zscaler™ | U.S. Government Solutions

Zscaler and Department of Defense (DoD)

Zero Trust Reference Architecture 2.0

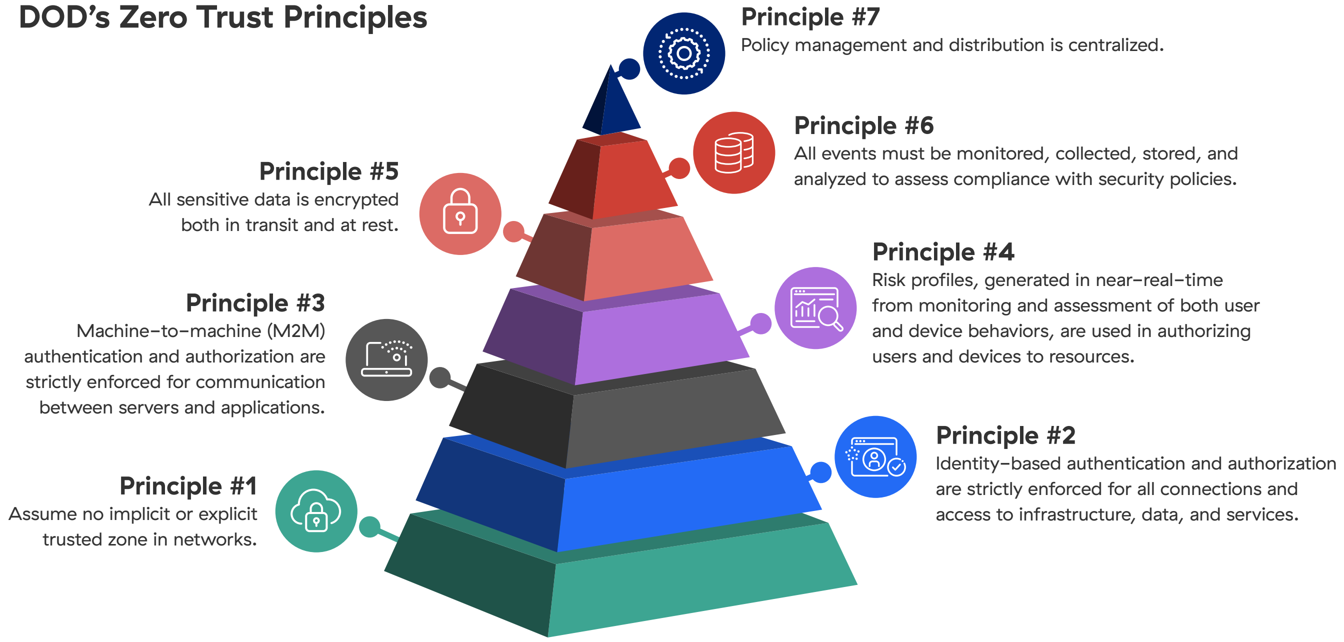
It's a matter of principles

In July 2022, the Department of Defense (DoD) completed its Zero Trust Reference Architecture (RA) Version 2.0. This document establishes a framework based on Zero Trust, a cybersecurity paradigm that assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership. In fact, the CIO of the Pentagon has stated that the DoD intends to have zero-trust deployed across the majority of enterprise systems by 2027.

"The Department of Defense (DOD) next generation cybersecurity architecture will become data centric and based upon Zero Trust principles. Zero Trust supports the creation of, 'a more secure, coordinated, seamless, transparent, and cost- effective IT architecture that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyber threat.'"

The goal of the RA is to secure and defend DoD information, systems, and critical infrastructure against malicious cyber activity, including DoD information on non DoD-owned networks using Zero Trust based on a core set of principles.(label) You can find the seven principles in Section 2.4, pages 23-24 OV-6a.

DOD's Zero Trust Principles



Principle #7
Policy management and distribution is centralized.

Principle #6
All events must be monitored, collected, stored, and analyzed to assess compliance with security policies.

Principle #5
All sensitive data is encrypted both in transit and at rest.

Principle #4
Risk profiles, generated in near-real-time from monitoring and assessment of both user and device behaviors, are used in authorizing users and devices to resources.

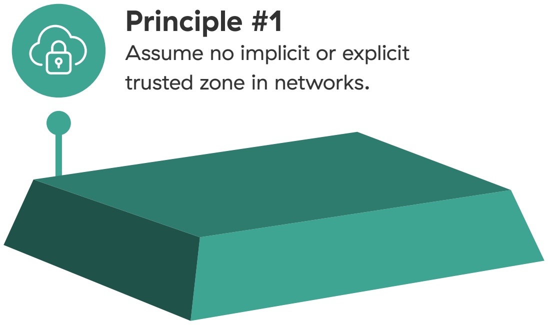
Principle #3
Machine-to-machine (M2M) authentication and authorization are strictly enforced for communication between servers and applications.

Principle #2
Identity-based authentication and authorization are strictly enforced for all connections and access to infrastructure, data, and services.

Principle #1
Assume no implicit or explicit trusted zone in networks.

How Zscaler Aligns to the New RA

Every strong fortress is built on a solid foundation, and principle number one is foundational to the DoD’s approach as it eliminates trust in the network itself regardless of how it is segmented.

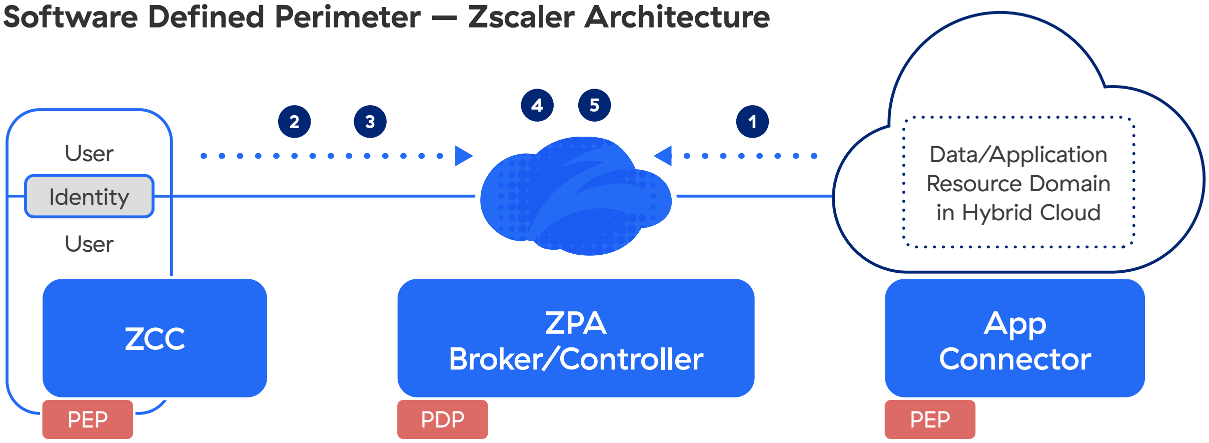


Principle #1
Assume no implicit or explicit trusted zone in networks.

With the assumption that the network is just non–trusted transport, security can be layered on top. OV–2 key enabling technology to deliver on the first principle is the software defined perimeter on page 73.

According to the DoD, a “Software Defined Perimeter will move away from the strong network perimeter concept and move towards conditional authorization with micro–segmentation and encryption. While creating an end–to–end encrypted communication path, all data and applications will have direct visibility removed from the public internet. Devices wanting to access resources would be required to pass through a ZT enabled SDP”.

Software Defined Perimeter — Zscaler Architecture



1. Registration
2. Registration: Broker/Controller handles policy, redirect to ICAM; acts as PDP and hides Hybrid Cloud infrastructure. Agent handles authentication, hygiene; acts as PEP.
3. Request
4. Policy Decision
5. Broker hides infrastructure — Brokers secured channel from user to App Connector

Common Use:

1. Resource Agent (App Connector) registers with Broker via Pinned Mutually Authenticated TLS connection outbound Z–Tunnel.
2. User via their Agent registers with Broker via Pinned Mutually Authenticated TLS connection outbound Z–Tunnel
3. User via their Agent requests access to resource.
4. Broker checks security controls and access policy.
5. Direct mTLS path created to Resource Agent through existing Z–Tunnels

Note:

- No active listeners at egress of Hybrid Cloud — all connections made outbound to broker
- User device never placed on Hybrid Cloud network — no opportunity for lateral movement
- Hybrid cloud infrastructure never exposed

The Foundation for Zero Trust – Zscaler Zero Trust Exchange

Five Major Tenants of the Zero Trust Exchange

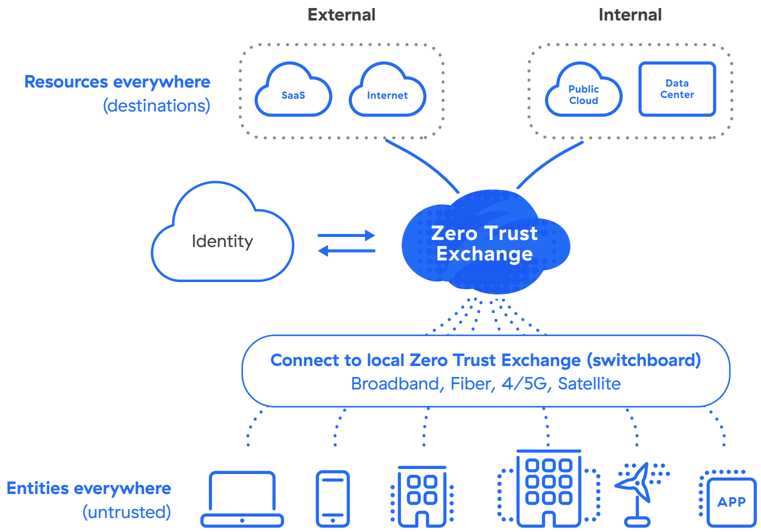
Assume a Hostile Environment: There are malicious personas both inside and outside the network. All users, devices, and networks/environments are treated as untrusted.

Presume Breach: There are hundreds of thousands of attempted cybersecurity attacks against DOD networks every day. Consciously operate and defend resources with the assumption that an adversary has presence within your environment. Enhanced scrutiny of access and authorization decisions to improve response outcomes.

Never Trust, Always Verify: Deny access by default. Every device, user, application/workload, and data flow are authenticated and explicitly authorized using least privilege, multiple attributes, and dynamic cybersecurity policies.

Scrutinize Explicitly: All resources are consistently accessed in a secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access to resources. Access to resources is conditional and access can dynamically change based on action and confidence levels resulting from those actions.

Apply Unified Analytics: Apply unified analytics for Data, Applications, Assets, Services (DAAS) to include behavioristics, and log each transaction.



FedRAMP

Zero Trust Exchange
Adaptive Policy Engine
Four Contexts

User:
Role
Location
Risk Score

Device:
Type
Managed/BYOD
Posture

App:
Private
Sanctioned
Unsanctioned

Content:
Malicious
Sensitive
Priority

Zero Trust Requires a simpler and more secure architecture without impeding operations or compromising security.

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.