controls.

Finally, added Sahlin, "if ICAM provides the core capabilities that are necessary to implement zero trust, the 'C' in ICAM also provides the core foundation of enabling machine-to-machine or device-to-device communication. This is why the 'C' is so important — we have to go beyond the person-based entities and look at non-person entities."





> *GDIT is working with various agencies…(to build) a baseline for ICAM at the enterprise level, then extends that baseline into a tactical environment [to test integrating data flows] between diverse vendor capabilities.*
>
> *-Chris Ward, GDIT*

"If we see a bad actor on a network, the first thing a lot of enterprise IT people will think is, 'Let's isolate that person from the network and quarantine them until further notice.' You do that for an industrial control system with a safety system, and suddenly you shut down a pump or secure a door that can't unlock — now you can hurt people," cautioned Sahlin.

Harmonizing ICAM for zero trust

"Zero trust — and ICAM as a coordinating component of it — is not just about wrapping walls around data to keep adversaries from getting access; it's about sharing data in an ad-hoc, dynamic fashion to execute the mission," said Sahlin. To achieve this, leaders must have some elements of a zero-trust solution such as localized policy definition, policy enforcement and cyber threat intelligence."

GDIT is working with various agencies, including the Defense Information Systems Agency (DISA), to build an integrated lab environment to test out a zero-trust stack for various situations, according to Chris Ward, senior ICAM growth lead at GDIT.

It starts with a baseline for ICAM at the enterprise level, then extends that baseline into a tactical environment — taking that model to inform zero-trust architecture to support a federated deployment. The approach is helping GDIT's customers to develop ICAM solutions that address the challenge of "integrating and monitoring data ingress and egress seamlessly between diverse vendor capabilities" and harmonize disparate sources of information.

One of the tools that GDIT is currently demoing is secure chat. "[Secure chat] is getting the attention of mission partners because right now, they are circumventing the process to get the mission done. Sometimes that is without the right security parameters in place, and it leaves us kind of open for data to get out there that doesn't need to get out there," said Ward. A solution authenticating at the device level like this would benefit humanitarian missions or disaster recovery.

GDIT is also helping customers develop custom dictionaries that can flag words like "water" or "food" for critical tasks or words that might suggest bad actors have gotten on the network. He said that the goal is to facilitate ICAM-on-the-go deployed to user devices.

Ultimately, ICAM is the key to making security a mission enabler, said Sahlin. It's not only about governance and protecting data. At the end of the day, ICAM is about executing a mission. That is how GDIT is focusing on ICAM, he said — striking the right balance between protecting data and accelerating the mission through dynamic security.

Learn more about how enterprise ICAM and ICAM at the edge are not just about achieving greater security but about accelerating mission success.

This report was produced by FedScoop and underwritten by GDIT.

FEDSCOOP GDIT