WHITE PAPER

Accelerate the public sector journey to zero trust with F5

Embrace key security technologies in the F5® Application Delivery and Security Platform (ADSP) to enable DoD Zero Trust Overlay.



What is DoD Zero Trust Overlay?
This roadmap guides the implementation of zero trust capabilities, policies, and best practices within public sector networks while following NIST and CISA standards.

Rethinking secure access to address modern threats

As the modern threat environment continues to evolve, the United States Department of Defense (DoD) is confronted by increasingly sophisticated and complex attack vectors targeting its mission-critical systems. Nation-state actors, cybercriminal organizations, and insider threats are leveraging advanced techniques to exploit vulnerabilities and disrupt operations, requiring the DoD to rethink how it secures its networks. Traditional perimeter-based security models, once sufficient to safeguard large-scale enterprise systems, are no longer adequate in this era where threats often originate inside and outside the network. Historically, once the users were successfully authenticated, their actions weren't monitored as they were trusted.

To address these urgent challenges, the DoD has adopted the zero trust security framework, a transformative approach designed to secure sensitive systems, applications, and data, regardless of user location or network permissions. Zero trust represents a shift in cybersecurity philosophy, moving away from implicitly trusted network boundaries and replacing them with a "never trust, always verify" model. By requiring continuous verification of all entities—users, devices, applications, and data flows—zero trust strengthens security postures against both external and internal threats.

The **DoD Zero Trust Overlay** provides a roadmap for implementing this approach within the sprawling scale and complexity of the military's networks and operational technology (OT). It incorporates best practices from established zero trust architectures, such as the frameworks outlined by the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA), while tailoring them to meet the unique requirements of the DoD. To operationalize this transition, the DoD must leverage cutting-edge technologies that simplify zero trust adoption while providing unprecedented visibility, control, and security for its mission-critical assets.

F5 solutions streamline the DoD's zero trust adoption

F5 solutions are uniquely positioned to help the DoD realize its zero trust objectives effectively, efficiently, and at scale. As a leader in application delivery, F5 provides the tools necessary to implement core zero trust principles, including secure access, traffic inspection, and continuous authentication. From enabling dynamic application-layer protections to enhancing visibility across hybrid and multicloud environments, F5 solutions deliver the agility and resilience required to meet the demands of zero trust environments.

F5 solutions align with the DoD's zero trust vision by enabling granular access management, adaptive security policies, and comprehensive telemetry for monitoring and analytics.

This white paper explores how public sector customers can harness F5 technologies as critical enablers across zero trust pillars. With capabilities that include identity-aware proxying, adaptive access control, policy enforcement, and secure traffic handling, The F5 portfolio provides a robust foundation to help achieve the following principles of zero trust:

- **User-to-application access:** Ensure secure, conditional, and segmented access to applications, using F5 advanced access control solutions such as F5® BIG-IP® Access Policy Manager® (APM), part of the F5 ADSP.
- **Application-to-application communication:** Protect application-layer communications through traffic inspection, encryption, and dynamic policy enforcement.
- **Visibility and threat detection:** Leverage F5 capabilities to monitor, analyze, and detect anomalous traffic flows across the IT ecosystem.
- **Data protection:** Secure sensitive data in transit and at rest by integrating encryption standards and traffic management.

F5 solutions align with the DoD's zero trust vision by enabling granular access management, adaptive security policies, and comprehensive telemetry for monitoring and analytics. With the evolution of cloud adoption, distributed architectures, and remote workforce demands, F5 ensures scalability and flexibility across environments—on-premises, hybrid, or multicloud—making the solutions ideally suited to support the DoD's operational and security goals.

The DoD's success in implementing zero trust depends on adopting technologies that simplify the integration of security controls while maintaining mission-readiness and operational continuity. F5 solutions address this critical need by providing end-to-end application security without compromising on performance, user experience, or scalability. F5 delivers essential capabilities to accelerate the deployment and operationalization of zero trust. By leveraging innovative F5 platforms and services, the DoD can achieve a robust, zero trust framework that safeguards its infrastructure, supports its mission, and upholds national security in an increasingly contested cyber domain.

The challenges confronting public sector agencies

The DoD's Zero Trust Overlay provides a foundational framework for enhancing security postures in response to an increasingly sophisticated threat environment. For public sector agencies tasked with implementing this framework, the journey to zero trust presents significant obstacles rooted in massive scale, complexity, legacy infrastructure, and operational burden. Addressing these challenges isn't just important, it's crucial right now. Cyber adversaries continue to escalate their attacks on sensitive government systems, targeting known vulnerabilities and exploiting outdated security models that fail to adapt to the modern, borderless threat landscape. Failure to act immediately leaves agencies—and the nation's security—dangerously exposed in an era where every second matters in the fight against cyberattacks.

Complex legacy environments

Public sector agencies often operate within sprawling, heterogeneous IT ecosystems composed of legacy infrastructure, modern applications, and proprietary technologies. Migrating or retrofitting these legacy systems to support essential zero trust capabilities is both cost- and effort-intensive.

Delays in adoption due to legacy system limitations are increasingly untenable in the current threat environment. Adversaries are actively exploiting gaps and vulnerabilities in older systems, launching attacks that not only compromise data but disrupt mission-critical operations. Addressing the integration of zero trust into legacy environments is urgent to close these gaps, increase resiliency, and minimize risk to sensitive operations.

Cultural and organizational shifts

Zero trust represents more than just a technological enhancement—it requires a fundamental shift in operational practices and organizational culture. Public sector agencies have traditionally relied on perimeter-based defenses, which implicitly trust internal users and devices after crossing the network boundary.

Nation-state adversaries and sophisticated attackers are capitalizing on weak internal controls, particularly in environments with unchecked permissions and implicit trust. The cultural changes driven by zero trust adoption are essential to countering these threats. By enforcing new practices such as least-privilege access and continuous monitoring, agencies can proactively secure their systems against escalating risks.

Scalability and operational complexity

Public sector agencies must implement zero trust principles across diverse user populations, including service members, contractors, and interagency partners who access systems across on-premises, cloud, and hybrid environments.

As agencies expand their reliance on cloud environments and remote workforces, cyber adversaries are exploiting the increased attack surface created by decentralized systems. Without scalable zero trust capabilities, agencies risk performance bottlenecks, operational disruptions, and vulnerabilities that jeopardize mission-critical operations. Implementing scalable zero trust solutions enables agencies to protect their systems from breaches while maintaining operational continuity in the face of ongoing global cyber threats.

The workforce cybersecurity skills gap

Successful implementation of the DoD Zero Trust Overlay demands skilled cybersecurity personnel who understand advanced techniques such as least-privilege access enforcement, identity verification, network segmentation, and continuous monitoring.

This challenge is especially urgent as the threat landscape grows more complex. Cyber adversaries are deploying increasingly sophisticated attacks, while agencies lack the workforce capacity to respond and adapt in real time.

Budget and resource constraints

For public sector organizations, budgetary constraints remain a persistent challenge. Although zero trust promises significant long-term benefits to security and operational resilience, implementation requires substantial investments in upgraded technologies, workforce training, and security integration efforts.

This impediment is increasingly dangerous given the rapid escalation in cyberattacks targeting vulnerable government systems. Agencies can no longer afford to delay zero trust adoption, as the cost of breaches—both financial and operational—is far greater than the initial investments required. Immediate action to fund zero trust implementations is necessary to protect critical assets against widening threat vectors.

Interoperability and standardization

The DoD Zero Trust Overlay emphasizes integration and interoperability across agencies, systems, and technologies to enforce consistent security postures. Fragmented security practices are a pressing concern in today's interconnected digital environment.

Inconsistent policies and tools prevent agencies from maintaining a unified approach to cybersecurity, leaving critical gaps that attackers can exploit. Resolving interoperability challenges now will enable agencies to standardize their implementations of zero trust principles, ensuring consistent defenses across systems and reducing vulnerabilities.

Key challenges

Navigate legacy IT stacks
Overcome sprawling, heterogeneous IT ecosystems that are complex, costly, and difficult to manage.

Move beyond implicit trust
Evolve operational practices past reliance on perimeter-based defenses to integrate security inside the network.

Eliminate operational bottlenecks
Minimize disruptions that jeopardize mission-critical services with zero trust capabilities that scale across hybrid multicloud environments.

Streamline overhead
Address technical skills shortages by enabling workforces to achieve more with centralized control, fast provisioning, and deep observability tools.

Continuous threat environment

Public sector agencies operate in highly dynamic threat environments, confronting targeted attacks from nation-state adversaries, insider threats, and advanced persistent threats (APTs). These evolving threats demand real-time visibility, monitoring, and adaptive response capabilities—key tenets of the zero trust paradigm.

The assumption that cyber adversaries are always present requires agencies to act immediately. Without robust monitoring and threat-detection capabilities, agencies will remain reactive, unable to identify and neutralize breaches before they escalate. Implementing zero trust right now aligns with the urgency of deploying proactive security measures that not only mitigate immediate threats but enhance long-term resilience.

User experience and mission continuity

Zero trust implementations, while critical to improving security, can introduce added friction for end users if not executed carefully. Frequent authentication prompts, restricted access to applications, and enforced micro-segmentation policies can hamper productivity and introduce frustration for personnel attempting to complete critical tasks.

Given the urgency of current national and DoD missions, disruptions to mission-critical operations are unacceptable, especially in defense environments where uptime is non-negotiable. Agencies must act now to design thoughtful zero trust architectures that secure systems without compromising user experience or mission continuity.

Immediate action is crucial

The DoD Zero Trust Overlay is not a hypothetical or long-term initiative—it is a critical framework that must be implemented now to address the immediate and escalating threats targeting national security systems. Adversaries are exploiting every weakness in outdated systems, processes, and security models, and public sector agencies must take action to reduce vulnerabilities, enhance control, and protect sensitive operations. Implementing zero trust at this moment safeguards critical systems, data, and processes from attacks designed to disrupt government functions, compromise sensitive information, and erode national resilience.

Key solutions

Never trust, always verify
Dynamically enforce access decisions based on user identity, device posture, location, and risk signals.

Inspect traffic in real time
Enforce policies consistently on application-level traffic, including encrypted traffic.

Secure APIs and segment workloads
Authenticate, authorize, and continuously monitor microservices workloads.

Respond dynamically to evolving threats
Integrate threat intelligence, AI-driven analytics, and automation to keep pace with emerging attack vectors.

F5 solutions for DoD Zero Trust Overlay

The F5 ADSP is designed to enforce rigorous security policies, secure applications, manage access control, and provide real-time visibility across hybrid and multicloud architectures. With F5, agencies gain robust tools to operationalize the DoD's Zero Trust Overlay efficiently and at scale, enabling them to face today's most advanced cyber threats with confidence.

Safeguard user-to-application access

F5 technologies enable secure user-to-application access as part of the DoD's "never trust, always verify" approach. With BIG-IP APM, access decisions are dynamically enforced based on user identity, device posture, location, and risk signals. By leveraging multi-factor authentication (MFA), single sign-on (SSO), and granular policy enforcement, agencies can ensure that only authenticated and authorized users can access sensitive resources. These tools help public sector organizations comply with zero trust mandates while mitigating unauthorized access risks and creating a seamless user experience.

Enable compliant application protection

Application security plays a critical role in zero trust, especially in hybrid and multicloud environments where traffic flows freely across disparate infrastructure. F5® BIG-IP Advanced Firewall Manager™ (AFM) and F5® BIG-IP SSL Orchestrator® provide real-time inspection and policy enforcement on application-level traffic, including encrypted traffic. These solutions help detect and block malicious payloads, ensure compliance with DoD security standards, and enforce consistent security across on-premises, cloud, and edge deployments. As agencies' application landscapes grow increasingly complex, F5 simplifies traffic security by providing unified visibility and control across all environments.

Secure and monitor app-to-app communications

Zero trust also requires securing application-to-application communication to prevent lateral movement within systems. F5® NGINX® App Protect and F5 NGINX Container Ingress Services provide robust tools for securing API traffic and enabling workload segmentation. By enforcing zero trust principles within the microservices layer, these solutions ensure that inter-application communications are authenticated, authorized, and continuously monitored. Whether securing APIs or isolating mission-critical workloads, F5 supports granular segmentation and minimizes vulnerabilities in internal interactions.

F5 solutions address the challenges of implementing the DoD's Zero Trust Overlay, providing trusted tools, technologies, and expertise to support future-ready cybersecurity architectures.

Respond faster with automated threat intelligence

Continuous monitoring and adaptive threat response are foundational to zero trust. F5® Distributed Cloud Services enable public sector agencies to detect anomalous activities in real time and respond dynamically to evolving threats. These solutions integrate threat intelligence, AI-driven analytics, and automation capabilities to identify risks and adapt policies on the fly. For the DoD's "assume breach" posture, these capabilities are invaluable, allowing agencies to neutralize emerging threats while maintaining operational stability and security.

Restrict lateral movement with network segmentation

Network segmentation is another essential component of zero trust, as it restricts lateral movement by isolating workloads and resources. With F5® BIG-IP Local Traffic Manager™ (LTM), agencies can implement micro-segmentation strategies that dynamically enforce traffic routing and isolation based on zero trust policies. Workload segmentation prevents malicious actors from gaining access to sensitive systems while ensuring secure communication only occurs where necessary. F5 solutions reduce the attack surface while supporting mission-critical operations.

Broaden visibility with deep telemetry

Visibility across users, endpoints, applications, and networks is required for effective zero trust deployment. F5 enhances visibility with logging and monitoring integrations that provide actionable insights into traffic patterns, user behavior, and system performance. These insights enable agencies to pinpoint vulnerabilities, respond proactively to threats, and maintain real-time oversight across distributed infrastructure. By streamlining visibility across hybrid and multicloud environments, F5 ensures that agencies can enforce the dynamic, adaptive controls necessary for zero trust success.

Close security gaps with trusted tools

The urgency to implement zero trust principles is clear. Cyber adversaries are becoming more sophisticated, targeting legacy systems, exploiting overlooked vulnerabilities, and leveraging advanced attack vectors to compromise national security systems. F5 solutions address the challenges associated with implementing the DoD's Zero Trust Overlay, providing trusted tools, technologies, and expertise to support robust, scalable, and future-ready cybersecurity architectures.

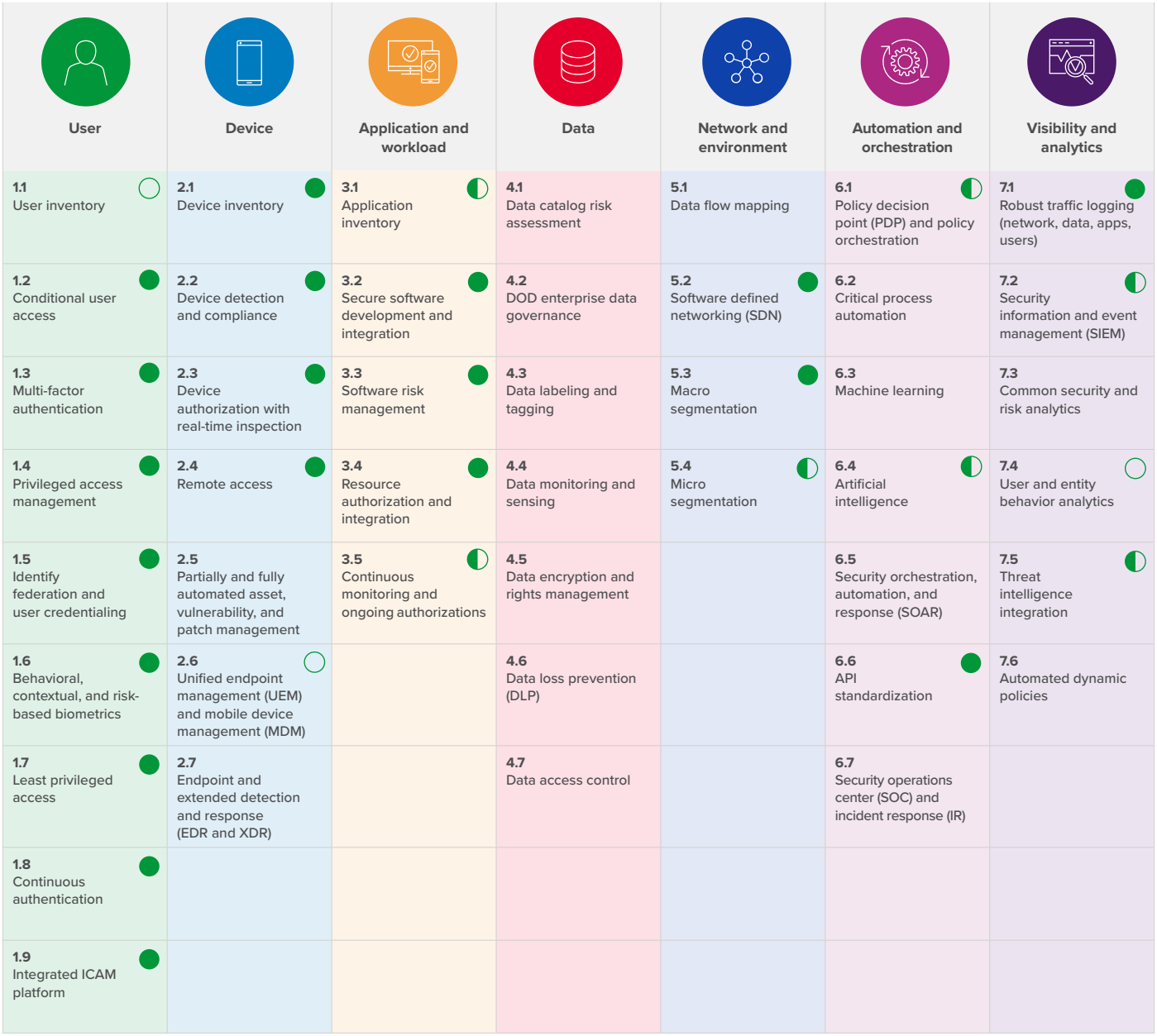


Figure 1: A complete view of how key F5 capabilities fit into end-to-end zero trust.

F5 offers a comprehensive set of capabilities that are essential to implementing zero trust architecture. These capabilities are available in multiple deployment models including hardware or virtual appliances (BIG-IP), pure software (F5 NGINX Plus®), and as-a-service offerings (Distributed Cloud Services).

F5 solutions span all major planes of the zero trust reference architecture—including transaction, data, identity, authorization, visibility, analytics, and automation—and are typically delivered as integrated solutions that operate seamlessly across multiple planes, enabling consistent security and policy enforcement.

Implement zero trust now for future-ready protection

Trusted partners such as F5 provide the expertise and technologies that government entities need to overcome implementation barriers and accelerate the zero trust journey. Advanced F5 solutions for identity-aware access, traffic management, monitoring, and multicloud security empower agencies to mitigate today's threats while positioning themselves for future challenges. With the urgency of the moment, public sector organizations can no longer afford to wait—zero trust implementation must begin now to secure the systems, missions, and lives it protects.

Next steps

Explore F5 solutions that enable zero trust for governmental agencies.

Contact F5 to get started.

©2025 F5, Inc. All rights reserved. F5, and the F5 logo are trademarks of F5, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com.
Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, expressed or implied, claimed by F5, Inc.
DC 10.2025 | JOB-CODE-1752661186