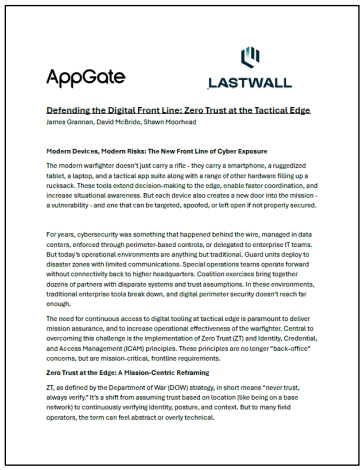
AppGate

carahsoft.


AppGate LASTWALL

Defending the Digital Front Line: Zero Trust at the Tactical Edge

James Grannan, David McBride, Shawn Moorhead

Modern Devices, Modern Risks: The New Front Line of Cyber Exposure

The modern warfighter doesn't just carry a rifle - they carry a smartphone, a ruggedized tablet, a laptop, and a tactical app suite along with a range of other hardware filling up a rucksack. These tools extend decision-making to the edge, enable faster coordination, and increase situational awareness. But each device also creates a new door into the mission - a vulnerability - and one that can be targeted, spoofed, or left open if not properly secured.

For years, cybersecurity was something that happened behind the wire, managed in data centers, enforced through perimeter-based controls, or delegated to enterprise IT teams. But today's operational environments are anything but traditional. Guard units deploy to disaster zones with limited communications. Special operations teams operate forward without connectivity back to higher headquarters. Coalition exercises bring together dozens of partners with disparate systems and trust assumptions. In these environments, traditional enterprise tools break down, and digital perimeter security doesn't reach far enough.

The need for continuous access to digital tooling at tactical edge is paramount to deliver mission assurance, and to increase operational effectiveness of the warfighter. Central to overcoming this challenge is the implementation of Zero Trust (ZT) and Identity, Credential, and Access Management (ICAM) principles. These principles are no longer "back-office" concerns, but are mission-critical, frontline requirements.

Zero Trust at the Edge: A Mission-Centric Reframing

ZT, as defined by the Department of War (DOW) strategy, in short means "never trust, always verify." It's a shift from assuming trust based on location (like being on a base network) to continuously verifying identity, posture, and context. But to many field operators, the term can feel abstract or overly technical.

Defending the Digital Front Line: Zero Trust at the Tactical Edge

Thank you for downloading this AppGate blog. Carahsoft is the Master Government Aggregator® for AppGate's Cybersecurity solutions available via GSA, NCPA, NJSBA, and other contract vehicles.

To learn how to take the next step toward acquiring AppGate's solutions, please check out the following resources and information:

For additional resources:
carah.io/AppGateResources

For upcoming events:
carah.io/AppGateEvents

For additional Appgate solutions:
carah.io/AppGateSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
AppGate@carahsoft.com
703-230-7577

To purchase, check out the contract vehicles available for procurement:
carah.io/AppGateContracts

Defending the Digital Front Line: Zero Trust at the Tactical Edge

James Grannan, David McBride, Shawn Moorhead

Modern Devices, Modern Risks: The New Front Line of Cyber Exposure

The modern warfighter doesn't just carry a rifle - they carry a smartphone, a ruggedized tablet, a laptop, and a tactical app suite along with a range of other hardware filling up a rucksack. These tools extend decision-making to the edge, enable faster coordination, and increase situational awareness. But each device also creates a new door into the mission - a vulnerability - and one that can be targeted, spoofed, or left open if not properly secured.

For years, cybersecurity was something that happened behind the wire, managed in data centers, enforced through perimeter-based controls, or delegated to enterprise IT teams. But today's operational environments are anything but traditional. Guard units deploy to disaster zones with limited communications. Special operations teams operate forward without connectivity back to higher headquarters. Coalition exercises bring together dozens of partners with disparate systems and trust assumptions. In these environments, traditional enterprise tools break down, and digital perimeter security doesn't reach far enough.

The need for continuous access to digital tooling at tactical edge is paramount to deliver mission assurance, and to increase operational effectiveness of the warfighter. Central to overcoming this challenge is the implementation of Zero Trust (ZT) and Identity, Credential, and Access Management (ICAM) principles. These principles are no longer "back-office" concerns, but are mission-critical, frontline requirements.

Zero Trust at the Edge: A Mission-Centric Reframing

ZT, as defined by the Department of War (DOW) strategy, in short means "never trust, always verify." It's a shift from assuming trust based on location (like being on a base network) to continuously verifying identity, posture, and context. But to many field operators, the term can feel abstract or overly technical.

In practical terms, ZT is simply about ensuring that every person, device, or service proves who they are, proves they're healthy, and only gets access to exactly what they need and nothing more. It's about granting precise access, minimizing risk, and maintaining control even when the network goes dark.

ICAM, meanwhile, is the foundation that makes this possible. It's how we manage identity (who you are), credentials (how you prove it), and access (what you're allowed to do). When implemented properly, ICAM ensures that even in disconnected or contested conditions, users can authenticate locally, access mission-critical systems, and maintain integrity without relying on external validation.

Consider a National Guard unit deployed to a remote domestic disaster zone where network access is unreliable, but coordination with local and federal agencies is critical. With containerized ICAM deployed on a ruggedized laptop or portable server, responders can issue and validate credentials locally, granting controlled access to mission systems, shared maps, or communications platforms. Even without cloud reach-back, responders maintain visibility and control over who is doing what, enforcing access policy on the ground, in real time. No more shared logins, no more unsecured apps. Just fast, secure, access to essential mission tooling.

Together, ZT and ICAM offer a strategy and a toolkit for securing the battlespace without slowing it down.

Why This Matters Now: The Operational Reality

Warfighters in DDIL conditions already rely on mobile technology. They bring it into the field because it works, it's intuitive, and it improves mission performance. But these tools weren't always designed with "defense-grade" cybersecurity in mind.

The challenge isn't to remove mobile devices, it's to secure them without adding barriers for the operator. And that means moving security closer to the edge. Instead of assuming systems can "call home" to authenticate users or update policy, we need identity and access solutions that run on-site, locally. We need capabilities that can be deployed in a Pelican case, mounted in a vehicle, or hosted on a rugged laptop.

This isn't hypothetical. The DOW's own ZT strategy calls for extending trust enforcement to tactical environments. The Department of Navy's Chief Technology Officer lists ZT access enforcement and ICAM federation among its top modernization priorities. And multiple directorates within the Air Force and Army are exploring how to authenticate, authorize, and secure data exchange in coalition environments using portable ICAM and resilient ZT Network Access (ZTNA).

Real-World Constraints and the Need for Edge-Ready Security Tools

The tactical edge isn't just disconnected, it's unpredictable. Power is unreliable, networks fluctuate, mission partners rotate, and yet, operations must continue without compromise. This reality demands tools that can survive and thrive at the edge.

First, there's the issue of connectivity. Most commercial identity systems and network access controls assume consistent reach-back to an enterprise controller or cloud service. But when a forward-deployed unit loses SATCOM or moves into a jammed environment, those assumptions fall apart. Security must continue working even when the network doesn't.

Second, coalition and joint access introduce complexity. Operations with NATO allies, FEMA, or state and local emergency services all involve different identity sources, credentialing mechanisms, and access policies. Without federation and dynamic access controls, commanders are left choosing between delays or dangerous workarounds.

Third, human behavior matters. When systems are slow or restrictive, users bypass them. In the field, that might mean shared logins, writing passwords on devices, or disabling security settings to keep operations moving. If secure access creates friction, it will be avoided.

Finally, legacy infrastructure and mission applications weren't built with ZT in mind. Many still rely on static role definitions, hardcoded access lists, or VPNs with broad entitlements. Overlaying a modern ZT/ICAM layer requires lightweight, interoperable solutions that are open-standards based, and can integrate without a full system rip-and-replace.

Edge-ready security tools must account for all of this. They must operate with autonomy, enforce policy locally, support secure coalition access, and stay invisible to the warfighter until needed. Capabilities that deliver containerized ICAM services, support federated access, and enable dynamic policy enforcement without relying on constant network connectivity are increasingly viable. These are the kinds of tools being evaluated across DOW organizations to meet emerging mission needs at the tactical edge.

Practical Solutions in Action: Identity, Access, and Autonomy at the Edge

Fortunately, real progress is being made. Emerging technologies are bringing ZT and ICAM principles to the edge.

On the identity side, lightweight ICAM stacks built on containerized architecture are now capable of running locally in disconnected environments. These systems can authenticate users, enforce policy, and revoke access autonomously whether deployed at a forward operating base or embedded in a mobile command platform. They support multifactor

authentication using biometrics, derived credentials, or passkeys and enable attribute-based access control tied to mission context.

On the network side, adaptive access technologies are helping implement ZTNA at the edge. Techniques like single packet authorization allow for cloaking of infrastructure and precision-based segmentation of access. Rather than granting users broad visibility or lateral movement, these solutions expose only what's needed, when it's needed creating a unique software defined perimeter for each individual user or group.

These approaches offer something powerful: a way to uphold the principles of ZT and ICAM in environments where infrastructure is limited, users are mobile, and operational tempo is high. They reflect not just what's possible, but what's increasingly necessary.

From Policy to Practice: Mission Outcomes that Matter

Ultimately, ZT at the edge isn't about architecture diagrams, it's about mission impact. When identity and access are enforced effectively, operations become faster, safer, and more resilient.

Warfighters don't have to memorize complex passwords or wait for reach-back. Secure login becomes seamless. Commanders don't need to compromise between speed and security when onboarding partners. And cyber teams don't have to rely on blanket network trust models that leave room for lateral movement and credential theft.

When done right, these solutions enhance rather than hinder the mission. They support rapid deployment, enable secure collaboration, and reduce operational burden. They allow commanders to maintain control and confidence even in environments where visibility is limited.

This is the vision behind ZT: not just another top-level compliance requirement or buzzy marketing trend, but a practical framework for enabling secure, agile operations. The tactical edge is where its value becomes clearest.

What Comes Next

The question isn't whether Zero Trust is coming to the edge, it's how quickly we can get there. The tools are emerging, the policy direction is clear, and the need is already here.

As identity and access technologies evolve, our collective challenge is to implement them in ways that serve the mission operator. That means designing for multi-domain operations, coalition complexity, and real-world friction. It means building solutions that don't just comply with strategy, but align with and support mission execution and success.

Above all, it means keeping our focus where it belongs: on the user, the mission, and the trust required to defend both. Because in today's digital battlefield, every credential, every connection, and every access request is a decision point. ZT and ICAM ensures those decisions are made wisely, and securely, ensuring the effectiveness of the warfighter in an ever changing and dynamic operational environment.