EXPERT TIPS INSIDE

VALIDATED ZERO TRUST 101

Brought to you by

ATTACKIQ illumio

FOREWORD

This guide was produced by two cybersecurity companies, AttackIQ and Illumio, and drafted on the basis of our experience advising private and public sector organizations on cybersecurity strategy and operations. It expands on findings we first published in *Lawfare* about how a validated zero trust architecture can help U.S. government civilian agencies defend themselves against SolarWinds-like intrusions. Building on that article, this guide offers specific, practical recommendations for how teams can invest in, build, and operate a validated zero trust architecture and achieve their zero trust goals.

Jonathan Reiber,
Senior Director for Cybersecurity Strategy and Policy, AttackIQ

Matthew Glenn,
Senior Vice President for Product, Illumio

PRIMER: WHAT IS ZERO TRUST?

"The hallmark of zero trust is simplicity. When every user, packet, network interface, and device is untrusted, protecting assets becomes simple." [1]

John Kindervag,
Founder of the Zero Trust Model

[1] https://deloitte.wsj.com/articles/john-kindervag-the-hallmark-of-zero-trust-is-simplicity-01618513330

STUDY PLAN

OBJECTIVES

1. How does an organization evolve towards a zero trust architecture?
2. What is the definition of “validated zero trust” (VZT)?
3. What key technology and organization components are required for validated zero trust?
4. How does the MITRE ATT&CK framework work as part of validated zero trust?

STUDY PLAN

STRUCTURE

1. Learn the basics of zero trust.
2. Identify the value of breach and attack simulation for validated zero trust.
3. Map breach and attack simulation capabilities to components in a zero trust architecture.
4. Outline the steps to evolve to validated zero trust and how it will help security teams.

INTRODUCTION

In December of 2021, the SolarWinds supply chain cyberattack showed the world in dramatic fashion how adversaries that have the time, personnel, imagination, and resources to pursue novel methods of intrusion will succeed in breaking past an organization's defenses. Unlike medieval warfare where large walls could keep an enemy out, in cyberspace, motivated adversaries can and will break past the outer walls of an organization's cyberdefenses.

For this reason, it is time for organizations to pivot and adopt a different cybersecurity mode: zero trust.

Here's an example: In the real world, a navy base's defenses validate every entrance and exit from a secure facility — that includes every person, vehicle or package. Why does a military base adopt this posture? It's simple — they assume that an adversary could already be inside the facility, believing that a breach *might* have already happened.

This is the zero trust mindset.

With the spate of cyberattacks on governments and businesses, organizations need to adopt an assume breach approach and invest in security controls beyond the perimeter — controls that greatly limit the movement of any malware or cybercriminals after they gain a foothold in your network. Assuming breach in cyberspace means to evaluate every interaction with systems and services on the basis if trust should be granted, thereby preventing an adversary from moving freely throughout a network once inside.

From there, security teams need to invest in automated breach and attack simulation capabilities to validate that their zero trust security controls work as intended. This is what it means to operate under a "validated zero trust" architecture. This guide will show you how.

APPROACH

ASSUME BREACH

EVALUATE EVERY INTERACTION TO GRANT TRUST OR NOT

STOP UNAUTHORIZED ADVERSARY MOVEMENT

WHY IS ZERO TRUST SO IMPORTANT?

- Zero trust is transforming the world's approach to cybersecurity. How? In the case of SolarWinds, the intruder harvested (i.e. read) and stole user credentials, and then used those stolen credentials to leverage and travel through communications paths between servers.
- Suddenly, systems that had never tried to communicate with other servers before — and never should have been able to do so — were communicating freely.
- The Internet works in much the same way — next time that you surf to a website that you have never used before, you are taking advantage of the fact that the Internet was designed to find a way to make things connect.
- For organizations affected by Solar Winds, they had little (or more often no) controls stopping these systems from communicating; this creates a huge advantage for an attacker.
- Once they get into a network, they can move freely within it – just as someone who gets behind a gate can move freely within a property.

HOW WOULD ZERO TRUST HAVE PREVENTED THIS FROM HAPPENING?

- Zero trust focuses on a policy of "default-deny," meaning that connections between assets are by default not allowed.

- There is no reason for a low-value server in the U.S. Department of the Treasury used for managing human resources matters, for example, to have a direct connection to a high-value server that hosts the secretary of the treasury's emails.

- A successful zero trust strategy defines acceptable connections between users and technology, including applications and the servers on which they reside, and anything that is not acceptable is denied. This default-deny policy prevents systems from establishing unauthorized connections. In a zero trust network connectivity model, a server cannot even present credentials to another system unless they are explicitly allowed to connect with one another.

- To put it another way: A network that doesn't have zero trust is like a hotel without unique room keys. Once you get past the front door of the hotel, you could effectively get into any room. If an organization implements zero trust, their card key would be required for entry into the hotel, and to enter a guest room, the pool, workout room, and any other segmented space in the hotel.

ZERO TRUST BUT VALIDATE

HOW DOES AN ORGANIZATION MOVE TOWARD A CONTINUOUSLY TESTED ZERO TRUST ARCHITECTURE?

Zero trust cybersecurity provides the necessary level of protection that modern, digital enterprises require, but implementing zero trust effectively can be challenging — just like any other integrated system of people, processes, and technologies.

In a zero trust world, security controls need to be tested and validated. This is no different than the military conducting a simulated attack on their own base.

- The purpose of this guide is to help organizations achieve a continuously validated zero trust architecture, particularly for their most important digital assets.

- A continuously tested architecture "validates" the zero trust claims of that infrastructure. Look at it like a credit check — a person can "claim" good credit but the behavior pattern tells the true story.

This is what it means to assume breach and prevent breaches from spreading. Among other tactics, zero trust defends against credential theft, a tactic in the MITRE ATT&CK® framework that enables an intruder's lateral movement within a data center. (ATT&CK is a publicly available knowledge base of adversary tactics, techniques and procedures.)

In the case of zero trust, even if the secretary of the treasury was targeted and fell victim to malware, the default-deny posture would stop any abnormal communications from her computer, limiting the spread of the breach.

THE VALIDATED ZERO TRUST SECURITY STACK

WHAT TECHNOLOGIES AND PROCESSES SHOULD YOUR ARCHITECTURE INCLUDE TO DEPLOY VALIDATED ZERO TRUST?

A zero-trust security stack includes the following aspects:

- **A zero-trust segmentation capability** to stop attacks from moving between endpoints and within the broader infrastructure. Such platforms build walls where there were no walls. This includes mapping out all communications between applications, containers, clouds, data centers, and networks, allowing only trusted communications to happen around high-value assets.

- **A next-generation firewall** to monitor and filter network traffic between large environments (zones) and agencies. It provides a deep packet inspection and filtering capability to monitor traffic between points on a network and ensure that malicious software is filtered out and stopped. It decrypts, holds, analyzes, and, if necessary, sandboxes files to destroy them if they are determined to present a threat.

- **An automated testing platform aligned to the MITRE ATT&CK framework** and robust cyberthreat intelligence to validate the organization's overall security program effectiveness. This platform should be testing security programs and security controls continuously, at scale, and in a production environment, and should emulate real-world adversary behaviors.

THE VALIDATED ZERO TRUST SECURITY STACK (CONT.)

These investments need to be considered holistically. If one endpoint is compromised, it should not be able to affect other laptops. If one application is compromised, it should not impact other applications. If a large zone is compromised, a security control should prevent the breach from compromising other aspects of the organization and spreading outside the organization.

This strategy looks at an organization's information technology infrastructure and creates compartments around endpoints, applications, and networks in the same way compartments are built within military bases and vessels.

VALIDATING YOUR ZERO TRUST ARCHITECTURE

To achieve validated zero trust means testing these capabilities continuously to ensure that they work and keep intruders from gaining access to your networks and data. What are the practical steps to achieve validated zero trust? How can you validate specific security controls within a zero trust architecture?

A good testing platform will emulate the adversary through all of their modalities across the tactics that are described in the MITRE ATT&CK lexicon, making you successful and credible.

"Since its publication in 2015, the MITRE ATT&CK® framework has become the common language describing real-world adversary behaviors. With the advent of zero trust architectures, it is even more critical that everyone in an organization is working from the same playbook of actual threats. The shared understanding of how adversaries operate provided by ATT&CK is essential – from the design of secure systems through the continuous evaluation of the effectiveness of security controls and capabilities."

- Rich Struse, Director, MITRE Engenuity's Center for Threat-Informed Defense

VALIDATING YOUR ZERO TRUST ARCHITECTURE (CONT.)

NEXT GENERATION FIREWALL

To ensure validated zero trust, you will also need to test and validate in-line network firewalls, like a next generation firewall.

A strong testing platform supports end-to-end validation of network-deployed security controls and gives technology-specific remediation guidance, ensuring that customers get the most out of their cyberdefense investments.

A next generation firewall is a multi-layered protection device.

- Next generation firewalls conduct in-line advanced anti-malware through a combination of stream-based file inspection and file behavior analysis.

- From a stream-based analysis, a next generation firewall serves as a man-in-the-middle to decrypt a file, hold a file, assemble it, hash it, and compare it through the behavior of a library of known files to determine whether it's a known good file, a known bad file, or an unknown file type.

- If the file is a known bad file or an unknown file, it puts the file into a sandbox to assess the file's memory, what's on the disk, and its processes and determines whether or not it needs to be destroyed.

VALIDATING YOUR ZERO TRUST ARCHITECTURE (CONT.)

VALIDATING NEXT GENERATION FIREWALLS

An effective breach and attack simulation platform will transmit files through network traffic and play back captures of known adversary behavior.

In the case of the WannaCry malware, for example, it spreads over protocols in a *worm-based propagation*.

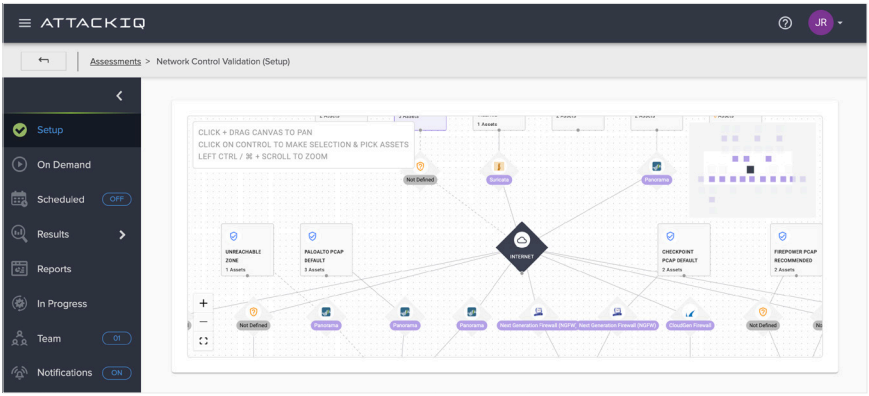
- In this instance, one system gets infected and immediately starts trying to infect as many targets as it can find by putting out network communication.

- It sends a Server Message Block, Application ID, or begins to upload a file. A next generation firewall will ask: what is someone trying to transfer? Is this a file I should move? Or should I sandbox it?

VALIDATING YOUR ZERO TRUST ARCHITECTURE (CONT.)

A strong adversary emulation platform preserves what the adversary communication patterns look like, and has the technological capabilities to make communication happen between two of the test points in the network to assess the next generation firewall.

The platform will then evaluate production level security controls to determine whether the malware (i.e. WannaCry) can spread past the inspection point between the two points. It will also allow you to test for data loss prevention by attempting to exfiltrate beyond the organization.



Figue 1: NGFW / NCV Testing Integration

SECURITY SEGMENTATION

The practice of security segmentation (or zero trust segmentation) builds policy-enabled walls between workloads, applications, and servers to permit only authorized access, preventing bad actors from moving laterally throughout an organization. It uses a default-deny white list natural language policy to control access.

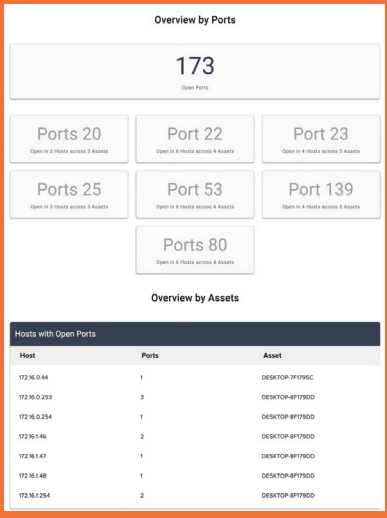


Figure 2: AIQ/Illumio Scanning/Workload Evaluation

VALIDATING SECURITY SEGMENTATION

A strong breach and attack simulation platform will emulate the adversary to test how well segmentation policies work.

- First, it should discover open ports and closed ports to determine the degree of exposure within the organization.
- Second, it should validate the organization's segmentation policy effectiveness between workloads, applications, and servers to guarantee effectiveness. Security segmentation helps ensure an effective zero trust strategy, in-depth, but only if it can be validated from multiple perspectives and in a continuous fashion.
- The goal is to evaluate whether or not targeted adversary communications of particular types are blocked or permitted based on the result of your segmentation policies.

CONCLUSION

We have discussed some of the capabilities that require testing for validated zero trust: next generation firewalls and security segmentation capabilities. Components that matter for effective cybersecurity validation and readiness include:

- Automated Adversary Emulations to stay current with threats by using an intelligence-based automated emulation platform that validates security effectiveness. A sophisticated breach and attack simulation platform constantly integrates threat streams and threat intelligence into the adversary emulation processes to stay ahead of current threats. You can also build your own emulations using current threat intelligence if you have the tools.

- Purple team operations can help move the organization towards a validated zero trust architecture by increasing security operations effectiveness. Traditionally, blue and red teams operated as separate organizations, with blue teams managing defensive operations and red teams, often outside of the organization, conducting annual or semi-annual tests of the security program. Such testing is sporadic and ineffective and doesn't provide sufficient coverage to determine whether the zero trust architecture works as it should. For more on how to move your teams to a purple team construct, check out the Purple Teaming for Dummies guide.

- The MITRE ATT&CK framework keeps your team focused on known threats and helps you prioritize defensive operations. Pairing the thorough, detailed MITRE ATT&CK framework with an automated breach and attack simulation (BAS) platform enables your security organization to routinely emulate the attacks that will most likely threaten you. Red and blue teams work together in a purple team construct to:
  - Design the testing regimen
  - Jointly identify security control errors and gaps
  - Undertake mitigation measures
  - Retest to validate that their security controls are effective

---

CONCLUSION (CONT.)

To achieve these steps in a zero trust environment, security leaders can begin to transition the team toward a purple team construct. The transition isn't simple. It involves building communication channels and fostering consensus and collaboration among groups of professionals who've historically seemed to operate on opposite sides of security testing.

The effort will pose challenges, but security leaders can bring red and blue teams closer until their knowledge and perspectives begin to blend into a unified team to validate zero trust. The process of continuous testing will give the management team data-driven control over their security program's overall performance to ensure a successful zero trust architecture.

That's what it means to operate under validated zero trust.

TEST YOUR KNOWLEDGE!

1. Which of the following is not a function of historic zero trust?

a. Automatically tests your security controls to ensure that they work as intended
b. Denys unauthorized communications between devices
c. Stops intruder's lateral movements
d. Monitors internal traffic and maps application dependencies

2. What are some key capabilities to deploy validated zero trust?

a. Antivirus, endpoint detection and response, email filtering
b. NIST Cybersecurity Framework, blue teaming, vulnerability scanning
c. Automated back-up, machine learning, data loss prevention
d. Next generation firewall, security segmentation, breach and attack simulation

3. A validated zero trust architecture needs to be able to test a next generation firewall's sandbox capability:

☐ TRUE
☐ FALSE

TEST YOUR KNOWLEDGE!

4. Security segmentation focuses on pre-breach activities at the perimeter:

- ☐ TRUE
- ☐ FALSE

5. What are three management components required for validated zero trust?

a. The NIST framework; incident response; vulnerability scanning
b. Zero day discovery; continuous monitoring; threat intelligence collection.
c. Adopt MITRE ATT&CK; organize as a purple team; conduct continuous testing.
d. Build inventory of IT assets; develop risk profile; determine budget

6. Which of the following is not a recommendation for moving to validated zero trust?

a. Use at least three threat frameworks like MITRE ATT&CK, NIST, and COBIT
b. Continuously test your cybersecurity capabilities
c. Adopt a "blue team" mindset that is focused on identifying threats in the operating environment
d. Adopt a "purple team" mindset that brings teams together to counter attacks.

TEST YOUR KNOWLEDGE!

7. Fill in the blank:
MITRE ATT&CK is a framework of _____ (TTPs).

a. Adversary tokens, tickets, and plans
b. Adversary tactics, techniques, and procedures
c. Adversary temperament, transactions, and prescriptions
d. Adversary tips, taxonomy, and patterns

8. One major positive aspect of zero trust is that it keeps intruders from breaking past your perimeter defenses:

☐ TRUE
☐ FALSE

9. Which is a key benefit of validated zero trust?

a. Deters nation-states from conducting advanced cyberattacks
b. Validates that security controls work to prevent unauthorized access
c. Will help cybersecurity teams better manage their program budgets
d. Creates a single, secure network architecture for vendors and customers

PAGE LEFT BLANK INTENTIONALLY

Test answers on next page.

ANSWER KEY

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

ABOUT ATTACKIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to identify security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity's Center for Threat Informed Defense.

For more information visit www.attackiq.com

ABOUT ILLUMIO

Illumio, the pioneer and market leader of Zero Trust Segmentation, stops breaches from becoming cyber disasters. Illumio Core™ and Illumio Edge™ automate policy enforcement to stop cyberattacks and ransomware from spreading across applications, containers, clouds, data centers, and endpoints. By combining intelligent visibility to detect threats with security enforcement achieved in minutes, Illumio enables the world's leading organisations to strengthen their cyber resiliency and reduce risk.

For more information visit www.illumio.com