changeis»

CHANGEIS INSIGHTS

Jeremy Hudson

Jeremy Hudson has over 15 years of experience in technology, cybersecurity, and cloud security architecture. He currently serves as Information Security Architect for the FAA Logistics Center in Oklahoma City, OK.

Contact Changeis

www.changeis.com
info@changeis.com
(703) 348-9669

Understanding Zero Trust Security

While the Zero Trust theory may not have coined the phrase *Never Trust, Always Verify* the continued growth in the frequency and scale of security threats across the IT domain ensures this to be a startling yet applicable theme. According to IBM's Cost of Data Breach Report, 2021, the United States has the world's highest data breach costs, averaging out at a whopping $8.6M **per attack**. If the gut punch of that dollar value doesn't impact the degree of concern in IT Security, it is worth noting that by September 2021, the Identity Theft Resource Center (ITRC) reported that data breaches had already exceeded those experienced in 2020 by 17% – not a trend to be enthusiastic about.

Both leaders and program offices have a responsibility to support the identification and mitigation of potential security risks for their respective organizations. Fulfilling that task goes far beyond stronger passwords. This is about a risk management approach, founded in the principles and maturity model levels of Zero Trust that enable organizations to combat these trends.

What is Zero Trust?

Zero Trust in IT Security is not a new concept but has recently become a buzzword in the world of IT best practices. Dr. Stephen Paul Marsh from the University of Stirling in Scotland coined "Zero Trust" almost 30 years ago when he wrote his doctoral thesis on the computational security strategy.

In simple terms, Zero Trust (ZT) is an approach to IT security designed to minimize uncertainty in enforcing decisions for IT user access, while providing only the minimal system access needed.

Dr. Marsh suggested that the concept of Zero Trust rises above factors of human behavior such as morality, ethics, lawfulness, justice, and judgement. Marsh ascertained that Zero Trust could possibly help with the very real threat to the security of computing, applications, and network systems.

We are all aware of the problems with traditional network security. McAfee defines traditional network security architecture and its' inherent risk as "firewalls, Virtual Private Networks (VPNs), access controls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Security Information Event Management (SIEM) tools, and email gateways … that cyber attackers have learned to breach."

What strategic concepts are involved in moving from traditional to Zero Trust security?

Zero Trust Security focuses on approaches to security such as:

- Creating perimeter control through identities, with an emphasis on strengthening user authentication and identity verification, thus eliminating security breaches involving stolen credentials
- Reducing implicit trust zones while maintaining availability and minimizing temporal delays in authentication mechanisms
- Creating granular access rules and policies to ensure enforcement of least privileges needed to perform the action in the request

The figure below shows a general access scheme. Zero Trust access is granted through a policy decision point (PDP) and corresponding policy enforcement point (PEP).

Adapted from NIST 800-207

Are there guidance resources?

In late 2018 the National Cybersecurity Center of Excellence (NCCoE), a group of cyber security researchers, created the National Institute of Standards and Technology (NIST) Special Publication 800-207 on Zero Trust Architecture.

NIST 800-207 provides an operational definition for Zero Trust Architecture:

"Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a Zero Trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan."

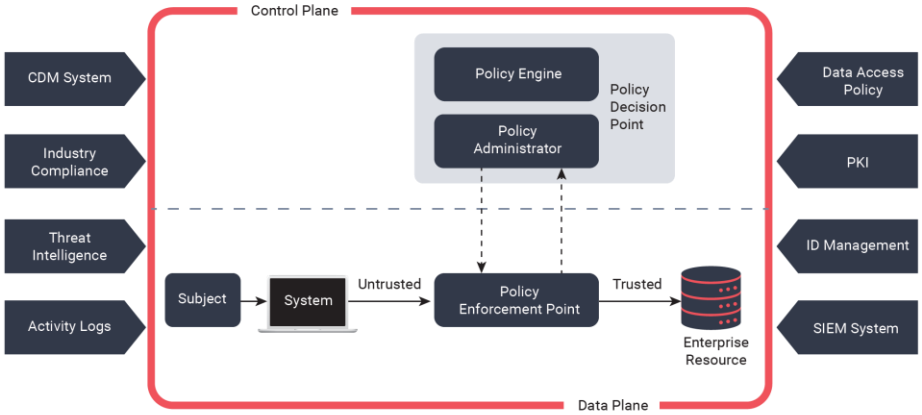
The NIST publication summarizes the requirements for a Zero Trust Architecture as follows:

Requirements / Basic Tenets (*NIST 800-207 – Zero Trust p 7*)

1. All data sources and computing services are considered resources
2. All communication is secured regardless of network location
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.

5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

As shown below, enterprise policies and enforcement of those policies are central to an effective Zero-Trust enterprise.



Adapted from NIST 800-207

The full enterprise private network is not regarded as an implicit trust zone. To design and implement a Zero Trust Architecture, several assumptions must be considered. First, it should be recognized that devices on the network may not be owned or configured by the enterprise, and local network connections of enterprise subjects and assets cannot be trusted. Secondly, resources may not reside on enterprise-owned infrastructure, and none can be inherently trusted. Finally, a consistent security policy is needed for assets and workflows between enterprise and non-enterprise infrastructure.

Implementing Zero Trust Architecture over traditional security can strengthen your IT security. Whether your organization is moving toward Department of Defense (DoD) requirements for cybersecurity or is proactively updating security in a world of remote work, Zero Trust should be considered. As recent as September 2021, the Cybersecurity and Infrastructure Security Agency (CISA) publicized a draft Zero Trust Maturity Model for utilization by civilian agencies in response to President Joe Biden's May Executive Order on Zero Trust implementation. Coupled with the Office of Management and Budget (OMB) push for agency Zero Trust compliance by 2024, Zero Trust isn't going away.

For sources, visit https://changeis.com/strategy/understanding-zero-trust-security/

Changeis' Core Capabilities

Strategy & Change Management

Changeis develops and executes strategies to maximize our customers' success. We apply in-depth industry knowledge, analytics expertise, and strategic acumen to design the right solution for their unique needs. Once the strategy is in place, we help customers communicate these changes and promote adoption among stakeholders.

Large Scale IT Solutions

In the age of digital business, organizations need highly flexible and responsive IT capabilities. This often means modernizing their legacy technology.

Changeis realizes large-scale IT transformation projects from conception to implementation — resulting in efficiency, automation and streamlined workflows through digital operations.

Investment & Acquisition Management

We help organizations obtain the resources they need to implement their strategic plans and initiatives. Rigorous data management, analytics tools, and compelling writing form the bedrock of our deliverables for customers.

Program Management Office (PMO) Support

We provide governance to ensure that strategies are implemented effectively, and that deliverables support organizational goals. Our services include resource management, risk management, performance management, and portfolio and program development and management.

Innovation & Optimization Management

There are major optimization opportunities within every organization. We help our customers identify and capitalize on them. Examples of some of our toolkit include Life Cycle Planning and Support, Technology Strategy and Systems Integration, Business Intelligence and Supply Chain Management.