Zero Trust Networks

Evan Gilman
About Me

@evan2645
Agenda

The Problem
What is Zero Trust?
Implementations
State of the Union
The Problem
Users feel safe inside

Enforcement
Even if they are not Bad Guy

Enforcement
Even if they are not

… Am I really *that* safe?

Bad Guy

Enforcement
What Are We Protecting?
Common Sense Security

Important Server

Enforcement
Common Sense Security

Important Server

Enforcement
What is Zero Trust?
What is Zero Trust?
What is a Zero Trust Network?

No Pools of Trust

Internet Security Everywhere

All Flows Strongly Authenticated + Authorized
Zero Trust Networks

Required

Primitive

Optional

Advanced
Manifestation
Control Plane Services

User Inventory

Device Inventory

Data Plane

Servers

Phones

Laptops
Control Plane Services

User Inventory

Device Inventory

Config Mgmt

Data Plane

Servers

Phones

Laptops
Control Plane Services

Data Plane

User Inventory
Device Inventory
Config Mgmt
Authentication Services

Servers
Phones
Laptops
Control Plane Services

User Inventory

Device Inventory

Config Mgmt

Authentication Services

Data Plane

Servers

Phones

Laptops
Examples
Server-Side
PagerDuty

Multiple Cloud Providers
PagerDuty

Multiple Cloud Providers
PagerDuty

Multiple Cloud Providers

Cross-WAN
PagerDuty

Multiple Cloud Providers

Cross-WAN

Strong Authenticity + Privacy
PagerDuty

Multiple Cloud Providers

Cross-WAN

Strong Authenticity + Privacy

Topology-Manager
Topology-Manager

Control Plane

Data Plane

Server
Agent
Contained Workload

Server
Agent
Contained Workload

Enforcement

@evan2645
Topology-Manager

Control Plane

Data Plane

Server
Agent
Contained Workload

Enforcement

Server
Agent
Contained Workload
Topology-Manager

Control Plane

Data Plane

Enforcement

Server
Agent
Contained Workload

Server
Agent
Contained Workload
Zero Trust: Building Systems in Untrusted Networks

Topology-Manager

Control Plane

Data Plane

Server
Agent
Contained Workload

Server
Agent
Contained Workload

Enforcement

@evan2645
Topography-Manager

Control Plane

Data Plane

Enforcement

Server
Agent
Contained Workload

Server
Agent
Contained Workload
Topology-Manager

Control Plane

Data Plane
Topology-Manager

Authorized User

Control Plane

Data Plane
Topology-Manager

Provisioner

Authorized User

Control Plane

Data Plane
Zero Trust: Building Systems in Untrusted Networks

Topology-Manager

Provisioner

Authorized User

Device Inventory

Control Plane

Data Plane
Topology-Manager

Provisioner

Device Inventory

User Inventory

Authorized User

Control Plane

Data Plane
Topology-Manager

Provisioner

Authorized User

Device Inventory

User Inventory

Control Plane

Data Plane

@evan2645
Topology-Manager

- Provisioner
- Device Inventory
- User Inventory
- Authorized User
- Config Mgmt

Control Plane
Data Plane
Topology-Manager

No Trust In Network
Topology-Manager

No Trust In Network

Compute Can Be Bootstrapped Anywhere
Topology-Manager

No Trust In Network

Compute Can Be Bootstrapped Anywhere

All Flows Get Strong AuthN/AuthZ
Client-Side
Client-Side
Client-Side
Google

Large Network, Large Perimeter
Google

Large Network, Large Perimeter

Many Remote Employees
Google

Large Network, Large Perimeter

Many Remote Employees

Perimeter + Remote Access Untenable
Google

Large Network, Large Perimeter

Many Remote Employees

Perimeter + Remote Access Untenable

BeyondCorp
BeyondCorp
BeyondCorp

Control Plane

Data Plane

Corp. Client
BeyondCorp

Control Plane

Data Plane

Corp. Client

Access Proxy
BeyondCorp

Control Plane

Data Plane

Corp. Client → Access Proxy

Enforcement
BeyondCorp

Control Plane

Data Plane

Corp. Client → Access Proxy → Backend

Enforcement
BeyondCorp

Control Plane

Data Plane

Corp. Client → Access Proxy → Backend

Enforcement

@evan2645
BeyondCorp

User Inventory

Control Plane

Data Plane

@evan2645
BeyondCorp

User Inventory

SSO

Control Plane

Data Plane
BeyondCorp

User Inventory

SSO

Device Inventory

Control Plane

Data Plane

@evan2645
BeyondCorp

User Inventory

SSO

Device Inventory

Control Plane

Data Plane
BeyondCorp

User Inventory -> SSO

Device Inventory -> Access Control Engine

Control Plane

Data Plane
BeyondCorp

User Inventory

SSO

Device Inventory

Access Control Engine

Control Plane

Data Plane
BeyondCorp

No Trust In Network
BeyondCorp

No Trust In Network

Users Safely Roam Free
BeyondCorp

No Trust In Network

Users Safely Roam Free

All Requests Get Strong AuthN/AuthZ
BeyondCorp

No Trust In Network

Users Safely Roam Free

All Requests Get Strong AuthN/AuthZ
Mature Zero Trust
BeyondCorp

User Inventory

SSO

Device Inventory

Access Control Engine

Trust Engine

Data Plane

Control Plane
BeyondCorp

User Inventory

SSO

Device Inventory

Access Control Engine

Trust Engine

Control Plane

Data Plane
BeyondCorp

Control Plane

Data Plane

Corp. Client → Access Proxy → Backend

Score → Score
Mature Zero Trust

User Data

Device Data

Trust Engine
Mature Zero Trust

User Data

Device Data

sFlow

Trust Engine
Mature Zero Trust

User Data → Device Data → sFlow → Trust Engine → Accounting
UX is Important
UX is Important
Earth is Calling...
Earth is Calling...
Earth is Calling...
Zero Trust Networks
Evan Gilman