Cisco Zero Trust

Secure access for the workforce, workloads and workplace

Milan Habrcetl, Cisco Cybersecurity Specialist

October 24th, 2019

Shift in IT Landscape

Users, devices and apps are everywhere

Remote Users, Contractors & Third-Parties

Personal & Mobile Devices

IoT Devices

Evolving Perimeter

Office 365

Cloud Applications

Hybrid Infrastructure

aws

Cloud Infrastructure

Business Challenges

Increased access, attack surface & gaps in visibility

How do we know users are who they say they are?

Are their devices secure & up to date?

What's on the network? How does it connect?

Excessive Trust

What data's in the cloud? Who/what accesses it?

How can we view & secure all connections?

What exists in the cloud? How does it connect?

Threats Today, As a Result

A new approach to security is needed – zero trust – to address identity, app & network threats.

Targeting Identity

81% of breaches involved compromised credentials

Targeting Apps

54% of web app vulnerabilities have a public exploit available

Targeting Devices

300% increase in IoT malware variants

Enabling Secure Access

Take a zero-trust approach to security to secure access across your entire IT environment.

Prevent Risks

Reduce risk of a breach before it happens

Gain Visibility

Identify risks and indicators of a breach of trust

Reduce Attack Surface

Contain breaches and stop attacker lateral movement

The Zero Trust Approach

Enable policy-based controls for every access request in a corporate environment

See who and what is accessing applications, workloads & the network

Segment your network & workloads by enforcing granular controls

Cisco Zero Trust

A zero-trust approach to securing access across your applications and environment, from any user, device and location.

Workforce
Ensure only the right users and secure devices can access applications.

Workload
Secure all connections within your apps, across multi-cloud.

Workplace
Secure all user and device connections across your network, including IoT.

Enforce Policy-Based Controls

How Cisco Verifies Trust

Establishing trust before granting access or allowing connections in your environment:

Workforce

+ Is the user who they say they are?

+ Do they have access to the right applications?

+ Is their device secure?

+ Is their device trusted?

Workload

+ What applications are used in the enterprise?

+ What is communicating with applications/data?

+ Is communication w/ the workload secure & trusted?

Workplace

+ Do users & devices authenticate for network access?

+ What access are they granted?

+ Are devices on the network secure?

+ Is their network segmentation based on trust?

Workforce
How to Verify Trust

Verify users' identities

WITH

Multi-factor authentication (MFA)

Gain device visibility & establish trust

WITH

Endpoint health & management status

Enforce access policies for every app

WITH

Adaptive & role-based access controls

Workloads
How to Verify Trust

Gain visibility into what's running & what's critical

BY

Identifying workloads & enforcing policies

Contain breaches & minimize lateral movement

WITH

Application micro-segmentation

Alert or block communication if policy is violated

BY

Continuously monitoring & responding to indicators of compromise

Workplace
How to Verify Trust

Grant the right level of network access to users and devices

WITH

Network authentication & authorization

Classify & segment users, devices & apps on your network

WITH

Network segmentation

Contain infected endpoints and revoke network access

BY

Continuously monitoring & responding to threats

Extended Protection

Complementary products to extend trust for any app, any workload & any network.

Workforce
Cloud & On-Prem Apps

Workload
Hybrid & Multi-Cloud

Workplace
LAN, WAN, SD-WAN, ACI

+ Extend Trust

Umbrella AMP Next-Generation Firewall AnyConnect ACI
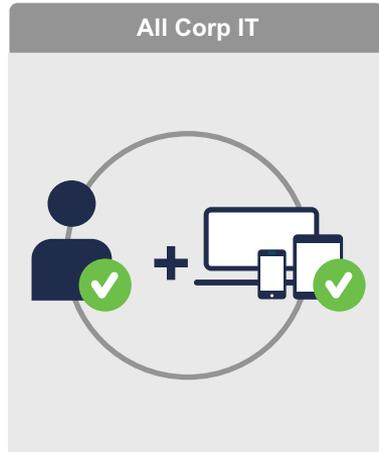
CloudLock Meraki Email Security

+ Detect & Respond

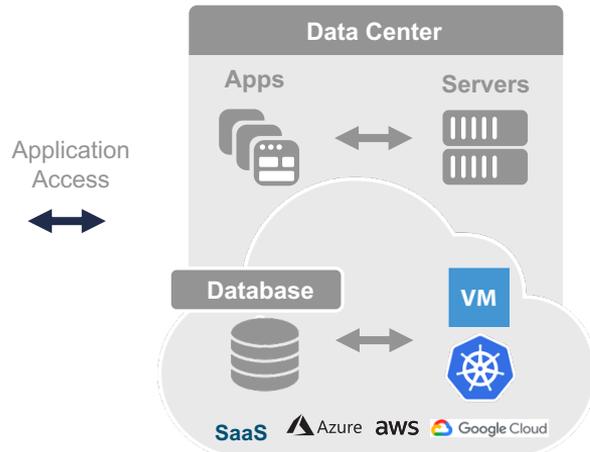Cisco Threat Response (CTR) Stealthwatch

Cisco Zero Trust

Secure the Workforce
With Duo

All Corp IT

Application
Access

Secure Your Workloads
With Tetration

Data Center

Apps   Servers

Database   VM

SaaS   ▲ Azure aws ☁ Google Cloud

WAN
Routing

Secure the Workplace
With Software-Defined Access

Corporate Network

Network
Traffic   Wireless

IoT
Devices   User &
Devices

User & Device Access

Workload Access

Network Access

MFA + Device Trust

Application Micro-Segmentation
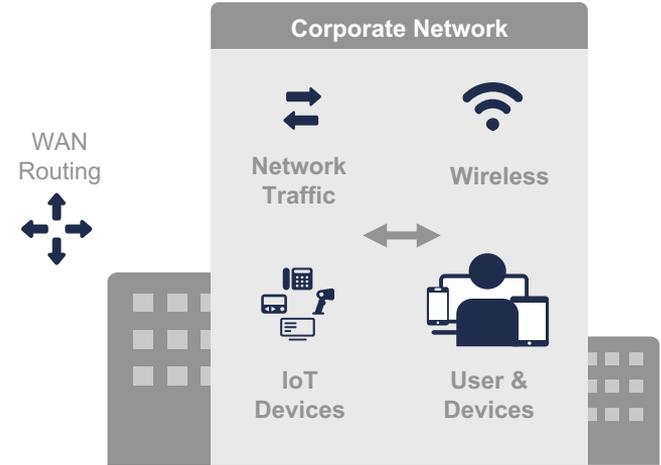
Network Segmentation

| **Visibility** | **Policy** | **Enforce** | **Report** |

Thank you!