Zero Trust

Cisco Partner
https://cs.co/1page

A **Zero Trust** Architectural Framework involves restricting access to system, application, and data resources to those users and devices that are specifically validated as needing access. It will then continuously authenticate their identity and security posture to ensure proper authorization for each resource to provide ongoing access.

Benefits:

Education:
- Holistic, complete view of data and devices.
- Ability to detect and remediate security incidents faster.
- Reduced complexity through consolidation of multiple security capabilities.
- Ability to support students, faculty and staff from anywhere on any device.

Financial Services, Manufacturing, Retail & Transportation:
- Eliminates the trade-off between business security and user productivity.
- Improves security resilience across the entire institution.
- Decreases risk and cost of a data breach.
- Delivers faster threat response and ROI.
- Addresses evolving security regulations.

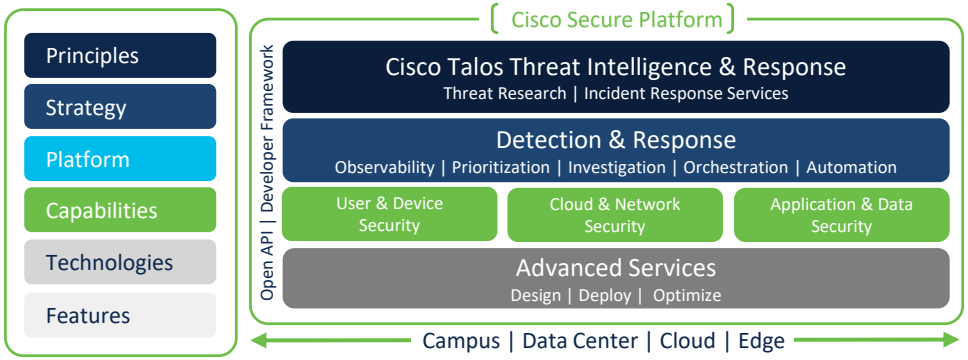
Healthcare:
- Enables secure access for employees, patients, ecosystem partners, applications and devices, across networks and cloud environments.
- Protect legacy applications, endpoints, medical and IOT devices via segmentation and continuous policy enforcement.

Media & Entertainment:
- Improves security resilience across an entire venue.
- Decreases risk and cost of a data breach.
- Provides the ability to manage dispersed infrastructure.
- Delivers faster threat response and ROI.

Utilities, Mining, Oil & Gas:
- Enables secure access for employees, customers, ecosystem partners, applications and devices, across networks and cloud environments.
- Protects legacy applications, endpoints, control systems and instrumentation devices via segmentation and continuous policy enforcement.

Discovery Questions:

- What users and devices are on the network?
- Is the user accessing the network who they say they are?
- Does the user have access to the right applications?
- How many devices in your network are unprotected, unmanaged?
- What would you do if anyone of these devices became infected?



Key Zero Trust Strengths:

Establish Trust:
- User / device / service identity
- Posture + context
- Risk-based authentication

Continuously Verify Trust:
- Re-assessment of trust
- Indicators of compromise
- Shared signals
- Vulnerability management
- Behavior monitoring (threat/non-threat)

Enforce Trust-Based Access:
- Micro-segmentation
- Unified access control
- Least privilege + explicit trust

Respond to Change in Trust:
- Prioritized incident response
- Orchestrated remediation
- Integrated + open workflows

Cisco Solutions:

User & Device Security:
- Cisco Duo
- Secure Endpoint
- Secure Email
- Vulnerability Mgmt.

Network & Cloud Security:
- Identity Services Engine (ISE)
- Umbrella
- Secure Firewall
- Secure Network Analytics
- Cyber Vision

Application & Data Security:
- Secure Workload
- Cloud Application Security

Resources:

SalesConnect
BDM / TDM
At-a-Glance
Proposal Template
Conversation Starters
ZT Architecture
ZT Frameworks
ZT Networking
ZT Workshops
ZT Workshop AAG
Public page