ATTACKIQ®

SOLUTION NOTE

Zero Trust

The Zero Trust Mandate

Cyber adversaries today move with speed and precision, exploiting trusted pathways, compromising credentials, and operating within networks long before detection. Traditional perimeter defenses are no longer sufficient to contain these threats.

To address this challenge, the **Department of Defense (DoD)** has committed to a department-wide Zero Trust transformation. **Guided by Executive Order 14028** and the **DoD Zero Trust Strategy**, the Department aims to secure the majority of enterprise systems through Zero Trust by 2027. [1][2][3] This initiative redefines how the Department authenticates, authorizes, and monitors every user, device, workload, and data flow.

Zero Trust is not a product or a single technology; it is a security framework built on continuous verification. It assumes breach, enforces least privilege, and requires validation of every access decision based on identity, context, and risk.

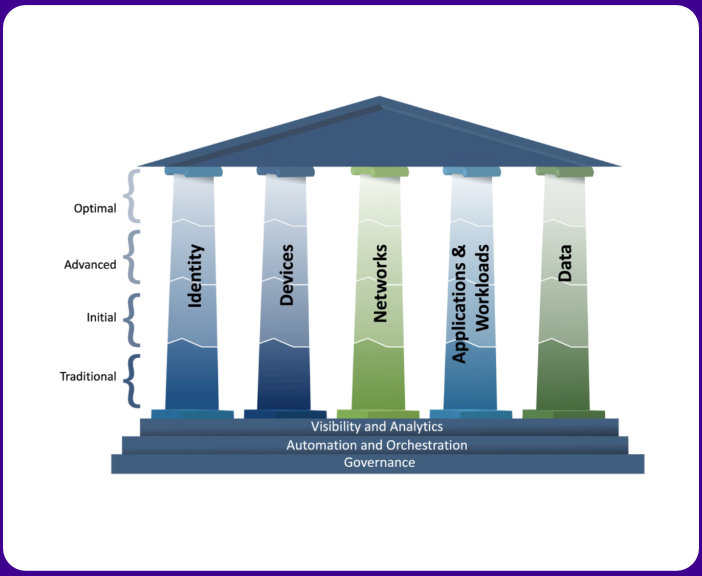
The **AttackIQ Adversarial Exposure Validation (AEV)** platform enables agencies to operationalize this approach by continuously testing and verifying that Zero Trust controls perform as intended across the seven pillars of the DoD Zero Trust Maturity Model (ZTMM).

The DoD Zero Trust Framework

The DoD Zero Trust Strategy envisions *"a DoD Information Enterprise secured by a fully implemented, Department-wide Zero Trust cybersecurity framework."* [2] It outlines a department-wide effort to build a culture of Zero Trust, defend critical systems, accelerate technology modernization, and align governance and policy to sustain implementation.

The **Zero Trust Maturity Model (ZTMM)** provides a roadmap for measuring and advancing adoption across missions and information environments. It defines four levels of maturity—Traditional, Initial, Advanced, and Optimal—and organizes capabilities across seven foundational pillars: ***User, Device, Applications & Workloads, Data, Network & Environment, Visibility & Analytics, and Automation & Orchestration.***

Together, these pillars guide how the DoD operationalizes and measures Zero Trust implementation to ensure progress toward enterprise-wide resilience.



Operationalizing the Seven Pillars with AttackIQ

Zero Trust depends on continuous validation to ensure that policies and controls perform as intended under real-world conditions.

The AttackIQ Adversarial Exposure Validation (AEV) platform enables organizations to test and measure Zero Trust maturity across all seven pillars, providing continuous assurance aligned with the MITRE ATT&CK® Framework and the DoD Zero Trust Maturity Model.

DoD Zero Trust Pillar	Zero Trust Focus	AttackIQ Validation Objective
User	Identity assurance and least-privilege enforcement	Emulate credential theft, phishing, and privilege escalation to test multi-factor authentication (MFA), identity proofing, and access policy enforcement under realistic adversary conditions.
Device	Endpoint integrity and compliance	Simulate malware execution, persistence, and device compromise to verify EDR performance, patching cadence, and policy compliance across managed and unmanaged devices.
Applications & Workloads	Secure application behavior and workload isolation	Test container and API exploitation techniques to assess runtime protection, workload segmentation, and detection of abnormal process execution. Validate use of trusted code repositories and libraries to maintain software integrity and reduce organizational risk.
Data	Protection of sensitive and mission-critical data	Execute controlled data-exfiltration attempts to validate encryption, data loss prevention (DLP), and access monitoring controls for both structured and unstructured data.
Network & Environment	Segmentation, boundary defense, and secure communications	Emulate lateral movement, command-and-control, and segmentation bypass to confirm enforcement of micro-segmentation and detection of unauthorized internal access attempts.
Visibility & Analytics	Detection, telemetry, and situational awareness	Assess coverage and fidelity of telemetry sources, evaluate alert thresholds, and identify analytic gaps by replaying stealthy and evasive adversary techniques.
Automation & Orchestration	Speed, accuracy, and consistency of response	Validate security orchestration, automation, and response (SOAR) and automated containment workflows to ensure policies trigger the correct mitigation and remediation actions in response to simulated compromise.

By validating each pillar through controlled, adversary-informed testing, the AttackIQ AEV platform provides continuous, data-driven insight into the effectiveness of Zero Trust controls. Assessment results feed directly into maturity measurement and readiness evaluation, enabling organizations to identify gaps, prioritize remediation, and demonstrate measurable progress toward the DoD's Zero Trust objectives.

This continuous validation loop ensures that Zero Trust is not only implemented, but proven to perform under operational conditions.

Continuous Validation & Measurement

Continuous validation is central to achieving Zero Trust maturity. The AttackIQ AEV platform provides a repeatable, evidence-based process for testing and measuring the effectiveness of Zero Trust controls against real-world adversary behaviors.

AttackIQ supports this capability through four core functions:

Real-world Adversary Emulation

Leverages a vast library of pre-built attack scenarios mapped to the MITRE ATT&CK® Framework, each replicating authentic adversary tactics, techniques, and procedures (TTPs). Scenarios can be tailored to reflect mission systems, networks, and operational environments, providing an accurate measure of exposure to known threat behaviors.

Testing of Security Controls

Validates that defensive technologies, including firewalls, intrusion detection systems, endpoint protection, and identity management solutions, perform effectively under simulated attack conditions. This process identifies detection, prevention, or response gaps before adversaries can exploit them.

End-to-End Control Validation

Conducts continuous testing of identity and access management (IAM), endpoint detection and response (EDR), network segmentation, cloud, and automation controls. Validation results confirm whether these components operate cohesively to enforce Zero Trust policies across hybrid and multi-domain environments.

Quantitative Maturity Metrics

Generates empirical data to identify coverage gaps, measure defensive performance, and prioritize remediation based on exploitability and mission impact. Results map directly to the DoD's Target and Advanced maturity outcomes, enabling objective assessment of progress toward Zero Trust readiness.[2][3]

The AttackIQ Adversarial Exposure Validation Platform

This approach provides a repeatable mechanism for assessing Zero Trust maturity and strengthening defensive readiness across missions and information environments. It supplies decision-makers with actionable data to inform governance, resource allocation, and performance reporting.

Secure by Design Alignment

AttackIQ supports federal cybersecurity modernization through its commitment to CISA's Secure by Design pledge, integrating security principles throughout product design, development, and validation.

By incorporating adversarial validation into the design process, AttackIQ helps the DoD build systems that are secure and resilient by default, ensuring controls are verified against real-world threats before deployment.

This approach reflects the Department's focus on proactive defense, continuous validation, and measurable assurance, which underpin both Secure by Design and Zero Trust principles.

Achieving Validated Zero Trust

By aligning with the DoD Zero Trust Strategy and validating performance across all seven pillars, AttackIQ enables agencies to demonstrate measurable assurance that Zero Trust controls function as intended.

Through continuous testing, measurement, and improvement, the Adversarial Exposure Validation (AEV) platform helps agencies move beyond compliance-driven implementation toward validated Zero Trust operations—where every control is verified, every assumption is tested, and every exposure is known before it can be exploited.

Every Zero Trust journey must be validated. AttackIQ helps federal and defense organizations accelerate progress toward the DoD's Zero Trust objectives, delivering the evidence, confidence, and mission assurance needed to achieve resilience by 2027 and beyond.

Learn how AttackIQ can help your organization validate Zero Trust readiness.

Contact us to schedule a technical consultation or Zero Trust validation briefing at: attackiq.com/demo.

[1] **Executive Order 14028**, Improving the Nation's Cybersecurity, The White House, May 12, 2021.
[2] **Department of Defense Zero Trust Strategy**, Chief Information Office (DoD CIO), November 2022.
[3] **Department of Defense Zero Trust Capability Execution Roadmap (ZTCER) FY23–FY27**, DoD CIO, January 2023.

ATTACKIQ

U.S. Headquarters
171 Main Street
Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading provider of Adversarial Exposure Validation (AEV) solutions, is trusted by top organizations worldwide to validate security controls in real time. By emulating real-world adversary behavior, AttackIQ closes the gap between knowing about a vulnerability and understanding its true risk. AttackIQ's AEV platform aligns with the Continuous Threat Exposure Management (CTEM) framework, enabling a structured, risk-based approach to ongoing security assessment and improvement.

The company is committed to supporting its MSSP partners with a Flexible Preactive Partner Program that provides turn-key solutions, empowering them to elevate client security. AttackIQ is passionate about giving back to the cyber-security community through its free award-winning AttackIQ Academy and founding research partnership with MITRE Center for Threat-Informed Defense.