REVISED EDITION

VALIDATED ZERO TRUST 101

Brought to you by

ATTACKIQ

EXPERT TIPS INSIDE

STUDY PLAN

OBJECTIVES

1. Define Validated Zero Trust (VZT) and explain its purpose.
2. Describe how organizations evolve toward a Zero Trust architecture.
3. Identify the key technologies, processes, and organizational elements that support validated Zero Trust.
4. Explain how the MITRE ATT&CK framework enhances Zero Trust validation.
5. Outline the steps required to operationalize validated Zero Trust and measure its effectiveness.

STUDY PLAN

STRUCTURE

1. Fundamentals and principles of Zero Trust
2. Evolution of Zero Trust in response to modern threats
3. Continuous validation and control measurement
4. Operationalizing validated Zero Trust for improved outcomes

PRIMER

Zero trust is a cybersecurity architecture and operating model that eliminates implicit trust and continuously verifies every access request. Unlike traditional perimeter-based security models, zero trust assumes compromise and evaluates each user, device, and session based on identity, context, and risk.

Rather than relying on static boundaries, zero trust focuses on limiting adversary movement by segmenting access, enforcing least privilege, and validating control performance in real time. It's not a single product or tool—it's a comprehensive security framework for managing access across modern environments, including cloud infrastructure, remote workforces, and hybrid networks.

> ***The hallmark of zero trust is simplicity. When every user, packet, network interface, and device is untrusted, protecting assets becomes simple."***
>
> John Kindervag,
> Founder of the Zero Trust Model

WHAT IS ZERO TRUST?

WHERE ZERO TRUST CAME FROM

The Zero Trust model was introduced by John Kindervag at Forrester Research in 2010. At the time, large-scale breaches exposed the inherent weakness of perimeter-based defenses: once attackers gained access to internal systems, lateral movement was largely unrestricted.

Zero Trust challenged this model by asserting that no entity—internal or external—*should be trusted by default*.

Over the past decade, Zero Trust has evolved from a theoretical concept into an operational framework adopted by the U.S. Department of Defense (DoD), NIST, and organizations worldwide. In the era of cloud infrastructure, remote work, and identity-targeted attacks, Zero Trust has become foundational, not optional.

CORE PRINCIPLES

1. **Never trust, always verify — Continuously authenticate and authorize every access request based on identity, device, and context.**
2. **Enforce least privilege — Restrict access to only the resources necessary for each user or process.**
3. **Continuously validate — Regularly test and monitor controls to ensure they function as intended.**

These principles shift security from static, perimeter-focused models to a dynamic, adaptive defense strategy built for modern enterprises.

WHY ORGANIZATIONS NEED ZERO TRUST

Modern adversaries exploit implicit trust within networks to move laterally and escalate privileges. Traditional perimeter defenses—firewalls, VPNs, and gateways—are no longer sufficient in cloud-first, hybrid, and remote environments.

Common attack vectors include credential theft, phishing, and supply chain compromise. Once attackers penetrate an environment, they exploit excessive permissions and untested controls to reach high-value assets undetected.

If access policies are overly broad or controls remain unvalidated, adversaries can persist inside the network for months. Incidents such as the SolarWinds supply chain attack demonstrated how implicit trust can be weaponized.

Zero Trust addresses this challenge by removing implicit trust, applying continuous verification, and enforcing strict access boundaries that prevent lateral movement.

APPROACH

ASSUME BREACH

EVALUATE EVERY INTERACTION TO GRANT TRUST OR NOT

STOP UNAUTHORIZED ADVERSARY MOVEMENT

WHY VALIDATED ZERO TRUST MATTERS

Many organizations pursue Zero Trust reactively—after a breach or in response to compliance mandates. However, static or checkbox implementations fail to deliver measurable security outcomes.

Validated Zero Trust (VZT) bridges this gap by embedding continuous testing and adversary emulation into the architecture itself. Through validation, organizations can confirm whether their Zero Trust controls actually stop real-world threats.

Integrating testing and verification into zero trust ensures:

- **Security investments target the most critical risks**
- **Controls are tested against relevant adversary techniques**
- **Security performance can be measured, tracked, and communicated effectively**

The unification of zero trust architecture with continuous validation through breach and attack simulation gives organizations a way to verify that their zero trust controls actually work as intended — something that's never been done until now.

THE PATH TO VALIDATED ZERO TRUST

STEP 1: ZERO TRUST ARCHITECTURE

1. Identify critical assets and sensitive data
2. Map communication flows and access dependencies
3. Implement network segmentation and access controls to restrict unauthorized movement

A zero-trust architecture establishes strict control over who can access which resources. However, architecture design alone doesn't ensure effectiveness. Without testing and validation, there's no assurance these controls will withstand a real attack.

STEP 2: SECURITY VALIDATION

1. Measure the effectiveness of zero trust controls using adversary emulation
2. Prioritize remediation based on exploitability, not just configuration gaps
3. Continuously validate defenses using real-world tactics, techniques, and procedures (TTPs)

Validation should occur continuously or at regular intervals — such as monthly, before major architecture changes, or after security incidents — to ensure that security controls adapt as threats evolve.

THE PATH TO VALIDATED ZERO TRUST (CONT.)

STEP 3: ALIGNING ARCHITECTURE WITH VALIDATION

Use security testing to verify that each control blocks or detects relevant attack techniques. This alignment provides:

- Evidence of security control effectiveness
- Data-driven prioritization of improvements
- Reduced breach impact through containment
- Measurable improvements in mean time to detect (MTTD) and respond (MTTR)
- Objective metrics for reporting and governance

THE ROLE OF THE MITRE ATT&CK FRAMEWORK

The MITRE ATT&CK® framework catalogs real-world adversary behaviors, particularly those involving credential abuse and lateral movement. By mapping controls to ATT&CK techniques, organizations can measure how their Zero Trust defenses perform against known threats.

Combining ATT&CK with breach and attack simulation enables security teams to:

- **Identify relevant adversary techniques to test against**
- **Measure how zero trust controls perform in real-world scenarios**
- **Communicate threat coverage and control efficacy across teams**

VALIDATION IN ACTION: NETWORK CONTROLS

Network controls—such as next-generation firewalls (NGFWs)—are essential enforcement points within Zero Trust architectures. Testing verifies that they work as designed.

- Through validation, organizations can:
- Simulate known malware to test lateral movement prevention
- Reproduce adversary techniques to evaluate traffic inspection and blocking
- Attempt unauthorized communication between network segments to verify controls are enforcing policy

This verifies not just that controls exist, but that they effectively block attacks.

THE SEVEN PILLARS OF ZERO TRUST SECURITY

To fully operationalize Zero Trust, organizations should implement and validate controls across seven DoD-defined pillars.

Pillar	Objective	Validation Focus
1. User	Enforce identity verification and contextual access.	Test for credential misuse, privilege escalation, and unauthorized logins.
2. Device	Allow only secure, compliant endpoints.	Validate endpoint detection and response (EDR) effectiveness and isolation workflows.
3. Network/Environment	Segment access paths and enforce encryption.	Test lateral movement, port misuse, and policy enforcement between segments.
4. Application & Workload	Protect application logic, interfaces, and the software supply chain.	Validate runtime protection, API security, and dependency integrity using adversary simulations. Leverage only trusted repositories and libraries, and verify code provenance through signing and continuous scanning.
5. Data	Encrypt and classify sensitive data.	Test Data Loss Prevention (DLP) and data classification controls against simulated data exfiltration attempts.
6. Visibility & Analytic	Maintain observability of all activity.	Verify alert fidelity, telemetry completeness, and response triggers.
7. Automation & Orchestration	Accelerate and standardize response.	Validate that automated containment and remediation runbooks execute correctly.

Validation is essential. Without continuous testing, zero trust becomes a checklist. With adversary-informed validation, it becomes a measurable, operational reality. Regular testing against real-world attack scenarios confirms whether controls actually work as designed.

VALIDATING PILLARS IN PRACTICE: A DEEPER LOOK AT NETWORK SEGMENTATION

Segmentation is fundamental to zero trust—but only if it effectively blocks unauthorized access. Traditional firewall rules and access controls may appear correct in configuration, but can contain flaws that attackers exploit to move laterally.

To verify segmentation effectiveness, organizations should:

1. **Map existing connections: Document open ports and communication paths between systems, services, and data stores.**
2. **Test security controls: Use security testing tools to attempt unauthorized network traversal using techniques like credential theft, port scanning, and protocol abuse.**
3. **Verify enforcement: Confirm that segmentation actually blocks unauthorized traffic rather than just logging it.**

This testing is essential for the Network/Environment pillar but applies across a zero-trust architecture. If a system can still communicate with resources it shouldn't access, segmentation exists in theory but not in practice.

Pro Tip: Test segmentation regularly—after network changes, when adding new systems, or as part of monthly security testing.

HOW TO EVOLVE FROM AN OPEN NETWORK TO VALIDATED ZERO TRUST

PHASE 1: ESTABLISH FOUNDATION

- Apply MFA and strong identity controls.
- Document high-value assets and data flows.
- Begin segmentation for critical systems.
- Run initial adversary emulations to establish a baseline.

PHASE 2: BUILD SECURITY CONTROLS

- Expand segmentation and least privilege access.
- Deploy visibility, logging, and behavior analytics.
- Map controls to MITRE ATT&CK techniques.
- Run targeted tests to validate key controls.

PHASE 3: MATURE AND OPTIMIZE

- Automate response and policy enforcement.
- Establish a continuous validation cadence.
- Use test results to inform control improvements.
- Integrate validation data into executive reporting.

Mature zero trust implementations are characterized by containment-focused design, continuous feedback loops between validation and control tuning, and quantifiable security metrics.

FROM RED AND BLUE TO PURPLE: SECURITY TEAM INTEGRATION

Testing zero trust controls requires operational collaboration. Traditional separation between offensive (red) and defensive (blue) security teams can limit testing effectiveness. An integrated team approach breaks down these barriers by enabling:

- Collaborative development of test scenarios
- Shared understanding of detection gaps
- Regular feedback loops between testing and improvement

This approach ensures that controls are both properly configured and effective against relevant threats.

CASE STUDY: SOLARWINDS AND ZERO TRUST

WHAT HAPPENED:

1. Attackers compromised SolarWinds' software update mechanism
2. Malicious code was deployed to thousands of organizations
3. Attackers moved laterally through networks, using trusted connections
4. Data was exfiltrated from high-value targets
5. Months passed before detection

HOW VALIDATED ZERO TRUST WOULD HAVE HELPED:

1. Initial compromise would still occur (zero trust assumes breach)
2. However, lateral movement would be blocked by micro-segmentation
3. Anomalous connection attempts would be flagged and investigated
4. Breach would be contained to the initial system, preventing catastrophic damage
5. Validation testing would have confirmed containment effectiveness

This example illustrates how zero trust principles, particularly micro-segmentation and continuous validation, can dramatically reduce breach impact even when perimeter defenses fail.

PRIMARY BENEFITS OF TESTING ZERO TRUST CONTROLS

- Provide evidence that security controls work against specific threats
- Limit unauthorized lateral movement within networks
- Quantify security effectiveness with objective metrics
- Support continuous improvement of security configurations
- Enable data-driven security decision making

CONCLUSION

Zero trust eliminates implicit trust and requires verification of every access request. However, implementing zero trust principles alone isn't enough—organizations must also regularly test that these controls actually prevent or detect unauthorized activity.

Combining zero trust architecture with security testing helps security teams verify that their implementations work as expected—ensuring that when real attacks occur, security controls respond effectively.

TEST YOUR KNOWLEDGE

1. WHICH OF THE FOLLOWING IS NOT A CORE PRINCIPLE OF ZERO TRUST?

A. Never trust, always verify

B. Trust but verify

C. Enforce least privilege

D. Continuously validate

2. WHICH COMBINATION BEST REPRESENTS VALIDATED ZERO TRUST?

A. Zero trust architecture, red teaming, penetration testing

B. NIST CSF, blue teaming, vulnerability scanning

C. Zero trust architecture, breach and attack simulation, MITRE ATT&CK

D. COBIT, blue teaming, data loss prevention

3. HOW WOULD ZERO TRUST HAVE HELPED IN THE SOLARWINDS ATTACK?

A. It would have prevented the initial compromise entirely

B. It would have detected the malicious code pre-deployment

C. It would have limited lateral movement

D. It would have encrypted all data accessed

TEST YOUR KNOWLEDGE

4. WHY DO MANY ORGANIZATIONS ADOPT ZERO TRUST REACTIVELY?

A. After breaches or to meet compliance mandates

B. To reduce security spending

C. Due to insurance requirements

D. To replace security teams with automation

5. HOW OFTEN SHOULD VALIDATION TESTING OCCUR?

A. Only after major incidents

B. Annually during audits

C. Continuously or regularly (e.g., monthly)

D. Only when deploying new controls

6. WHICH OF THE FOLLOWING IS NOT A PILLAR IN THE DOD ZERO TRUST MATURITY MODEL (ZTMM)?

A. User

B. Device

C. Network/Environment

D. Hardware

TEST YOUR KNOWLEDGE

7. WHAT IS A KEY METRIC THAT DEMONSTRATES VALIDATED ZERO TRUST MATURITY?

A. Number of tools used

B. Improvements in MTTD and MTTR

C. Security budget percentage

D. Number of frameworks adopted

8. VALIDATED ZERO TRUST SHOULD ONLY EXIST IN CONFIGURATIONS, NOT TESTING.

TRUE

FALSE

9. WHAT IS A KEY BENEFIT OF VALIDATED ZERO TRUST?

A. Eliminates the need for perimeter defenses

B. Prevents all breaches

C. Provides data for executive reporting

D. Requires a single vendor

PAGE LEFT BLANK INTENTIONALLY

Test answers on next page.

ANSWER KEY

1. Answer: B
2. Answer: C
3. Answer: C
4. Answer: A
5. Answer: C
6. Answer: D
7. Answer: B
8. Answer: FALSE
9. Answer: C

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 cybersecurity community through its free, award-winning AttackIQ Academy and its founding research partnership with the MITRE Center for Threat-Informed Defense.

For more information visit www.attackiq.com