Z

Zero Trust Architecture: Principles, Components, and Roadmap

Zero trust removes implicit trust based on network location or device ownership. Learn its core components, policy flow, implementation roadmap, and common mistakes.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What NIST means by zero trust
02 Core principles
03 Logical components
04 Zero trust pillars
05 Practical migration roadmap
06 Common mistakes
07 How to measure progress
08 Availability and privacy
09 Frequently asked questions

Quick answer: Zero trust is a security approach that grants no implicit trust solely because a user, device, or workload is inside a network or owned by the organization. Access to a resource is evaluated using identity, device, application, data, context, and policy, then limited to what is needed. Zero trust architecture is not one product and does not mean blocking everyone; it means making explicit, continuously informed access decisions.

01 What NIST means by zero trust

NIST SP 800-207 describes a shift from static network perimeters toward protecting users, assets, and resources. Network location and ownership do not create automatic trust. Authentication and authorization occur before a session to an enterprise resource is established, and policy can be reevaluated as conditions change.

Zero trust does not declare that every employee is malicious. It recognizes that credentials can be stolen, devices compromised, cloud services external, and internal networks traversed. The architecture reduces the confidence placed in any single signal.

02 Core principles

- Protect individual resources and data, not only network segments.
- Identify users, services, workloads, and devices reliably.
- Grant least-privilege access for the specific resource and task.
- Evaluate device posture and other context, not identity alone.
- Assume communication networks may be monitored or hostile and protect traffic accordingly.
- Collect telemetry and continuously improve policy from observed risk.
- Limit session duration and scope; reevaluate when risk or state changes.

03 Logical components

NIST’s model separates decision and enforcement functions:

- **Policy Engine:** decides whether access should be granted, denied, or revoked based on policy and inputs.
- **Policy Administrator:** establishes or terminates the communication path and issues the information needed to enforce the decision.
- **Policy Enforcement Point:** sits in the access path and permits, monitors, or blocks communication.
- **Information sources:** provide identity, device health, threat intelligence, resource sensitivity, logs, and other context.

Products may combine these roles or use different names. The architectural requirement is a trustworthy decision process with enforcement close enough to the resource.

04 Zero trust pillars

Implementation commonly spans identity, devices, networks, applications/workloads, and data, with visibility, analytics, automation, and governance across them. CISA’s Zero Trust Maturity Model organizes progress from traditional toward more advanced and optimized capabilities.

A strong identity program with unmanaged devices, unclassified data, and flat application access is not a complete zero trust architecture. Progress can be uneven, but dependencies must be visible.

05 Practical migration roadmap

1. **Inventory resources and flows.** Identify applications, data, users, service accounts, devices, dependencies, owners, and business-critical transactions.
2. **Choose a bounded use case.** Start with remote administration, one sensitive application, contractor access, or a cloud workload rather than “the whole network.”

3. **Strengthen identity.** Use phishing-resistant MFA, lifecycle management, privileged separation, and short-lived service credentials.
4. **Measure device and workload posture.** Define supported software, configuration, protection, and attestation requirements with recovery paths.
5. **Design least-privilege policy.** Express who or what may access which resource, for which action, under which conditions.
6. **Deploy enforcement and telemetry.** Pilot in observation mode, verify application dependencies, then enforce by controlled rings.
7. **Automate carefully.** Use risk changes to step up authentication, reduce access, or isolate systems while preserving break-glass operations.
8. **Measure and expand.** Apply lessons to the next resource set and retire redundant broad access.

06 Common mistakes

- buying a “zero trust product” without defining resources, policy, and ownership;
- requiring frequent MFA prompts while leaving broad standing privileges;
- trusting any managed device or network segment indefinitely;
- microsegmenting without understanding application dependencies and failure modes;
- ignoring service accounts, APIs, automation, and machine identities;
- collecting posture data without a response process or privacy governance;
- making controls so brittle that users create unsafe bypasses.

07 How to measure progress

Track coverage of strong identity, device visibility, resource-level policy, short-lived access, segmented high-value flows, and centralized decisions. Operational metrics include time to revoke access, percentage of dormant privileges removed, policy exceptions by age, lateral movement paths eliminated, and incidents contained to one resource set.

Do not measure zero trust only by product deployment or number of MFA prompts. The outcome is reduced implicit trust and smaller impact when one identity or device is compromised.

08 Availability and privacy

Policy engines, identity providers, device posture services, and enforcement points become critical dependencies. Design redundant decision paths, cached policy with safe limits, and tested emergency access. Collect only the telemetry needed for security decisions, protect it, set retention limits, and make employee monitoring transparent and lawful.

09 Frequently asked questions

Does zero trust eliminate VPNs?

No. A VPN may still protect transport, but network connection alone should not grant broad application access.

Is zero trust only for large enterprises?

No. Smaller organizations can start with strong MFA, device inventory, least privilege, application-specific access, and reliable logging.

Does every request require a new password prompt?

No. Policy can reuse strong session and device evidence while continuously evaluating risk and requiring step-up authentication when needed.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com