SmartSuite

Framework / Cybersecurity / Other

DoD Zero Trust Reference Architecture v2.0

The DoD Zero Trust Reference Architecture v2.0 (July 2022) defines seven pillars, five tenets and a capability taxonomy that DoD Mission Owners use to move to zero trust.



What it is

The DoD Zero Trust Reference Architecture (ZT RA) Version 2.0 is the Department of Defense's authoritative, capability-centric description of a zero trust end state, built on seven pillars, five tenets and seven architecture principles. DoD Mission Owners use it to guide and constrain how their existing IT and enterprise environments evolve toward a data-centric model. Version 2.0 is dated July 2022 and replaced Version 1.0, published on the DoD CIO Library on May 13, 2021.

The Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team prepared it, and it is distribution statement A, approved for public release. It is a reference architecture, not a regulation or a certification: it guides capability planning, portfolio management and IT investment decisions, and it supports the 2021 Executive Order on Improving the Nation's Cybersecurity.

At a glance

PUBLISHER DISA and NSA Zero Trust Engineering Team, for the DoD CIO	TYPE Architecture / Technical Model	VERSION Version 2.0
EFFECTIVE July 2022	DOMAIN Cybersecurity	FAMILY Other
REGION United States	INDUSTRY Aerospace & Defense	ADOPTION MODEL Voluntary
IMPLEMENTATION COMPLEXITY High		

Source: dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

Why it matters

- **A common vocabulary** The seven pillars and a capability taxonomy give DoD and vendors the same terms for identity, devices, networks, applications, data, visibility and automation (sections 2.3 and 3.1).
- **Five tenets that drive design** Assume a hostile environment, presume breach, never trust and always verify, scrutinize explicitly, and apply unified analytics (section 2.2).
- **Data at the center** The data pillar sits at the center of the model, surrounded by the protection pillars that work together to secure it (section 2.3).
- **Use cases that show the pattern** The use cases in section 4 and the architecture patterns in section 7, such as micro-segmentation and conditional authorization, show how capabilities combine.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports DoD ZTRA v2.0

Pillar and Capability Register

List each of the seven pillars and its capabilities with the current and target state, owner and linked systems (sections 2.3 and 3).

Tenet and Principle Checklist

Review designs and changes against the five tenets and seven principles and record exceptions with an approver (sections 2.2 and 2.4).

Baseline and Transition Plan

Capture the baseline view, target state and the steps between them as tracked actions with dates (section 8).

Use Case and Pattern Library

Keep the segmentation, authentication and policy patterns used in your environments, linked to the systems that implement them (sections 4 and 7).

Evidence and Assessment Tracking

Attach test results, diagrams and review notes to each capability so an assessor can see what was verified and when.

Zero Trust Progress Reporting

Report capability coverage by pillar and open transition actions to the architecture board.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-207 ZTA | NIST 800-53 Rev.5

Official resources

DoD Zero Trust Reference Architecture v2.0

Defines the comprehensive approach for securing DoD information systems via zero trust principles.

dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

Frequently asked questions

What is the DoD Zero Trust Reference Architecture?

It is the Department of Defense's reference architecture for zero trust, prepared by the DISA and NSA Zero Trust Engineering Team. Version 2.0, dated July 2022, describes pillars, tenets, principles, capabilities, use cases and patterns that DoD Mission Owners use to guide their environments (section 1.3).

What are the seven pillars?

User, Device, Network/Environment, Applications and Workload, Data, Visibility and Analytics, and Automation and Orchestration (section 2.3). The data pillar sits at the center, surrounded by the protection pillars.

What are the five zero trust tenets in the architecture?

Assume a hostile environment, presume breach, never trust and always verify, scrutinize explicitly, and apply unified analytics (section 2.2). The architecture also lists seven principles, such as no implicit trusted zone and centralized policy management (section 2.4).

Is the DoD ZT RA mandatory or certifiable?

It is a reference architecture that guides and constrains Mission Owners' designs; it is not a certification scheme. It primarily supports capability planning, portfolio management and IT investment decisions (section 1.2).

How does it relate to NIST SP 800-207?

The architecture summarizes NIST SP 800-207, Zero Trust Architecture, in section 5.3.3 and treats it as a linked architecture, along with the DoD Cybersecurity Reference Architecture and the DoD ICAM design (section 5.3).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

License included / downloadable: Yes The reference architecture is a U.S. Government document approved for public release (distribution statement A) and is included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/dod-zero-trust-reference-architecture-v2-0