NIST SP 800-207 (2020) — Zero Trust Architecture

NIST SP 800-207 provides guidance for designing and implementing zero trust architecture to continuously verify and limit access.

What it is

NIST SP 800-207 — Zero Trust Architecture is a cybersecurity framework that establishes principles and guidelines for implementing a Zero Trust model to strengthen data protection and reduce organizational risk. The framework shifts traditional security paradigms by assuming that no user or device, whether inside or outside the network perimeter, should be inherently trusted.

Published by the National Institute of Standards and Technology (NIST), SP 800-207 is used by federal agencies, critical infrastructure operators, and private sector organizations aiming to modernize their cybersecurity controls. It outlines core Zero Trust concepts, access management practices, and requirements for secure network architectures, supporting compliance and risk management objectives in alignment with other NIST frameworks, such as NIST SP 800-53 and the NIST Cybersecurity Framework.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Architecture / Technical Model	VERSION Rev. 1
EFFECTIVE August 11, 2020	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY High

Source: https://csrc.nist.gov/pubs/sp/800/207/final

Why it matters

- **Reduce attack surface exposure** Limit unauthorized access by verifying users, devices, and applications before permitting network or data access.
- **Strengthen incident detection capabilities** Enable faster identification and isolation of threats through continuous authentication and real-time network activity monitoring.
- **Enhance data protection practices** Protect sensitive data by enforcing granular access controls and least-privilege policies across all resources.
- **Support regulatory compliance efforts** Demonstrate adherence to stringent security requirements and privacy regulations through rigorous controls and logging.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST SP 800-207

Zero Trust Policy and Architecture Governance

Document Zero Trust principles, policies, and architecture components governing access decisions.

Identity and Access Verification Controls

Manage identity verification requirements, authentication policies, and device trust decisions.

Continuous Authorization and Monitoring

Track ongoing access decisions, monitoring signals, and trust evaluations across systems.

Device and System Trust Management

Maintain inventory and trust status of devices and systems interacting with protected resources.

Anomalous Access Investigation

Investigate abnormal access patterns and coordinate response actions for suspicious activity.

Zero Trust Governance Reporting

Provide dashboards summarizing identity assurance, trust posture, and security control coverage.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | GDPR | HIPAA | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2 | SWIFT CSCF

Official resources

NIST Special Publication 800-207: Zero Trust Architecture

Defines the Zero Trust Architecture framework, outlining principles and components for security.

csrc.nist.gov/publications/detail/sp/800-207/final

NIST Cybersecurity Framework

Describes common policies to improve cybersecurity risk management.

nist.gov/cyberframework

NIST SP 800 Series Index

Offers a comprehensive index of NIST's cybersecurity-related special publications, including Zero Trust guidance.

csrc.nist.gov/publications/sp800

NIST Zero Trust Architecture Project

Describes the ongoing NIST efforts to develop and refine Zero Trust security models.

nist.gov/itl/applied-cybersecurity/ncat/zero-trust-architecture

Frequently asked questions

What is NIST SP 800-207 Zero Trust Architecture used for?

NIST SP 800-207 provides guidance for implementing a Zero Trust Architecture (ZTA) to improve organizational cybersecurity by enforcing strict access controls. It is used to minimize risk from both external threats and insider attacks by treating all network traffic as untrusted, regardless of its origin.

Is NIST SP 800-207 Zero Trust mandatory or certifiable?

NIST SP 800-207 is not a mandatory or certifiable standard; it is a set of best-practice guidelines published by NIST. However, federal agencies are encouraged to adopt Zero Trust principles, and private organizations may do so to align with industry-recognized security models.

What entities or systems does NIST SP 800-207 apply to?

NIST SP 800-207 is applicable to any organization seeking to modernize its security posture, especially those managing sensitive systems or data. It is particularly relevant for architectures that use cloud services, remote access, and distributed resources.

What are the key concepts or components required by Zero Trust Architecture?

Zero Trust Architecture centers around principles such as continual authentication, least privilege access, micro-segmentation, and strong identity management. Key artifacts include policy enforcement points (PEPs), policy decision points (PDPs), robust logging, and monitoring systems.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does an organization implement NIST SP 800-207 Zero Trust Architecture?

Implementation involves mapping organizational assets, users, and data flows; enforcing dynamic, context-aware access policies; and deploying monitoring and response mechanisms. Organizations should assess current controls and incrementally apply Zero Trust principles to all network resources.

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

NIST SP 800-207 complements existing frameworks like the NIST Cybersecurity Framework (CSF) and ISO 27001 by providing targeted guidance on network and identity-centric security. It can be implemented alongside these frameworks to enhance overall security posture and reduce residual risk.

What are the ongoing compliance requirements for maintaining Zero Trust Architecture?

Maintaining a Zero Trust Architecture requires continuous monitoring, regular policy and access reviews, verification of user and device identities, and timely response to incidents. Organizations must also update configurations and documentation as technology and threat landscapes evolve.

How would SmartSuite support NIST SP 800-207 Zero Trust Architecture?

SmartSuite enables organizations to manage their Zero Trust transformation by tracking risks, mapping and managing control implementations, collecting evidence for policy enforcement, and supporting audit readiness. It also streamlines compliance reporting and continuous monitoring to help demonstrate adherence to NIST SP 800-207 guidance.

License included / downloadable: Yes NIST SP 800-207 is publicly available for free on NIST's website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/nist-sp-800-207-2020-zero-trust-architecture