Evolver

AI-Powered Cybersecurity: 3-Part Series

Part 1:

Zero Trust Architecture (ZTA) Implementation, Challenges, Best Practices, & Tools

June 2026

U.S. Federal government agencies have moved beyond debating whether Zero Trust Architecture (ZTA) is the right strategy. The challenge today is implementing ZTA at scale across hybrid-multi-cloud environments, mission partners, cloud services, and legacy systems without disrupting operations.

The original ZTA requirement was driven by an Executive Order from the Biden Administration on May 12, 2021, as an unfunded mandate, which in late 2021 the Office of Management and Budget (OMB) Federal Zero Trust Strategy established a government-wide baseline and required agencies to meet specific goals by the end of FY 2024. OMB's FY 2025 guidance then made clear that the implementation of ZTA would take several years longer to achieve than was originally mandated.

OMB recognized that the next phase of ZTA implementation will be focused on enhancing zero trust maturity: performance measurement, automated reporting, and continued expansion of critical security capabilities across the enterprise.[1] Senior officials should read that shift correctly. Federal ZTA is no longer a planning exercise or a series of isolated pilots. It is becoming an operating model for how agencies govern access, data, telemetry, and cyber risk across mission systems.

The implementation challenge is that zero trust is not a simple plug-and-play software or hardware product. Rather, zero trust is a set of design tenets and architectural decisions spanning identity, device, networks, applications, data, automation, continuous monitoring, security orchestration, and governance. NIST's foundational guidance states that zero trust removes implicit trust based solely on network location and instead requires policy-based decisions grounded in user identity, asset state, and resource context.[2]

NIST's 2025 practice guide reinforces that agencies can implement ZTA incrementally with existing commercial technologies but also shows why execution is difficult: integrations are uneven, multiple policy decision points create complexity, and many deployments still struggle to unify telemetry and control across vendors and environments.[3]

The latest federal evidence points to six recurring obstacles:

- **legacy infrastructure**
- **incomplete visibility**
- **policy sprawl in hybrid estates**
- **authorization and reporting friction**
- **third-party risk blind spots**
- **cryptographic modernization pressure.**

These are not abstract technical concerns. They translate directly into delayed modernization, higher operating cost, slower authorizations, weaker supply chain assurance, and persistent exposure of high-value data. This whitepaper outlines those challenges, identifies practical best practices and tooling patterns, and explains why Evolver CLEAR and Evolver SHIELD are valuable complements to agency ZTA roadmaps rather than separate side initiatives.[4]

© EVOLVER 2026

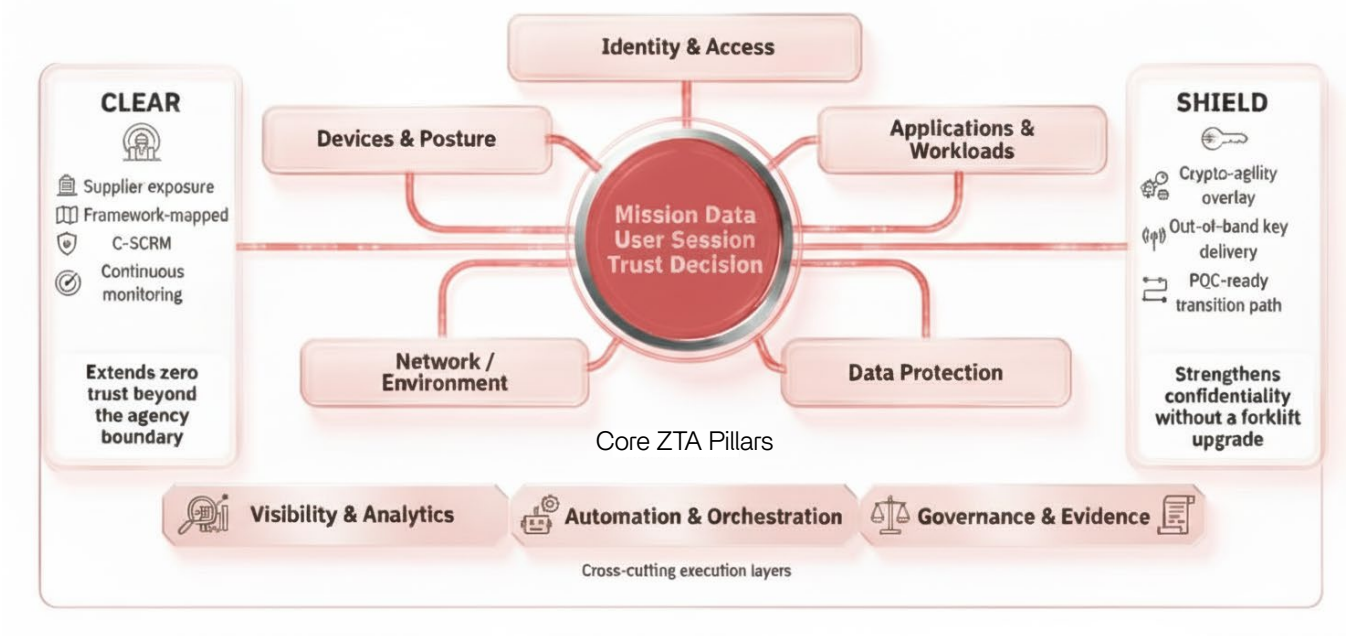


Figure 1. A practical federal ZTA execution model. CLEAR extends zero trust into supplier ecosystems, while SHIELD strengthens cryptographic resilience across hybrid connections.

What is Zero Trust Architecture?

Zero trust can be summarized as "never trust, always verify," but that slogan is incomplete and often misleading. Under NIST SP 800-207, ZTA is an enterprise architecture in which every access request is evaluated against policy using available signals such as identity, device health, service attributes, workload context, and data sensitivity; trust is continuously reevaluated during the session rather than granted once at login.[5]

The architecture usually includes a policy engine, policy administrator, and policy enforcement points, but NIST also emphasizes that there are multiple deployment models, including enhanced identity governance, software-defined perimeter, data micro-segmentation, and SASE-style approaches.[6]

For federal leaders, the key implication is strategic: ZTA should be funded and governed as an architecture program, not as a single network security refresh. Identity modernization without device health, data tagging without policy enforcement, or cloud migration without machine-readable evidence will not produce meaningful zero trust outcomes. Agencies showing the strongest progress are those treating ZTA as a phased discipline anchored to mission data, system boundaries, acquisition decisions, and operational telemetry.[7]

Latest Federal ZTA Implementation Challenges:

1) Legacy modernization still constrains ZTA execution

The U.S. Government Accountability Office (GAO) continues to report that U.S. federal government agencies' information technology (IT) portfolios remain dominated by operations and maintenance spending and that critical legacy system modernization has advanced unevenly. In its 2025 review, GAO found that agencies still spend about 80 percent of their IT budgets on operations and maintenance, and only a minority of the highest-priority legacy modernization efforts had been completed.[8]

That matters to ZTA because legacy environments often

© EVOLVER 2026

lack reliable identity federation, modern logging, policy APIs, granular data segmentation, and automated configuration management. Agencies then face a false choice between delaying zero trust controls or wrapping them around brittle systems in expensive one-off ways. Either path slows mission modernization.

2) Visibility is improving, but authoritative telemetry remains uneven

Most government agency progress in zero trust implementation progress has been strongest in identity and access management (IAM) and endpoint detection and response (EDR) capabilities, but visibility across devices, workloads, cloud services, and east-west traffic is still uneven. OMB's FY 2025 FISMA guidance places unusual emphasis on automated reporting, Continuous Diagnostics and Monitoring (CDM)-aligned telemetry, and measurable security outcomes, because many agencies still cannot produce authoritative machine-readable views of assets and controls across the enterprise.[9]

GAO similarly found that the U.S. Department of Homeland Security (DHS) Cybersecurity Infrastructure Security Agency (CISA)'s network monitoring program generally met expectations but still required further guidance and action in areas directly relevant to endpoint detection and cloud asset management.[10] Without dependable visibility, conditional access and risk-based policy are reduced to static rules.

3) Hybrid and multi-cloud estates create policy sprawl

Hybrid (on-premises and cloud-based) information systems and multi-cloud architectures create distributed policy decision points that are difficult to coordinate. NIST SP 800-207A specifically addresses cloud-native, multi-cloud, and multi-location environments because policy enforcement must work across users, services, devices, application programmable interfaces (APIs), and east-west workload communications rather than just north-south traffic.[11]

NIST's implementation findings add that many vendor solutions do not integrate out of the box as needed, and that multiple policy decision points can make it difficult to articulate, test, and maintain a coherent enterprise policy model.[12] CISA's 2025 data micro-segmentation guidance underscores the same point: data segmentation is essential, but planning data flows, dependencies, and policy boundaries in live environments is resource intensive and easy to get wrong.[13]

4) Authorization and reporting friction slows secure cloud adoption

U.S. Federal government agency ZTA implementation is increasingly inseparable from enterprise IT modernization and automation. OMB's FedRAMP modernization memo and the FY 2025 FISMA guidance both push toward standardization, automation, and reusable evidence, including machine-readable approaches such as OSCAL. Yet many agencies still operate with document-heavy authorization-to-operate (ATO) processes that lag cloud change velocity and slow adoption of secure commercial tools.[14] This is a governance problem as much as a security problem. If telemetry cannot be converted into durable evidence for Authorizing Officials, zero trust controls remain harder to scale than they need to be.

5) Third-party and supplier ecosystems remain a major blind spot

Many U.S. federal government ZTA implementation programs are still too inward looking. They focus on agency users and devices while underestimating the trust decisions created by suppliers, government contractors, subcontractors, managed service providers, and cloud-delivered business applications. NIST's recent cybersecurity supply chain risk management (C-SCRM) quick-start guides make the point directly: agencies need a standing supplier risk capability and a repeatable due diligence process, not ad hoc questionnaires performed only during procuremen.[15] For senior leaders, this is a material ZTA issue because suppliers often possess access, process data, support mission platforms, or influence software provenance outside the agency's immediate control plane.

© EVOLVER 2026

6) Crypto agility and post-quantum readiness lag mission urgency

A final challenge is increasingly urgent: cryptographic modernization. OMB's memorandum on migration to post-quantum cryptography explicitly states that U.S. federal government agencies moving to zero trust rely on strong encryption and must prepare now because adversaries can capture encrypted data today for future decryption. It directs agencies to inventory cryptographic systems and prioritize high-value assets and high-impact systems, with a goal of mitigating as much quantum risk as feasible by 2035.[16]

NIST finalized FIPS 203 for ML-KEM in 2024 and selected HQC in 2025 as a backup algorithm, but widespread vendor-native adoption will take time.[17] Many agencies therefore face a gap between strategic urgency and practical deployment readiness.

Pro Tip: Do not fund zero trust as a single enterprise contract line. Fund it as sequenced control outcomes tied to mission data, system boundaries, and measurable risk reduction.

Best Practices for Federal ZTA Programs

1) Govern ZTA as mission architecture, not as a product rollout

Effective U.S. federal government ZTA implementation programs are managed as enterprise architecture efforts with explicit executive ownership for each pillar and each cross-cutting capability. Agencies should maintain a policy-to-control map that ties mission systems, high-value data, users, devices, applications, and external dependencies to specific zero trust objectives, metrics, and evidence sources. This aligns with CISA's maturity model and with OMB's shift toward performance measurement in FY 2025 FISMA reporting.[18] The practical value is that acquisition, engineering, cyber operations, and authorizing staff can all work from the same architecture map rather than interpreting zero trust differently.

2) Start with authoritative discovery and dependency mapping

ZTA implementation should begin with authoritative inventories of identities, devices, workloads, applications, APIs, data stores, network paths, suppliers, and cryptographic systems. NIST's implementation guidance recommends discovering the environment, identifying existing capabilities, and using risk-based prioritization before making large-scale enforcement changes.[19]

OMB's PQC memo makes the same point for encryption. Leaders should not approve later-phase tooling until inventories are good enough to show what will actually be controlled.[20] In practice, discovery is what separates scalable ZTA programs from expensive pilot activity.

3) Phase control enforcement in an order that reduces risk without breaking operations

The most reliable rollout sequence is to establish strong identity and device signals first, then add conditional access, application mediation, data micro-segmentation, and data-centric controls in stages. NIST's 19 example implementations show that agencies do not need to replace every control family at once; they can leverage existing identity credential and access management (ICAM), endpoint, network, and analytics investments incrementally.[21]

CISA's data micro-segmentation guidance reinforces the need to plan with application owners and data flows before turning on broad east-west controls.[22] Phasing matters because poorly sequenced ZTA programs create outages, policy exceptions, and loss of stakeholder confidence.

4) Treat evidence as architecture

Agencies should design their ZTA telemetry, logging, configuration evidence, and reporting pipeline at the same time they design controls. OMB now expects agencies to report progress in increasingly automated and measurable ways, while FedRAMP modernization explicitly pushes machine-readable, reusable security artifacts.[23] A mature pattern is to normalize telemetry from ICAM, endpoint, cloud posture, segmentation, and data protection tools into SIEM, SOAR, and GRC processes that can support continuous monitoring and authorization updates. This is the operational foundation for continuous ATO.

© EVOLVER 2026

Pro Tip: If a control cannot produce usable evidence for operators, auditors, and Authorizing Officials, it is not ready to scale government wide.

5) Extend zero trust beyond the agency boundary

A U.S. federal government agency ZTA implementation program that ignores supplier posture, SaaS configuration, contractor, and subcontractor connectivity will inherit avoidable blind spots. NIST's C-SCRM quick-start guides provide a pragmatic path: establish supplier governance, define tiered requirements, and conduct due diligence with enough rigor to inform acquisition and onboarding decisions without overburdening low-risk vendors.[24] Zero trust is strongest when supplier decisions, onboarding gates, and continuous monitoring are part of the same operational discipline as internal conditional access and endpoint posture.

6) Build crypto agility into the baseline now

ZTA is only as strong as the confidentiality and integrity of the cryptographic systems underpinning it. U.S. federal agencies should establish crypto inventories, key lifecycle governance, rotation policy, and a migration plan for high value flows rather than waiting for a later "quantum program." OMB's post-quantum cryptography (PQC) memorandum and NIST's finalized standards make clear that this work has already started across government.[25]

The best near-term strategy is to pilot crypto-agile overlays or transition patterns in enclaves where mission impact is high and downtime tolerance is low, then expand as commercial stacks mature.

Common Tooling for Federal ZTA

U.S. federal government ZTA software tooling should be evaluated as a stack of interoperable control functions rather than a vendor competition. In practice, common categories include

- **identity providers and phishing-resistant multi-factor authentication (MFA);**
- **least privileged access (LPA) management;**
- **endpoint detection and response (EDR);**
- **secure access service edge (SASE) or software-defined perimeter (SDP) capabilities;**
- **data micro-segmentation and workload policy;**
- **API and application access brokers;**
- **data classification, data loss prevention (DLP),**
- **key management; security information and event management (SIEM), security orchestration and automated response (SOAR), and user evaluation behavior and analytics (UEBA);**
- **cloud posture plus configuration baselines.**

NIST's SP 1800-35 is especially useful because it demonstrates that agencies can assemble these functions from multiple commercial vendors and existing infrastructure instead of waiting for a single comprehensive platform.[26]

Government standards and shared approaches should also be part of the tooling discussion. FedRAMP and OSCAL improve the adoption of secure cloud services, while CISA guidance on maturity modeling and data micro-segmentation helps agencies choose implementation order and control depth.[27] Yet one lesson recurs across federal programs: mainstream ZTA tooling often leaves two important gaps under-addressed in early phases - supplier exposure management and crypto agility. Those are the spaces where Evolver CLEAR and Evolver SHIELD offer differentiated value.

How Evolver CLEAR Strengthens Federal ZTA

Evolver CLEAR addresses a gap many agencies discover only after implementing core zero trust controls: the agency can tighten internal trust decisions and still remain exposed through suppliers and third-party services. CLEAR combines program governance, supplier onboarding, framework mapping, and non-intrusive external risk analytics so agencies can assess large supplier populations without credentialed scans or months of questionnaire exchange.[28] That operating model is well suited to federal acquisition realities where agencies must balance speed, evidence, and burden across both prime contractors and smaller suppliers.

© EVOLVER 2026

From a ZTA perspective, CLEAR contributes in four ways. First, it expands visibility beyond the agency boundary by providing observable risk signals on suppliers that support mission systems, data processing, or managed services. Second, it translates those signals into framework-aligned scorecards and prioritized remediation plans that can inform onboarding, tiering, and continuous monitoring. Third, it gives acquisition, enterprise risk management (ERM), and cyber leaders a portfolio view of supplier risk rather than isolated case files. Fourth, because the model is non-intrusive and scalable, it is practical for the long tail of vendors that are frequently omitted from deeper technical reviews.[29]

CLEAR isn't a full substitute for deep supplier assessments. Critical vendors still need direct evidence, on-site reviews, penetration tests, or contract controls. Its value lies in offering a repeatable supplier risk layer missing in most ZTA roadmaps. Piloting 25-50 suppliers by mission criticality can improve onboarding speed, visibility, remediation, and risk acceptance with less friction (Evolver Federal, Evolver CLEAR). For departments adopting zero trust enterprise-wide, this is a key advantage.

How Evolver SHIELD Strengthens Federal ZTA

Evolver SHIELD addresses a different but equally strategic gap: protecting sensitive federal data as agencies modernize cryptography in hybrid environments. OMB has already directed agencies to inventory cryptographic systems and prepare for a transition to post-quantum cryptography because strong encryption is foundational to the federal move toward zero trust, and because harvested ciphertext may later be decrypted when quantum capabilities mature.[30]

The challenge is that few agencies can afford disruptive forklift upgrades to virtual private networks (VPN), software defined (SD)-wide area network (WAN), and application stacks while maintaining mission availability and existing authorizations.

SHIELD's value proposition is that it pursues crypto agility as an overlay. SHIELD pairs Evolver services with Quantum Xchange Phio TX to perform crypto discovery, define policy, deploy an out-of-band key delivery mesh, and update risk management framework (RMF) and ATO artifacts so agencies can strengthen confidentiality without rerouting packets or replacing the existing data plane.[31] That is an attractive pattern for federal environments because it aligns with how ZTA is adopted (incrementally) around mission systems that cannot tolerate downtime or large boundary changes.

For senior officials, SHIELD offers three practical advantages. First, it supports immediate risk reduction for high-value flows while broader vendor-native PQC support continues to mature. Second, it preserves current network and application investments, which lowers adoption friction and budget shock. Third, it turns cryptographic modernization into a governable workstream with evidence, policy, and pilot-based expansion rather than a future aspiration. NIST's finalized FIPS 203 standard for ML-KEM and the ongoing PQC standardization work reinforce why that posture matters now, not later.[32]

As with CLEAR, the most credible adoption path is a bounded pilot. Agencies can start with a high-value enclave, external partner connection, or data flow that carries sensitive information and then validate that SHIELD improves key management, rotation discipline, performance, and authorization evidence without disrupting operations. SHIELD does not replace ICAM, EDR, or segmentation controls. It complements them by hardening the cryptographic fabric that zero trust decisions depend upon. In that role, it is a strategically important accelerator for agencies that want their ZTA program to remain viable through the PQC transition rather than requiring a second major redesign later.[33]

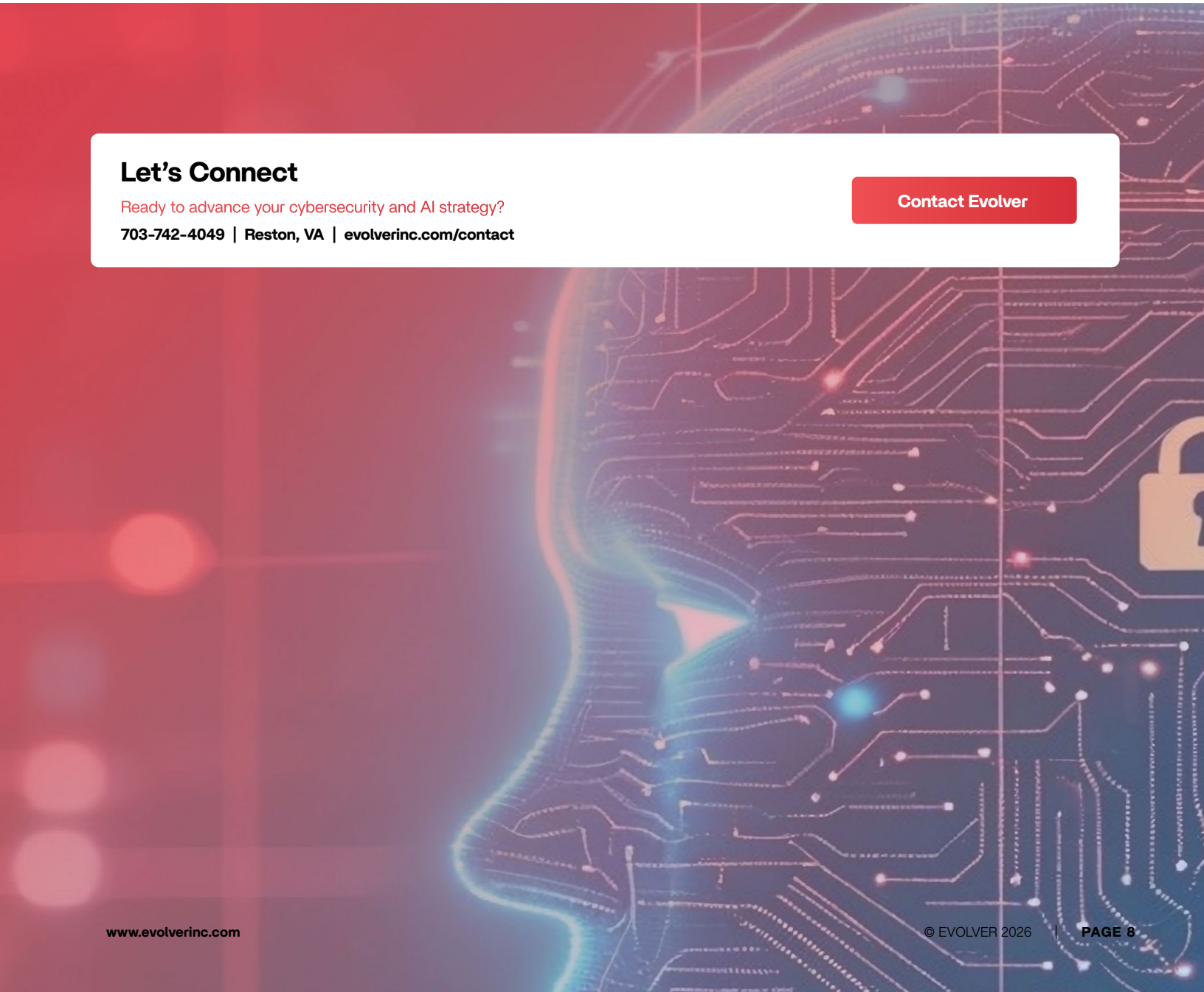
© EVOLVER 2026

Conclusion

U.S. Federal government zero trust architecture (ZTA) implementation is now more demanding. The initial policy is set; the focus is on enterprise-scale execution across hybrid clouds, legacy systems, partners, and evolving threats. The strongest programs treat ZTA as a mission architecture with discovery, phased enforcement, machine-readable evidence, supplier assurance, and crypto agility from the start.

Senior officials must decide beyond buying a "zero-trust product." They need to fund missing control layers that block maturity. CLEAR extends zero trust to suppliers and acquisitions. SHIELD helps agencies boost confidentiality and prepare for post-quantum security without network disruption or reauthorizations.

These tools address two gaps often delayed in ZTA programs. Agencies should combine core ZTA controls with pilots managing supplier risks and crypto-agile encryption, then expand capabilities that reduce risk, improve authorization, and strengthen mission resilience.



Let's Connect

Ready to advance your cybersecurity and AI strategy?

703-742-4049 | Reston, VA | evolverinc.com/contact

Contact Evolver

© EVOLVER 2026

About the Authors

Gregory A. Garrett is Chief Operating Officer and Chief Innovation Officer at Evolver, leading technology strategy and innovation across cybersecurity, Zero Trust Architecture (ZTA), federal IT modernization, digital transformation, and eDiscovery solutions. With more than 25 years of executive leadership experience as a CIO, CTO, CISO, and COO, he has managed over $40 billion in global technology programs. A retired U.S. Air Force Colonel and author of 24 books, Garrett is a recognized thought leader in cybersecurity, Zero Trust, and secure enterprise transformation.

Rahul Johri is a cybersecurity and enterprise transformation leader specializing in Zero Trust Architecture (ZTA), AI-driven modernization, cloud security, and secure federal IT environments. He helps government agencies implement Zero Trust frameworks, cyber resilience strategies, and multi-cloud architectures that strengthen security and operational effectiveness. His expertise spans cybersecurity modernization, data protection, risk visibility, compliance, and mission-critical digital transformation initiatives.

Dr. Brian McElyea is a cybersecurity executive specializing in digital transformation, cyber risk management, compliance, and Cyber Centers of Excellence. He has led enterprise cybersecurity initiatives across healthcare, defense, and federal sectors, helping organizations strengthen security, resilience, and operational performance. With more than two decades of leadership experience, Brian advises organizations on cybersecurity strategy, federal IT modernization, risk management, and secure digital transformation.

© EVOLVER 2026

Works Cited

Office of Management and Budget. M-22-09: Advancing the U.S. Government Toward Zero Trust Cybersecurity Principles. 26 January 2022. [1]

Office of Management and Budget. M-25-04: Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements. 15 January 2025. [1, 7, 9, 14, 18, 23]

National Institute of Standards and Technology. Zero Trust Architecture. NIST SP 800-207, August 2020. [2, 5, 6]

National Institute of Standards and Technology. Implementing a Zero Trust Architecture. NIST SP 1800-35, June 2025. [3, 12, 19, 21, 26]

Evolver. Evolver CLEAR: Continuous Landscape Exposure & Assurance of Risk (C-SCRM). Internal solution document, n.d. [4, 28, 29]

Evolver. Evolver SHIELD: Secure Hybrid Integrated Encryption & Lattice-ready Key Delivery. Internal solution document, n.d. [4, 31, 33]

CISA. Zero Trust Maturity Model. Version 2.0, April 2023. [7, 18, 27]

GAO. Agencies Must Plan to Modernize Critical Systems That Are Decades Old. GAO-25-107795, 17 July 2025. [8]

GAO. Cybersecurity: Network Monitoring Program Requires Additional Guidance and Actions. GAO-25-107470, 11 June 2025. [10]

National Institute of Standards and Technology. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications Across Multi-Cloud Environments. NIST SP 800-207A, September 2023. [11]

CISA. Microsegmentation in Zero Trust Part One: Introduction and Planning. Version 1.0, 29 July 2025. [13, 22]

Office of Management and Budget. M-24-15: Modernizing the Federal Risk and Authorization Management Program. 25 July 2024. [14, 23, 27]

National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM). NIST SP 1305, 21 October 2024. [15, 24, 29]

National Institute of Standards and Technology. NIST Cybersecurity Supply Chain Risk Management: Due Diligence Assessment Quick-Start Guide. NIST SP 1326, initial public draft, 30 October 2024. [15, 24]

Office of Management and Budget. M-23-02: Transitioning to Post-Quantum Cryptography. 18 November 2022. [16, 20, 25, 30]

National Institute of Standards and Technology. "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption." 11 March 2025. [17, 31]

National Institute of Standards and Technology. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. 13 August 2024. [25]

General Services Administration. "GSA Announces FedRAMP 20x." 24 March 2025. [27, 31]