CS-004 · Foundations

Zero Trust

Never trust by default, always verify, and grant only the access that is needed right now.

Executive Summary

Zero trust is a security model that removes automatic trust based on network location. Every request to access a resource is verified using identity, device health, and context, and access is granted narrowly and only for as long as it is needed. It replaces the old idea of a trusted internal network protected by a hard outer perimeter.

What It Is

Zero trust is a strategy built on a simple premise: being inside the network does not make you trustworthy. In older designs, once a user or device was past the firewall it was largely trusted, which meant a single breach could spread freely. Zero trust treats every request as if it comes from an untrusted network. Each access decision considers who is asking, what device they are on, whether that device is healthy, and whether the request fits normal behavior. Access is then granted at the smallest scope possible and re-evaluated continuously. NIST SP 800-207 provides a widely referenced description of zero trust architecture.

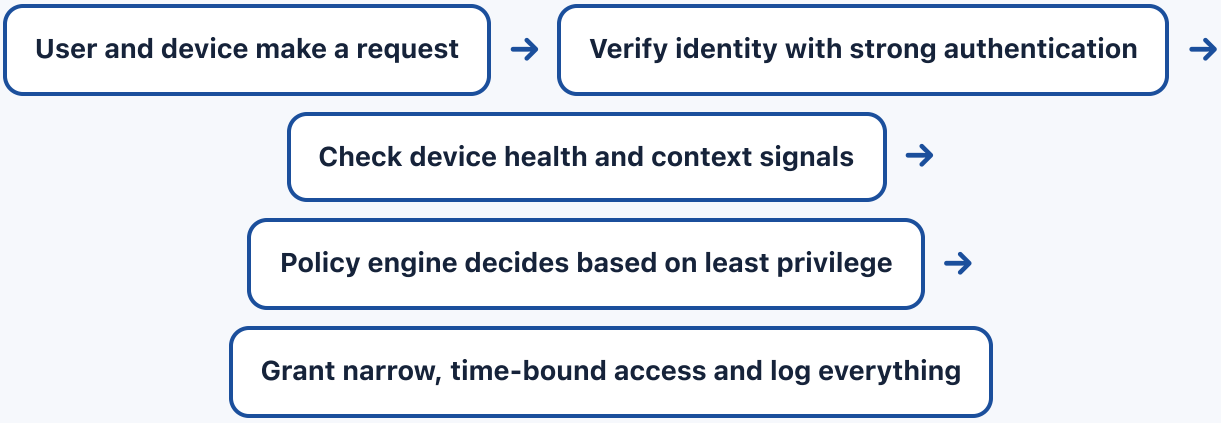
Why It Matters

Work no longer happens neatly inside one office network. Cloud services, remote work, contractors, and mobile devices mean the perimeter is porous or gone. Attackers exploit implicit trust to move laterally after an initial foothold. Zero trust directly attacks that problem by verifying every step and limiting what any single compromised account or device can reach. For organizations, it reduces the blast radius of a breach. For professionals, zero trust has become a standard expectation in architecture, engineering, and governance conversations, and many public sector programs now require progress toward it.

How It Works

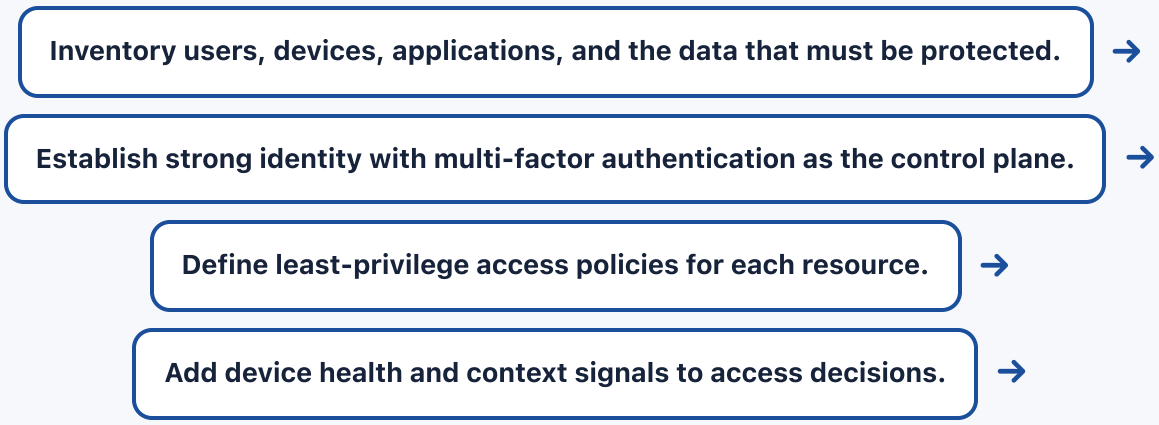
At the center of zero trust is a policy decision point that evaluates each request against rules and signals, and a policy enforcement point that carries out the decision. Signals include verified identity, device posture, location, sensitivity of the resource, and behavioral context. Strong identity with multi-factor authentication is foundational, because identity becomes the primary control plane. Microsegmentation limits how systems can talk to each other, so a breach in one area cannot spread. Access is least privilege and time bound, and everything is logged so decisions can be monitored and improved. Zero trust is a journey applied across identity, devices, networks, applications, and data, not a single product to install.

Architecture Diagram



Each request is evaluated by a policy engine using identity and context before limited, monitored access is granted.

Visual Workflow



Segment networks and applications to limit lateral movement. →

Monitor, log, and refine policies continuously based on real behavior.

Common Attacks

- Lateral movement after an attacker gains an initial foothold
- Stolen credentials used to reach systems the account should not touch
- Compromised devices connecting to sensitive resources
- Over-permissioned accounts abused to access broad data
- Insider misuse relying on implicit trust inside the network

Common Mistakes

- Treating zero trust as a single product to buy rather than a strategy
- Adding verification but leaving broad standing access in place
- Ignoring device health and relying on identity alone
- Skipping segmentation so a breach can still spread internally
- Rolling out strict controls with no logging to tune or troubleshoot them

Best Practices

- Make strong, phishing-resistant authentication the foundation
- Grant least privilege and prefer time-bound, just-in-time access
- Include device posture and context in every access decision
- Use microsegmentation to contain lateral movement
- Log all access decisions and monitor for anomalies
- Adopt zero trust incrementally, starting with the most sensitive assets

Quick Checklist

- [ ] MFA enforced everywhere, phishing-resistant methods for high-risk access

- [x] Standing broad access removed in favor of least privilege
- [x] Device health checked before granting access to sensitive resources
- [x] Network and application segmentation limiting lateral movement
- [x] Access decisions logged and reviewed
- [x] A documented roadmap moving from perimeter trust to zero trust

Recommended Tools

Identity provider with MFA and conditional access
Verifies identity and applies policy per request

Device management and posture checks
Confirms a device is healthy before granting access

Microsegmentation and software-defined perimeter
Limits which systems can reach each other

SIEM and access logging
Monitors and tunes access decisions over time

Industry Standards

NIST SP 800-207
Foundational description of zero trust architecture

CISA Zero Trust Maturity Model
Framework for measuring progress across pillars

NIST Cybersecurity Framework (CSF) 2.0
Protection and detection outcomes that zero trust supports

Career Relevance

Zero trust is a core topic for security architects, security engineers, and identity specialists, and it appears constantly in modern job descriptions. GRC analysts, auditors, and AI governance professionals must understand it to assess maturity and compliance, especially where public sector or regulated environments require progress toward it. It is one of the most in-demand security concepts today.

Interview Questions

- What problem does zero trust solve that a traditional perimeter does not?
- Why is identity often called the control plane in zero trust?
- What is microsegmentation and how does it limit an attacker?
- How would you begin a zero trust rollout in an existing environment?
- What signals besides identity should factor into an access decision?

Related Certifications

ISC2 CISSP | **CompTIA Security+** | **ISACA CISM (for governance tracks)**

Further Reading

- NIST SP 800-207 Zero Trust Architecture
- CISA Zero Trust Maturity Model
- NIST Cybersecurity Framework 2.0

Key Takeaways

- Zero trust removes automatic trust based on network location.
- Every request is verified with identity, device health, and context.
- Access is least privilege and, ideally, time bound and monitored.
- Microsegmentation limits how far a breach can spread.
- It is a strategy and a journey, not a single product to install.

FAQ

▶ **Does zero trust mean no one is trusted at all?**

▶ **Is zero trust a product I can buy?**

▶ **How is zero trust different from defense in depth?**

Related Careers

RELATED ROLES

Security Engineer | Security Architect | Grc Analyst

RELATED CERTIFICATIONS

ISC2 CISSP | CompTIA Security+ | ISACA CISM (for governance tracks)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Zero Trust**
3. Go deeper: Cybersecurity
4. Go deeper: Defense in Depth
5. Validate it: work toward **ISC2 CISSP**
6. Find the role: browse current openings

RELATED SHEETS

CS-001 Cybersecurity | CS-003 Defense in Depth | CS-005 Attack Surface | CS-009 Core Security Principles | CS-002 The CIA Triad