

DoD Zero Trust Reference Architecture v2.0

DoD Zero Trust Reference Architecture v2.0 guides implementation of continuous verification, least privilege, and segmentation to secure DoD information systems.



What it is

At a glance

<div>PUBLISHER</div> <div>U.S. Department of Defense (DoD)</div>	<div>TYPE</div> <div>Architecture / Technical Model</div>	<div>VERSION</div> <div>DoD Zero Trust Reference Architecture v2.0</div>
<div>EFFECTIVE</div> <div>September 2022</div>	<div>DOMAIN</div> <div>Cybersecurity</div>	<div>FAMILY</div> <div>Other</div>
<div>REGION</div> <div>United States</div>	<div>INDUSTRY</div> <div>Aerospace & Defense</div>	<div>ADOPTION MODEL</div> <div>Regulatory Compliance</div>
<div>IMPLEMENTATION COMPLEXITY</div> <div>Very High</div>		

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

Why it matters

- **Strengthen cybersecurity governance** Promote consistent policy enforcement and continuous verification to ensure effective security oversight across users, devices, and applications.
- **Enhance regulatory alignment** Support compliance with federal mandates by aligning security practices with DoD and NIST requirements across agency operations.
- **Improve threat detection capabilities** Enable adaptive monitoring and authentication to identify abnormal behavior and mitigate security incidents before significant damage occurs.
- **Increase audit readiness** Simplify the demonstration of security controls and incident response processes to auditors and regulatory bodies with integrated logging and reporting.

How SmartSuite supports DoD ZTRA v2.0

Zero Trust Capability Roadmap Track capability requirements across identity, device, network, app, data, and visibility.	Policy and Control Implementation Tracking Manage implementation tasks, owners, and evidence for each capability area.	Continuous Verification and Access Governance Track MFA, conditional access, privileged access, and access reviews with proof.
Segmentation and Data Protection Controls Document segmentation decisions, enforcement evidence, and data access controls.	Monitoring and Telemetry Evidence Centralize logging, detection coverage, and validation evidence across pillars.	Leadership Reporting Report progress, gaps, and maturity by pillar and implementation phase.

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](https://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 v2.0 used for?**
The DoD Zero Trust Reference Architecture v2.0 is used to help defense agencies and contractors implement a zero trust security model that minimizes implicit trust and supports continuous verification across users, devices, and systems. It guides the deployment of advanced security controls to protect critical Department of Defense (DoD) information assets from evolving cyber threats.
- Is the DoD Zero Trust Reference Architecture v2.0 mandatory or certifiable?**
The framework is a mandated set of security principles and requirements for DoD agencies, but it is not a certifiable standard in itself. Instead, compliance with its tenets is expected for organizations operating within the DoD ecosystem, and adherence is verified through audits and assessments aligned with DoD policies and federal mandates.
- Who does the DoD Zero Trust Reference Architecture v2.0 apply to?**
The framework applies to all DoD agencies, military departments, defense contractors, and partners with access to DoD networks and information systems. It is relevant for both government and partner organizations that must comply with DoD cybersecurity policies and protect sensitive information.
- What are the key concepts and artifacts required by the DoD Zero Trust Reference Architecture v2.0?**
Key concepts in the architecture include identity-centric security, least-privilege access, microsegmentation, data protection, and continuous monitoring. Required artifacts often include asset inventories, mapped security controls, risk assessment records, and governance documentation to demonstrate compliance.
- How is the DoD Zero Trust Reference Architecture v2.0 implemented in practice?**
Implementation involves adopting a phased approach guided by the architecture's maturity model, starting with asset inventory and risk assessment before deploying identity, access management, segmentation, and monitoring controls. Organizations align their existing security programs to architecture domains and control families to close compliance gaps and enhance security posture.

How does the DoD Zero Trust Reference Architecture v2.0 relate to other frameworks such as NIST?

The DoD Zero Trust Reference Architecture v2.0 aligns closely with NIST frameworks, especially NIST SP 800-207 for Zero Trust, and leverages federal cybersecurity mandates as foundational requirements. Organizations use the framework to bridge DoD-specific requirements with broader federal and NIST standards to achieve cohesive compliance.

What are the ongoing compliance requirements for the DoD Zero Trust Reference Architecture v2.0?

Ongoing compliance requires continuous monitoring, periodic risk assessments, evidence collection, regular policy reviews, and audit-ready documentation. Organizations must demonstrate that implemented controls remain effective and are closely aligned with DoD governance, operational risk management, and regulatory updates.

How would SmartSuite support DoD Zero Trust Reference Architecture v2.0?

SmartSuite enables organizations to manage the DoD Zero Trust Reference Architecture v2.0 by supporting risk tracking, control mapping, and compliance oversight. The platform facilitates evidence collection, establishes robust audit readiness, and provides reporting dashboards to monitor security posture, document compliance activities, and manage policy governance across zero trust domains.

License included / downloadable: Yes The DoD Zero Trust Reference Architecture is publicly available through U.S. Department of Defense publications.

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