

DHS Zero Trust Capability Framework (ZTCF) v1.0

DHS Zero Trust Capability Framework guides organizations to implement continuous authentication, access controls, and segmentation to eliminate implicit trust.



What it is

At a glance

PUBLISHER Cybersecurity and Infrastructure Security Agency (CISA)	TYPE Framework	VERSION Current DHS Zero Trust Capability Framework
EFFECTIVE January 29, 2025	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://www.dhs.gov/sites/default/files/2025-04/2025_0129_cisa_zero_trust_architecture_implementation.pdf

Why it matters

- **Strengthen cybersecurity governance** Support leadership in making informed risk management decisions and allocating resources to safeguard critical systems and data.
- **Enhance regulatory alignment** Facilitate alignment with federal cybersecurity mandates and streamline efforts to maintain compliance with evolving regulatory requirements.
- **Improve access controls** Reduce unauthorized access risk through continuous authentication and authorization, ensuring users and devices are consistently verified.
- **Promote operational resilience** Improve the organization's ability to withstand and recover from cyber incidents by applying comprehensive segmentation and monitoring strategies.

How SmartSuite supports DHS ZTCF

Zero Trust Program Structure Organize goals, scope, and roles for a consistent zero trust implementation program.	Identity and MFA Rollout Tracking Manage MFA and access control initiatives with evidence and coverage reporting.	Device Posture and Endpoint Governance Track device compliance requirements, exceptions, and verification evidence.
Network and Application Access Controls Document segmentation and conditional access policies with proof of enforcement.	Visibility, Monitoring, and Response Workflows Centralize telemetry evidence and incident response processes tied to zero trust goals.	Executive Reporting Dashboards Report program status, gaps, and readiness across capability areas.

Common framework mappings

CIS Controls v8.1

FedRAMP Rev. 5

ISO 27001:2022

MITRE ATT&CK

NIST CSF 2.0

NIST 800-207 ZTA

NIST 800-53 Rev.5

Official resources

DHS Zero Trust Capability Framework
Provides guidance on implementing zero trust principles to enhance security posture.
dhs.gov/sites/default/files/2025-04/2025_0129_cisa_zero_trust_architecture_implementation.pdf

Frequently asked questions

- What is the DHS Zero Trust Capability Framework (ZTCF) used for?**
The ZTCF guides organizations in adopting zero trust principles to improve cyber defense and reduce implicit trust across IT environments. It provides a comprehensive structure for enhancing access controls, identity verification, and continuous monitoring to manage modern cyber risks and comply with federal cybersecurity mandates.
- Is the ZTCF mandatory or certifiable?**
The ZTCF is not a certifiable standard, but it is recommended and often required for federal agencies and organizations supporting critical infrastructure per U.S. government cybersecurity policy. Adherence demonstrates alignment with executive orders and federal requirements but does not result in a formal certification.
- Who does the ZTCF apply to?**
ZTCF primarily applies to U.S. federal agencies and organizations operating or supporting critical infrastructure sectors. However, any organization seeking to strengthen their security posture through zero trust principles can adopt its guidelines.
- What are the key concepts and artifacts in the ZTCF?**
Key concepts in ZTCF include identity verification, least-privilege access, microsegmentation, device security, data protection, and continuous authentication and monitoring. Artifacts include capability mappings, risk assessments, maturity models, and control libraries aligned with governance and compliance requirements.

How does an organization implement the ZTCF?

Organizations implement ZTCF by assessing their current architecture, mapping existing controls to ZTCF capability areas, conducting gap analyses, and identifying risk mitigation priorities. Implementation involves lifecycle processes for policy alignment, strong authentication, data protection and continuous improvement, through iterative maturity assessments.

How does ZTCF relate to other frameworks like NIST SP 800-207?

ZTCF aligns closely with zero trust principles outlined in frameworks such as NIST SP 800-207, providing a structured approach tailored for federal and critical infrastructure contexts. Organizations can leverage existing controls and practices from related standards to meet ZTCF requirements and ensure harmonized compliance reporting.

What are the ongoing compliance requirements under the ZTCF?

Maintaining ZTCF alignment requires regular risk assessments, control reviews, ongoing monitoring, updating access policies, and responding to incidents. Continuous improvement and maturity model benchmarking are essential for demonstrating compliance and strengthening cybersecurity posture over time.

How would SmartSuite support the DHS Zero Trust Capability Framework (ZTCF)?

SmartSuite facilitates ZTCF management through centralized risk tracking, control library management, evidence collection, and support for audit readiness. The platform automates remediation workflows, aggregates compliance evidence, and provides dashboards for monitoring posture, visualizing progress, and aligning with ZTCF maturity and reporting requirements.

License included / downloadable: Yes The DHS Zero Trust Capability Framework is publicly available through U.S. DHS and CISA resources.

Full framework page and mappings: smartsuite.com/frameworks/dhs-zero-trust-capability-framework-ztcf-v1-0