

ZERO TRUST ARCHITECTURE.



Zero trust replaces a single perimeter check with continuous verification of every request — **network location stops implying trust, and identity, device posture, and policy decide access instead.**

- CONTINUOUS VERIFICATION
- MICROSEGMENTATION
- LEAST-PRIVILEGE ACCESS
- IDENTITY AS THE PERIMETER

01 THE MECHANISM

No Implicit Trust from Network Location

Being inside the corporate network or VPN no longer grants trust by itself — **every request is authenticated and authorized on its own merits**, regardless of whether it originates inside or outside the traditional perimeter.

Per-Session, Least-Privilege Access

Access is granted for a specific session to a specific resource, not as a standing network-wide privilege — **a credential that works for one application doesn't automatically open the door to everything else.**

Continuous Verification, Not One-Time Login

A policy engine re-evaluates identity, device posture, and behavioral signals throughout a session, not just at initial login — **a device that becomes compromised mid-session can lose access before real damage happens.**

02 THE FLOW

The Zero Trust Network CONTAINED

1

Every access request, wherever it originates, is authenticated and authorized against dynamic policy before a policy enforcement point opens a session-specific connection.

2

Microsegmentation confines each resource to its own isolated zone, so **a compromised device can only reach what its specific session was authorized to touch.**

3

Continuous monitoring of device posture and behavior lets the policy engine **revoke access mid-session** the moment risk signals change, not just at the next login.

The Perimeter-Trust Network EXPOSED

1

A user or device that authenticates once at the network edge, whether via VPN or corporate Wi-Fi, is treated as broadly trusted for the rest of the session.

2

Flat network architecture means **a single compromised device can move laterally** to reach systems it was never specifically authorized to touch.

3

Access decisions are made once at login and never revisited, so **a device compromised after authentication keeps its access** until someone notices and manually intervenes.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Identity Verification & Least Privilege	Authenticates and authorizes every user and service identity per request, granting only the minimum access needed for that specific session.
Device Posture & Health Assessment	Continuously evaluates whether a requesting device meets security requirements, patched, encrypted, uncompromised, before and during access.
Microsegmentation & Network Isolation	Divides the network into small, isolated zones so a breach in one segment can't freely reach resources in another.
Application & Data-Layer Access Control	Enforces access decisions at the individual application and data-resource level, not just at the network perimeter.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
VPN as the Zero Trust Solution	No	A VPN extends network-level trust to a remote device; it doesn't verify or limit what that device can reach once connected, which is the actual goal of zero trust.
One-Time Authentication at Login Only	No	Leaves no mechanism to revoke access when a device's risk posture changes mid-session, such as after a compromise.
Flat Network with Perimeter Firewall Only	No	Stops external attackers at the edge but does nothing to contain lateral movement once any single device inside is compromised.
Buying a 'Zero Trust' Product Without an Architecture	No	No single product implements zero trust; without policy, identity, device, and segmentation working together, a point product is just one control among many.
Continuous Verification + Microsegmentation + Least Privilege + Dynamic Policy	Yes	Combines identity, device, network, and policy layers so no single trusted zone or one-time check becomes the weak link.

ZERO TRUST ARCHITECTURE.

VERIFY · SEGMENT · ENFORCE

05 PROGRAM OPERATIONS

Zero trust is an architecture, not a product. NIST SP 800-207 defines it as a set of principles and a reference architecture — no single vendor tool implements the whole model on its own.

Identity becomes the primary control plane once network location stops implying trust. That shifts significant investment toward identity verification and device posture, not just network firewalls.

The policy engine's decision is dynamic, not static. Access can be granted, narrowed, or revoked in real time based on changing signals, not fixed once at provisioning.

U.S. federal adoption was driven by specific incidents, not abstract best practice. Executive Order 14028 followed SolarWinds and Colonial Pipeline, directing agencies toward the CISA Zero Trust Maturity Model.

06 CONTROL MAPPING

NIST SP 800-207

The foundational Zero Trust Architecture reference, defining core tenets and the policy engine, administrator, and enforcement point components.

CISA ZERO TRUST MATURITY MODEL

Five pillars — Identity, Devices, Networks, Applications & Workloads, and Data — each scored from Traditional through Optimal maturity.

EXECUTIVE ORDER 14028

The 2021 U.S. presidential order directing federal agencies to develop zero trust implementation plans following major incidents.

OMB M-22-09

Specific federal zero trust strategy goals and deadlines, operationalizing Executive Order 14028 for U.S. agencies.

07 WHAT THIS DOES NOT SOLVE

Insider Threat with Legitimate Access

Zero trust limits what a compromised credential can reach, but a **legitimately authorized insider acting within their granted access** isn't stopped by access controls alone.

Application-Layer Vulnerabilities

Verifying identity and device posture doesn't patch a **vulnerability in the application code itself** that an authorized session can still exploit.

Third-Party & Supply Chain Risk

Zero trust governs access within the enterprise's own policy engine; it doesn't extend automatically to **trust decisions inside a vendor's separate environment**.

Overnight Implementation

Zero trust maturity models exist specifically because **the migration from perimeter-based architecture is a multi-year program**, not a single deployment.

08 MYTHS VS. REALITY

MYTH

"Zero trust means the network trusts nothing and no one, ever."

REALITY

It means **trust is never implicit or permanent** — access is still granted, just continuously verified against dynamic policy rather than assumed from network location.

MYTH

"A VPN with strong MFA is basically zero trust."

REALITY

A VPN still grants broad **network-level access once connected**; zero trust replaces that with per-application, per-session access decisions instead.

MYTH

"Zero trust is a single product you can purchase and deploy."

REALITY

NIST describes it as **an architecture and set of principles** spanning identity, device, network, and data controls — no one tool implements the whole model.

MYTH

"Zero trust is only relevant to large enterprises or government agencies."

REALITY

The **core principles apply at any scale** — the CISA and NIST models describe a maturity journey, not a threshold an organization must be large enough to reach.

MYTH

"Once zero trust is implemented, ongoing monitoring becomes less important."

REALITY

Continuous monitoring and policy re-evaluation are **core to how zero trust actually works**, not a legacy practice it replaces.

09 SPEAK THE PROGRAM — KEY TERMS

POLICY ENGINE (PE)

The component that **decides whether to grant, deny, or revoke access** to a resource based on enterprise policy and real-time signals.

POLICY ENFORCEMENT POINT (PEP)

The component that **opens, monitors, and terminates the actual connection** between a subject and a resource per the policy engine's decision.

MICROSEGMENTATION

Dividing a network into **small, isolated zones** so lateral movement between them requires its own separate authorization.

ZERO TRUST NETWORK ACCESS (ZTNA)

The practical technology replacing VPNs, granting access to **specific applications after verification**, rather than broad network-level connectivity.

CONTINUOUS VERIFICATION

Re-evaluating identity, device posture, and behavior **throughout a session**, not only at the initial login.

LEAST-PRIVILEGE ACCESS

Granting only the **minimum access necessary for a specific task or session**, often on a just-in-time basis rather than as a standing permission.