Zero Trust Fundamentals

What is Zero Trust?

- Zero Trust is a security model, strategy, and framework that trusts nothing by default.
  - ✓ Never Trust, Always Verify
  - ✓ Assume Breach
  - ✓ Verify Explicitly
  - ✓ Least Privileged Access

It's not a singular technology.

No singular authoritative definition of Zero Trust.

Basic Assumptions

- The Network Is Assumed to Be Hostile
- External and Internal Threats Are Always Present
- Network Locality Isn't Sufficient for Determining Trust
- Every Single Device, User, and Network Flow Is Authenticated and Authorized With Dynamic Policies

Key Takeaway: Zero Trust is a strategy and framework similar to how ITIL is for IT service management, and Agile is project management.

Some Zero Trust Definitions

Zero Trust is a **security model**, a set of **system design principles**, and a coordinated cybersecurity and system management **strategy** based on an acknowledgment that threats exist both inside and outside traditional network boundaries.[1]

Zero Trust is a **conceptual framework** that commits to removing implicit trust within the IT ecosystem, replacing it with a risk-based approach that **continuously verifies** each connection and implements granular access control to enterprise resources.[2]

Zero Trust is the name for an approach to IT security that assumes there is no trusted network perimeter, and that **every network transaction must be authenticated** before it can transpire.[3]

Key Takeaway: Zero Trust is an improvement on the traditional perimeter security model, which is insufficient in modern IT infrastructure environments.

[1] National Security Agency: Embracing a Zero Trust Security Model
[2] Deloitte: Zero Trust Access
[3] VMWare: What is Zero Trust?

Never Trust, Always Verify

- Trust isn’t implicit in Zero Trust.
- Trust is a vulnerability.
- Every device, user, and request is treated as a potential threat until thoroughly verified.
- Utilizes **Just-in-Time** and **Just-Enough-Access** least privilege access controls.

Key Takeaway: Zero Trust trusts no one and nothing by default and assumes all devices, users, and requests are a potential threat until proven otherwise.

Zero Trust Enterprise

Zero Trust (ZT)

- A security model, framework, and strategy.

Zero Trust Architecture (ZTA)

- An organization's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.[1]

Zero Trust Enterprise = ZT + ZTA

[1] NIST SP 800-207: Zero Trust Architecture

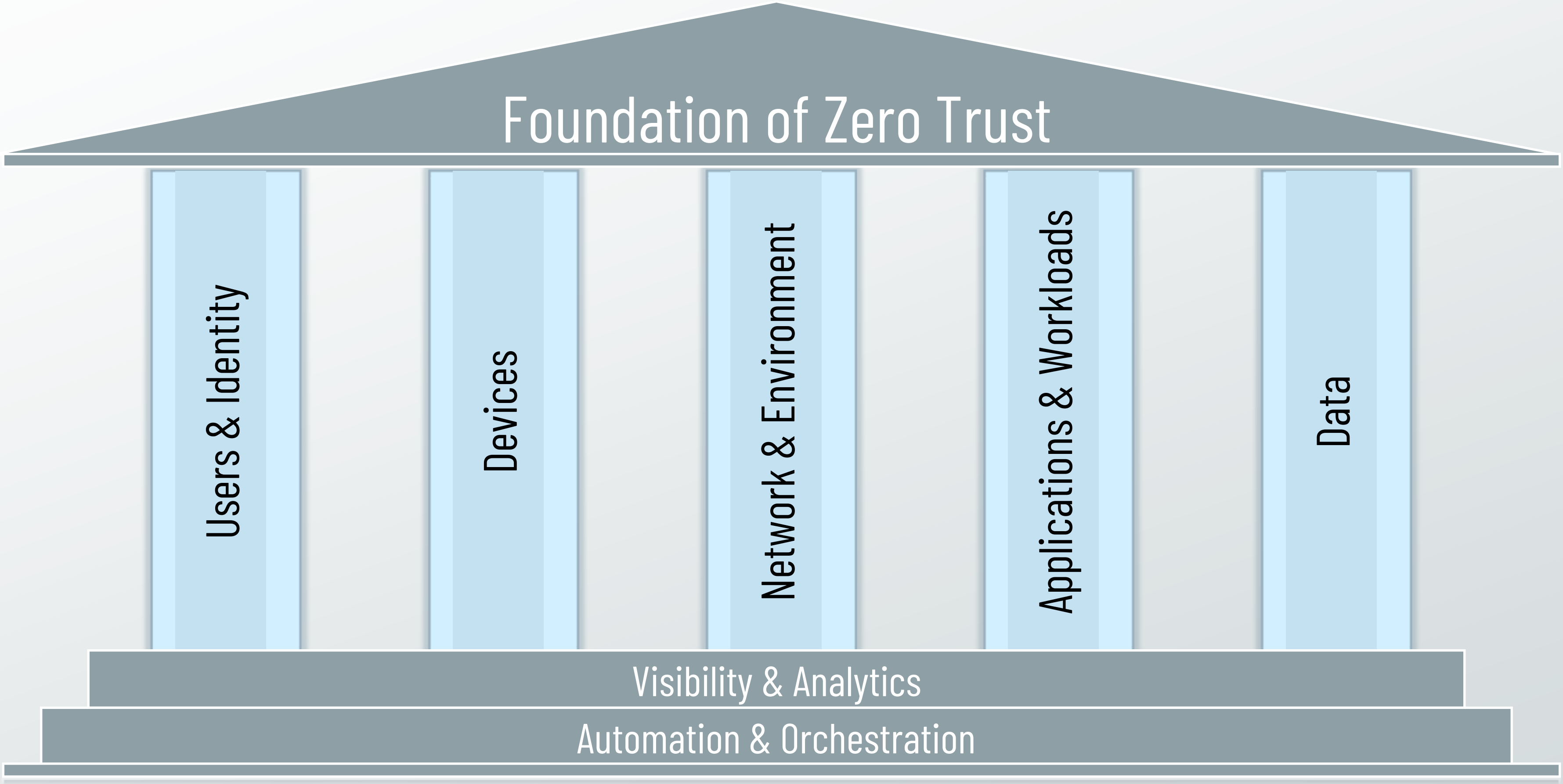
Tenets of Zero Trust

Seven Tenets of ZTA

- **Consider Every Data Source and Computing Device as a Resource**
  Any device with network access is considered a resource.
- **Keep All Communication Secured Regardless of Network Location**
  Regardless of location, all communication should be done securely.
- **Grant Resource Access on a Per-session Basis**
  *Users should be granted **Just-in-Time** and **Just-Enough-Access** least privilege access.*
- **Moderate Access With a Dynamic Policy**
  Dynamic attribute-based policies that consider the state of a user and asset.
- **Maintain Data Integrity**
  Continuously monitor the integrity and security posture of devices and applications.
- **Rigorously Enforce Authentication and Authorization**
  Utilize robust identity and access management with multi-factor authentication.
- **Gather Data for Improved Security**
  Collect and aggregate data to improve the organization's security posture.

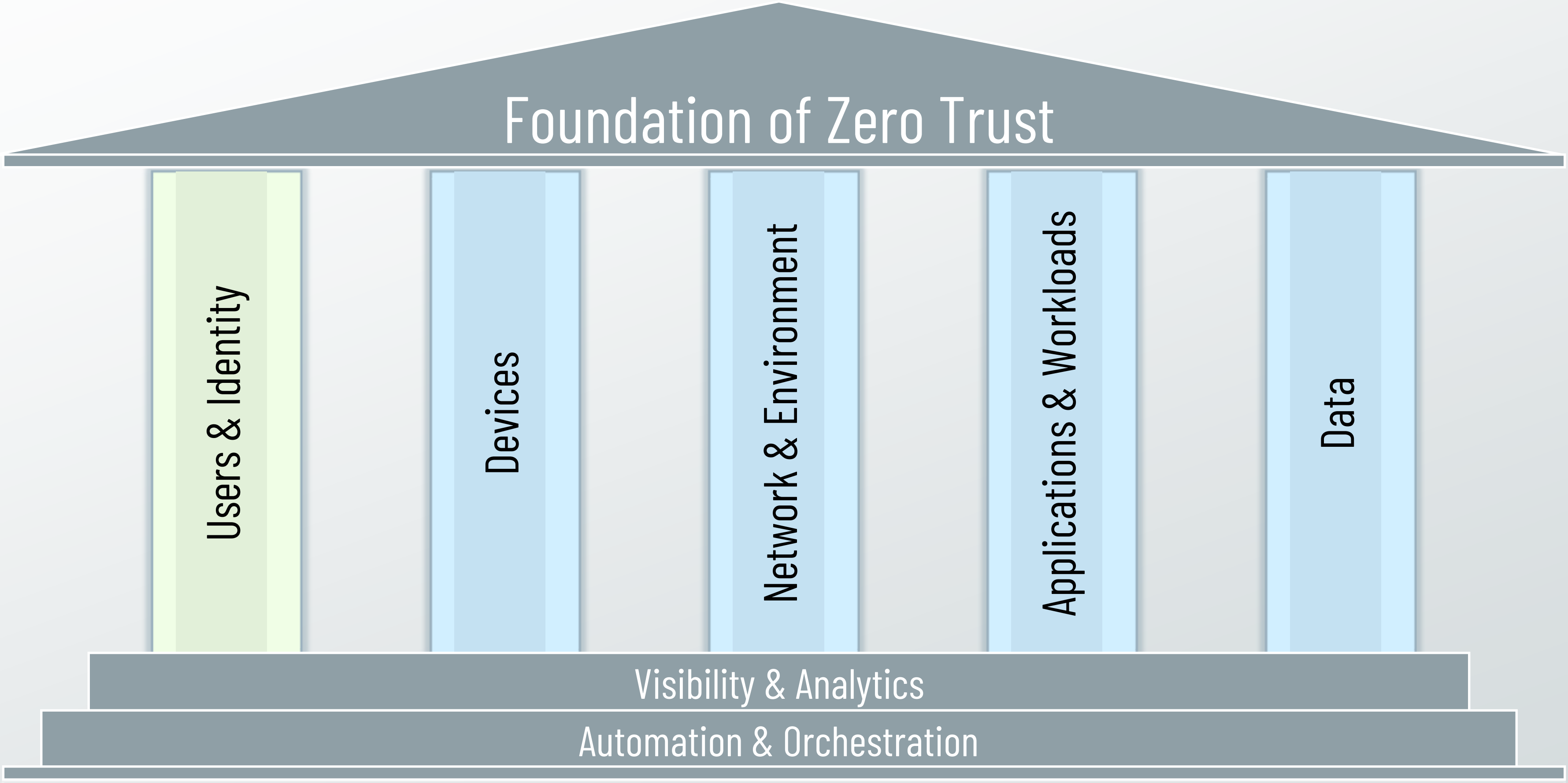
NIST SP 800-207: Zero Trust Architecture

Zero Trust Pillars



1. GSA and DoD Zero Trust Pillars

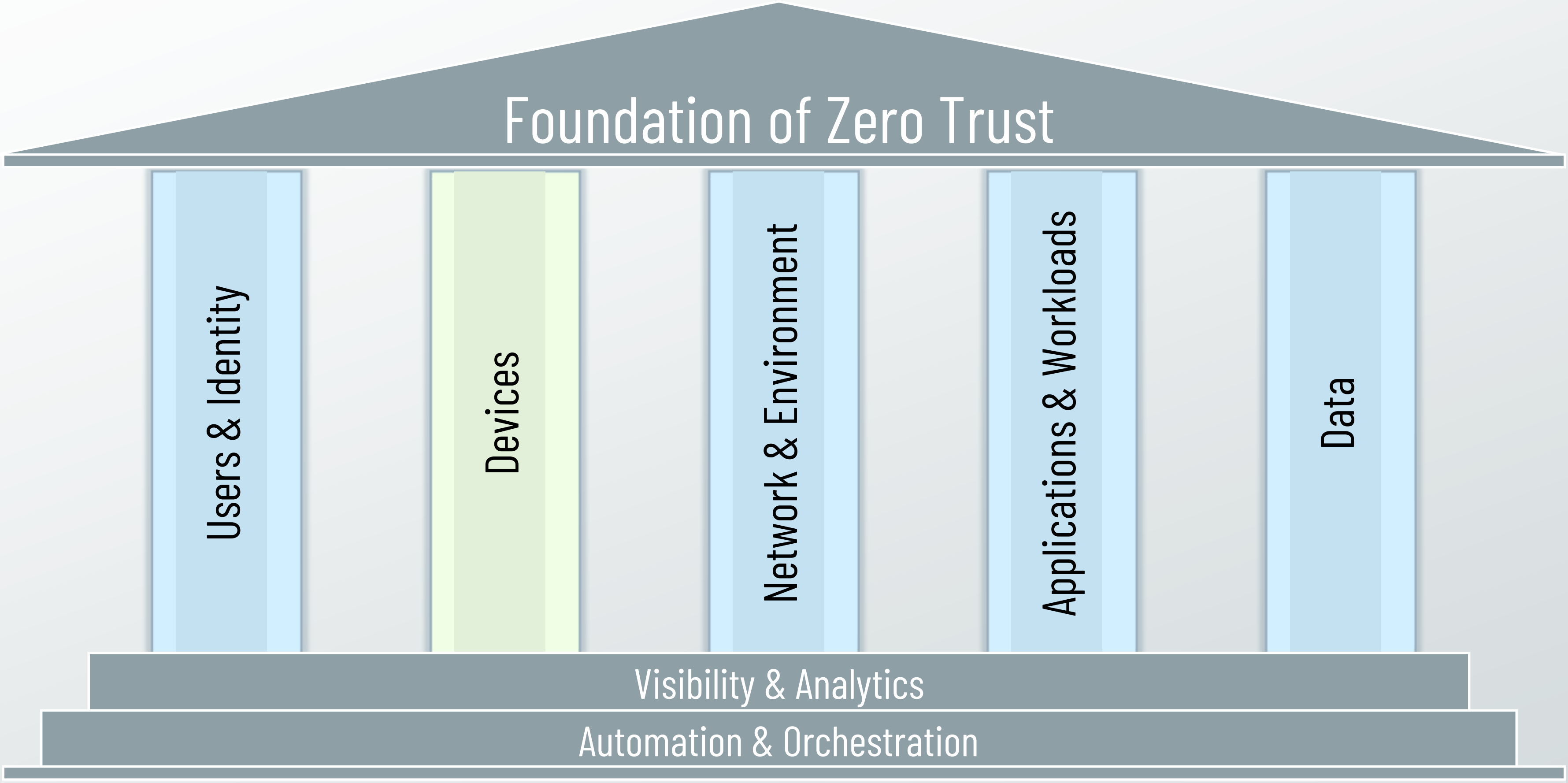
Zero Trust Pillars



The Users & Identity Pillar focuses on user identification, authentication, and access control policies using dynamic and contextual data analysis.[2]

1. GSA and DoD Zero Trust Pillars
2. GSA: Zero Trust Architecture: Acquisition and Adoption

Zero Trust Pillars



Foundation of Zero Trust

Users & Identity

Devices

Network & Environment

Applications & Workloads

Data

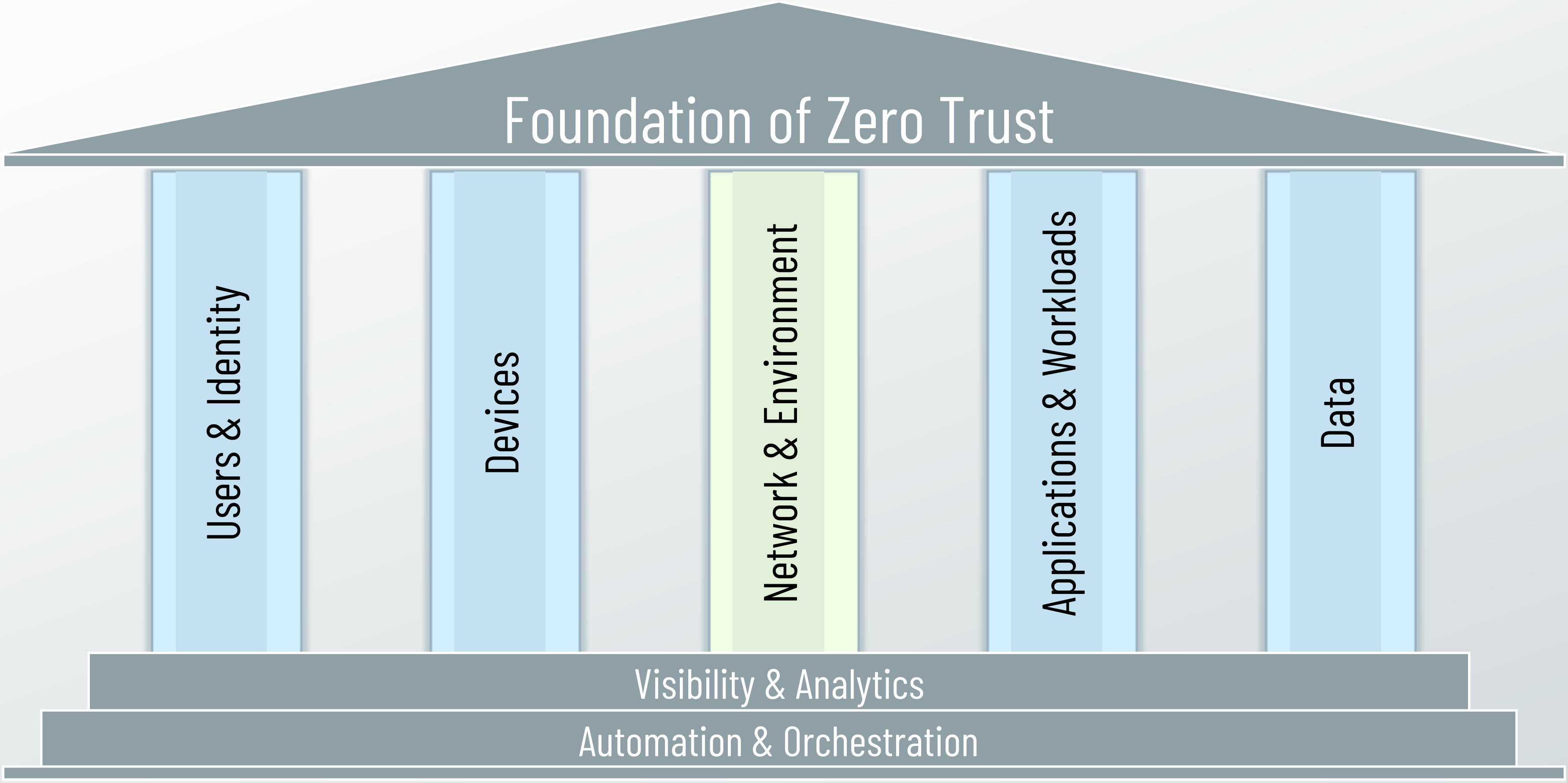
Visibility & Analytics

Automation & Orchestration

The Devices Pillar performs validation of user-controlled and autonomous devices to determine acceptable cybersecurity posture and trustworthiness.[2]

1. GSA and DoD Zero Trust Pillars
2. GSA: Zero Trust Architecture: Acquisition and Adoption

Zero Trust Pillars

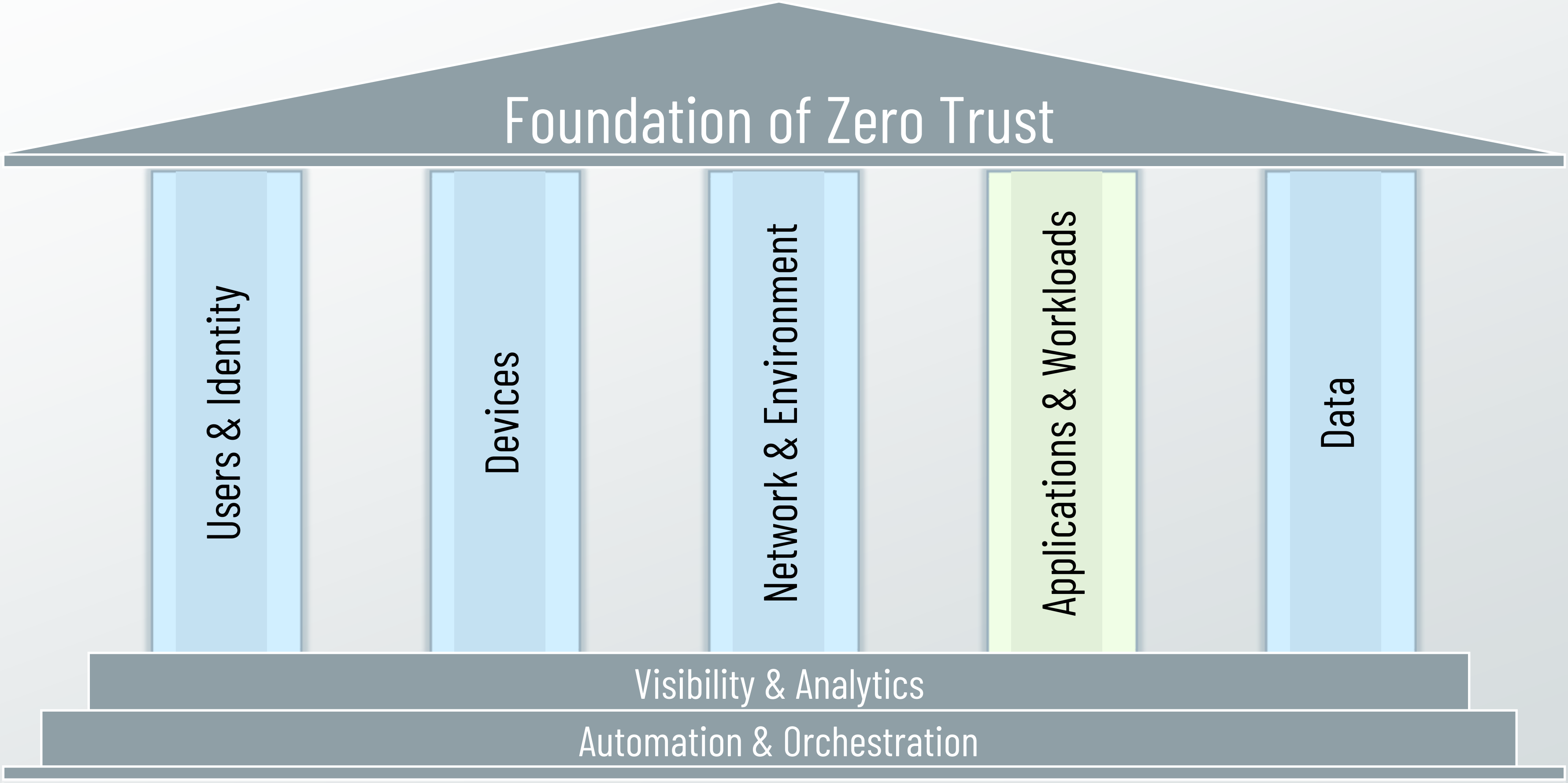


The Network & Environment Pillar segments, isolates, and controls the network environment with granular policy and access controls.[2]

[1] GSA and DoD Zero Trust Pillars

[2] DoD Zero Trust Strategy

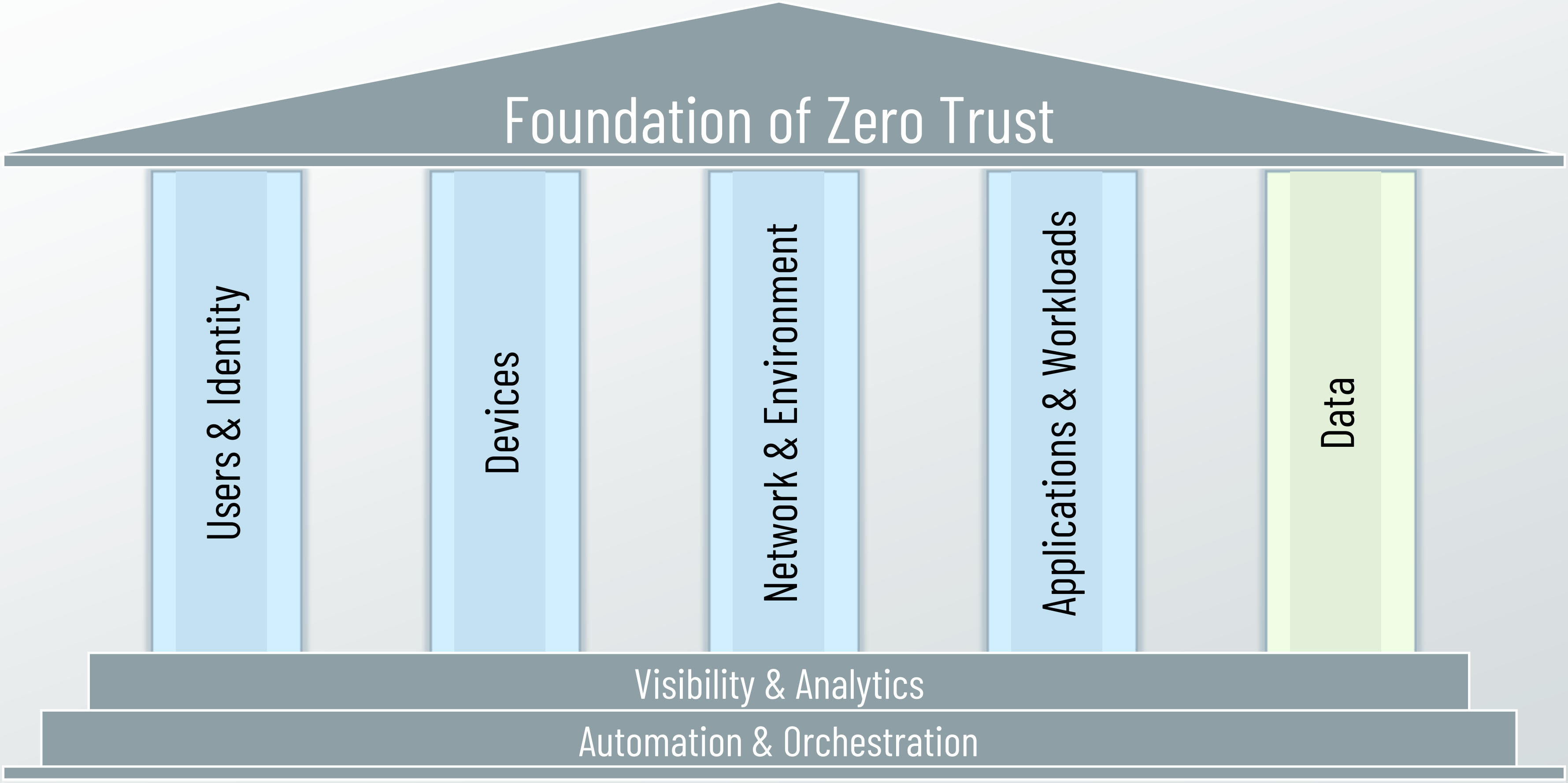
Zero Trust Pillars



The Applications & Workloads Pillar secures everything from applications to hypervisors, including containers and virtual machines.[2]

1. GSA and DoD Zero Trust Pillars
2. DoD Zero Trust Strategy

Zero Trust Pillars

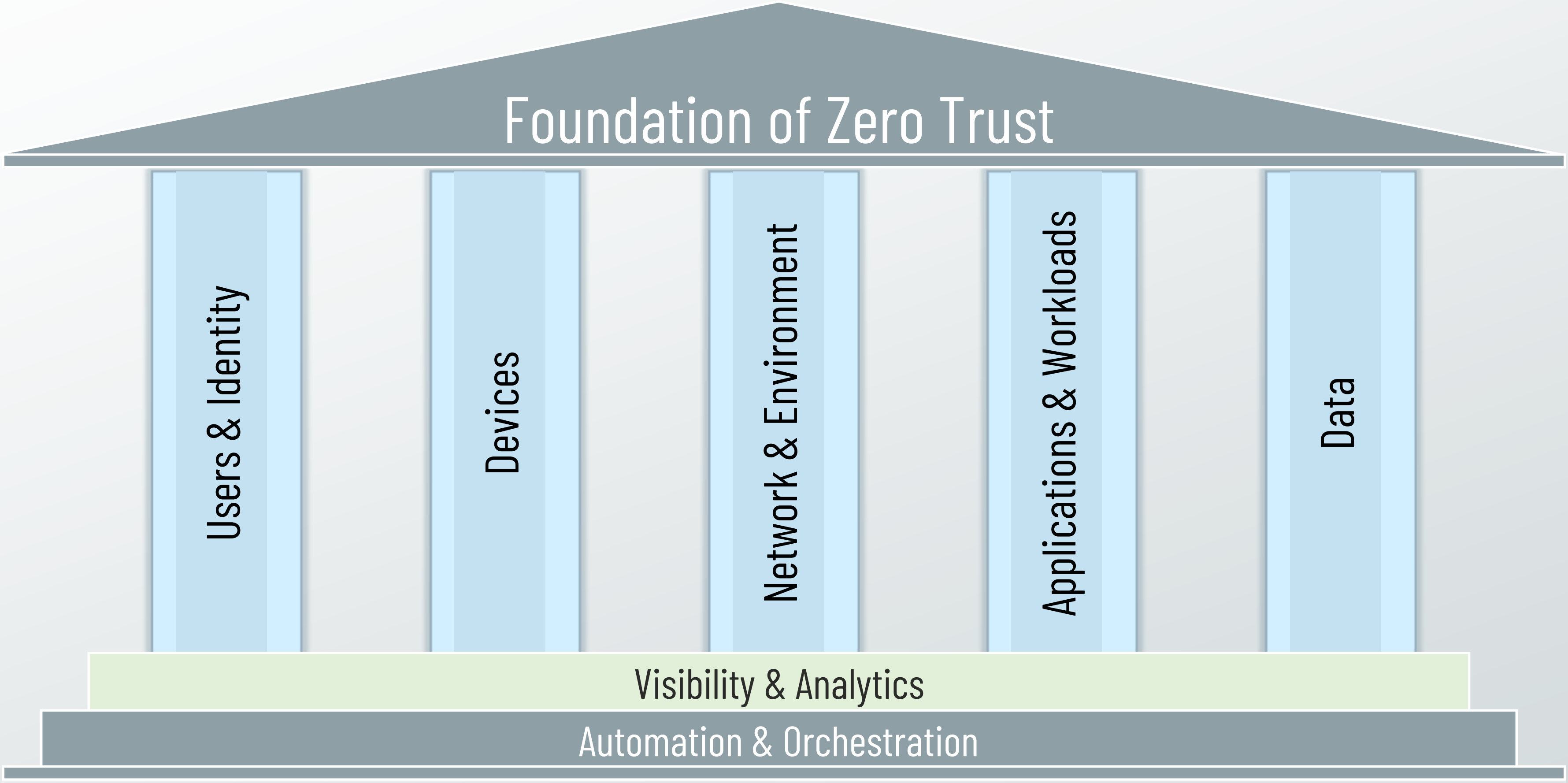


The Data Pillar focuses on securing and enforcing access to data based on an data's categorization and classification to isolate the data from everyone except those that need access.[2]

[1] GSA and DoD Zero Trust Pillars

[2] GSA: Zero Trust Architecture: Acquisition and Adoption

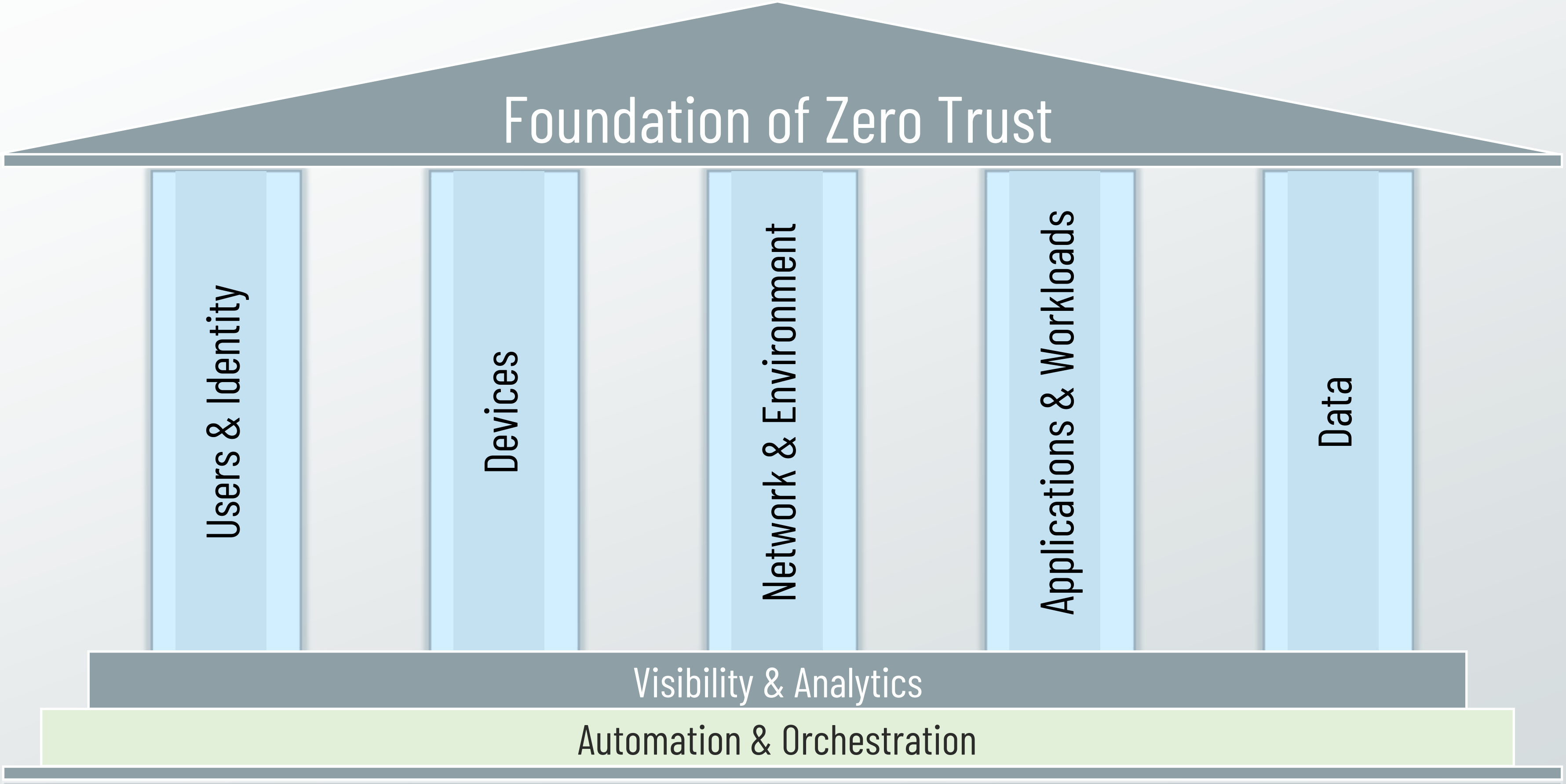
Zero Trust Pillars



Visibility & Analytics provide insight into user and system behavior by observing real-time communications between all Zero Trust components.[2]

[1] GSA and DoD Zero Trust Pillars
[2] GSA: Zero Trust Architecture: Acquisition and Adoption

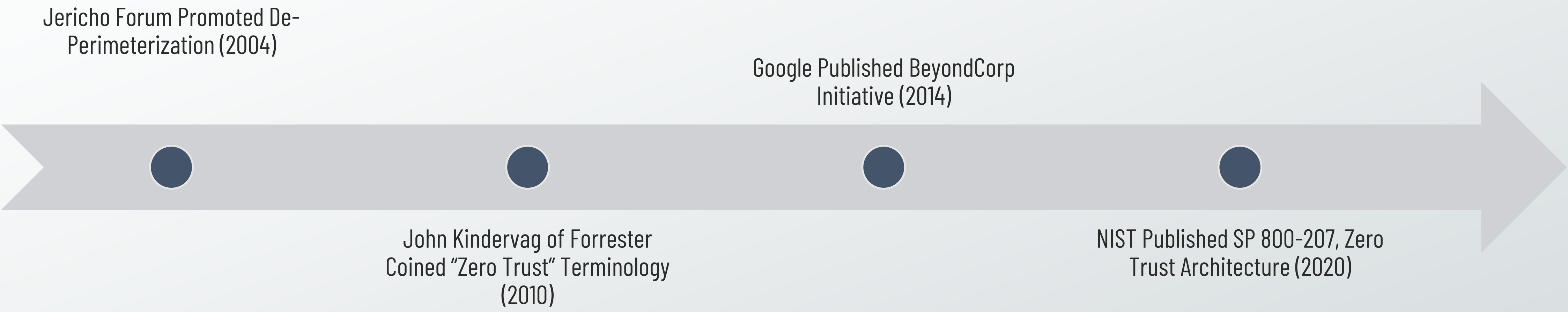
Zero Trust Pillars



Automation & Orchestration automates security and network operational processes across the ZTA by orchestrating functions between similar and disparate security systems and applications.[2]

1. GSA and DoD Zero Trust Pillars
2. GSA: Zero Trust Architecture: Acquisition and Adoption

Zero Trust Has Been Around for Awhile



Jericho Forum Promoted De-Perimeterization (2004)

John Kindervag of Forrester Coined "Zero Trust" Terminology (2010)

Google Published BeyondCorp Initiative (2014)

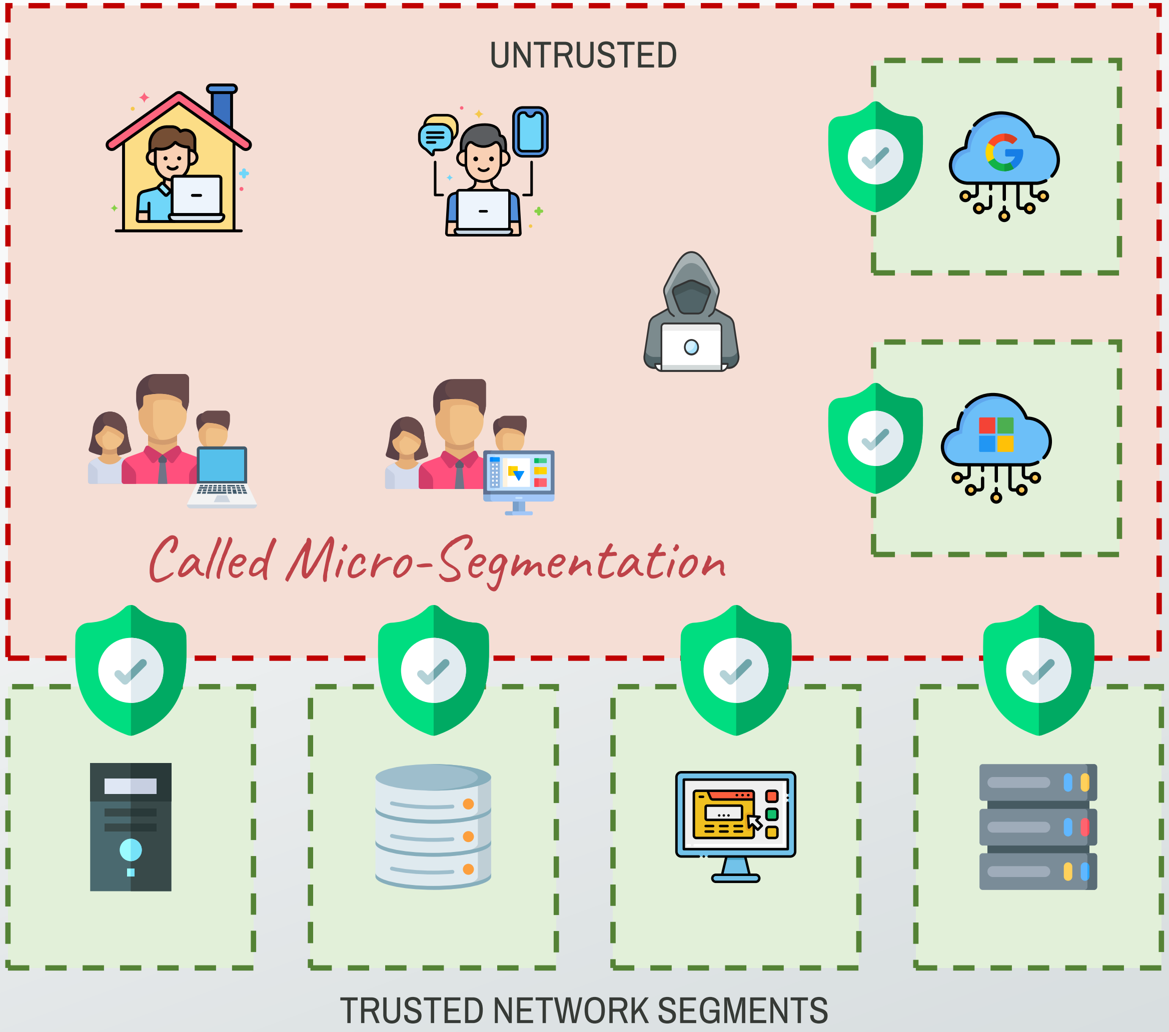
NIST Published SP 800-207, Zero Trust Architecture (2020)

Key Takeaway: Zero Trust isn't a new IT security strategy; it's been around for a while.

A Glimpse Into Zero Trust Architecture

INSTRUCTOR ALTON

Introduction to ZTA



Zero Trust Architecture

- All Users and Associated Devices Are Untrusted
- Trusted Network Broken up Into Segments
  - ✓ Protects Individual Business Assets & Resources
  - ✓ Minimizes the Blast Radius by Preventing Lateral Movement
- Cloud Services Are Segmented as Well
- Segments Protected by Intelligent Policy Decision Point