How DoD Can Extend Zero Trust to the Tactical Edge

MARKET TRENDS REPORT

govloop PRESIDIO FEDERAL Red Hat

Introduction

The Department of Defense (DoD) is moving computing platforms to the tactical edge, bringing high-powered data processing, analysis and sharing to deployed units even in remote, austere and conflicted environments. Tactical teams will employ a wide array of sensors and devices, artificial intelligence (AI) and machine learning (ML) models, and other means of supporting near real-time decision-making, while communicating across multiple domains with joint forces and coalition partners.

This approach, which is necessary for dealing with asymmetric and near-peer adversaries, will create massive amounts of data. That data not only must be ingested, processed and analyzed, but must also be secured. It's a substantial challenge that can be brought down to size by applying the principles of zero-trust security.

The department's zero-trust strategy, released in October 2022, establishes a roadmap for implementation of zero-trust principles across the DoD enterprise and sets a 2027 deadline for full implementation. The department's Outside the Continental United States (OCONUS) Cloud Strategy, which specifically addresses deployed forces, emphasizes the importance of zero trust at the tactical edge.

Full implementation of zero trust doesn't have to be as daunting as it might seem, with the right help. But it is something that the miliary services and DoD components need to get moving on, if they aren't already.

In this market trends report, GovLoop partnered with zero-trust solution providers Presidio Federal and Red Hat. We'll examine the challenges of securing data in contested environments, how zero trust meets those challenges, best practices for implementation and examples of what zero trust can provide.

THE 7 PILLARS OF ZERO TRUST

The National Security Agency's zero-trust security model identifies seven pillars of the strategy, along with the key focus of securing each one.

- **User:** continuously authenticate, monitor activity
- **Device:** real-time inspection, assessment and patching
- **Data:** ensure visibility and security via enterprise infrastructure, applications, standards, end-to-end encryption and data tagging
- **Application/Workload:** secure everything from applications to hypervisors, including containers and virtual machines
- **Network/Environment:** segment, isolate and control
- **Visibility and Analytics:** analyze events, activities and behaviors; apply AI/ML to improve detection, reaction time
- **Automation and Orchestration:** automate response based on defined processes, enabled by AI

By The Numbers

Top 5 Threats to DoD Information Systems

The Government Accountability Office interviewed **25 DoD components**, including all of the military services, for a September 2022 report on DoD's information environment. When asked to identify actions they considered a threat, the top five responses were:

#1 Malicious cyber activity against component information systems
(identified by 24 components)

#2 Actions to implant, modify, destroy or extract data within component information systems
(identified by 24 components)

#3 Collection of information or intelligence to understand component's mission, operations or personnel
(identified by 22 components)

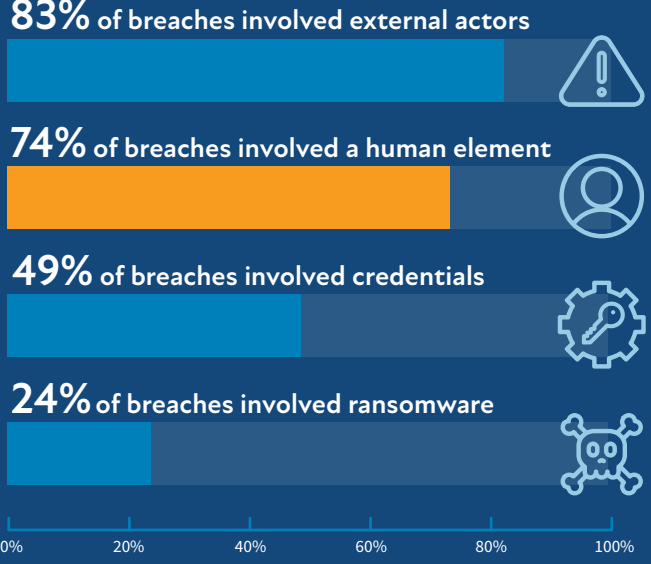
#4 Target or try to influence policy-making or planning efforts
(identified by 20 components)

#5 Physical attacks against component information systems
(identified by 20 components)

[Zero trust] enables information dominance across the communications spectrum in the tactical environment by ensuring the security of data, applications, assets and services. Execution plans must account for the potential ramifications of [zero trust] in the tactical environment.

- DoD Zero Trust Strategy

According to Verizon's 2023 Data Breach Investigations Report, **74% of all breaches involve a human element**, whether through error, privilege misuse, stolen credentials or social engineering.



DoD Pushes the Enterprise to the Edge

DoD's OCONUS Cloud Strategy includes providing forces in the field with access to powerful enterprise capabilities. The technology the strategy calls for using includes:

- Deployable cloud computing
- 5G and open radio access network
- Agile software development
- AI/ML analytics
- High-performance computing
- Critical supervisory control and data acquisition systems
- Edge computing capabilities, including containers

How Zero Trust Secures the Tactical Edge

Challenge: An Expanding Attack Surface in Contested Environments

Deployed forces must be able to share data across platforms that aren't always compatible. A vehicle such as a tank, for instance, may have 15 or 16 different information systems, each made by a different vendor using different operating systems, software and programming languages. And they must be able to communicate and share data with other echelons across domains — land, air, sea, space and cyber — as well as with coalition forces.

"There are different types of data collections and different systems in different locations," said Jon S. Kim, Vice President of Solutions and Services at Presidio Federal. "They're not always seamless, as far as emulation is concerned. So that makes it difficult to share data."

Beyond just ingesting and sharing massive amounts of data, deployed units must be able to analyze and prioritize the data, quickly turning it into actionable insights.

"The interesting thing about data is that the plural of data … is data. It is not intelligence," said Chris Yates, DoD Army Chief Architect for Red Hat. **"How you process that data is how you develop intelligence, and that intelligence will give us an advantage on the battlefield."**

In the face of asymmetrical warfare environments or potential confrontations with near-peer or peer adversaries, DoD's doctrine now supports multi-domain operations against adversaries whose own capabilities have improved. "Our ability to respond to threats needs to be more responsive," Yates said.

Securing data — always a top priority for DoD — is a critical challenge. The military services need to ensure that their personnel are properly trained, since about a third of cyber-related threats come from the inside, whether accidental or intentional, Kim said.

But DoD also needs to control access and privileges for users and devices on its networks, ensuring that devices are secured and that network identities (human or non-human) don't have privileges they don't need.

The Solution: Better Visibility, Control Through Zero Trust

Zero trust's "never trust, always verify" approach is necessary at the tactical edge, as the Zero Trust Strategy makes clear. But rather than seeing its implementation as a burden, DoD can look at it as an advantage.

"The tactical, distributed edge isn't the challenge to zero trust — it's what is driving the adoption of it," Yates said. Making the best use of data in a tactical environment with thousands of sensors and other systems means recognizing that a traditional perimeter-based approach won't work. "That is what is pushing us towards adopting zero trust, rather than it being a challenge to the adoption of zero trust," Yates said.

Against near-peer or peer adversaries, the United States can no longer assume it has superiority because it has the best tanks or submarines or aircraft carriers. "We have to develop an advantage through superior operations, logistics and coordination of our capabilities," said Yates. "And the way to develop that advantage is through tight coordination between these platforms. We need to share data, and we need to be concerned about how that data is protected."

The time is right for implementing zero trust, because advances the DoD has made with its systems make it easier than some people might think. Traditionally, silos were the norm because they were necessary. And precepts like Conway's Law — which posits that organizations build solutions that reflect their internal communication silos — also slowed down integration efforts, Yates noted.

Over the past decade, however, DoD has moved interoperability to the forefront of its designs and adopted open-source standards and programming interfaces such as Open API.

Best Practices

Emphasize Education and Training

In addition to the automated functions that go into a zero-trust strategy, leaders must be sure that personnel are adept at securely storing and sharing data.

Zero trust isn't a technology, nor is it a product that comes out of the box. "Zero trust is just an envelope to encapsulate a lot of security concerns and behaviors that have been talked about for the last 20 years," Yates said.

Personnel need to understand zero trust and how it works. They'll have new procedures for sustaining and operating systems, for example. "It doesn't start from an engineering level and work its way up," Kim said. "It's a whole different understanding," involving the entire organization, starting with buy-in from leadership and extending throughout the ranks.

Crawl Before You Run

As with any new model of operations, implementation should be iterative. Before trying to roll out zero trust across the enterprise, start with pilots and small implementations, refining the variables and addressing any problems that surface. It's important to prioritize deployments, starting with the most critical assets.

And a large-scale deployment should be done in phases, or parallel deployment, with a legacy system running in parallel during the transition. In addition to working out any bugs, a phased deployment allows teams maintaining the new environment to become familiar with it. "It's not just a technology transition, it's a human transition as well," Kim said.

Monitor and Measure

Military and tactical teams need to constantly measure zero-trust security controls to be sure they are minimizing risk and exposures, especially as computing moves further to the edge. DoD is deploying containerized applications, using Kubernetes and other solutions to orchestrate, which can make zero trust easier to adopt because containers already encapsulate the dependencies and configurations for applications, Yates said.

Cloud computing also can solve bandwidth and connectivity issues, at least in areas that aren't denied, which helps enable zero trust. But monitoring controls across the enterprise is essential to ensuring that you're addressing all the gaps, Kim said. "You don't want find out if it works after you get it deployed," he said.

3 Examples of How Zero Trust Improves Security

1 Detecting Compromised User Credentials

With traditional network security, a threat actor who compromises a user's credential is likely to gain access to the network, whether by accessing that device remotely or using stolen credentials with their own device.

A zero-trust environment, however, could foil the attempt in a couple ways. For one, if the device is not known to the network, it will be denied access, while the system will log the attempted entry. For another, zero-trust implementation requires strong authentication, including multi-factor authentication (MFA), which makes it more difficult to steal a user's credentials.

2 Limiting an Attacker's Mobility

In the event an attacker gains entry to the network — and a principle of zero trust is that hacks are a matter of when, not if — the intruder's ability to move about will be limited due to network segmentation.

Without a zero-trust strategy, an attacker could use compromised credentials to gain access, escalate privileges and then move laterally through the network to damage or steal stores of data. In a zero-trust environment, segmentation has been added to prevent movement within the network without authentication and authorization at each stage, which constricts an attacker's movement.

3 Detecting Anomalous Activity

Once zero trust is in place, continuous monitoring and analytics – often bolstered by AI/ML – can detect anomalous activity in user accounts, network activity, connected devices and data access. Site-to-site encryption can be applied to vehicles, devices and applications, as well as users, to ensure secure communications and prevent hacking.

HOW PRESIDIO FEDERAL AND RED HAT CAN HELP

Presidio Federal and Red Hat are trusted partners with extensive experience in securing government systems.

Presidio Federal's Zero Trust Networking (ZTN) Solution employs a five-step process to ensure that only authorized users or network identities have access to specific information. Its end-to-end solution includes a thorough review of the organization's architecture to identify cybersecurity gaps, and continuous monitoring to ensure controls are up to date with the constantly evolving cyber threat landscape.

Red Hat's zero-trust platform for the tactical edge, with Mainsail's Metalvisor, provides security at the operating systems core level. Originally designed for DoD, Metalvisor meets and exceeds National Institute of Standards and Technology (NIST) SP 800-207 guidelines for zero-trust architectures. It enhances Red Hat's Red Hat OpenShift Container Platform, which streamlines the implementation of a zero-trust strategy.

The companies are partnering to bring their experience, platforms and tools to implementing zero trust at the tactical edge.

Conclusion

DoD is increasingly operating at the tactical edge, which means bringing a data center's worth of computing power to remote and contested environments. The data generated by hundreds or thousands of sensors and other sources in land, air, sea and ground operations must be secured, which makes implementing zero-trust principles an absolute must.

The military services and other DoD organizations need to identify and prioritize their sources of data, map data dependencies and access behavior, and implement strong access controls. They need to implement an architecture to protect against vulnerabilities, and continuously monitor their environment to keep up with evolving threats and ensure their protections remain in place.

It's a big job, but some of the components that go into a zero-trust strategy are already in place at many organizations. With some assistance, they will be able to implement their zero-trust approach all the way out of the edge of deployed environments.

ABOUT

PRESIDIO FEDERAL

Presidio Federal, a wholly owned subsidiary of Presidio, is a mid-tier integrator that is exclusively focused on federal government. We work with large prime contractors as well as small businesses to become a sort of "easy button" for our federal customers.

We are proud to be an outcome focused, trusted advisor with a credentialed team that has experience and understanding with the legacy systems and unique challenges of government agencies. We have an extensive partner ecosystem, including many of the best-of breed OEMs in the business like Red Hat, but we layer in an unbiased, broad perspective that is driven by mission and a long-term, accountable relationship.

For more information, please visit www.presidiofederal.com.

Red Hat

Red Hat helps customers integrate new and existing IT applications, develop cloudnative applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. As a strategic partner to cloud providers, systems integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

To learn more, please visit www.redhat.com/government

govloop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop