

Breaking the firewall:

Navigating security in a world without borders!

Keynote by:



Muzamil Rashid
Head of Cyber Security
Mazda Australia

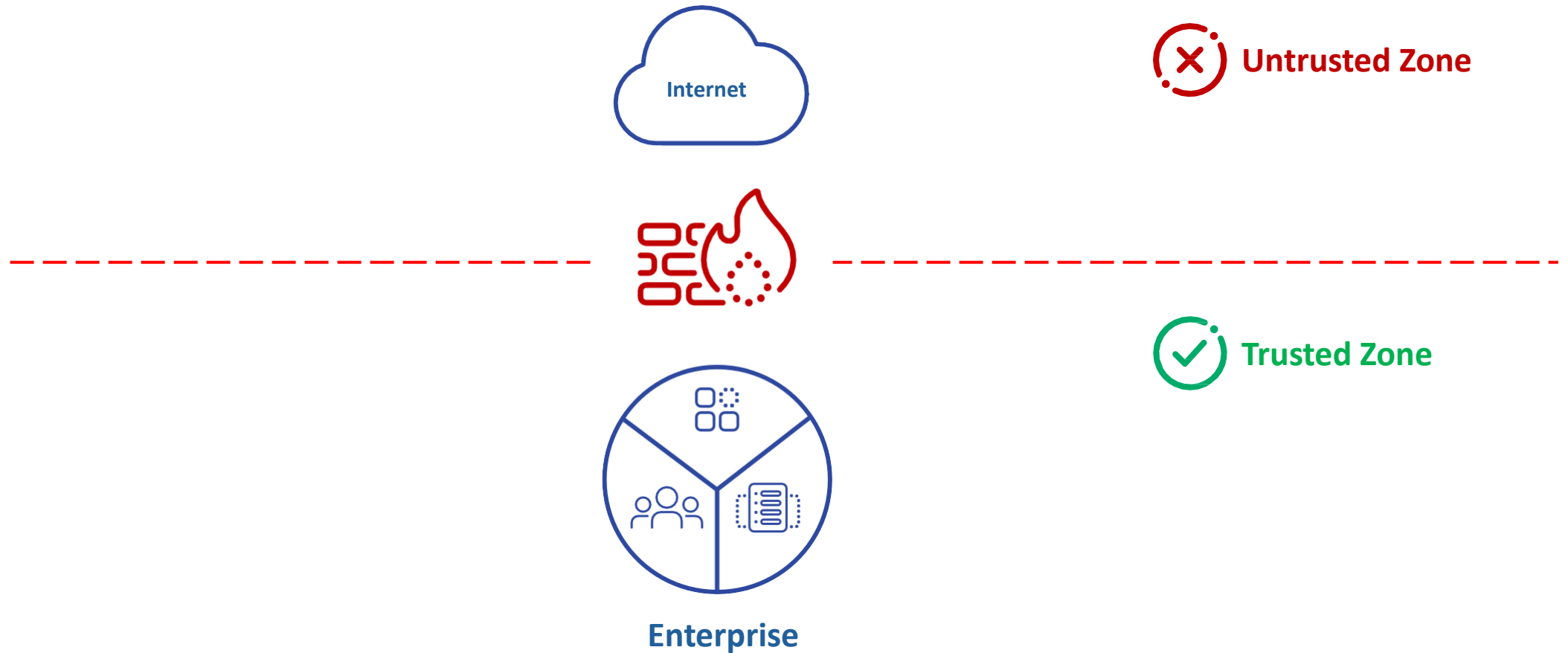
AGENDA

- 
- 01 Evolution of Corporate Networks
 - 02 Zero Trust & Micro Segmentation
 - 03 Zero Trust Use Cases
 - 04 Zero Trust Network Access (ZTNA)
 - 05 How to Get Started with Zero Trust?

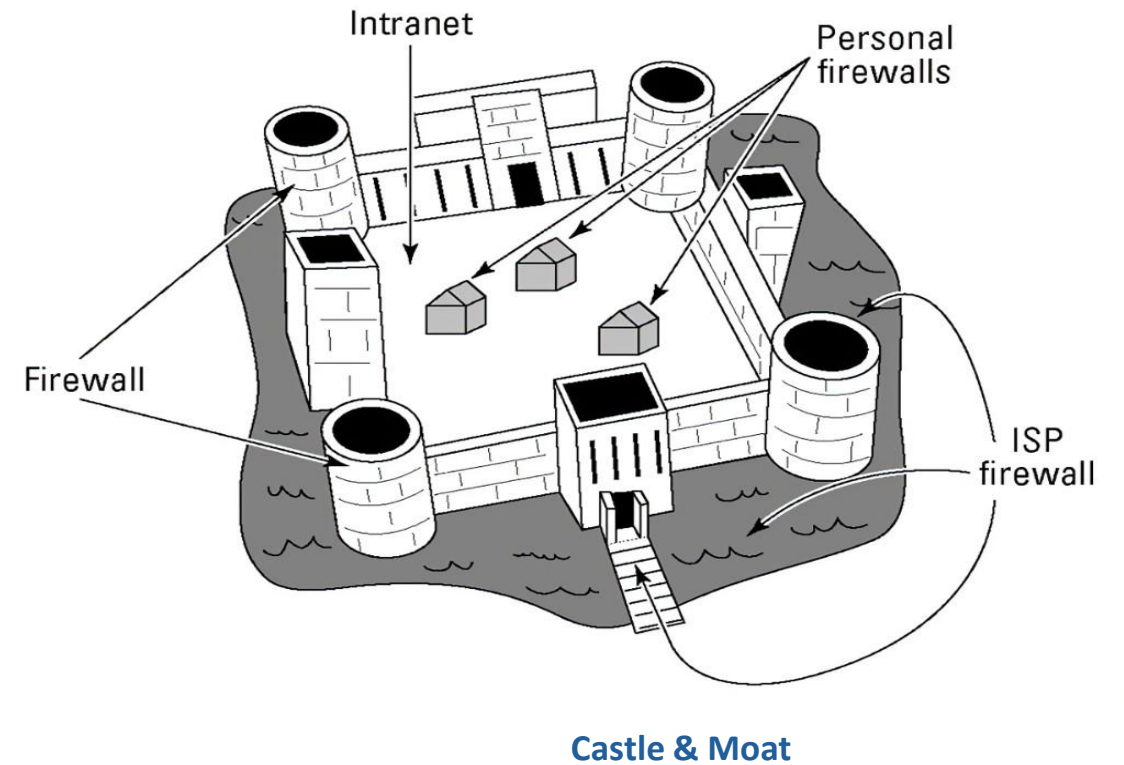
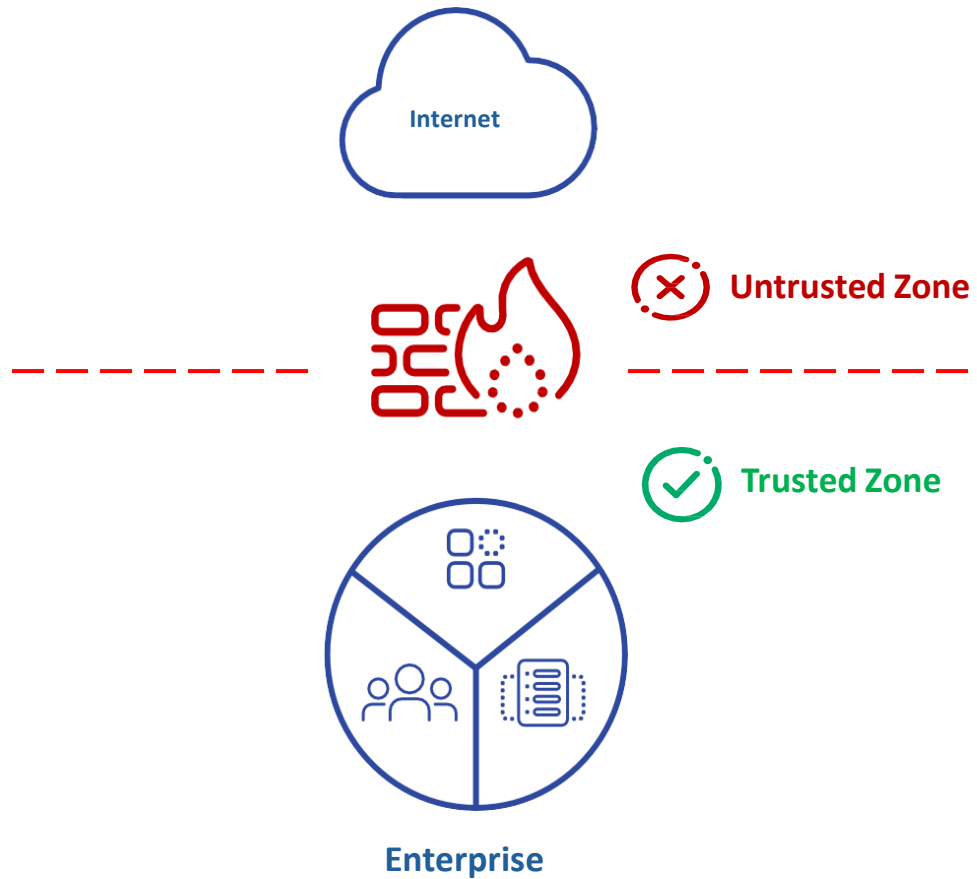
Evolution of Corporate Networks



1990s: Perimeters were *well-defined*



1990s: Perimeters were *well-defined*



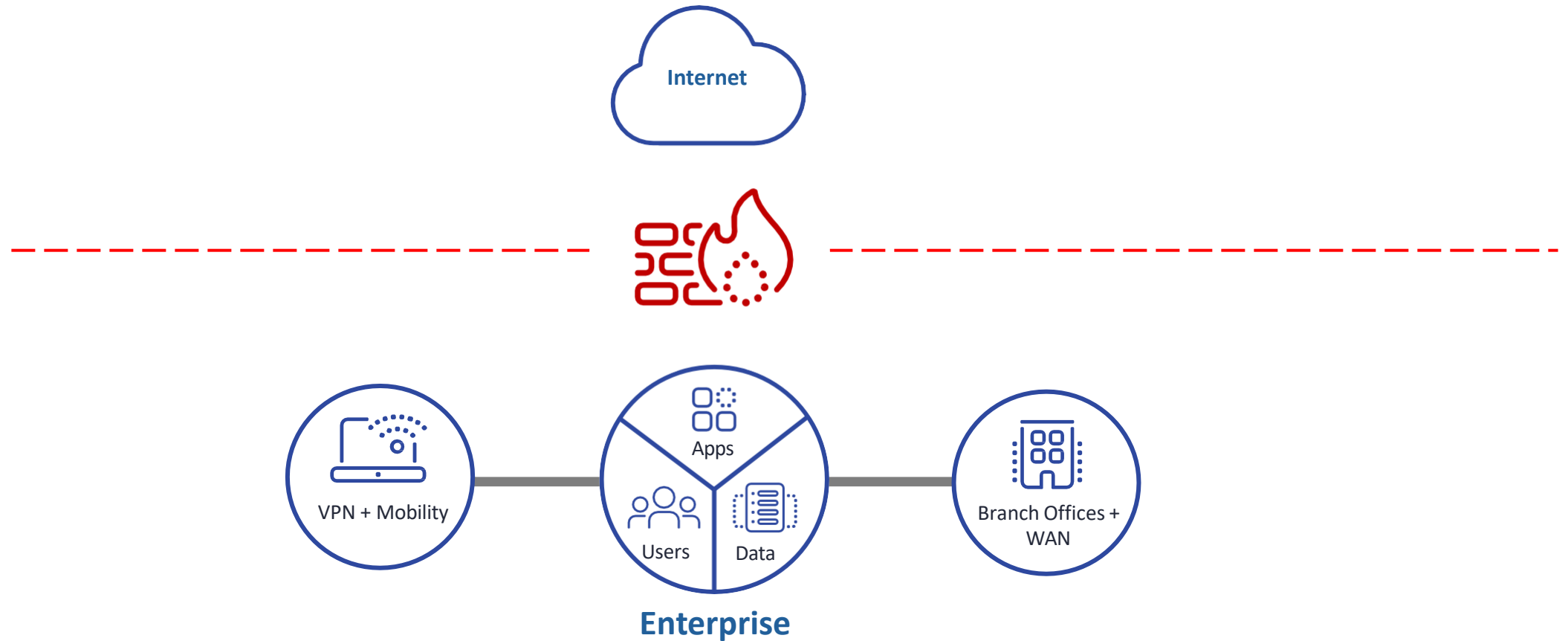
1990s: Trust Model expressed in *Hardware*



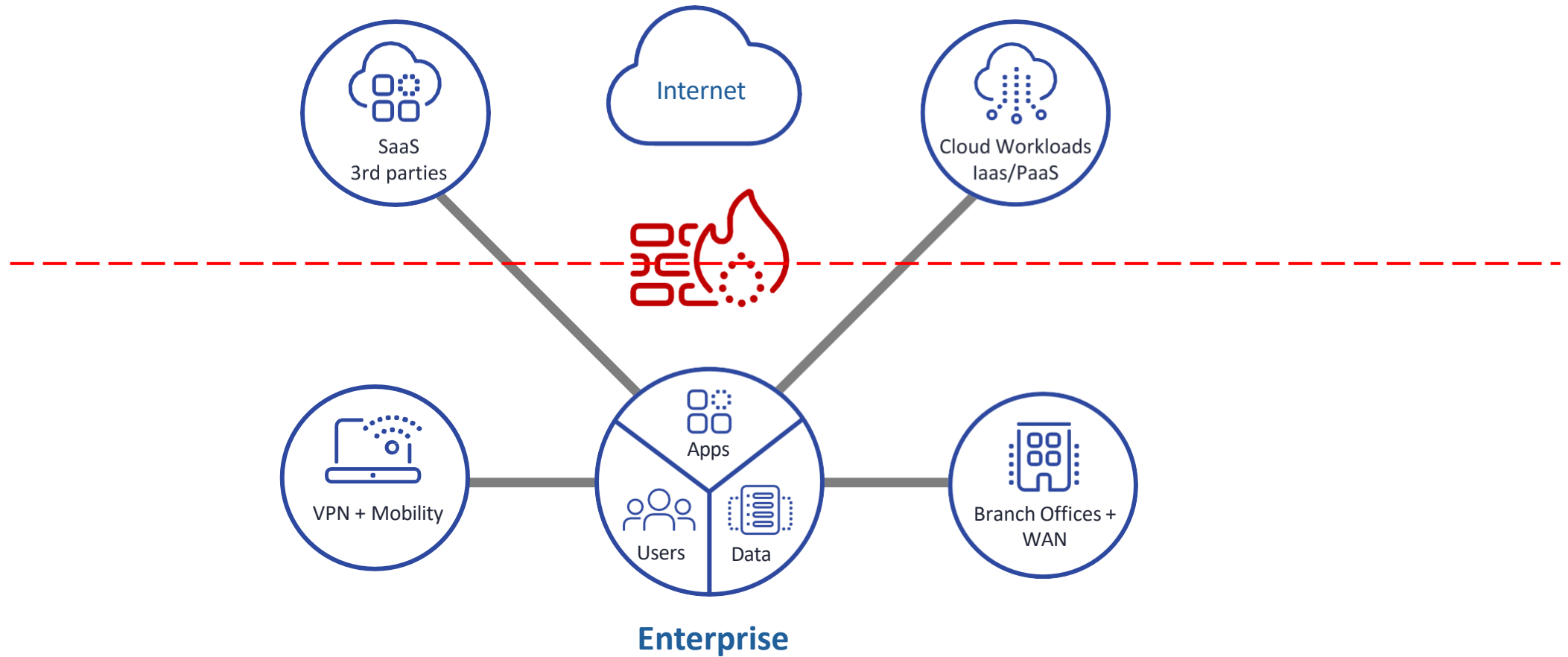
1990s: Trust Model expressed in *Hardware*



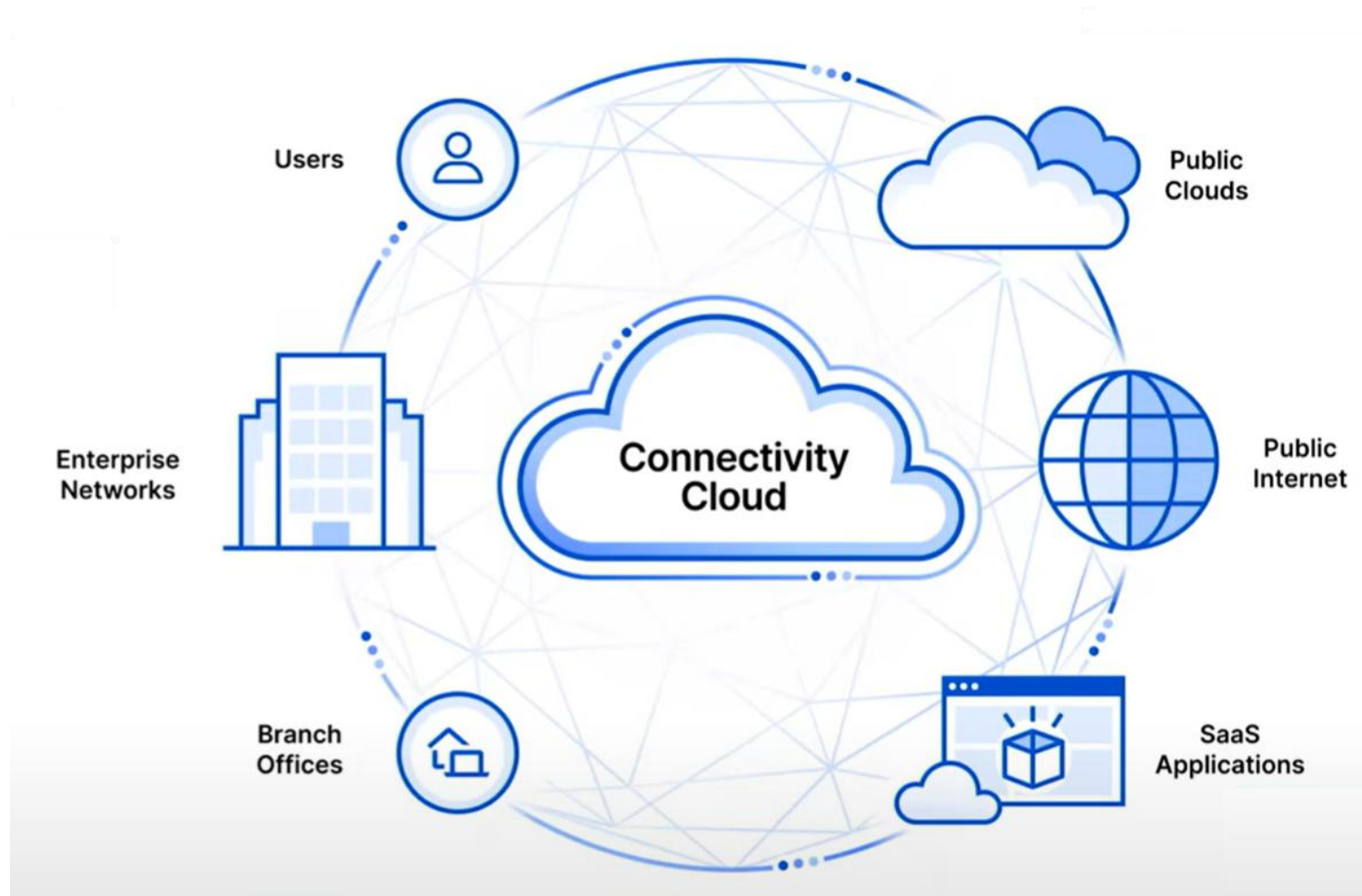
2000s: Perimeters got *extended*



2010s: Perimeters got even *extended further*



2020s: Perimeters *reimagined*

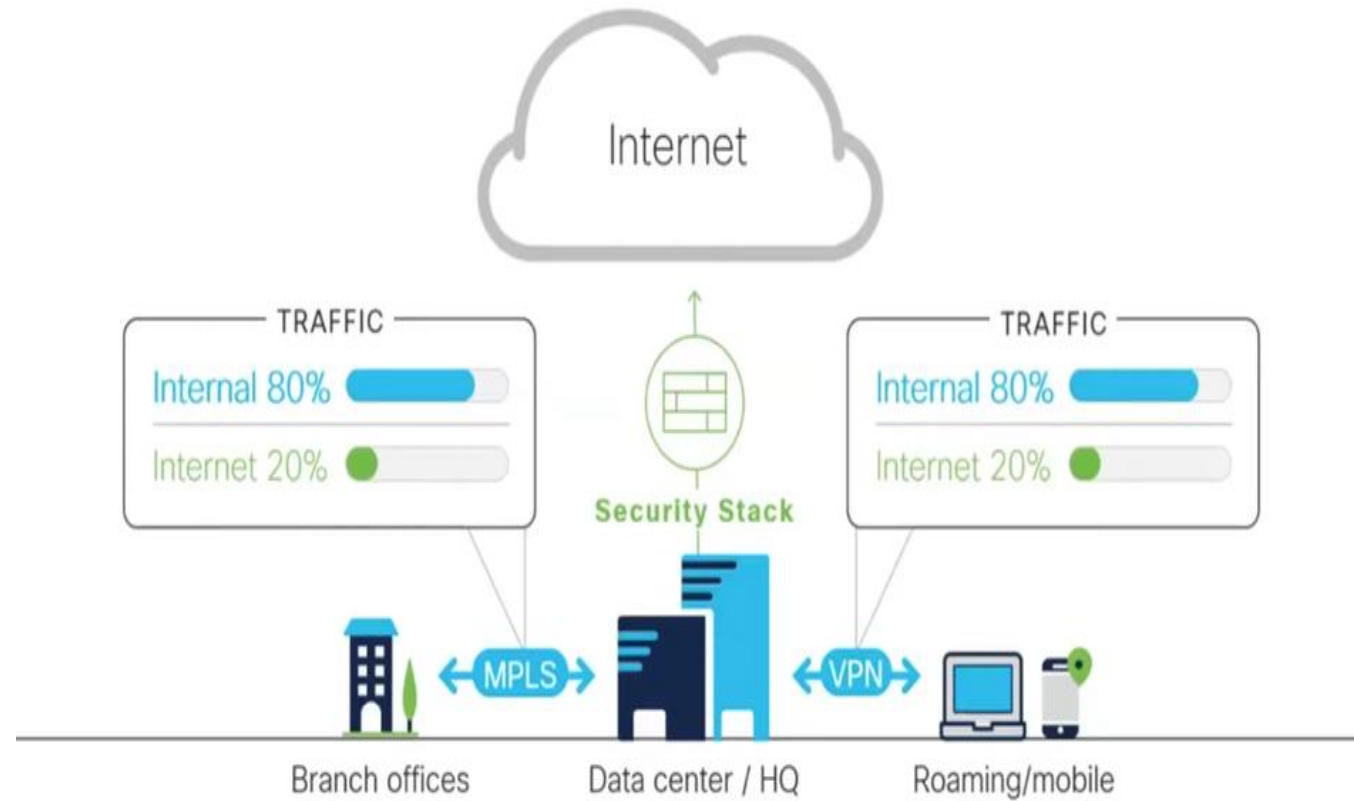


Challenge with Network-based Security



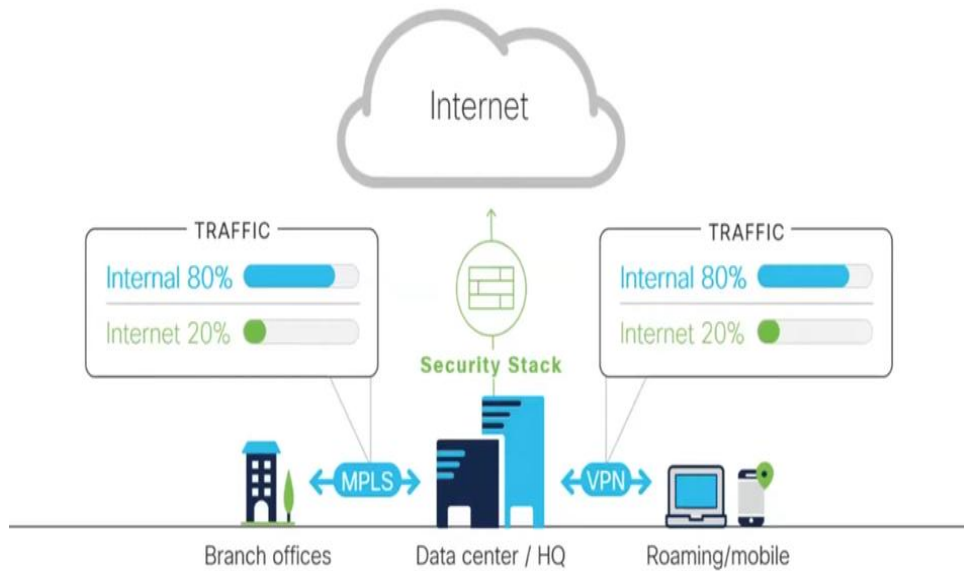
Digital Transformation inverted *traffic model*

Yesterday

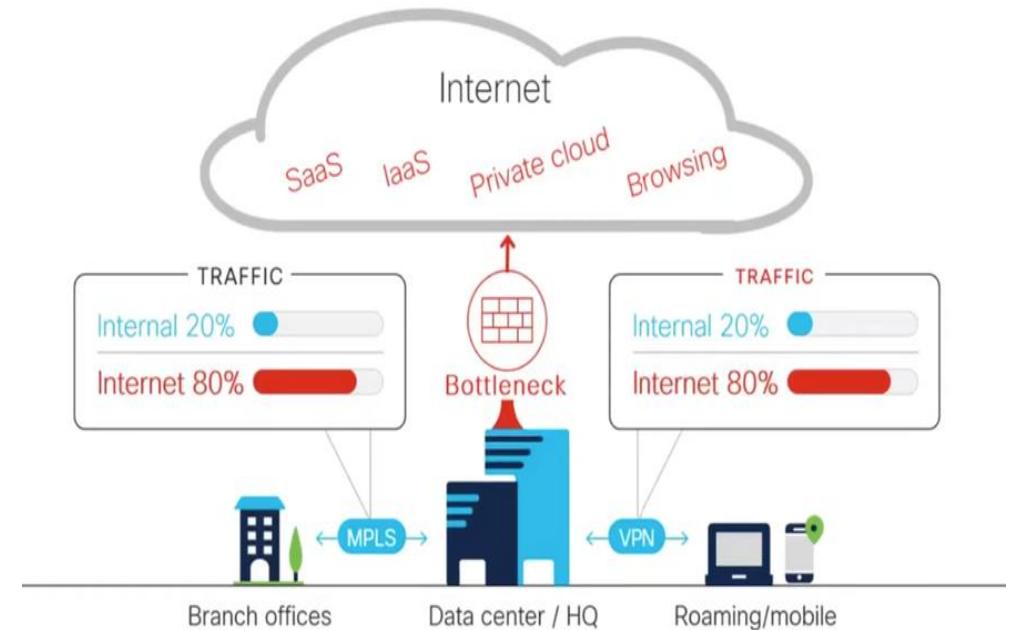


Digital Transformation inverted *traffic model*

Yesterday



Today



Insights from *DBIR REPORT 2025*



1. Verizon DBIR Report 2025: <https://www.verizon.com/business/resources/reports/dbir/>

Security Challenges posed by *users/networks*

60%

of breaches involved
*human element*¹

44%

of breaches involved
*ransomware*¹

22%

of breaches involved
*credential abuse*¹

22%

of breaches involved exploitation of
vulnerabilities on *VPN/Edge devices*¹



1. Verizon DBIR Report 2025: <https://www.verizon.com/business/resources/reports/dbir/>

Security *Blind spots*



Zero Trust to the rescue!



Zero Trust *Principles*



1. Never Trust, Always Verify

No implicit trust; **every user, device, app, and request must be authenticated and authorized**, regardless of location.



2. Enforce Least Privilege Access

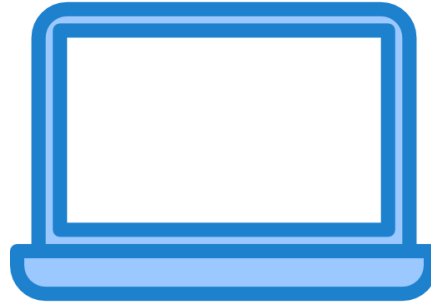
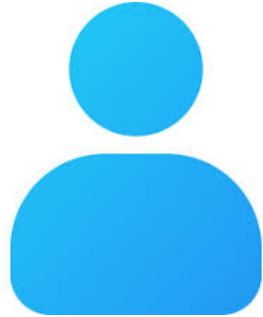
Users and devices should be **granted only the minimum access** necessary to perform their function and **nothing more**.



3. Assume Breach

Operate with the mindset that your network is already compromised.

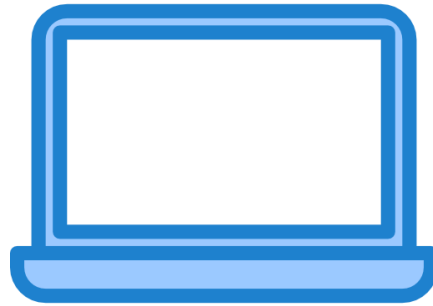
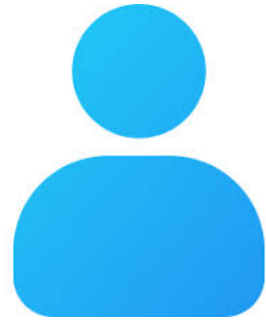
PRINCIPLE ONE : *Never trust Always verify*



= NO TRUST



PRINCIPLE ONE : *Never trust Always verify*



= NO TRUST



CREDENTIALS

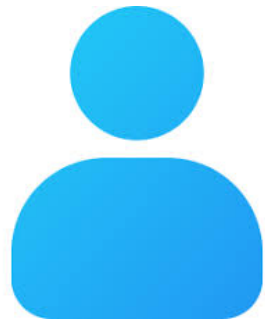


DEVICE



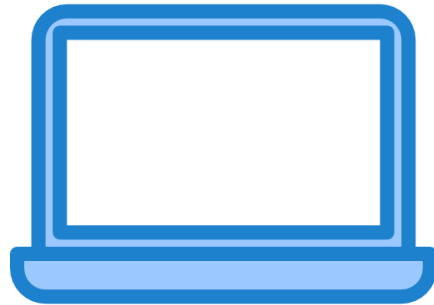
LOCATION

PRINCIPLE ONE : *Never trust Always verify*



✓ CREDENTIALS

✓ MFA

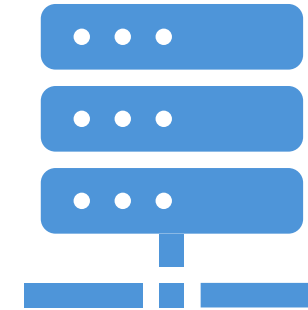


✓ UP-TO-DATE OS

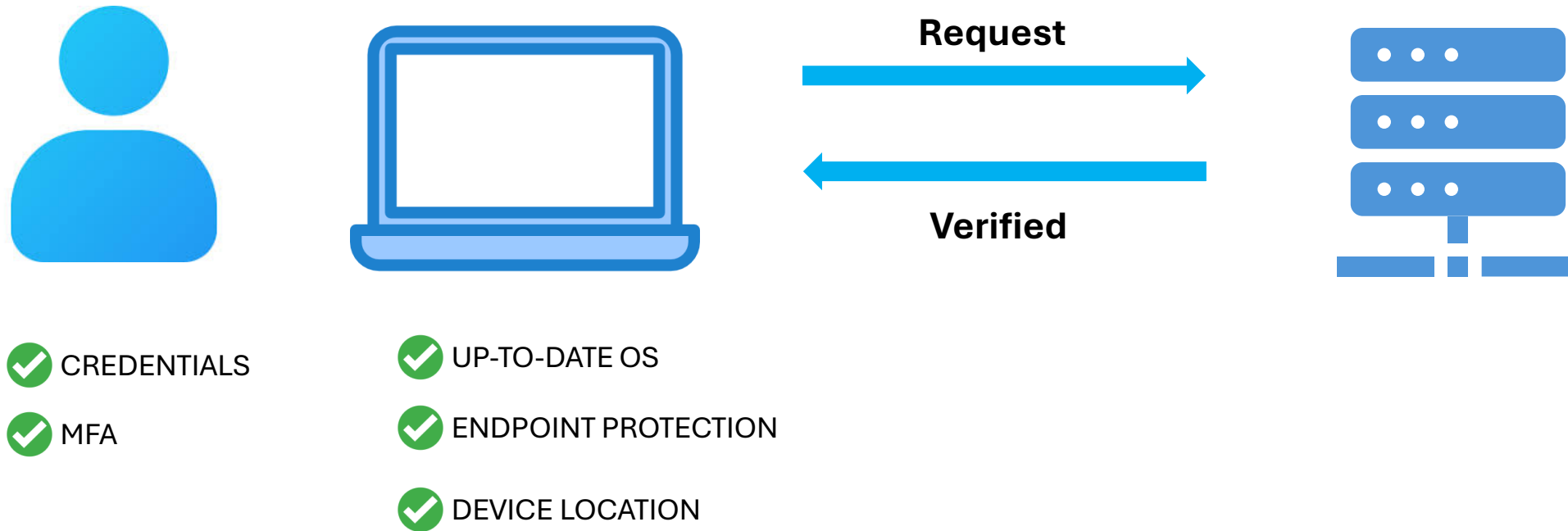
✓ ENDPOINT PROTECTION

✓ DEVICE LOCATION

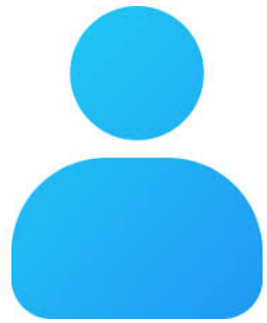
REQUEST



PRINCIPLE ONE : *Never trust Always verify*

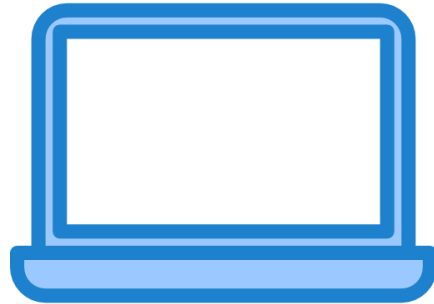


PRINCIPLE ONE : *Never trust Always verify*



✓ CREDENTIALS

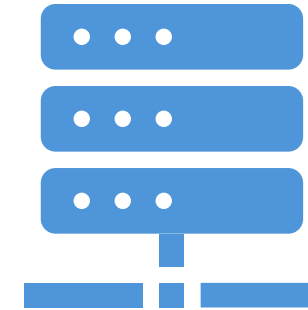
✓ MFA



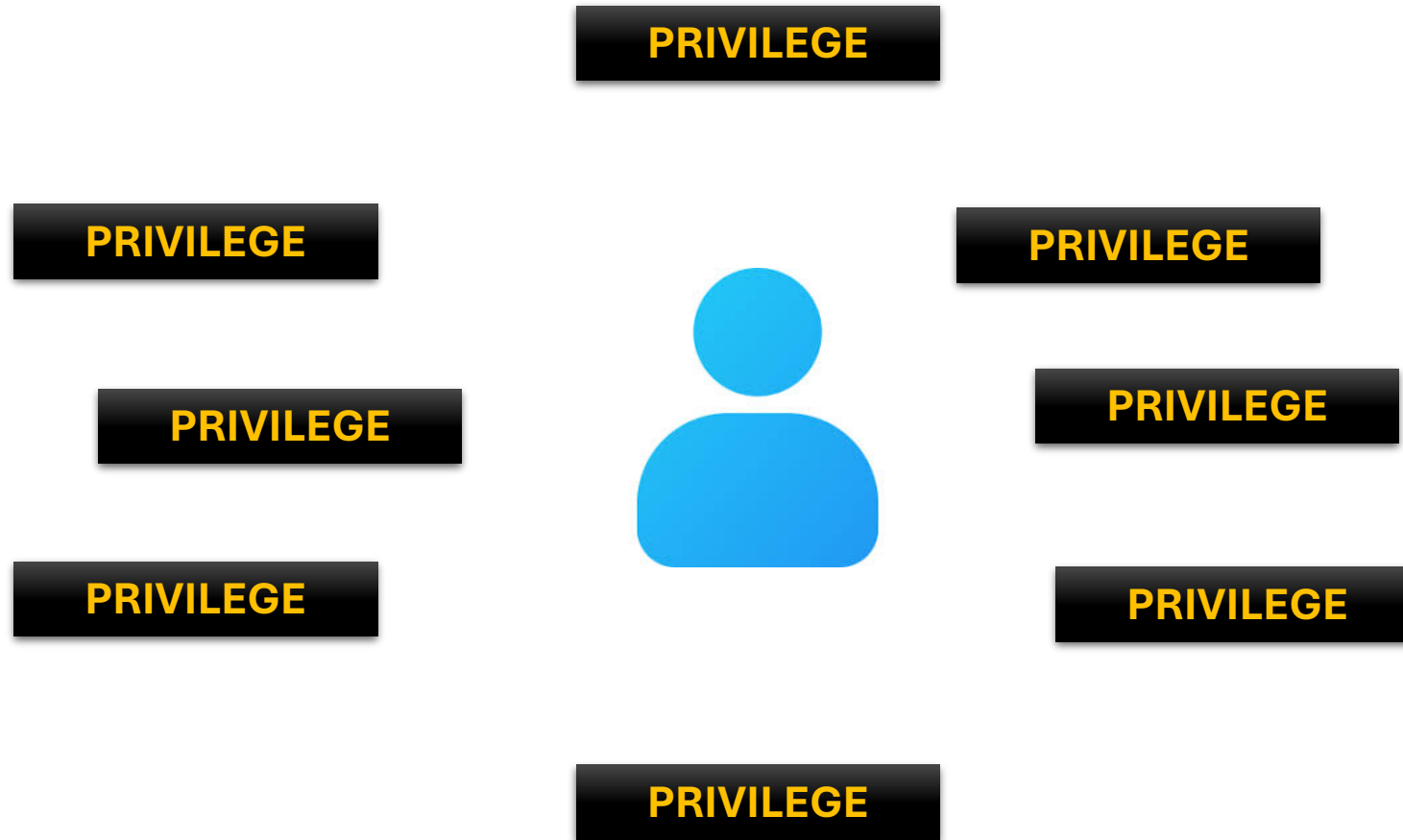
✓ UP-TO-DATE OS

✓ ENDPOINT PROTECTION

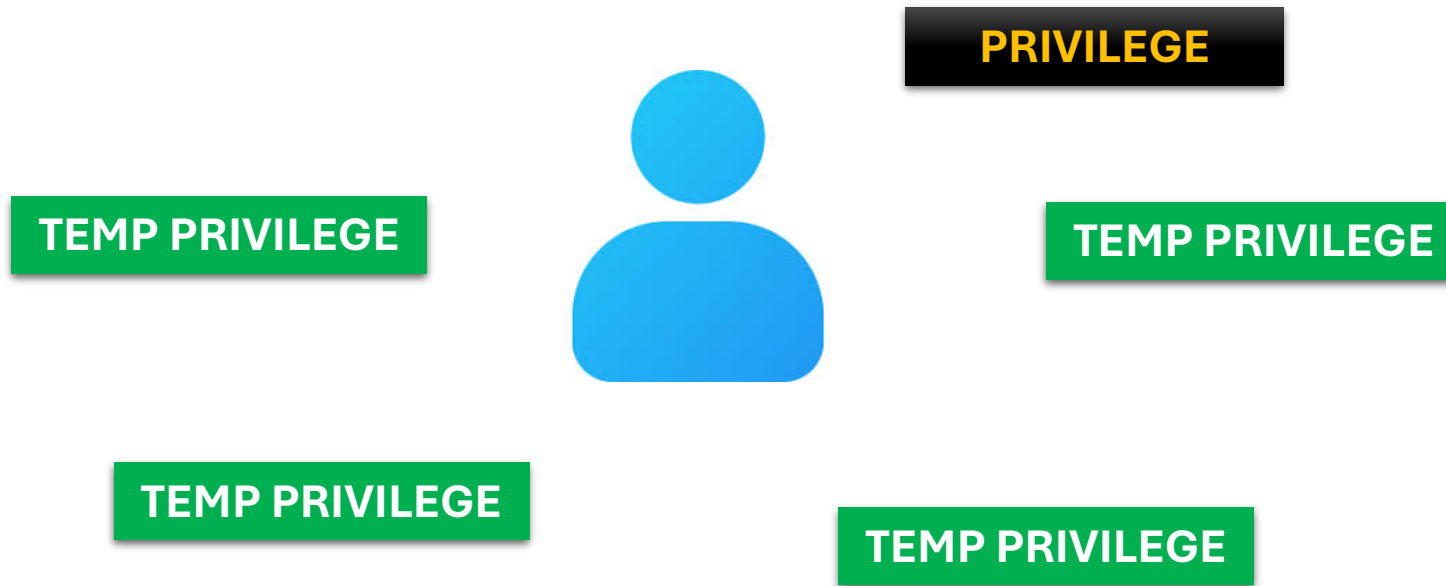
✓ DEVICE LOCATION



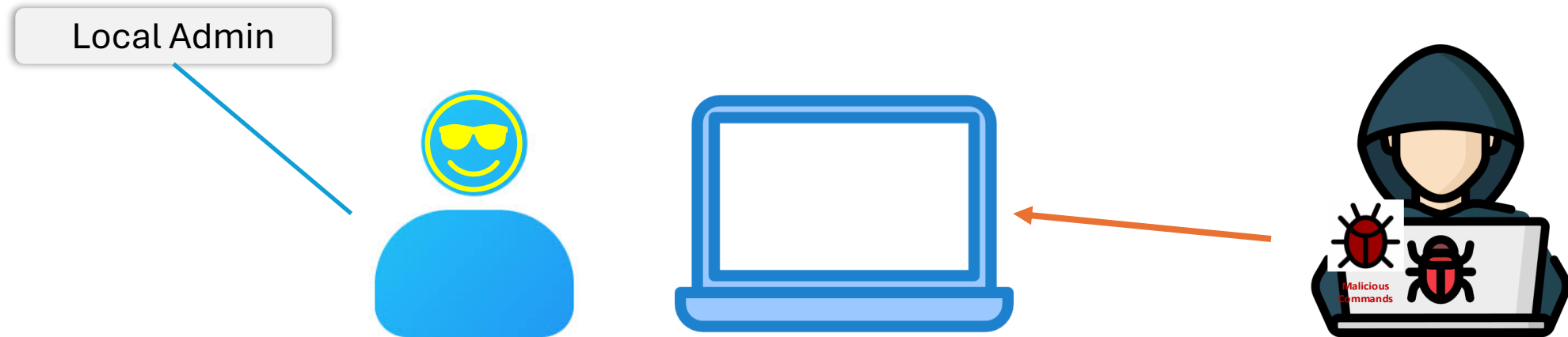
PRINCIPLE TWO : LEAST *Privilege*



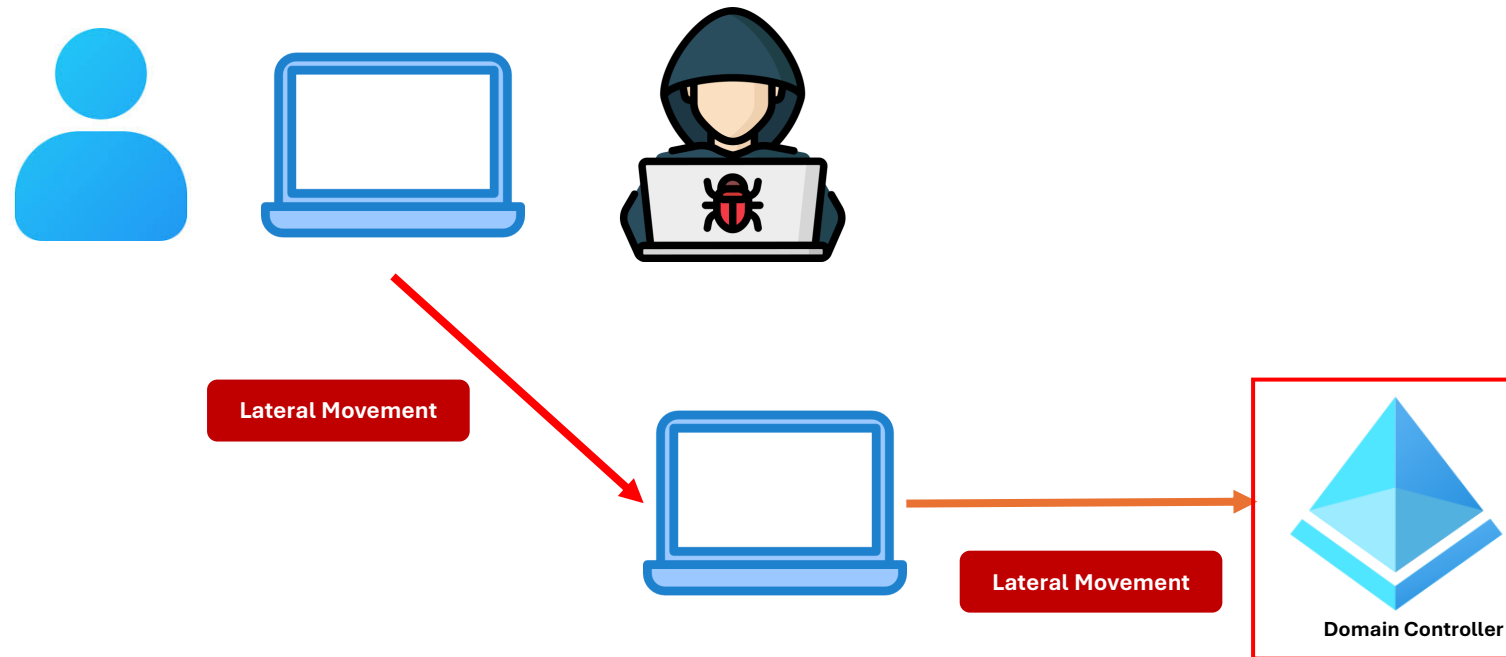
PRINCIPLE TWO : LEAST *Privilege*



PRINCIPLE TWO : *Least Privilege*

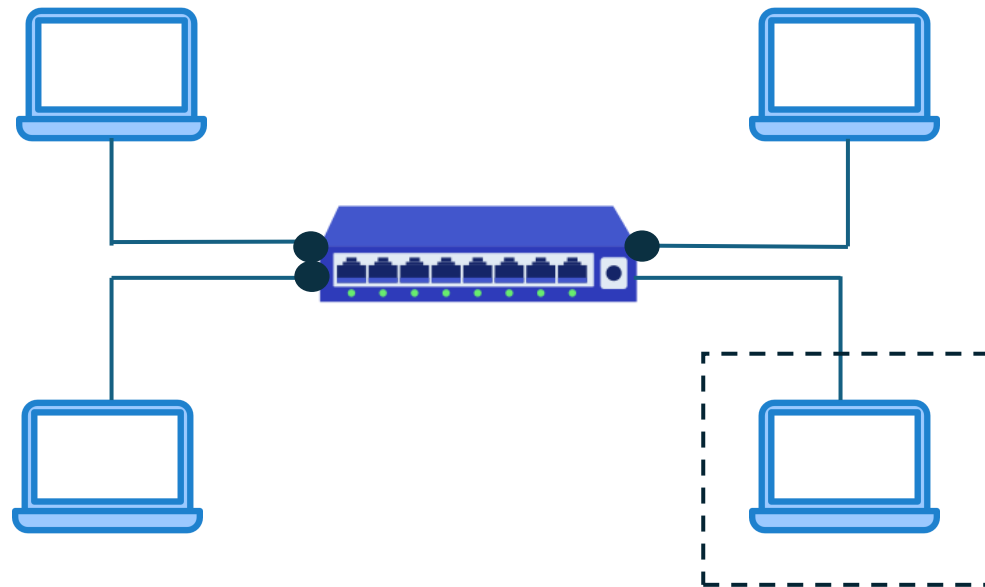


PRINCIPLE TWO : Least *Privilege*



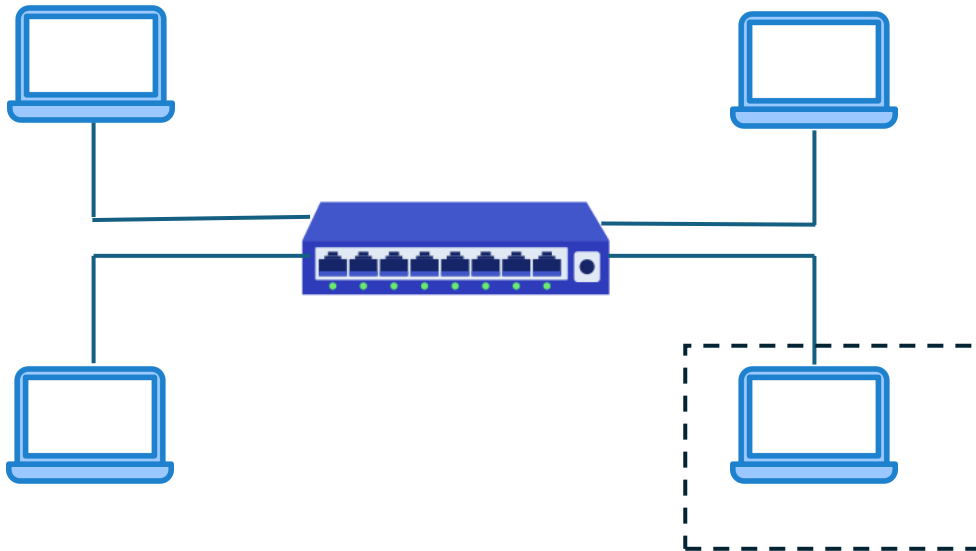
PRINCIPLE THREE : *Assume Breach*

➤ Reduce Blast Radius



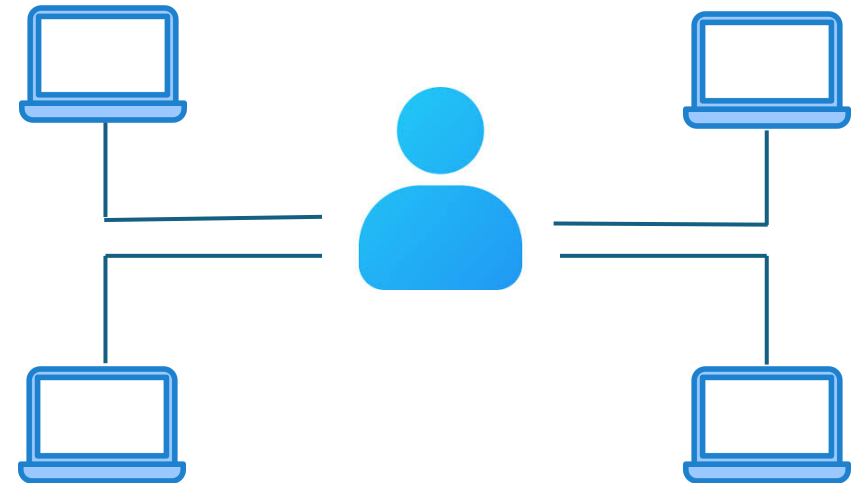
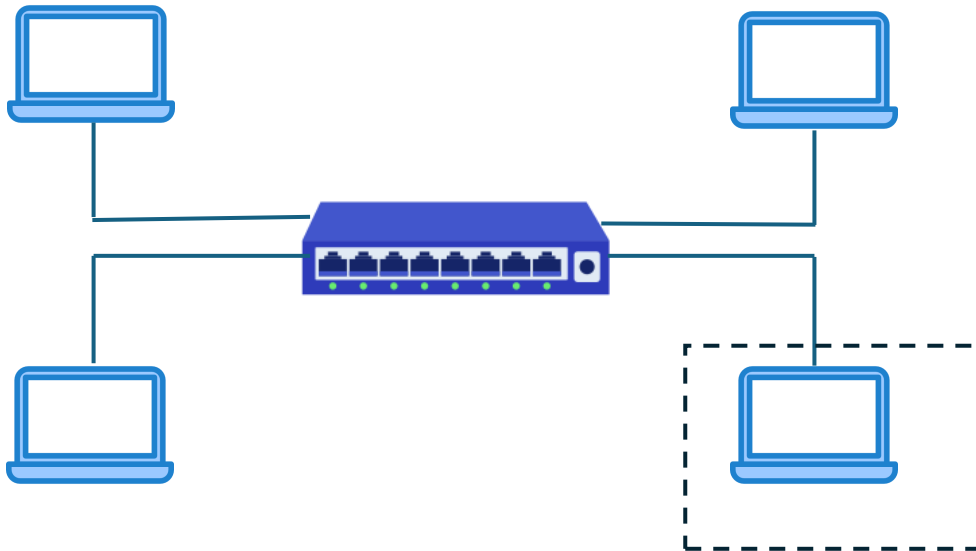
PRINCIPLE THREE : *Assume Breach*

➤ Reduce Blast Radius



PRINCIPLE THREE : *Assume Breach*

➤ Reduce Blast Radius



PRINCIPLE THREE : *Assume Breach*

- **Reduce Blast Radius**
- **Analytics for Visibility & Detection**



ZERO TRUST ARCHITECTURE (ZTA) as per NIST

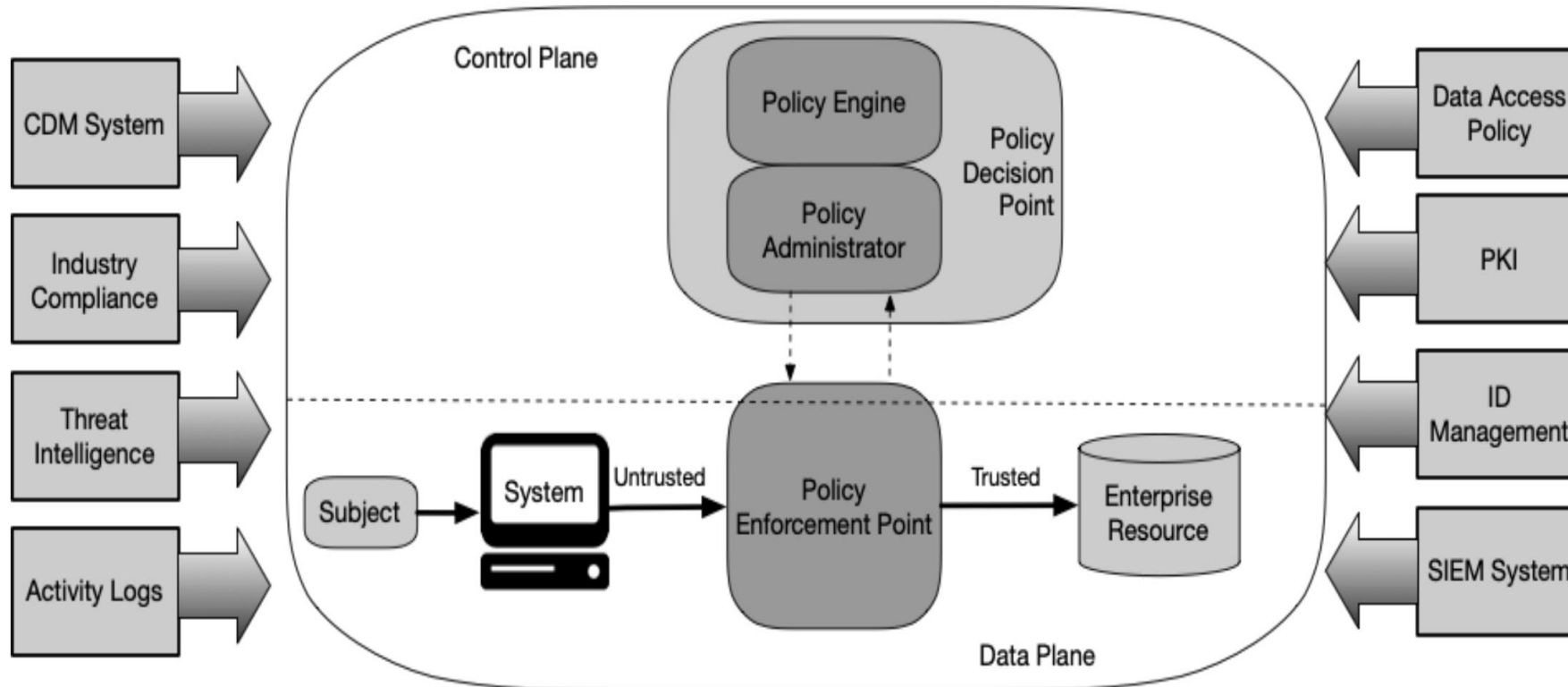
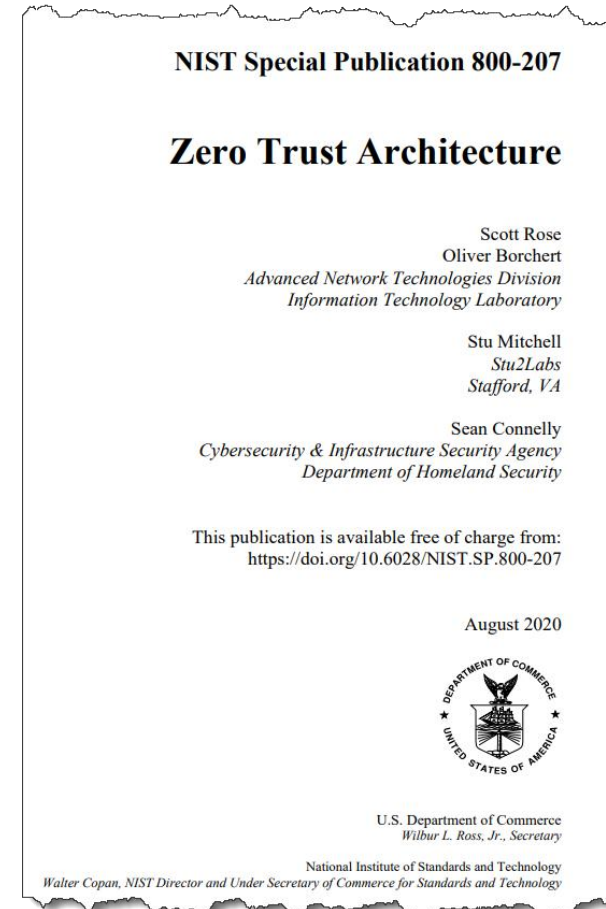


Figure 2: Core Zero Trust Logical Components

[NIST SP 800-201: Pg-9]



ZERO TRUST USE CASES



Threat Protection

Reduce Attack Surface &
Blast Radius



Data Protection

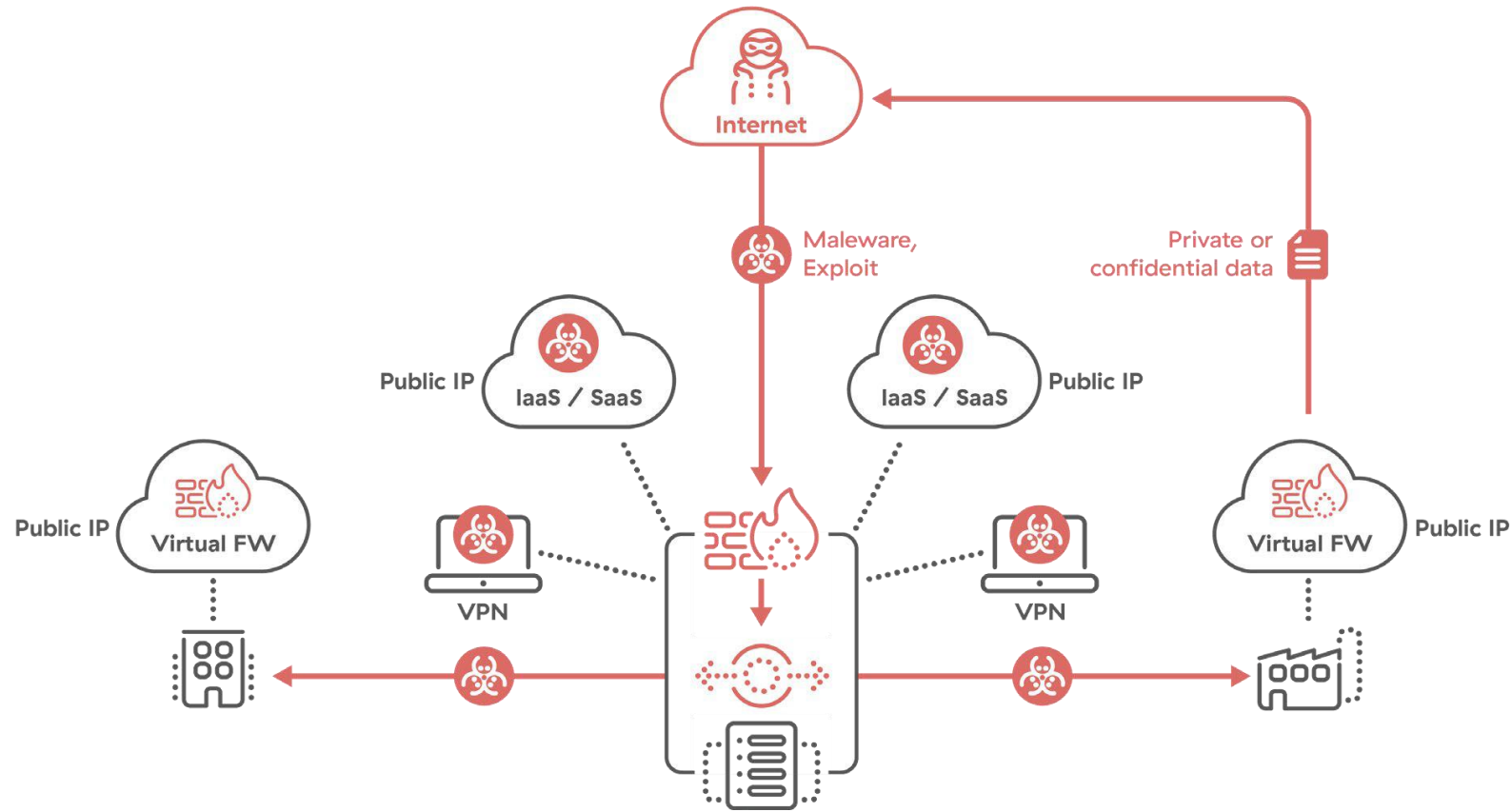
Prevent loss and
exfiltration of sensitive
enterprise data



Network Segmentation

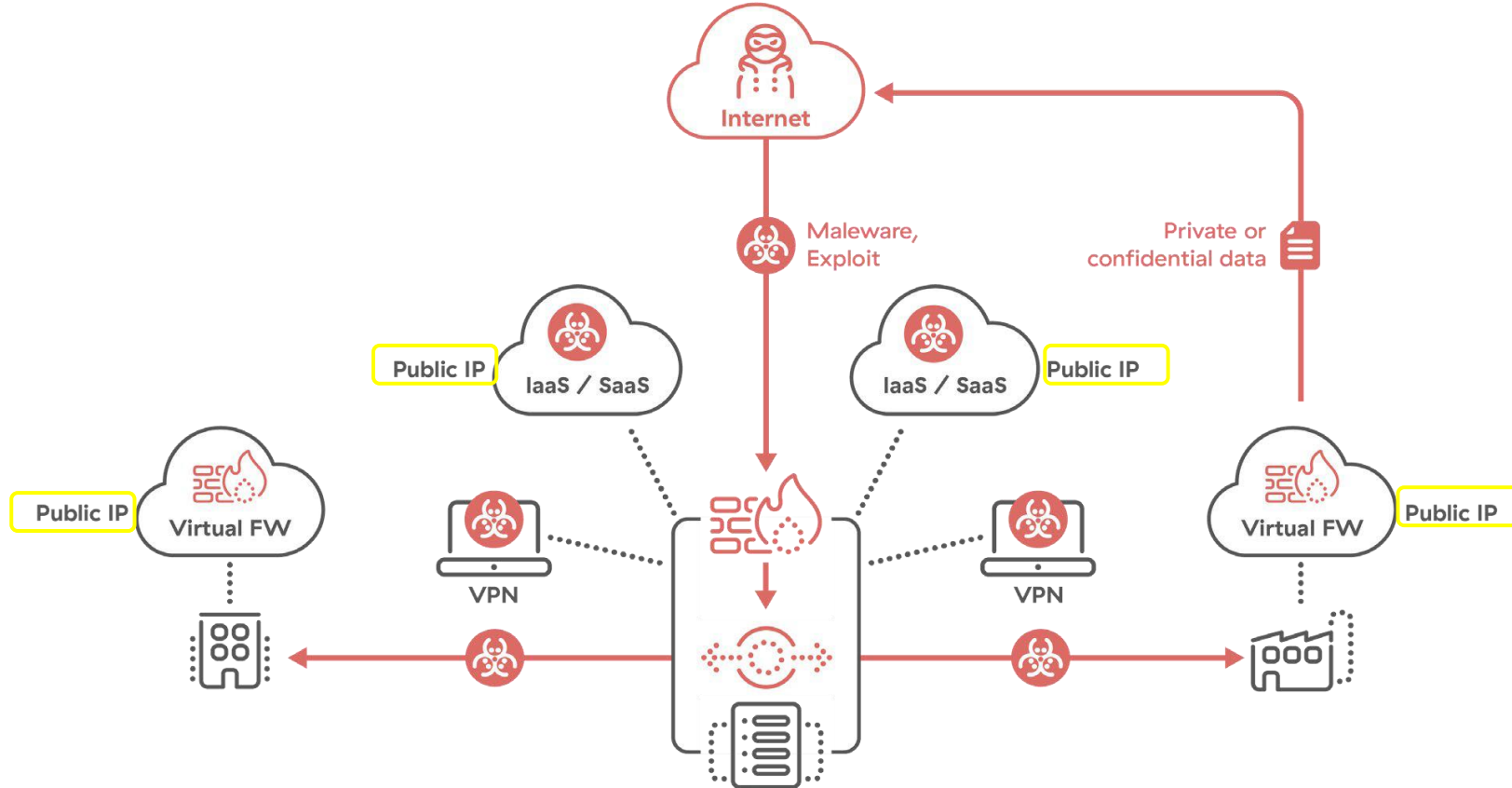
Prevent lateral movement

Threat Protection: *Legacy* vs *Zero Trust* Networks



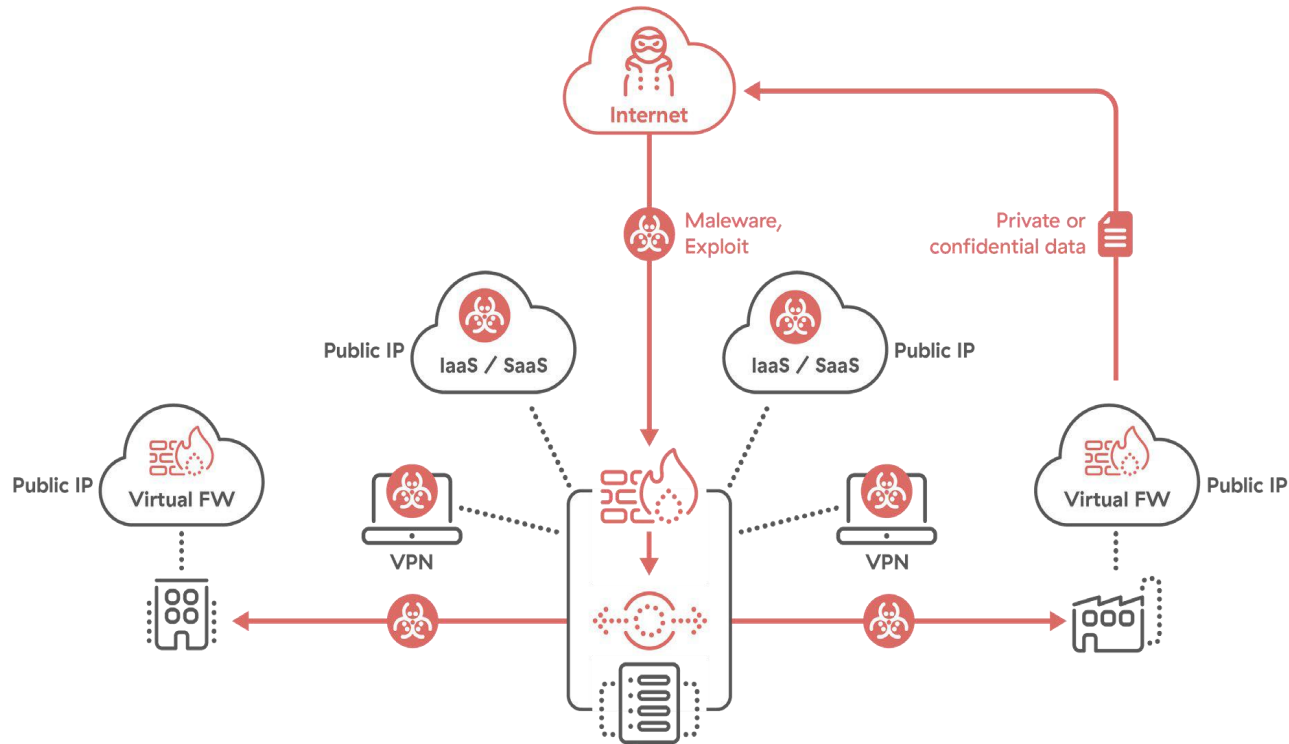
Legacy Networks

Threat Protection: *Legacy vs Zero Trust Networks*

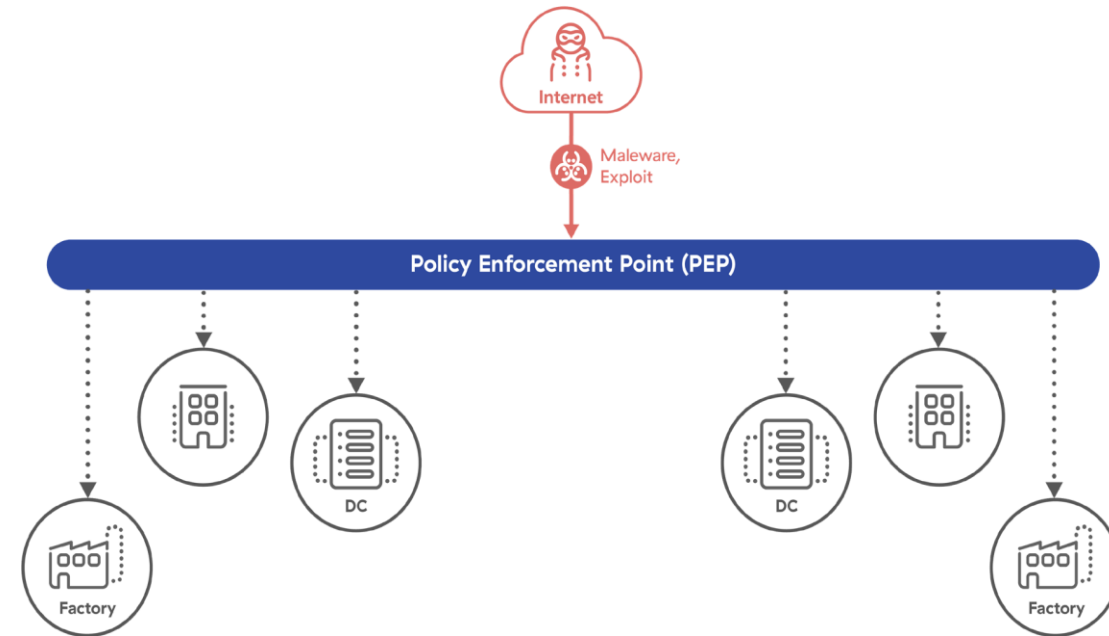


Legacy Networks

Threat Protection: *Legacy* vs *Zero Trust* Networks

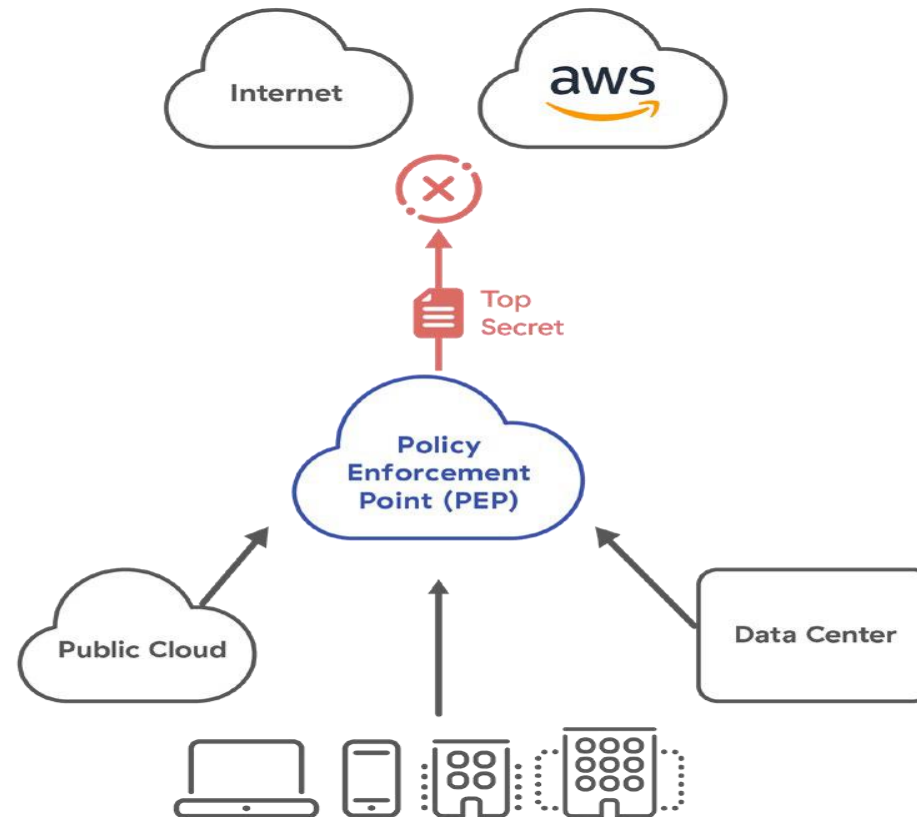


Legacy



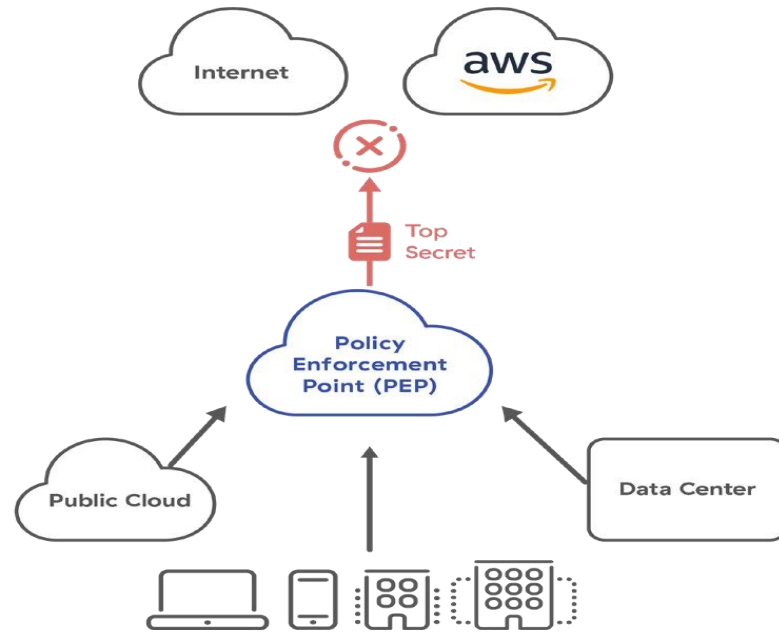
ZTA

Data Protection with *Zero Trust*

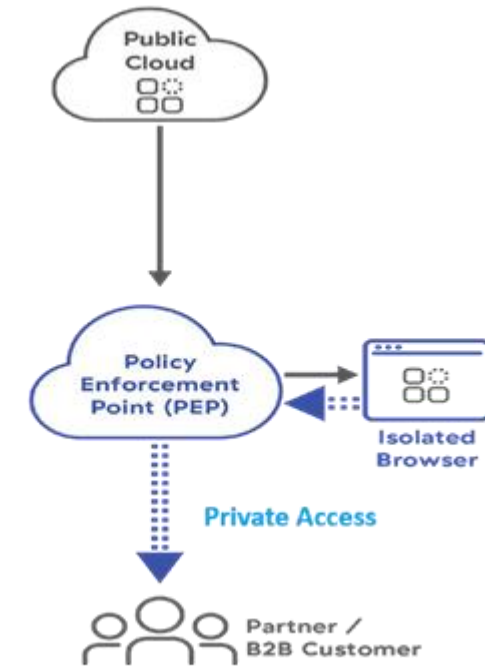


In-Line DLP Policies

Data Protection with *Zero Trust*

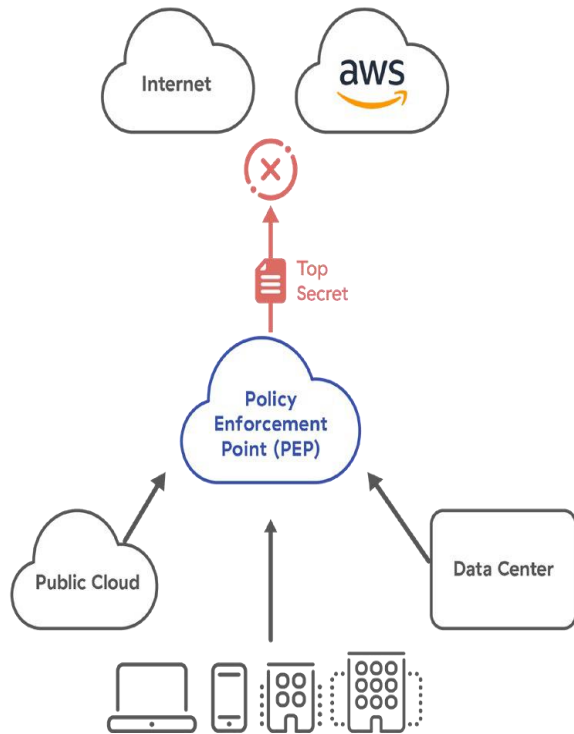


In-Line DLP Policies

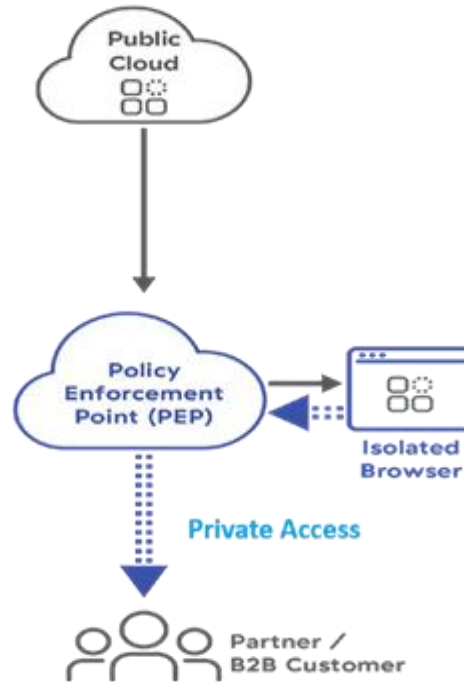


Manage 3rd Party Access

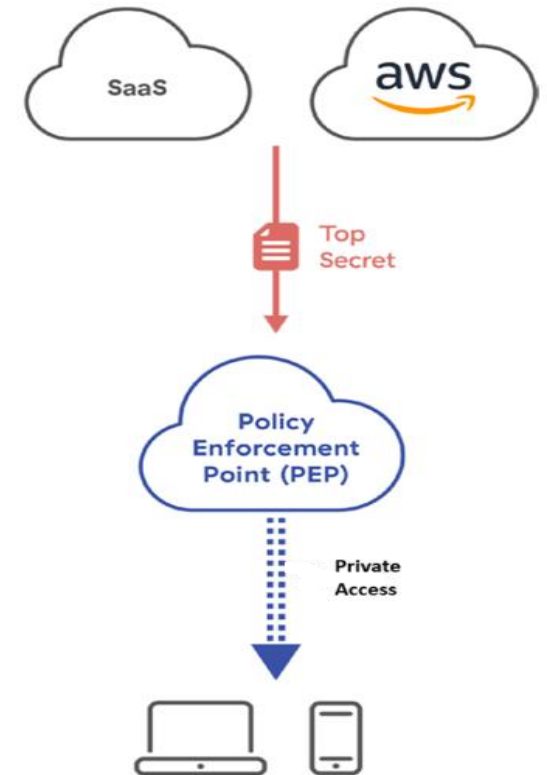
Data Protection with *Zero Trust*



In-Line DLP Policies



Manage 3rd Party Access



BYOD

Segmentation with *Zero Trust*

➤ Attack Surface Elimination

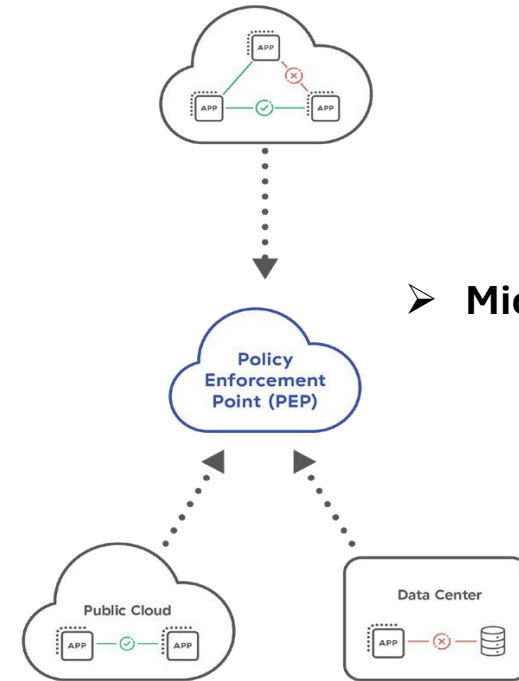


User-App Segmentation

Segmentation with *Zero Trust*



User-App Segmentation



➤ **Micro Segmentation**

App-App Segmentation

ZTNA vs VPN

VPN



- **Connect first,**
Authenticate later
- **Coarse access,**
All or Nothing
- **Open Ports,**
visible to attackers
- **Virtually place device
on the network**
(IP-based routing)

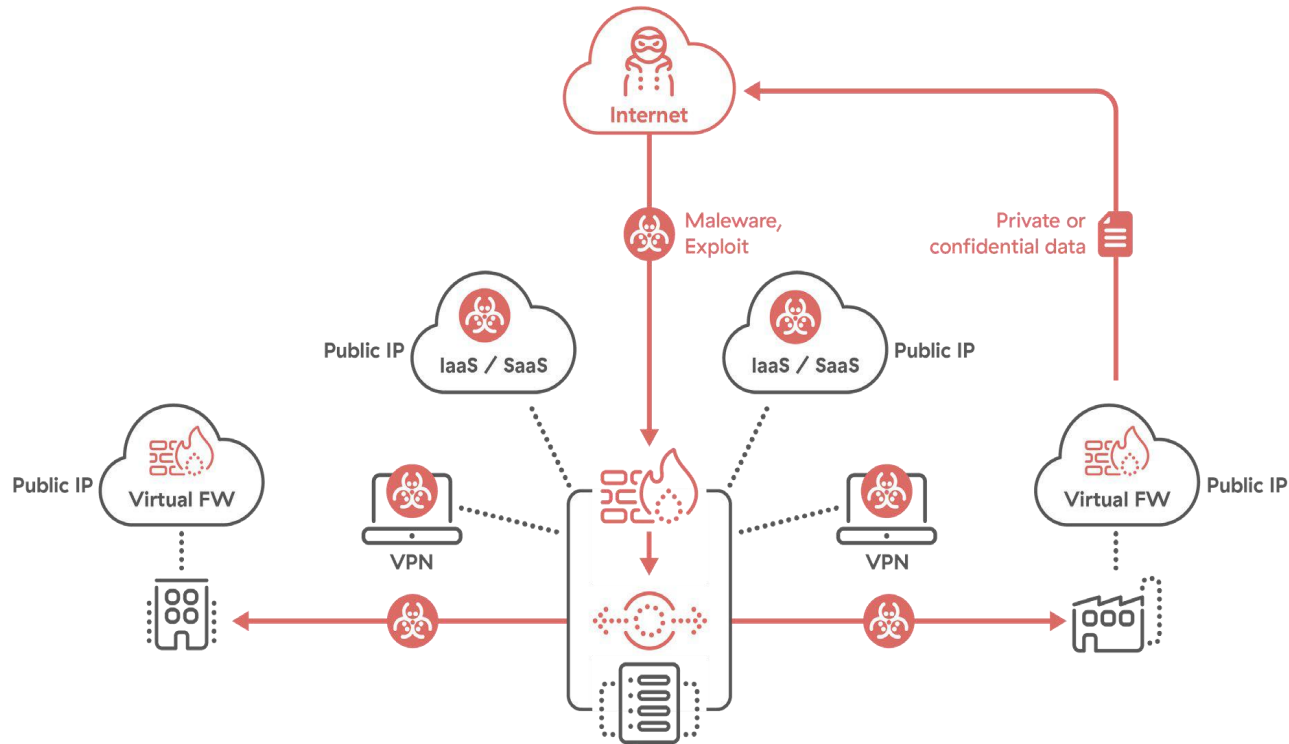


ZTNA

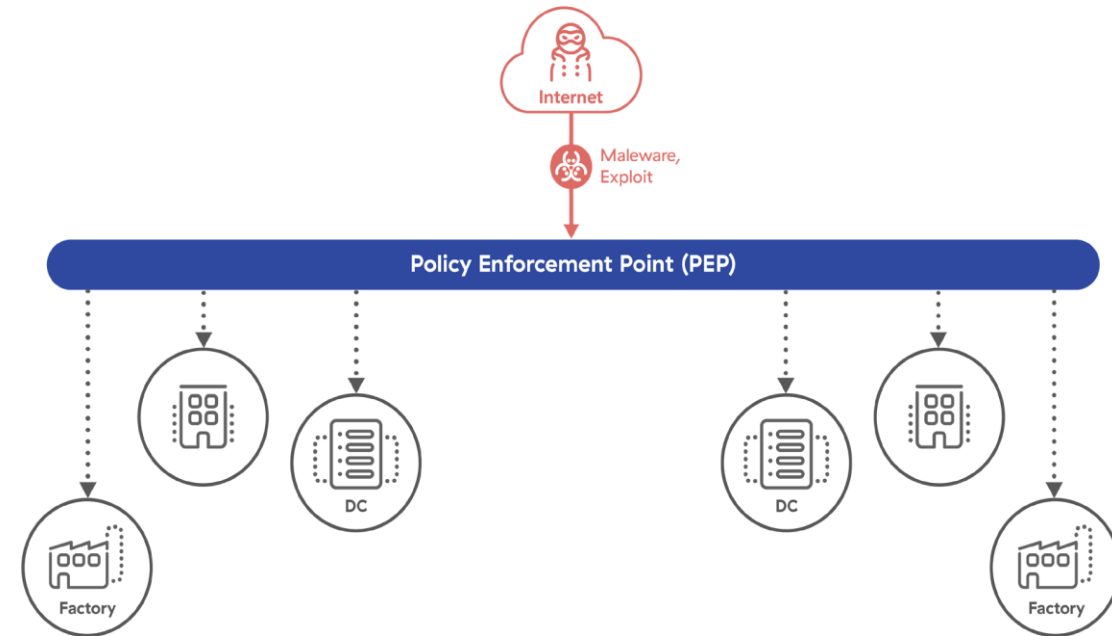


- **Authenticate first,**
Connect later
- **Granular access,**
constrain later movement
- **Inside-out connectivity,**
hides assets
- **Connects users to** specific
resources

Threat Protection: *Legacy* vs *Zero Trust* Networks

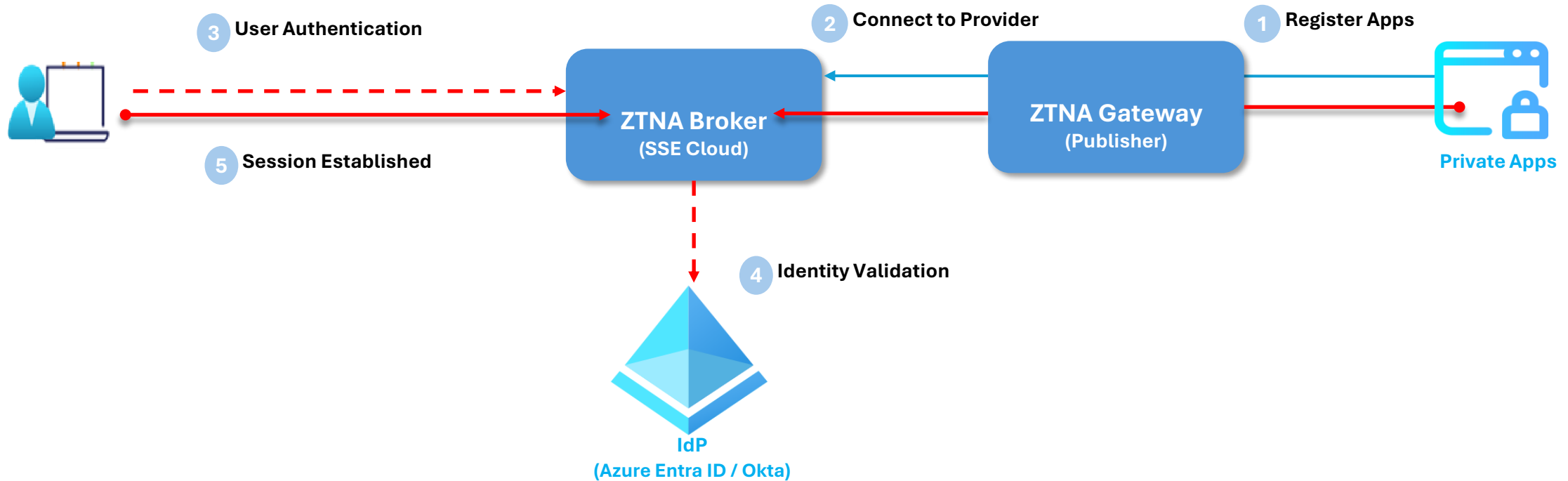


Legacy



ZTA

How ZTNA works ?



Eliminate Attack Surface ✓

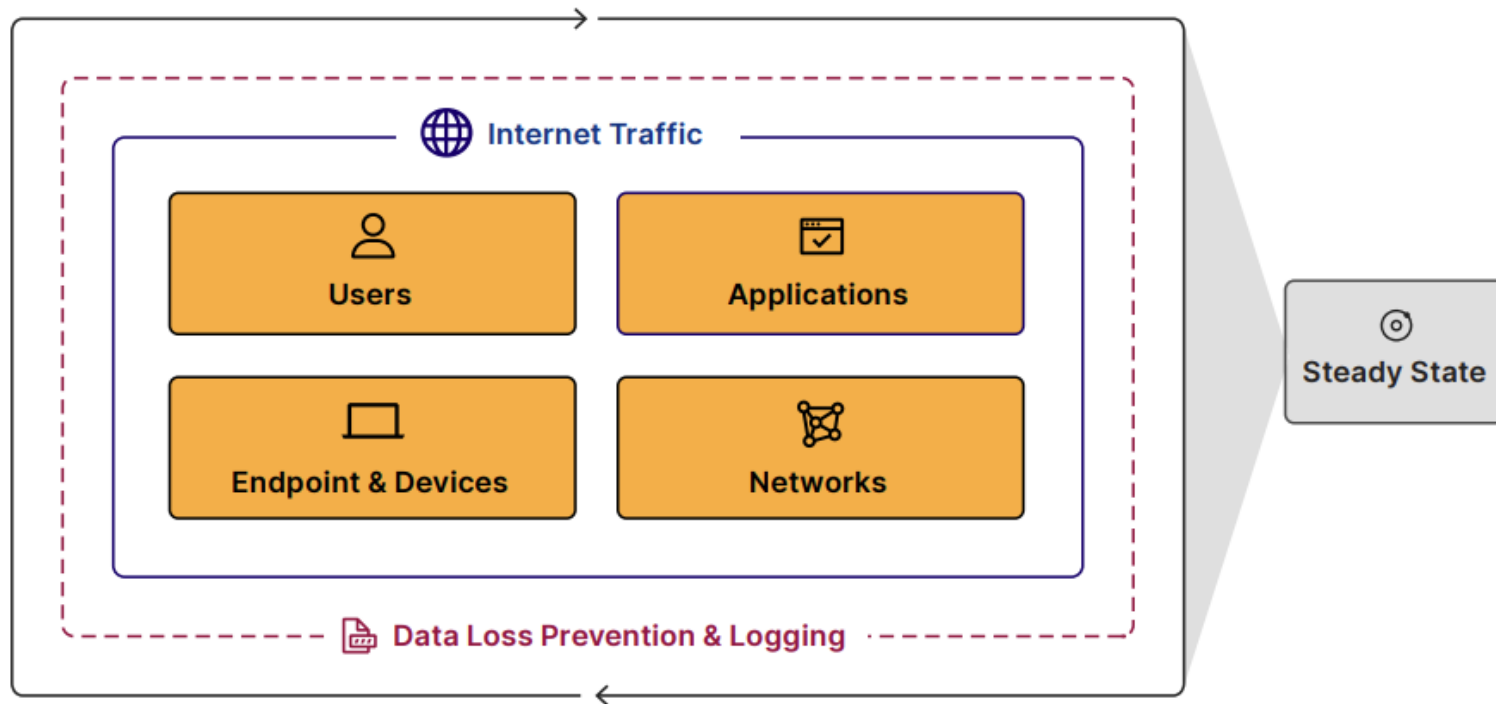
Limit Lateral Movement ✓

Improved end-user experience ✓

How to Get Started **with** Zero Trust?



How to get started with Zero Trust?






Scan Me to access Zero Trust White Paper

Reference: [CLOUDFLARE Whitepaper on Roadmap to Zero Trust Architecture](#)

How to get started with Zero Trust?

| | Component | Goal | Level of Effort |
|---------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Phase 1 |  Internet traffic | Deploy global DNS filtering |  |
| |  Applications | Monitor inbound emails and filter out phishing attempts |  |
| |  DLP & logs | Identify misconfig and publicly shared data in SaaS tools |  |
| Phase 2 |  Users | Establish corporate identity |  |
| |  Users | Enforce basic MFA for all applications |  |
| |  Applications | Enforce HTTPS and DNSsec |  |
| |  Internet traffic | Block or isolate threats behind SSL |  |
| |  Applications | ZT policy enforcement for publicly addressable apps |  |
| |  Applications | Protect applications from layer 7 attacks |  |
| |  Networks | Close all inbound ports open to the Internet for app delivery |  |
| Phase 3 |  Applications | Inventory all corporate applications |  |
| |  Applications | ZT policy enforcement for SaaS applications |  |
| |  Networks | Segment user network access |  |
| |  Applications | ZTNA for critical privately addressable applications |  |
| |  Devices | Implement MDM/UEM to control corporate devices |  |
| |  DLP & logs | Define what data is sensitive and where it exists |  |
| |  Users | Send out hardware based authentication tokens |  |
| |  DLP & logs | Stay up to date on known threat actors |  |
| Phase 4 |  Users | Enforce hardware token based MFA |  |
| |  Applications | ZT policy enforcement and network access for all applications |  |
| |  DLP & logs | Establish a SOC for log review, policy updates and mitigation |  |
| |  Devices | Implement endpoint protection |  |
| |  Devices | Inventory all corporate devices, APIs and services |  |
| |  Networks | Use broadband Internet for branch to branch connectivity |  |
| |  DLP & logs | Log and review employee activity on sensitive apps |  |
| |  DLP & logs | Stop sensitive data from leaving your applications |  |
| |  Steady state | DevOps approach for policy enforcement of new resources |  |
| |  Steady state | Implement auto-scaling for on-ramp resources |  |

Level of Effort

-  - Small effort; this can be done by an individual or small team
-  - Medium effort; this will require a team and advanced preparation
-  - Large effort; this will require multiple teams and a project plan









Scan Me to access Zero Trust White Paper

How to get started with Zero Trust?

| | Component | Goal | Level of Effort |
|---------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Phase 1 |  Internet traffic | Deploy global DNS filtering |  |
| |  Applications | Monitor inbound emails and filter out phishing attempts |  |
| |  DLP & logs | Identify misconfig and publicly shared data in SaaS tools |  |
| Phase 2 |  Users | Establish corporate identity |  |
| |  Users | Enforce basic MFA for all applications |  |
| |  Applications | Enforce HTTPS and DNSsec |  |
| |  Internet traffic | Block or isolate threats behind SSL |  |
| |  Applications | ZT policy enforcement for publicly addressable apps |  |
| |  Applications | Protect applications from layer 7 attacks |  |
| Phase 3 |  Networks | Close all inbound ports open to the Internet for app delivery |  |
| |  Applications | Inventory all corporate applications |  |
| |  Applications | ZT policy enforcement for SaaS applications |  |
| |  Networks | Segment user network access |  |
| |  Applications | ZTNA for critical privately addressable applications |  |
| |  Devices | Implement MDM/UEM to control corporate devices |  |
| |  DLP & logs | Define what data is sensitive and where it exists |  |
| |  Users | Send out hardware based authentication tokens |  |
| Phase 4 |  DLP & logs | Stay up to date on known threat actors |  |
| |  Users | Enforce hardware token based MFA |  |
| |  Applications | ZT policy enforcement and network access for all applications |  |
| |  DLP & logs | Establish a SOC for log review, policy updates and mitigation |  |
| |  Devices | Implement endpoint protection |  |
| |  Devices | Inventory all corporate devices, APIs and services |  |
| |  Networks | Use broadband Internet for branch to branch connectivity |  |
| |  DLP & logs | Log and review employee activity on sensitive apps |  |
| |  DLP & logs | Stop sensitive data from leaving your applications |  |
| |  Steady state | DevOps approach for policy enforcement of new resources |  |
| |  Steady state | Implement auto-scaling for on-ramp resources |  |



Phase 1















| Component | Goal | Level of Effort |
|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|-------------------------------------------------------------------------------------|
|  Internet traffic | Deploy global DNS filtering |  |
|  Applications | Monitor inbound emails and filter out phishing attempts |  |
|  DLP & logs | Identify misconfig and publicly shared data in SaaS tools |  |

How to get started with Zero Trust?

| | Component | Goal | Level of Effort |
|---------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Phase 1 |  Internet traffic | Deploy global DNS filtering |  |
| |  Applications | Monitor inbound emails and filter out phishing attempts |  |
| |  DLP & logs | Identify misconfig and publicly shared data in SaaS tools |  |
| Phase 2 |  Users | Establish corporate identity |  |
| |  Users | Enforce basic MFA for all applications |  |
| |  Applications | Enforce HTTPS and DNSsec |  |
| |  Internet traffic | Block or isolate threats behind SSL |  |
| |  Applications | ZT policy enforcement for publicly addressable apps |  |
| |  Applications | Protect applications from layer 7 attacks |  |
| Phase 3 |  Networks | Close all inbound ports open to the Internet for app delivery |  |
| |  Applications | Inventory all corporate applications |  |
| |  Applications | ZT policy enforcement for SaaS applications |  |
| |  Networks | Segment user network access |  |
| |  Applications | ZTNA for critical privately addressable applications |  |
| |  Devices | Implement MDM/UEM to control corporate devices |  |
| |  DLP & logs | Define what data is sensitive and where it exists |  |
| |  Users | Send out hardware based authentication tokens |  |
| Phase 4 |  DLP & logs | Stay up to date on known threat actors |  |
| |  Users | Enforce hardware token based MFA |  |
| |  Applications | ZT policy enforcement and network access for all applications |  |
| |  DLP & logs | Establish a SOC for log review, policy updates and mitigation |  |
| |  Devices | Implement endpoint protection |  |
| |  Devices | Inventory all corporate devices, APIs and services |  |
| |  Networks | Use broadband Internet for branch to branch connectivity |  |
| |  DLP & logs | Log and review employee activity on sensitive apps |  |
| |  DLP & logs | Stop sensitive data from leaving your applications |  |
| |  Steady state | DevOps approach for policy enforcement of new resources |  |
| |  Steady state | Implement auto-scaling for on-ramp resources |  |

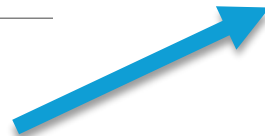


Phase 2

| Component | Goal | Level of Effort |
|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------------------------------------------------|
|  Users | Establish corporate identity |  |
|  Users | Enforce basic MFA for all applications |  |
|  Applications | Enforce HTTPS and DNSsec |  |
|  Internet traffic | Block or isolate threats behind SSL |  |
|  Applications | ZT policy enforcement for publicly addressable apps |  |
|  Applications | Protect applications from layer 7 attacks |  |
|  Networks | Close all inbound ports open to the Internet for app delivery |  |

How to get started with Zero Trust?

| | Component | Goal | Level of Effort |
|---------|------------------|---------------------------------------------------------------|-----------------|
| Phase 1 | Internet traffic | Deploy global DNS filtering | ■ |
| | Applications | Monitor inbound emails and filter out phishing attempts | ■ |
| | DLP & logs | Identify misconfig and publicly shared data in SaaS tools | ■ |
| Phase 2 | Users | Establish corporate identity | ■ ■ |
| | Users | Enforce basic MFA for all applications | ■ ■ |
| | Applications | Enforce HTTPS and DNSsec | ■ ■ |
| | Internet traffic | Block or isolate threats behind SSL | ■ ■ |
| | Applications | ZT policy enforcement for publicly addressable apps | ■ ■ |
| | Applications | Protect applications from layer 7 attacks | ■ ■ |
| Phase 3 | Networks | Close all inbound ports open to the Internet for app delivery | ■ |
| | Applications | Inventory all corporate applications | ■ ■ |
| | Applications | ZT policy enforcement for SaaS applications | ■ ■ |
| | Networks | Segment user network access | ■ ■ ■ |
| | Applications | ZTNA for critical privately addressable applications | ■ ■ |
| | Devices | Implement MDM/UEM to control corporate devices | ■ ■ |
| | DLP & logs | Define what data is sensitive and where it exists | ■ ■ |
| | Users | Send out hardware based authentication tokens | ■ ■ |
| | DLP & logs | Stay up to date on known threat actors | ■ |
| Phase 4 | Users | Enforce hardware token based MFA | ■ ■ |
| | Applications | ZT policy enforcement and network access for all applications | ■ ■ ■ |
| | DLP & logs | Establish a SOC for log review, policy updates and mitigation | ■ ■ |
| | Devices | Implement endpoint protection | ■ ■ |
| | Devices | Inventory all corporate devices, APIs and services | ■ ■ |
| | Networks | Use broadband Internet for branch to branch connectivity | ■ ■ ■ |
| | DLP & logs | Log and review employee activity on sensitive apps | ■ ■ |
| | DLP & logs | Stop sensitive data from leaving your applications | ■ ■ ■ |
| | Steady state | DevOps approach for policy enforcement of new resources | ■ ■ |
| | Steady state | Implement auto-scaling for on-ramp resources | ■ ■ |



Phase 3

| Component | Goal | Level of Effort |
|--------------|------------------------------------------------------|-----------------|
| Applications | Inventory all corporate applications | ■ ■ |
| Applications | ZT policy enforcement for SaaS applications | ■ ■ |
| Networks | Segment user network access | ■ ■ ■ |
| Applications | ZTNA for critical privately addressable applications | ■ ■ |
| Devices | Implement MDM/UEM to control corporate devices | ■ ■ |
| DLP & logs | Define what data is sensitive and where it exists | ■ ■ |
| Users | Send out hardware based authentication tokens | ■ ■ |
| DLP & logs | Stay up to date on known threat actors | ■ |

How to get started with Zero Trust?

| | Component | Goal | Level of Effort |
|---------|------------------|---------------------------------------------------------------|-----------------|
| Phase 1 | Internet traffic | Deploy global DNS filtering | ■ |
| | Applications | Monitor inbound emails and filter out phishing attempts | ■ |
| | DLP & logs | Identify misconfig and publicly shared data in SaaS tools | ■ |
| Phase 2 | Users | Establish corporate identity | ■ ■ |
| | Users | Enforce basic MFA for all applications | ■ ■ |
| | Applications | Enforce HTTPS and DNSsec | ■ ■ |
| | Internet traffic | Block or isolate threats behind SSL | ■ ■ |
| | Applications | ZT policy enforcement for publicly addressable apps | ■ ■ |
| | Applications | Protect applications from layer 7 attacks | ■ ■ |
| Phase 3 | Networks | Close all inbound ports open to the Internet for app delivery | ■ |
| | Applications | Inventory all corporate applications | ■ ■ |
| | Applications | ZT policy enforcement for SaaS applications | ■ ■ |
| | Networks | Segment user network access | ■ ■ ■ |
| | Applications | ZTNA for critical privately addressable applications | ■ ■ |
| | Devices | Implement MDM/UEM to control corporate devices | ■ ■ |
| | DLP & logs | Define what data is sensitive and where it exists | ■ ■ |
| | Users | Send out hardware based authentication tokens | ■ ■ |
| Phase 4 | DLP & logs | Stay up to date on known threat actors | ■ |
| | Users | Enforce hardware token based MFA | ■ ■ |
| | Applications | ZT policy enforcement and network access for all applications | ■ ■ ■ |
| | DLP & logs | Establish a SOC for log review, policy updates and mitigation | ■ ■ ■ |
| | Devices | Implement endpoint protection | ■ ■ |
| | Devices | Inventory all corporate devices, APIs and services | ■ ■ |
| | Networks | Use broadband Internet for branch to branch connectivity | ■ ■ ■ |
| | DLP & logs | Log and review employee activity on sensitive apps | ■ ■ |
| | DLP & logs | Stop sensitive data from leaving your applications | ■ ■ ■ |
| | Steady state | DevOps approach for policy enforcement of new resources | ■ ■ |
| | Steady state | Implement auto-scaling for on-ramp resources | ■ ■ ■ |



| Component | Goal | Level of Effort |
|--------------|---------------------------------------------------------------|-----------------|
| Users | Enforce hardware token based MFA | ■ ■ |
| Applications | ZT policy enforcement and network access for all applications | ■ ■ ■ |
| DLP & logs | Establish a SOC for log review, policy updates and mitigation | ■ ■ ■ |
| Devices | Implement endpoint protection | ■ ■ |
| Devices | Inventory all corporate devices, APIs and services | ■ ■ |
| Networks | Use broadband Internet for branch to branch connectivity | ■ ■ ■ |
| DLP & logs | Log and review employee activity on sensitive apps | ■ ■ |
| DLP & logs | Stop sensitive data from leaving your applications | ■ ■ ■ |
| Steady state | DevOps approach for policy enforcement of new resources | ■ ■ |
| Steady state | Implement auto-scaling for on-ramp resources | ■ ■ ■ |

Thank You!

Let's make Australia Global Leader in Cybersecurity by 2030 – Australian Cyber Strategy 2030



Muzamil Rashid
Head of Cyber Security
Mazda Australia



Connect with me on



CISOMelbourne2025