

ZERO TRUST
ARCHITECTURE.

A security model where **no user, device, or network flow is trusted by default** — inside the perimeter or outside it. Every request is verified, authorized, and continuously re-evaluated before access is granted.

- NEVER TRUST, ALWAYS VERIFY
- LEAST PRIVILEGE ACCESS
- MICRO-SEGMENTATION
- CONTINUOUS VERIFICATION

01 THE MECHANISM



Identity Verification
Every user and device is **authenticated and authorized before every access request**, not just at login.



Micro-Segmentation
Networks are broken into **small, isolated zones** so lateral movement is contained if one segment is compromised.



Continuous Monitoring
Session risk is **re-evaluated in real time** using signals like device posture, location, and behavior.

02 THE FLOW

The Access Cycle PER-REQUEST

1

A user or device requests access to a **specific resource** — never granted network-wide trust.

2

The policy engine evaluates **identity, device posture, and context** against policy before granting a session.

3

Access is **scoped to the minimum privilege** needed for that specific task.

The Trust Cycle CONTINUOUS

1

Session signals — location, device health, behavior — are monitored throughout the session, not just at login.

2

Anomalies trigger **re-authentication or step-up verification** mid-session.

3

Trust decays over time — sessions and tokens expire and must be re-verified.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT ENFORCES
Identity & Access Management	Verifies who is requesting access via MFA, SSO, and continuous authentication.
Device Trust & Posture	Confirms device health, patch level, and compliance before granting access.
Network Micro-Segmentation	Isolates workloads and resources so compromise in one zone doesn't spread.
Data & Application Access	Enforces least-privilege, resource-level authorization for every request.

04 ACCESS MODELS COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
VPN Perimeter Access	No	Grants broad network trust once connected; lateral movement goes undetected.
Firewall Rules Alone	No	Static rules don't adapt to user identity, device health, or behavior.
One-Time Login Authentication	No	Trust is assumed for the entire session regardless of changing risk.
Network Location (Internal Trust)	No	Assumes anything inside the perimeter is safe — the core flaw zero trust eliminates.
Combined Zero Trust Architecture (Identity + Device + Micro-Segmentation)	Yes	Continuously verifies every request regardless of network location.

ZERO TRUST.

VERIFY · SEGMENT · MONITOR

05 PROGRAM OPERATIONS

Trust is never implicit, even inside the network.

Every access request is evaluated on its own merits.

Least privilege must be enforced by default.

Users and services get only the access required for their specific task.

Assume breach as a design principle.

Segmentation limits how far an attacker can move if one credential or device is compromised.

Rollout is incremental, not a one-time switch.

Most organizations phase in identity, then device, then network segmentation.

06 CONTROL MAPPING

NIST SP 800-207

Foundational **zero trust architecture** reference model.

CISA ZERO TRUST MATURITY MODEL

Five-pillar **maturity roadmap** for federal and enterprise adoption.

NIST CSF 2.0

Protect function coverage for access control and identity management.

CIS CONTROLS V8.1

Account and access control management safeguards.

07 WHAT THIS DOES NOT SOLVE

Insider threats with valid access

Authorized users can still **misuse** legitimately granted permissions.

Supply chain compromise

Trusted vendor software can still introduce **backdoors** before access controls apply.

Social engineering

A convincing phishing attempt can still trick a **verified user** into approving access.

Poor policy design

Overly broad policies **re-create implicit trust** even inside a zero trust model.

08 MYTHS VS. REALITY

MYTH	REALITY
"Zero trust means we don't trust our employees."	It means access is verified continuously , not that people are inherently suspect.
MYTH	REALITY
"A VPN makes us zero trust."	VPNs grant broad network access once connected — the opposite of the zero trust model.
MYTH	REALITY
"Zero trust is a single product we can buy."	It's an architecture and set of principles applied across identity, device, and network tools.
MYTH	REALITY
"Once implemented, zero trust is done."	Policies and trust signals must be continuously tuned as the environment changes.
MYTH	REALITY
"Zero trust only applies to remote access."	It applies equally to on-premises traffic — internal network location grants no special trust .

09 SPEAK THE PROGRAM — KEY TERMS

ZERO TRUST

A security model that treats **no user, device, or network** as trusted by default, regardless of location.

MICRO-SEGMENTATION

Dividing a network into **small isolated zones** to contain lateral movement after compromise.

LEAST PRIVILEGE

Granting only the **minimum access required** to complete a specific task.

POLICY ENGINE

The component that evaluates identity, device, and context signals to **grant or deny** each access request.

DEVICE POSTURE

The security health state of a device, including **patch level, encryption, and compliance**.

CONTINUOUS AUTHENTICATION

Ongoing verification of user and session trust **throughout access**, not just at login.