Zero Trust:

The Key to Non-Kinetic Dominance in Multi-Domain Operations

TechNet Augusta 2025

zscaler™

Speaker Today

Rich Johnson

Zscaler

As a Principal Sales Engineer, Rich Johnson works with Zscaler's DoD and federal customers to solve their most challenging technical challenges. He leverages his 35 plus years of experience in the IT and cybersecurity industry to assist agencies with their migration to cloud computing and zero trust architectures. Rich is a certified ethical hacker and enjoys studying the adversary's tactics and working with agencies to build a strong cyber security defense.

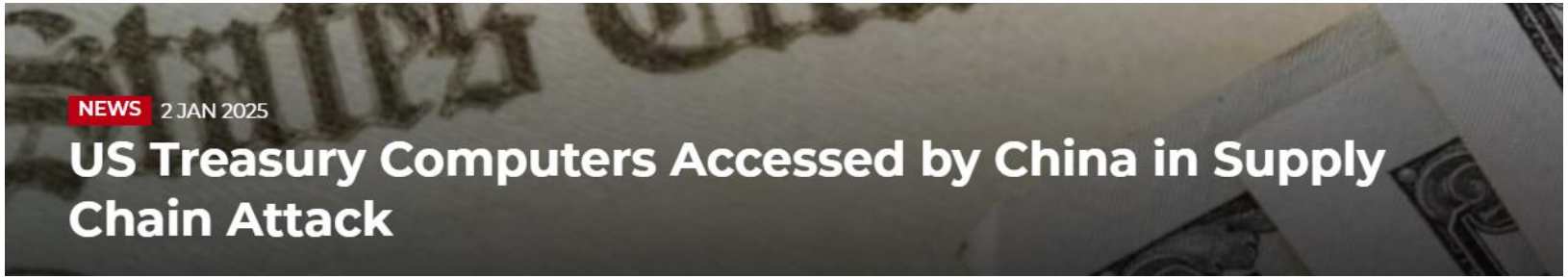
Zero Trust: The Key to Non-Kinetic Dominance in Multi-Domain Operations

Non-kinetic dominance in multi-domain operations relies on secure, resilient, and adaptive systems that support operational readiness across land, sea, air, space, and cyberspace. The Department of Defense (DoD) Zero Trust Strategy, released in October 2022 by the Zero Trust Portfolio Management Office (PfMO), serves as a critical framework for addressing modern threats. It outlines the activities and outcomes needed to achieve Target and Advanced Zero Trust implementation levels, with the Target level representing the minimum standard to secure the Department's Data, Applications, and Assets (DAAS) against known risks.

This strategy, informed by work from NIST, DISA, NSA, and CISA, defines core Zero Trust capabilities vital for securing multi-domain operations. Organizations can leverage a structured approach to address the 91 Target and 61 Advanced activities while laying a strong foundation for enduring non-kinetic operational superiority. Foundational Zero Trust capabilities help identify and close security gaps, preparing organizations to handle complex mission requirements. By integrating these elements, Zero Trust serves as a transformative enabler in achieving operational resilience and dominance across today's interconnected and dynamic battlespace.

Cyber is the Non-Kinetic Weapon of choice

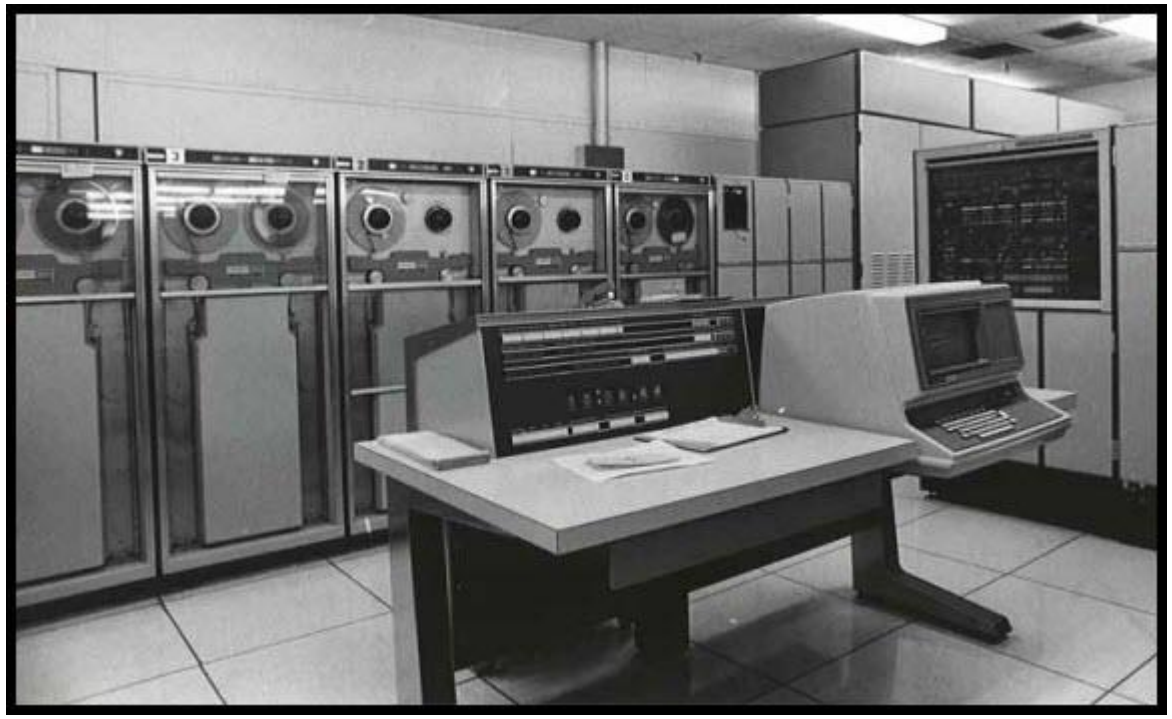
Iran nuclear attack: Mystery surrounds nuclear sabotage at Natanz

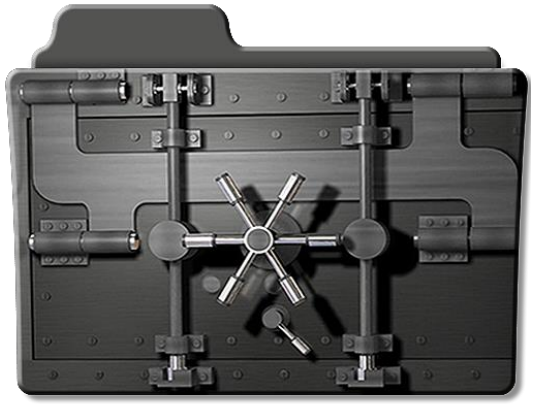


The Era of Blind Trust

The good ol' days of computing

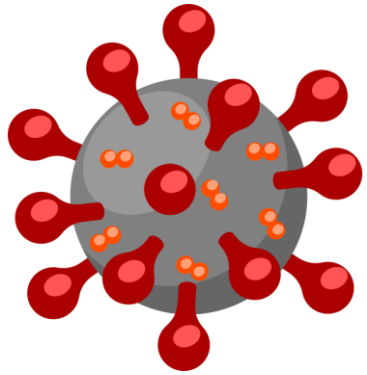
- During the period of time from the 40s to the early 80s nobody really thought twice about cyber security.
- The ARPANET, the predecessor to the Internet, was being used to tie computers together for the purpose of research, and TCP/IP was a brand-new protocol for facilitating this communication.





PHYSICAL PERIMETER SECURITY

Pandora's Box



Good intentions – bad results

The "Creeper" program demonstrated that self-replicating malicious programs were possible and by the mid-80s, computer viruses such as "Brain Boot Sector" and "LoveLetter" were proving that cyber security was a real threat that needed to be taken seriously.

Timeline of Significant Cyber Events

The Era of Naïve Trust

- The false assumption that the Local Area Network could be a safe place if we could secure the perimeter and ensure that devices met our “comply to connect” policies before being connected to our “safe” networks.

- This network centric approach to security proliferated for decades and was ingrained into the minds of every up-and-coming network engineer.

- This idea that we could achieve our goals of security, if we carved up the network into virtual segments with controlled access to those segments, was fundamentally flawed. It was flawed, because it overlooked the human element and the dynamic constantly evolving security state of endpoints on the network itself.

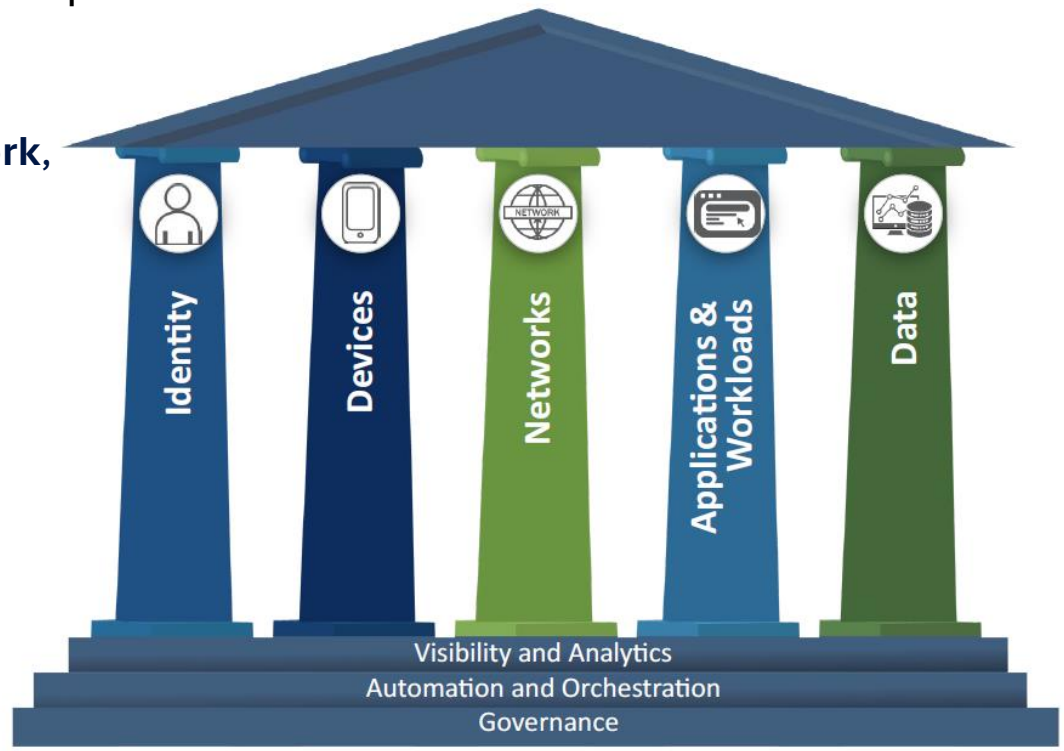
Enter the Era of Zero Trust

The wake-up call

- Putting band-aid on band-aid will never achieve the desired goal

- Rip off the band-aids off and started with a fresh new **ground-zero**, treating the problem systematically and thoroughly from the ground up.

- The 5 main areas of trust, the **Device**, **User**, **Network**, **Application**, and the **Data** itself are all called into question.
- Two supporting areas, **Analysis/Logging** and **Automation/Orchestration** exist to build a continuous cycle of interrogation and validation.



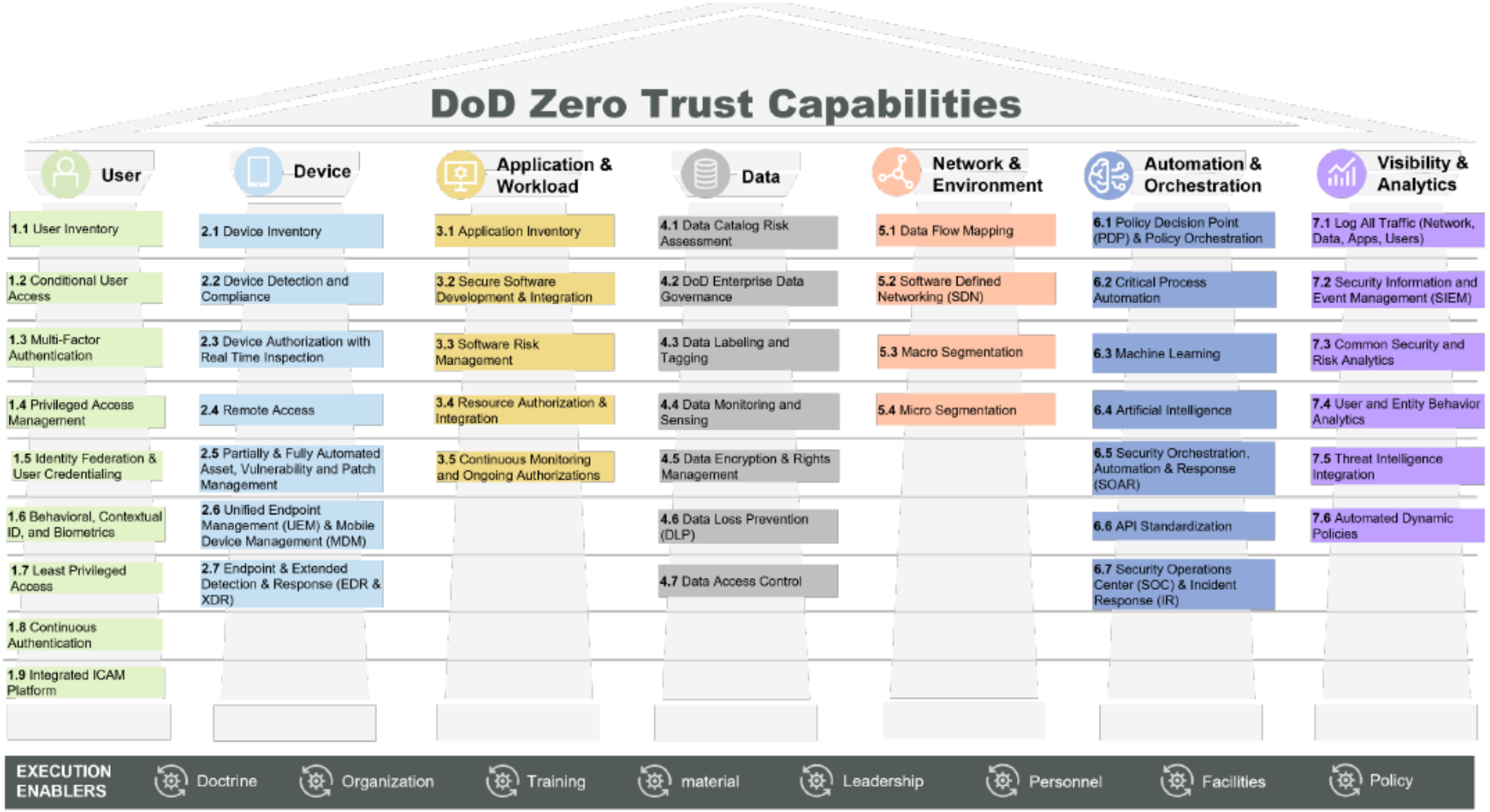
Zero Trust Primer

What's all the hullabaloo about Zero Trust?

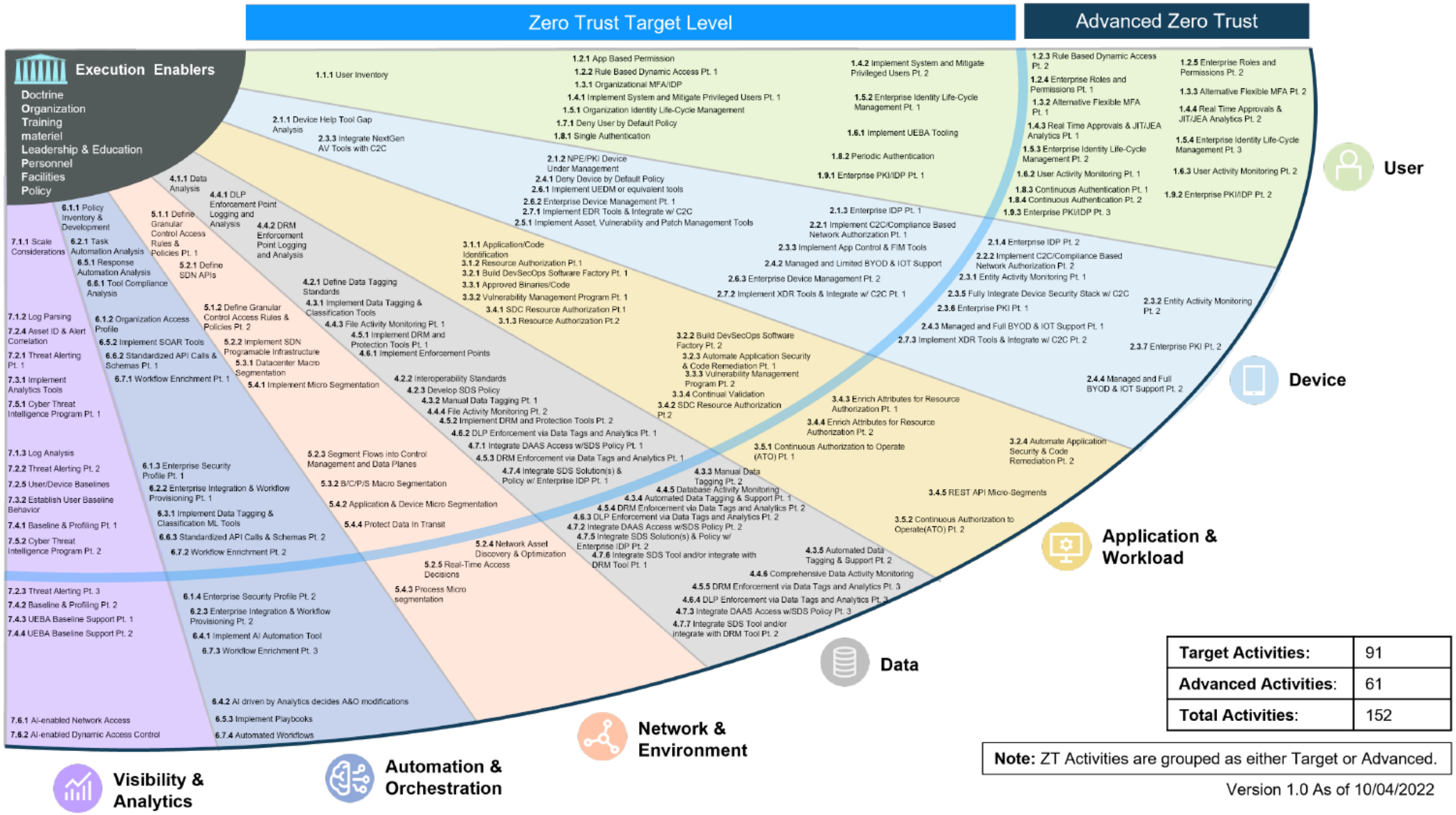
- Zero Trust is defined in NIST SP 800-207
- Zero Trust is a strategy and not a product, and it can't be achieved overnight – it's a journey
- The **CISA Zero Trust Maturity Model** explains the journey from inception to maturity
- Unless you are starting from scratch, in a green-field environment, it is going to take work and effort to transform your existing environment incrementally to a point that it eliminates all assumptions of trust

DoD Zero Trust Capabilities

DoD Zero Trust Strategy



DoD Zero Trust Activities (Target & Advanced Levels)



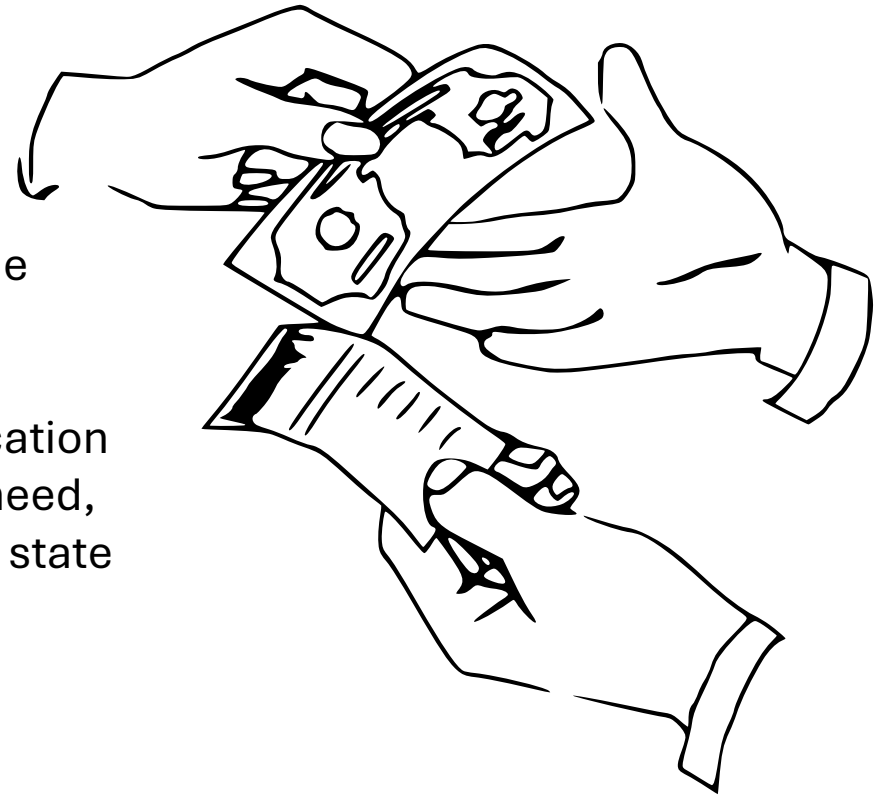
Target Activities:	91
Advanced Activities:	61
Total Activities:	152

Note: ZT Activities are grouped as either Target or Advanced.

Version 1.0 As of 10/04/2022

Reaching **Verified Trust**

The state where secure communication occurs



Zero Trust is not the end goal – it's the required starting point, the new **Cyber Ground Zero**

Digital computer communication (or any productive communication for that matter) can not occur in a state of zero trust. What we need, to facilitate any level of confidential communication, is the end state of zero trust, which I will refer to as **Verified Trust**.

Continuous Assessment

Trust but verify

- Zero trust is the starting point you must achieve so that you can progress to verified trust. If you try to cheat the process and start with Blind or Naïve Trust – you'll never get there

- Once trust is verified, then and only then, can you conduct business with assurance that you've taken the proper precautions. One aspect of advancing from zero trust to a state of verified trust, is that of continuous assessment

- It is not enough to assess any of the key pillars of digital communication a single time and hope that nothing ever changes. That would be like going to the airport and passing through security without any checks simply because you passed those same checks when you took a flight yesterday

TSA Example of Continuous Assessment

You arrive at the Security Checkpoint in a state of Zero Trust

1. Enter Restricted Area by means of Security Checkpoint
2. Provide ID to agent / Facial Recognition
3. They verify that you have a valid reason to be there
4. They Scan Your Person
5. They Scan Your Bags
6. You might be randomly selected for extra screening

Post Checkpoint

7. If you “See Something – Say Something”
8. Some Airports restrict which gates you can reach
9. The Gate agent will verify that you’re at the right plane

You board your plane in a state of Verified Trust

Achieving the right Balance between Security and Performance

The tension

There is **tension** that exists between tight security and end-user experience.

Technologies need to work together, leveraging projects like the Shared Signal Framework and Machine Learning algorithms to improve the efficiency and thoroughness of the continuous assessment process.

The verified level of trust can vary across each of the zero trust pillars, and with that variance, access to more sensitive resources should also be adjusted adaptively.

Staying Focused on What Really Matters

Outcomes matter more than activities

- The last document that Mr. Resnick's team produced is the most important in my opinion.
- The Overlays associate the security controls to the security protection needs as defined by the zero trust capabilities, activities, and outcomes.
- The overlay describes the **context** for implementing a control, which can be lost when controls are published as a list, without supporting guidance.

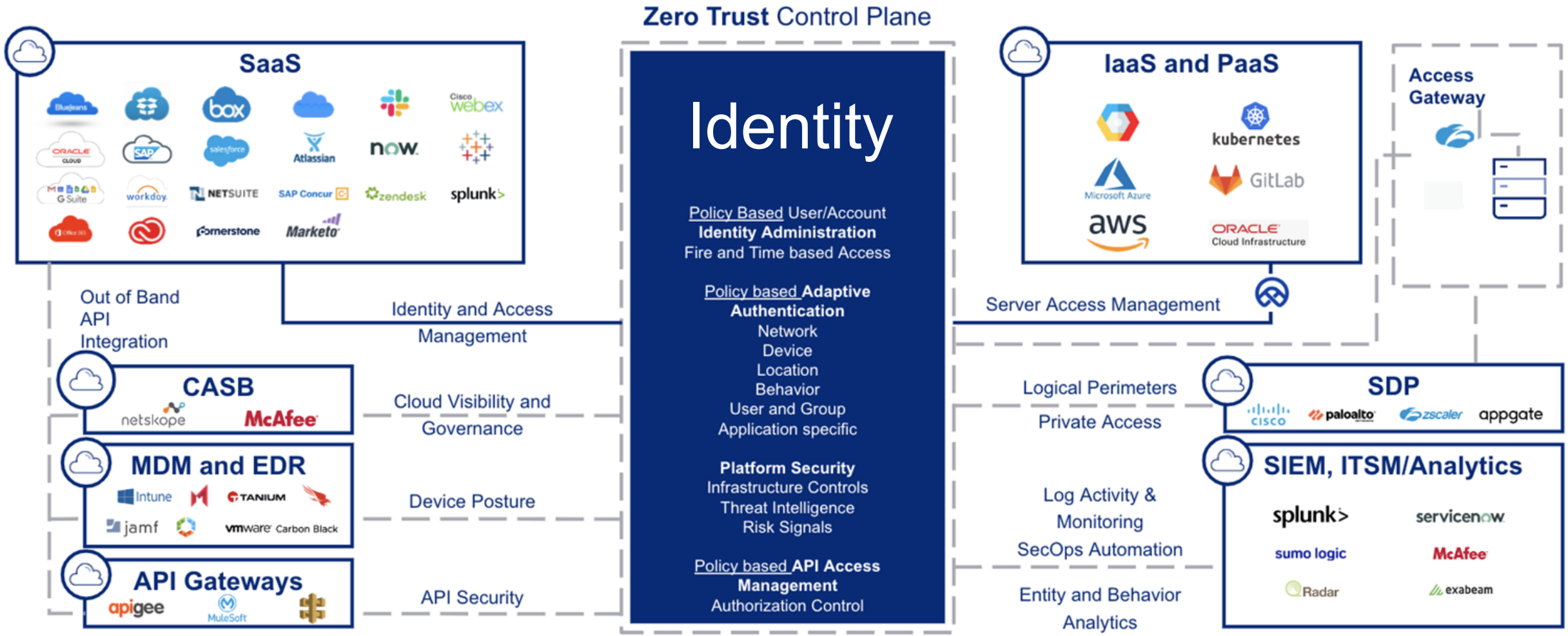
Department of Defense

Zero Trust Overlays

Office of the Chief Information Officer

February 2024
(Version 1.0)

Identity based access control



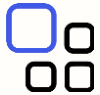
Identity Provider Security Fabric

Secure Identity Products

Governance	Posture Management	PAM	Access Management	Device Access	Identity Threat Protection
Identity Governance (**IGA**)	Identity Security Posture Management	Privileged Access (**PAM**)	Universal Directory (**MUR**) Single Sign-On (**SSO**) Adaptive MFA (**IDP**) Lifecycle Management (**AAP**) API Access Management Access Gateway Customer Identity Inbound/Outbound Federation	Device Access Management	Identity Threat Protections (AI/ML)

Secure Identity Orchestration

Secure Identity Integrations

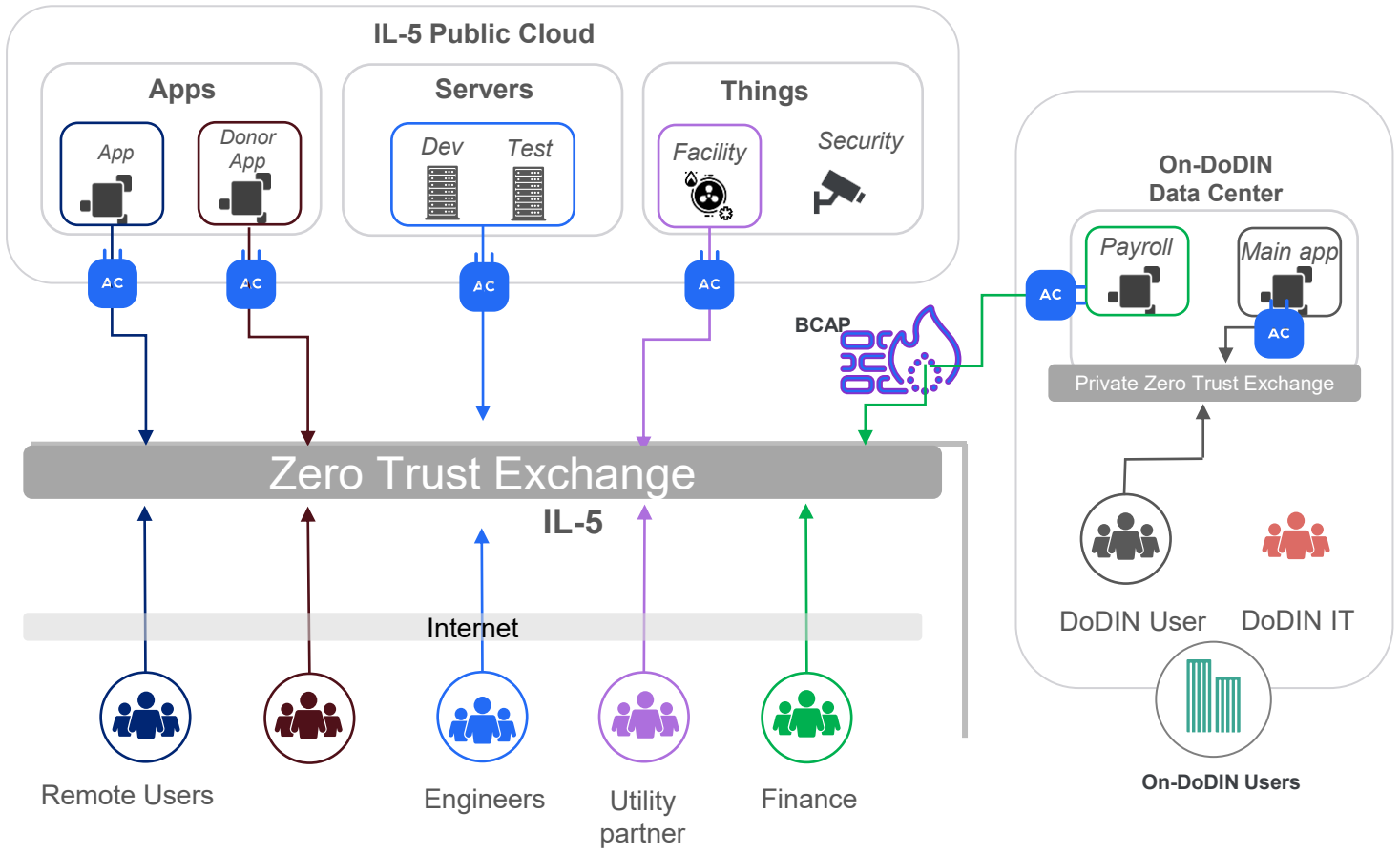
Infrastructure	Applications	APIs	Identities
IaaS  On Prem Servers	Cloud Apps  On Prem Apps	Public  Private	Directories  Non Human / AI Agents

Operates as a SaaS: 99.99% Uptime. Should Scale for Billions of Monthly Logins. Zero Planned Downtime.

Continuous Assessment (keep an eye on your assets)

Real-Time Security Posture Assessment and Zero Trust Policy Control

Limit the Attack Surface (Restrict Access)



Minimize attack surface

- Enterprise network is not visible to the internet
- Inside-out connections hide apps behind the exchange

Eliminate lateral movement

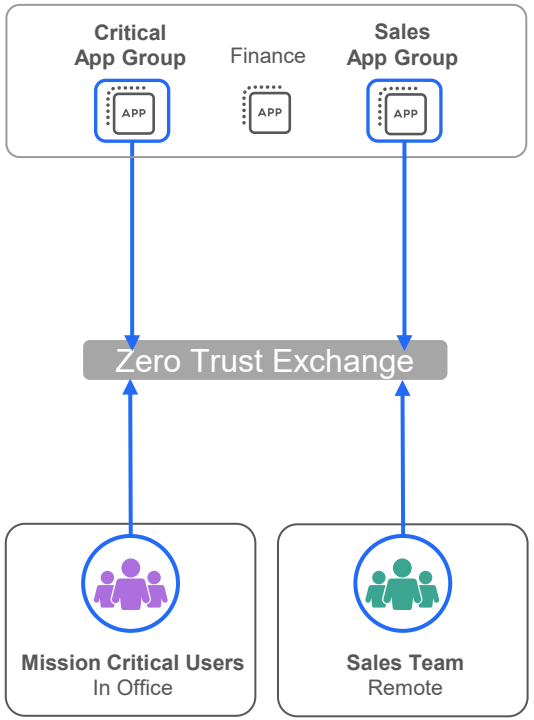
- Connect users to apps, without putting them on the corporate network
- Granular AI-powered user-to-app segmentation

Simplify Operations

- Eliminate all routing complexity
- Secure, direct access for all users, to all apps, from any location

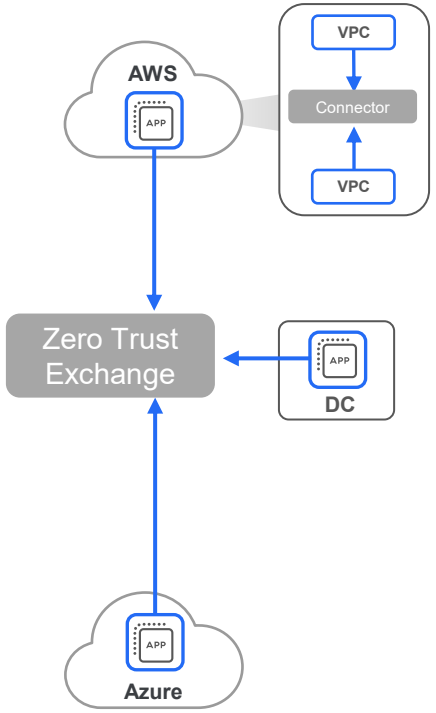
Restrict Lateral Movement

1 User Segmentation
Remote, In Office



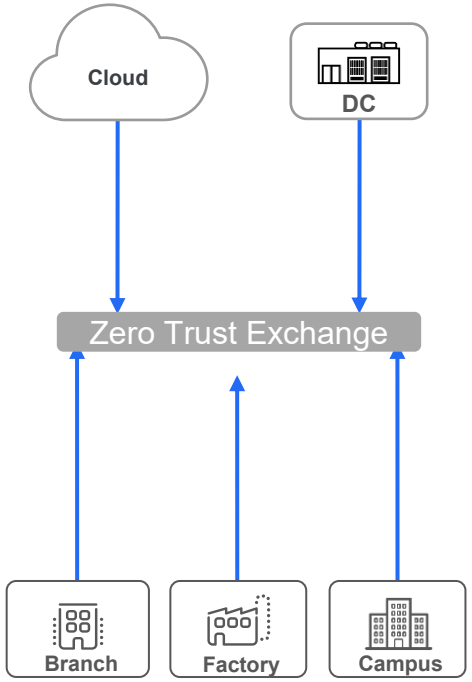
Only Mission Critical Users can access Critical Apps
Sales Team can only access Sales Group Apps

2 Workload Segmentation
Cloud, DC, Branch



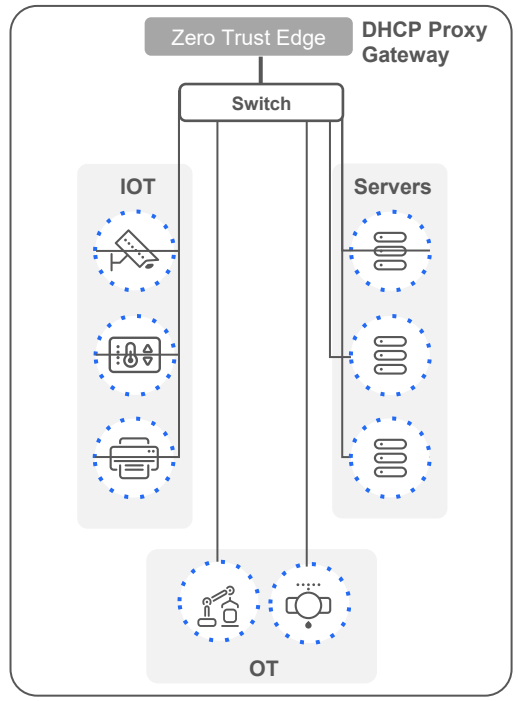
VPC to VLAN
VPC to VPC / VNET
Workload to Workload

3 Branch/Campus Segmentation
Between branches, campus, cloud, DC



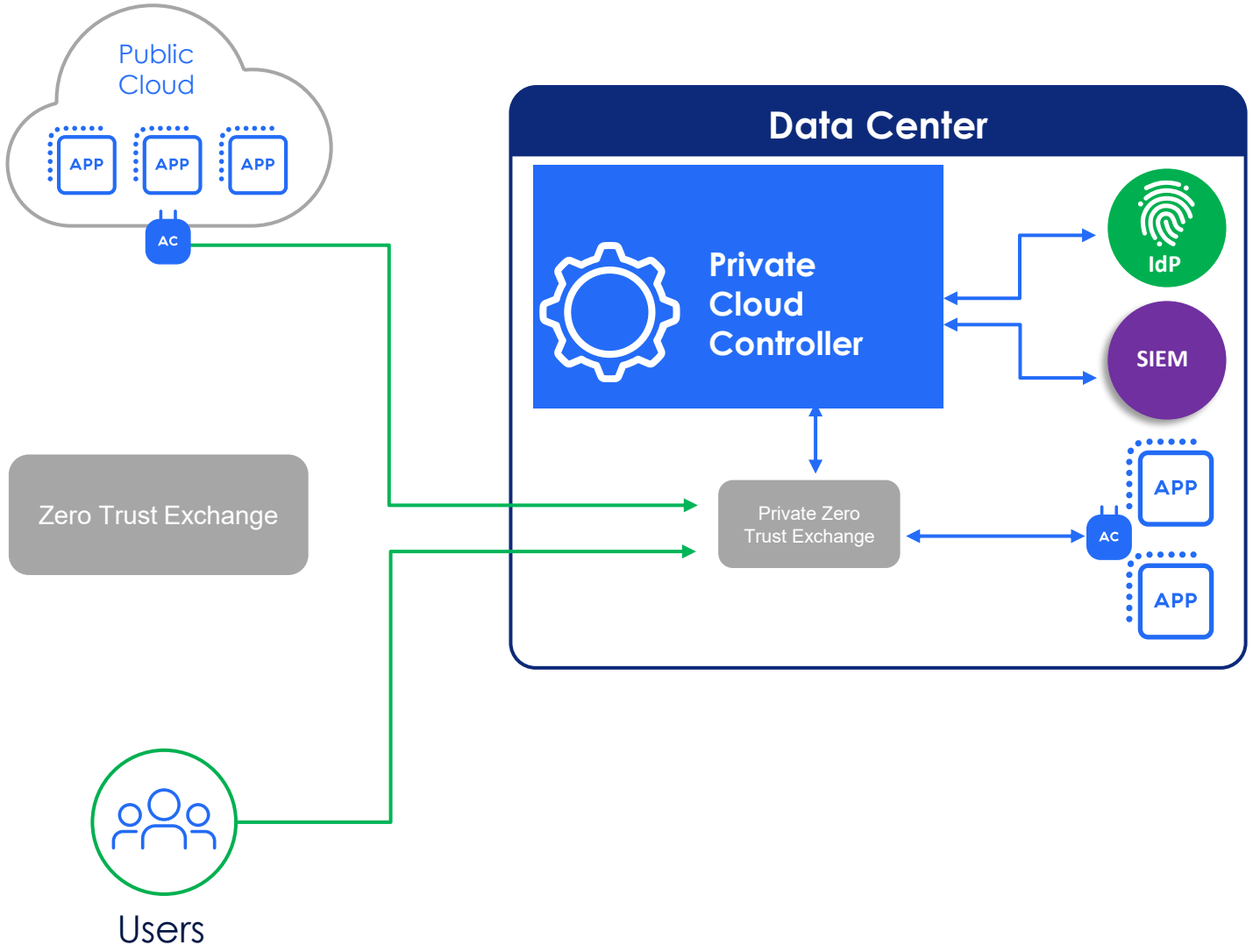
Zero Trust SD-WAN (No Site-to-Site VPN / MPLS)
Each branch is a Starbucks

4 Device Segmentation
Inside branch, factory, campus



Automated IoT / OT Segmentation
Segment of 'one' for every device

Operate Anywhere at Anytime (Enterprise to Tactical Edge)



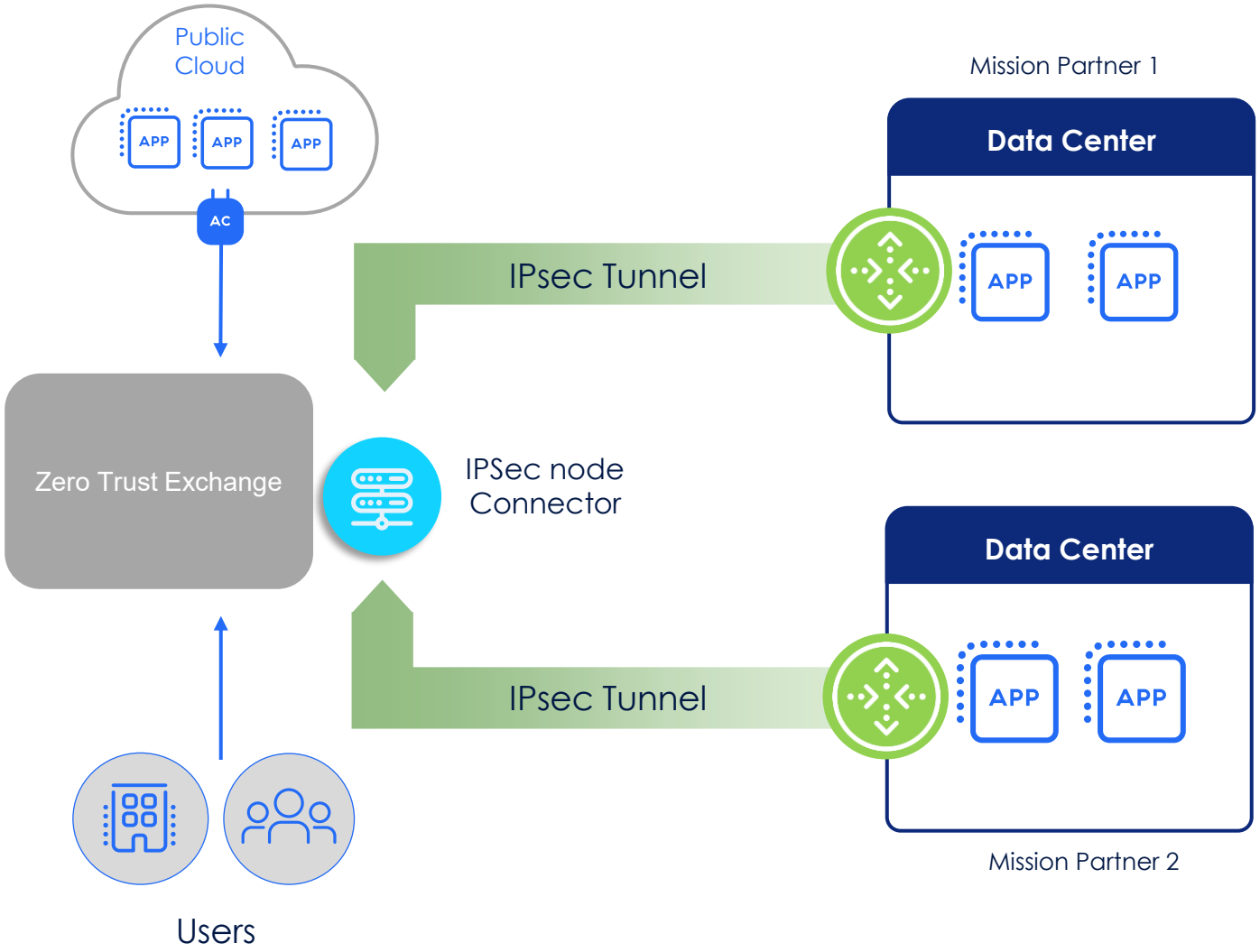
Eliminate the impact of disrupts with Mission Continuity Service

Zero Trust access even during an outage

Demonstrate compliance

Streamline IT ops with automatic switch over

Interoperate with disparate Zero Trust Islands



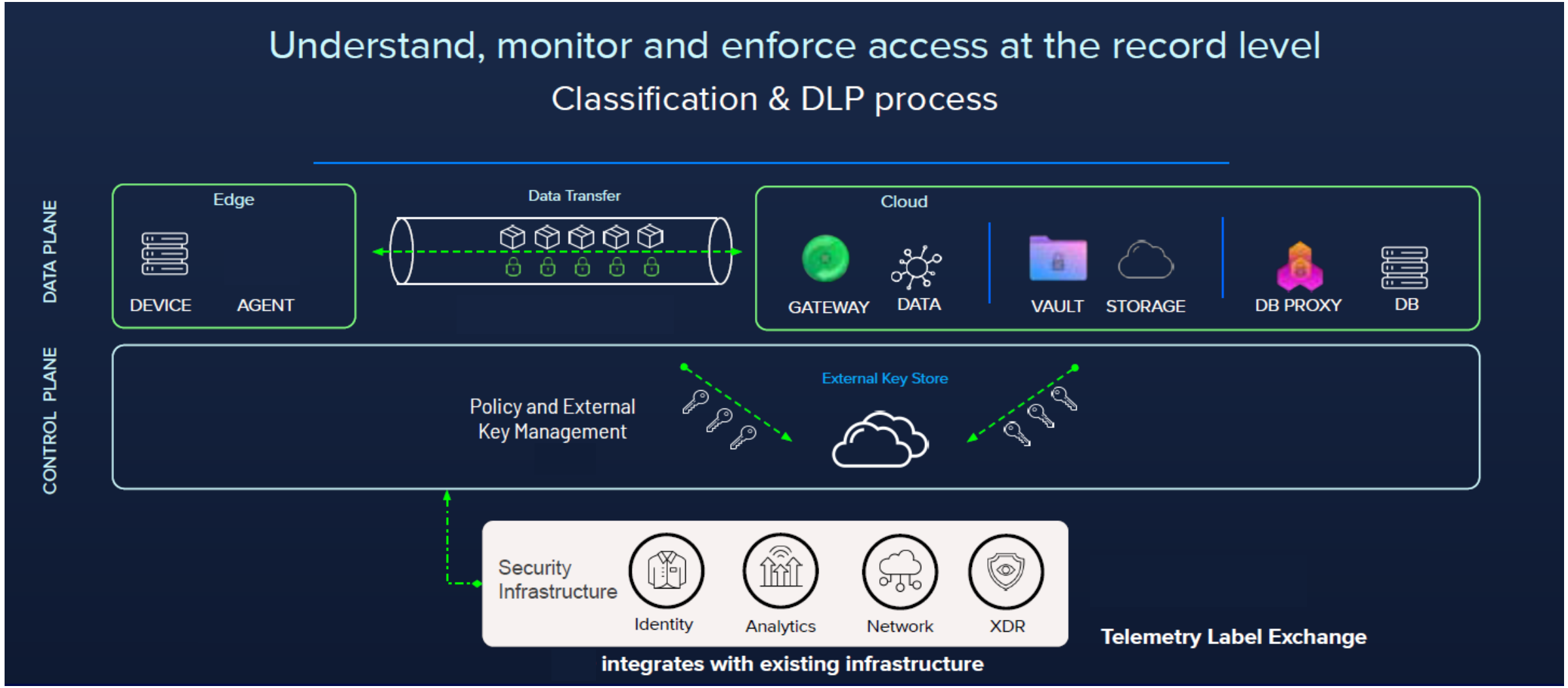
Simple & Secure connectivity to multiple mission partners

Streamline onboarding for new mission partners

Optimize performance for low latency

Ensure high availability and redundancy

Protect the Data



Reduce Complexity

Network Segmentation Complexity Jeopardizes Security

95% of security breaches are due to human error or inadequate access control measures*
53% of enterprises breached via VPN vulnerabilities say threat actors moved laterally**

VPN

Network Segmentation

- Manual, slow and complex policy configuration
- Constant upkeep needed
- Security gaps, further increased with third party access

Zero Trust User-to-App Segmentation

Zero Trust User-to-App Segmentation

- Connect user to app without placing them on the network
- App discovery
- Application and User-focused granularity of segmentation

AI-powered Segmentation & Insights

- Analyzes application traffic to intelligently segment apps and recommend policies
- Customer-preferred groupings
- Optimized policy generation

Reduce Complexity

Accelerate Zero Trust Segmentation with AI-powered User-to-App Segmentation

Import Apps

Bootstrap apps by importing from customers' CSV or third-party sources (Qualys, Tenable, ServiceNow)

Save time and reduce errors

Easily create granular policies

AI/ML Recommendations

Dynamically discover apps

Generate AI/ML recommendations for user-app assignments, and apply granular policies

Segmentation Insights

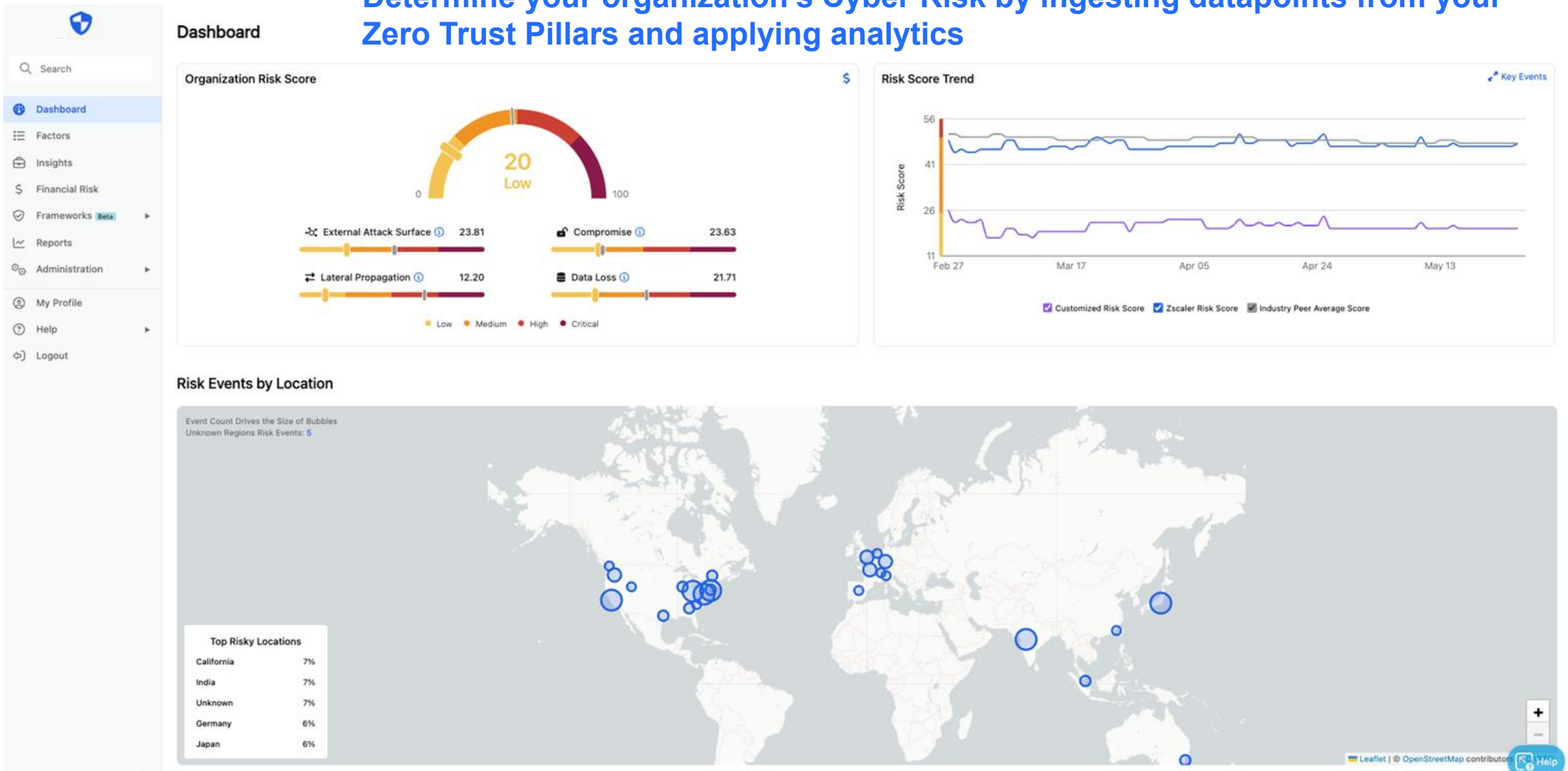
Visibility into user's access patterns and policy usage

Evaluate access-policy utilization

Enforce least-privileged access

Working Smarter by Working Together

Determine your organization's Cyber Risk by ingesting datapoints from your Zero Trust Pillars and applying analytics



Thank You