Teleport

Implementing Zero Trust with Teleport

Align with the DoD's Seven Pillars & NIST 800-53 Controls

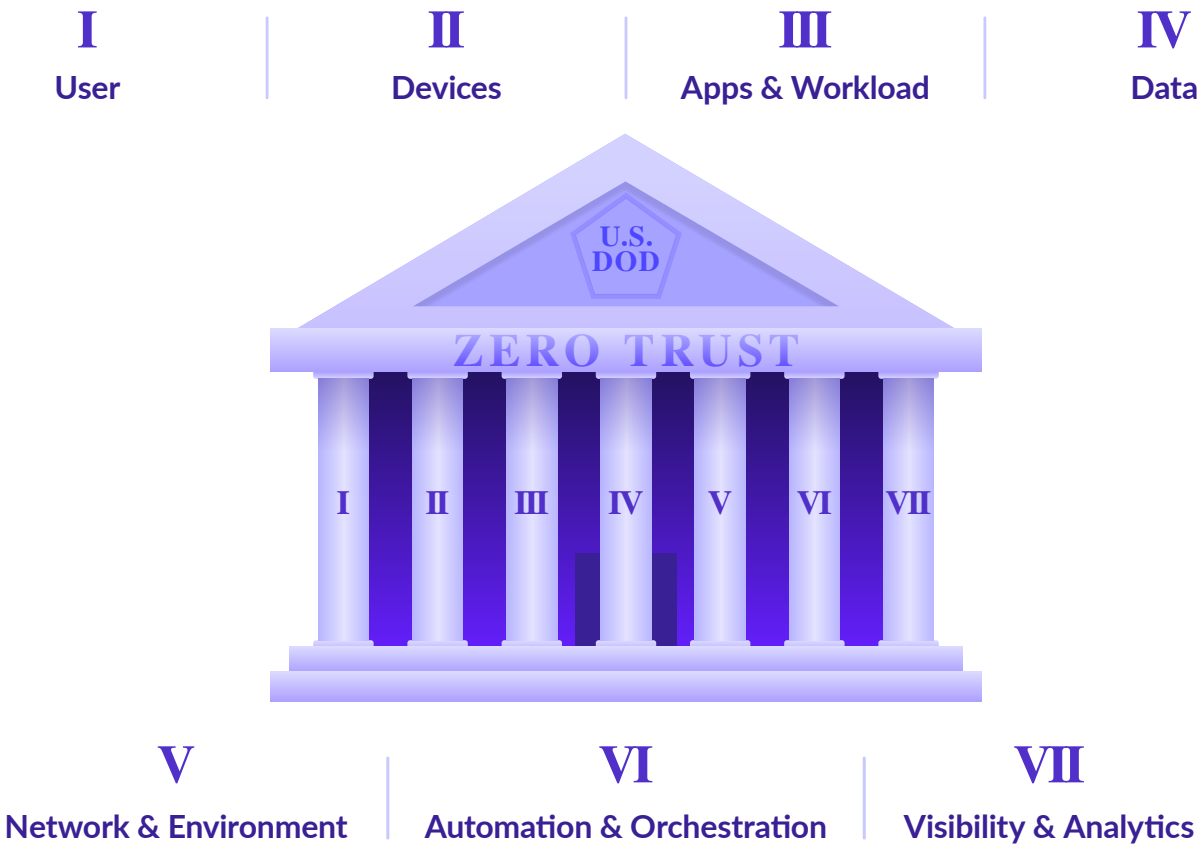
© 2025 Gravitational Inc. All rights reserved.

Contents

This report provides insights and information to help you achieve compliance with the Department of Defense's (DoD) Zero Trust strategy, emphasizing how the DoD's seven pillars of Zero Trust security map to specific NIST 800-53 controls designed to align organizations with federal requirements.

This document also demonstrates how Teleport can help secure critical systems, enforce access policies, and support continuous monitoring and reporting to ensure compliance with both the DoD's Seven Pillars and NIST 800-53 controls.

© 2025 Gravitational Inc. All rights reserved.



Introduction to DoD Zero Trust and NIST 800-53

The DoD's Zero Trust strategy promotes a multi-layered security framework across seven core pillars. At its foundation, Zero Trust seeks to protect data and systems through stringent identity verification, fine-grained access management, and continuous monitoring. The NIST 800-53 framework offers a comprehensive set of controls designed to safeguard sensitive information, serving as the basis for much of the DoD's Zero Trust strategy. This framework also articulates complementary controls to each of the seven Zero Trust pillars, in addition to Privileged Access Management (PAM) best practices.

Teleport's Infrastructure Identity Platform helps organizations meet these stringent requirements by securing modern infrastructure with fine-grained access controls, role-based access control (RBAC), integration with identity providers, comprehensive audit capabilities, and modern privileged access management (PAM) features. Teleport is built to ensure only authorized identities – human or non-human – can access critical systems and data while maintaining compliance with the DoD's Zero Trust principles and NIST 800-53 controls.

© 2025 Gravitational Inc. All rights reserved.

DoD Zero Trust Pillar 1: User Identification and Access Management

The first Zero Trust pillar emphasizes strong identity and access management (IAM) by continuously authenticating and authorizing users, enforcing identity through multifactor authentication, role mapping, and centralized policy enforcement.

Highlighted Alignment with NIST 800-53 Controls

- **IA-2 (Identification and Authentication):** Requires all users to be uniquely identified and authenticated before accessing any systems.
- **AC-2 (Account Management):** Involves strict control over user accounts and permissions.

Teleport's Approach

Teleport's Infrastructure Identity Platform enhances IAM with unified, trusted identities for people, hardware, and software, coupled with short-lived privileges. This eliminates the fragmentation of identities and standing privileges that get exploited by hackers via impersonation and other types of identity attacks.

Teleport further integrates with leading identity providers, enabling organizations to streamline identity and user management while unifying and simplifying access control across complex infrastructure environments. Capabilities include:

- **Cryptographic Identities:** Teleport issues cryptographic identity to users, devices, machines, and workloads, including AI agents. These identities are verified by biometrics or hardware-backed (e.g., using TPMs or HSMs) eliminating the risks of credential theft or misuse.
- **Identity Provider Integration:** Teleport integrates seamlessly with major SSO and IdP solutions (e.g., Okta, Azure AD, Google Workspace) to centralize authentication and simplify the user onboarding/offboarding.
- **Role-Based Access Control (RBAC):** Teleport uses fine-grained RBAC to define access policies by user role, group, environment, and even time of day. This policy-based control helps enforce least privilege principles and simplifies security policy management across distributed infrastructure. **Access Lists** further automate provisioning/deprovisioning and eliminate errors that can occur from manual steps.
- **Just-in-Time Access (JIT):** Teleport delivers JIT access workflows based on task, allowing users to request time-limited access to specific systems or resources. Access is granted only upon approval, eliminating standing privilege risks, improving accountability and auditability, and preventing lateral movement threats.
- **Short-Lived Privileges:** All access in Teleport is issued using ephemeral, short-lived certificates designed to expire automatically. This eliminates the risks and compliance headaches of static credentials and long-lived standing privileges, encouraging close alignment with Zero Standing Privileges (ZSP) best practices.

© 2025 Gravitational Inc. All rights reserved.

DoD Zero Trust Pillar 2: Device Security

The second pillar of the DoD Zero Trust architecture emphasizes device trust to ensure only authorized devices are allowed to access critical systems and data, including evaluating device posture dynamically as part of the access decision.

Highlighted Alignment with NIST 800-53 Controls

- **SI-4 (System Monitoring):** Continuous monitoring to detect and respond to unauthorized access.
- **CA-7 (Continuous Monitoring):** Ongoing assessment of systems to ensure only secure devices access sensitive resources.
- **IA-3 (Device Authentication & Authentication):** Unique identification and authentication of devices before establishing connections.

Teleport's Approach

Teleport strengthens device security by enforcing end-to-end encrypted sessions, ensuring that device identity and health posture are verifiable and trustworthy before access is granted. This is accomplished with Device Trust and MDM integrations. Capabilities include:

- **Device Trust:** Teleport introduces strong device trust by enforcing cryptographic identification tied to hardware-backed device keys. Devices are registered and authenticated using TPMs (Trusted Platform Modules) or secure enclaves, creating an unimpeachable hardware-rooted identity. KMS (Key Management Service) and HSM (Hardware Security Module) integrations further enhance cryptographic key storage and operations, preventing key leakage or software-based tampering.
- **Mobile Device Management (MDM) Integration:** Teleport integrates with leading MDM solutions like Jamf to enforce access policies based on device compliance status, and can be configured to conditionally restrict access to sensitive infrastructure unless the device is enrolled, monitored, and meets predefined security baselines.

© 2025 Gravitational Inc. All rights reserved.

DoD Zero Trust Pillar 3: Network Security

The third pillar of the DoD Zero Trust strategy focuses on securing the network by enforcing strict traffic inspection, access control, and continuous verification across both internal and external communication paths. In a Zero Trust model, the network is no longer considered inherently trustworthy. Instead, security must be maintained regardless of location or topology.

Highlighted Alignment with NIST 800-53 Controls

- **SC-7 (Boundary Protection):** Protects system boundaries, restricting access to authorized entities.
- **AC-17 (Remote Access):** Controls secure access to systems, especially for remote users.

Teleport's Approach

Teleport eliminates the need for exposed public-facing services using a reverse tunnel architecture. Rather than relying on VPNs, firewalls, or jump hosts, Teleport treats identity as the new perimeter, enforcing policy-based access directly at the protocol layer. Capabilities include:

- **End-to-End Encryption & Session Recording:** Every session through Teleport is end-to-end encrypted using modern cryptographic protocols. Session recordings and audit logs ensure full traceability and enable quick detection of unauthorized or anomalous access patterns.
- **Network Access Control & Protocol-Aware Proxies:** Teleport handles multiple protocols (SSH, RDP, Kubernetes, MySQL, PostgreSQL, MongoDB, HTTP) through a single port, reducing complexity and enhancing observability.
- **Mutual mTLS Authentication:** Remote infrastructure initiates outbound connections to the Teleport proxy, creating mutual TLS-authenticated tunnels. This avoids opening inbound ports on sensitive systems, reducing the attack surface and simplifying firewall rules. All connections are authenticated with identity-bound, short-lived certificates.

© 2025 Gravitational Inc. All rights reserved.

DoD Zero Trust Pillar 4: Application Workload Security

This pillar focuses on protecting the integrity, availability, and confidentiality of applications and workloads; whether they reside on-premises, in the cloud, or at the edge. In a Zero Trust architecture, workloads must not inherently trust other workloads, even if they exist on the same network or environment. Instead, access must be tightly controlled, continuously verified, and fully observable

Highlighted Alignment with NIST 800-53 Controls

- **AC-3 (Access Enforcement):** Enforces access controls based on predefined policies.
- **AC-06 (Least Privilege):** Employ the principle of least privilege, allowing only authorized access necessary to accomplish assigned organizational tasks.
- **SI-7 (Software, Firmware, and Information Integrity):** Protects the integrity of software and applications from unauthorized changes.Teleport offers robust network security controls by securing session traffic and restricting access to only authorized users.

Teleport's Approach

Teleport delivers workload protection by unifying the identity model across all humans, machines and workloads. This approach ensures policy consistency across all non-human access and continuous verification of all users and actors interacting with applications, databases, and infrastructure. Capabilities include:

- **Fine-Grained Access Control (RBAC & ABAC):** Teleport supports both role-based access control (RBAC) and attribute-based access control (ABAC), which can be fine-tuned to specific workloads or based on user role, team, region, or risk level.
- **Cross-Service Authentication:** Teleport issues SVIDs that can be used by microservices, apps, and data pipelines to ensure consistent, secure communication across infrastructure.
- **Just-in-Time (JIT) Access for Sensitive Applications:** Teleport supports JIT access requests for workloads handling sensitive data. This includes time-bound, approval-gated access for critical systems, automatic revocation after the task window expires, and full auditability of access decisions, approvers, and session actions.
- **Dual Authorization & Session Moderation:** For sensitive operations, Teleport enables organizations to require two or more parties to approve access before a session can begin. Admins can monitor, pause, or terminate sessions in real-time, ensuring oversight and policy enforcement during sensitive activity.
- **Device Trust Enforcement:** All access to workloads is gated by device posture checks. Devices must be enrolled, verified (via TPM or MDM integration), and cryptographically trusted. This ensures that not only the user identity but also the device identity and security posture are validated before workload access is permitted.

© 2025 Gravitational Inc. All rights reserved.

DoD Zero Trust Pillar 5: Data Security

The fifth pillar of the DoD Zero Trust architecture centers on protecting sensitive data throughout its lifecycle. In a Zero Trust model, data is never assumed to be safe simply because it's inside a trusted environment. Instead, access to data must be explicitly granted, continuously monitored, and cryptographically secured.

Highlighted Alignment with NIST 800-53 Controls

- **SC-28 (Protection of Information at Rest):** Requires encryption and strong safeguards to protect sensitive data stored on physical or cloud systems.
- **AC-19 (Access Control for Mobile Devices):** Mandates restrictions and protections for devices that handle or process organizational data, especially in mobile or remote environments.

Teleport's Approach

Teleport enforces a multi-layered, identity-driven data security model to ensure all access to data is strictly controlled, logged, and encrypted. This helps to eliminate risks of data exposure caused by credential misuse, weak perimeter defenses, or lateral movement. Capabilities include:

- **Access Lists:** Teleport applies fine-grained access lists and RBAC to govern who can access which data resources. Roles can define read/write privileges down to specific nodes, databases, clusters, or even Kubernetes namespaces. Access Lists introduce temporal and conditional logic, enabling access only within defined time frames or upon multi-party approval.
- **Encrypted Communication via Reverse Tunnels:** Teleport secures all data in transit through reverse tunnels with mutual TLS authentication. All traffic flows through encrypted tunnels, initiated outbound from protected systems, eliminating the need for inbound ports or public IPs while enforcing identity-bound, certificate-based encryption, significantly reducing the risk of interception or spoofing.
- **Short-Lived Certificates:** Teleport uses ephemeral, identity-linked certificates for authentication. These credentials are short-lived and automatically expire, reducing risks from leaked keys or session hijacking. Every certificate is tied to a verified user, role, and optionally a trusted device, making each data access attempt fully attributable and auditable.
- **Session Recording & Audit Logs:** All access sessions to sensitive resources (e.g., SSH, databases, web apps) are recorded in full, capturing terminal output, commands, and keystrokes alongside metadata; all exportable to SIEM tools or long-term storage.
- **Active Session Controls:** Teleport enables security teams to respond in real-time to evolving threats with active session locking, which can immediately terminate live sessions based on signals (e.g., from an MDM, SIEM alert, or manual trigger).

© 2025 Gravitational Inc. All rights reserved.

DoD Zero Trust Pillar 6: Visibility and Analytics

The sixth pillar of the DoD Zero Trust framework emphasizes comprehensive visibility into user behavior, access attempts, and system activity. Organizations must continuously monitor their environments and analyze data in real time to detect threats, verify trust, and support informed decision-making. Visibility is foundational to both proactive defense and incident response in a Zero Trust model.

Highlighted Alignment with NIST 800-53 Controls

- **AU-2 (Auditable Events):** Requires identification and logging of key events that are security-relevant, such as access attempts, changes to permissions, and administrative actions.
- **AU-6 (Audit Record Review, Analysis, and Reporting):** Mandates regular review and analysis of audit logs to detect anomalies and support investigations or compliance requirements.

Teleport's Approach

Teleport delivers deep observability by capturing detailed logs and metadata for all infrastructure access: servers, databases, Kubernetes clusters, or web applications. This ensures that every action is recorded, attributable, and analyzable. Capabilities include:

- **Full Session Logging:** Teleport records every interactive session end-to-end, including terminal, RDP, and application sessions (e.g., kubectl exec, database queries) incorporating granular session metadata like start and end times, user identity and role, device identity, source IP and geolocation, access method, and resource target. Session recordings are stored securely, indexed, and available for real-time playback and forensic analysis.
- **Centralized Audit Trails:** Teleport generates centralized, tamper-resistant audit logs across all activity types. This includes login attempts and authentication methods used, resource access (by user, time, system, and method), privilege escalations, role changes, and administrative actions, and JIT access or approvals. Logs can be exported to SIEM platforms (e.g., Splunk, Datadog).
- **Anomaly Detection & Investigation:** By combining detailed audit trails with real-time metadata, Teleport detects unusual access patterns like logins from unfamiliar IPs, access outside business hours, or privilege misuse. Suspicious activity can be configured to be alerted, accelerating threat investigations and increasing forensic context via indexed session logs and recordings.
- **Resource-Level Insights:** Teleport's identity-aware architecture eliminates anonymous computing, spotlighting not just what happened in a session, but who did it, for what reason, and how. Insights are tied to identity, not IP address or device name, ensuring precision, and access data can be filtered by role, project, environment, or compliance classification.

© 2025 Gravitational Inc. All rights reserved.