TechVision RESEARCH

Zero Trust Networking

MACC 2018

Sorell Slaymaker
Principal Consulting Analyst
TechVision Research

Sorell Slaymaker, Principal Consulting Analyst at TechVision Research

Sorell Slaymaker is a seasoned technology architect, analyst, and consultant. He has a B.S. & M.E. in Telecom Engineering and has worked on the Internet backbone, built firewall and routing products (one which was sold to Cisco), a Gartner analyst, and was the network and communications architect at several Fortune 100 companies including Target and United Health Group.

Core areas of focus include: open source routing, software defined networks, network security, security/risk management, digital transformation. Sorell recently published a 48 page report on Zero Trust Networking.

sorell@techvisionresearch.com
@sorellslaymaker
#zero trust

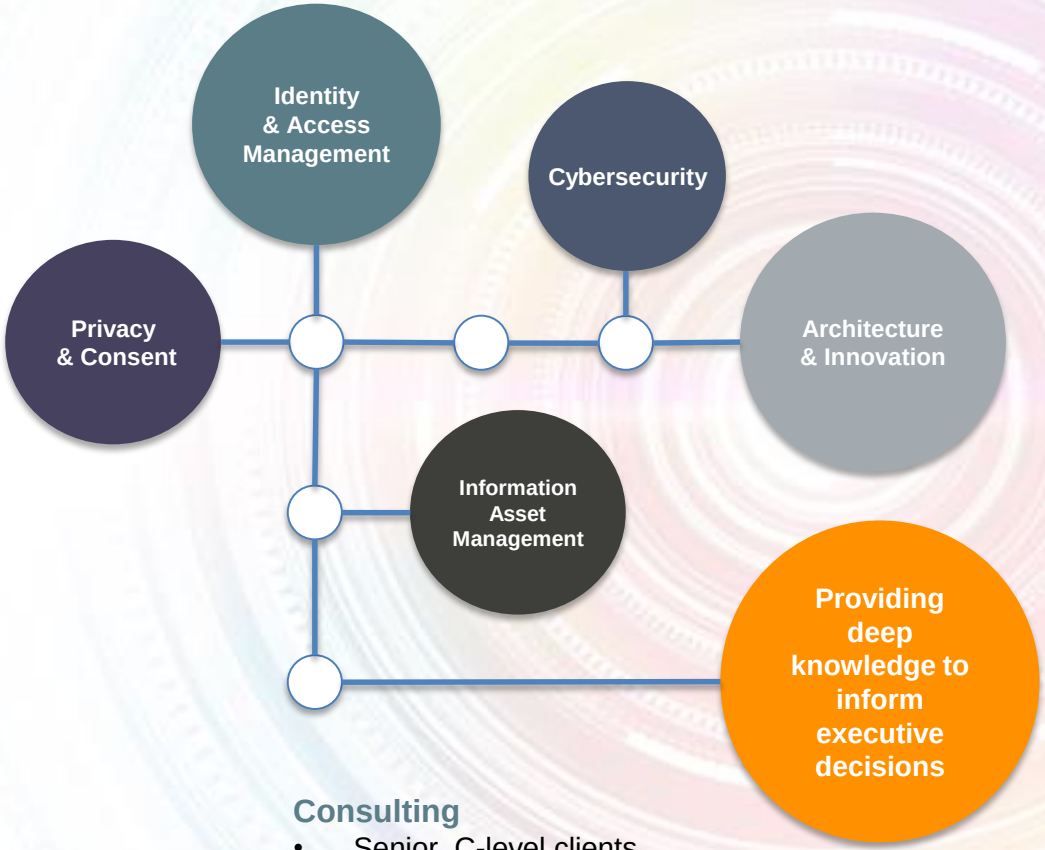
TechVision RESEARCH

TechVision Research: What we do

Take a client theme

- Identity and Access Management
- Security and Risk Management
- Data Architecture & Strategies
- Digital Transformation
- Innovation and Disruption
- Privacy and Information Protection
- Blockchain Adoption
- Internet of Things
- Network Architecture & Security
- Public, Private and Hybrid Cloud

and Connect the Dots



Research

- Broad and deep experience
- Industry specialists
- Technology pioneers
- Global perspective

Consulting

- Senior, C-level clients
- Bridge between board-level strategies and technical solutions

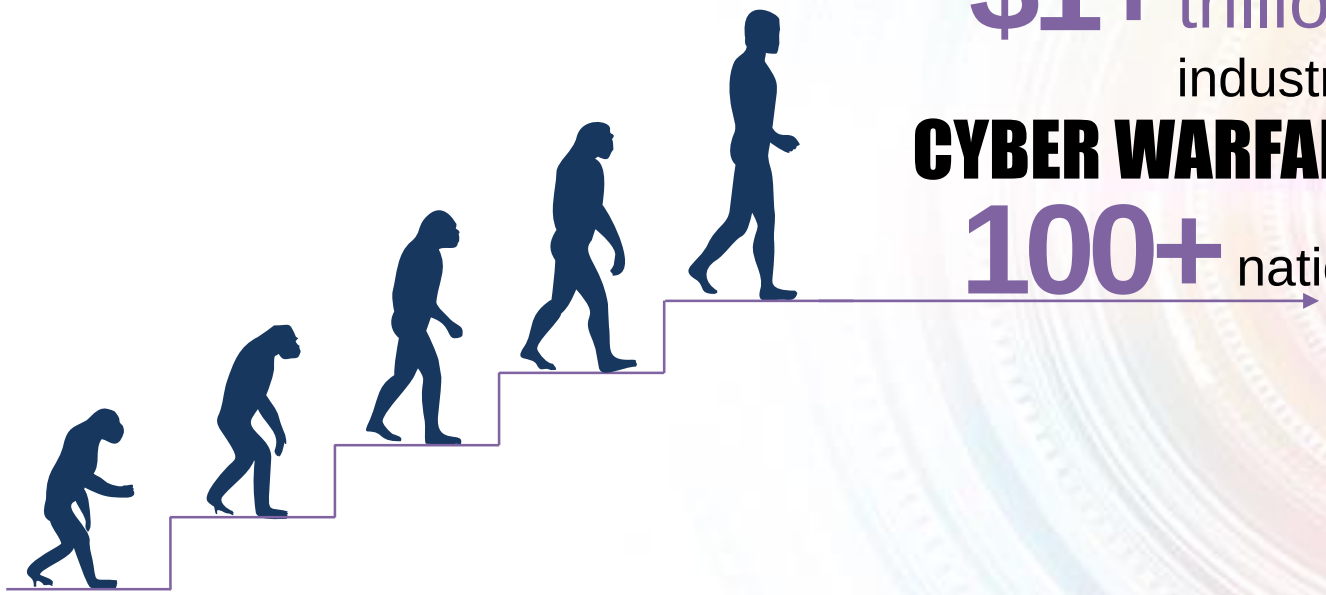
TechVision RESEARCH

Agenda

- The Evolving & Increasing Threat
- Why Today's Networks Are Not Secure
- Creating A New Security Model
- How Zero Trust Networking Works
- Measuring Network Risks
- Moving To A Zero Trust Network
- Q&A

Threats Will Continue To Grow

THE EVOLUTION OF THE **ATTACKER**



CYBERCRIME NOW

$1+ trillion industry

CYBER WARFARE

100+ nations

We Must Evolve Quicker!

Attack Vectors

- **Hacking** - Data theft, corporate espionage (a stolen EMR sells for $1,000/record, company intellectual property worth 100+B)
- **Social Engineering -** Phishing, bribing, threatening
- **Internal Attacks -** Unauthorized access (hackers, like spies, are recruiting employees and some reports claim 80% of breaches have some one/thing on the inside)
- **Compromised Partner** – APIs, network
- **Cloud Breaches** - Dropbox, iCloud, OneDrive, Etc.
- **Virus/Malware/Botnet** – Embedded into chipsets (200,000+ new malware signatures a month)
- **Ransomware –** Paid in bitcoin and becoming more frequent

Your organization will be compromised

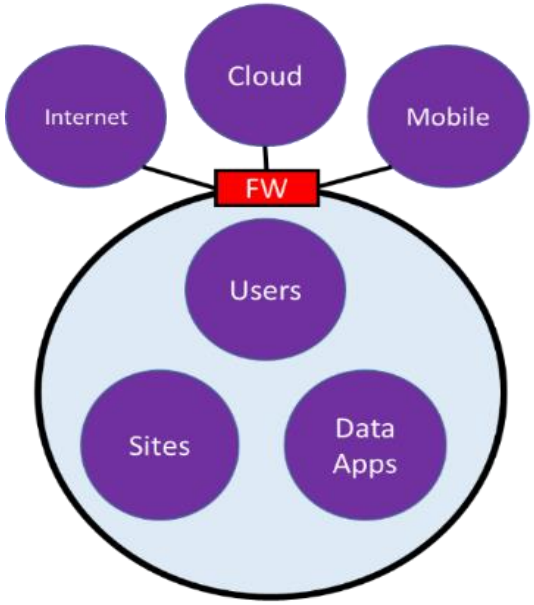
Understanding An Attack Vector

Zero Trust Networking can stop an attach at each step, which is why we are here today

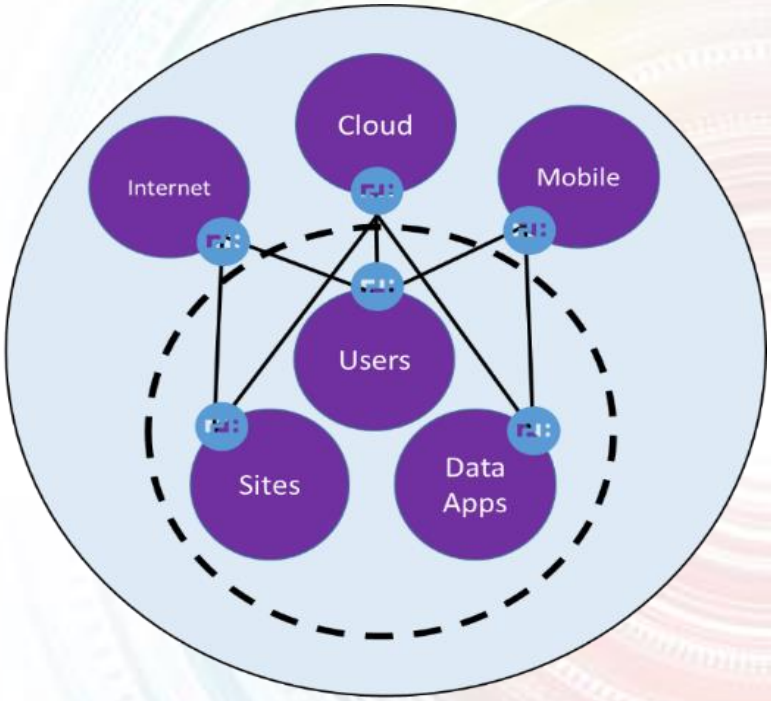
Agenda

- The Evolving & Increasing Threat
- Why Today's Networks Are Not Secure
- Creating A New Security Model
- How Zero Trust Networking Works
- Measuring Network Risks
- Moving To A Zero Trust Network
- Q&A

Gone Is The Secure Network Perimeter



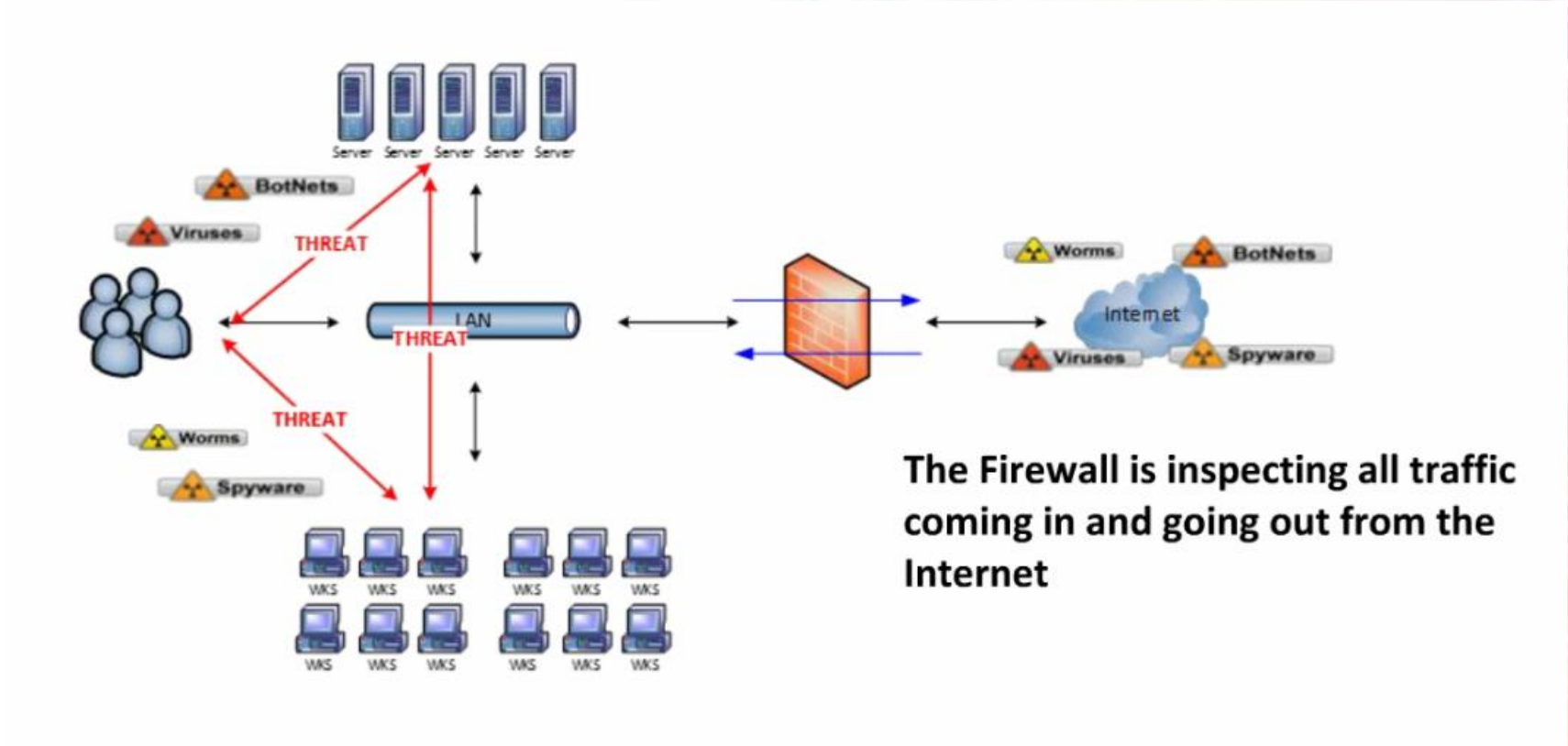
Secure Network Perimeter
With Clear Demarcation Point



Fluid Network Perimeter

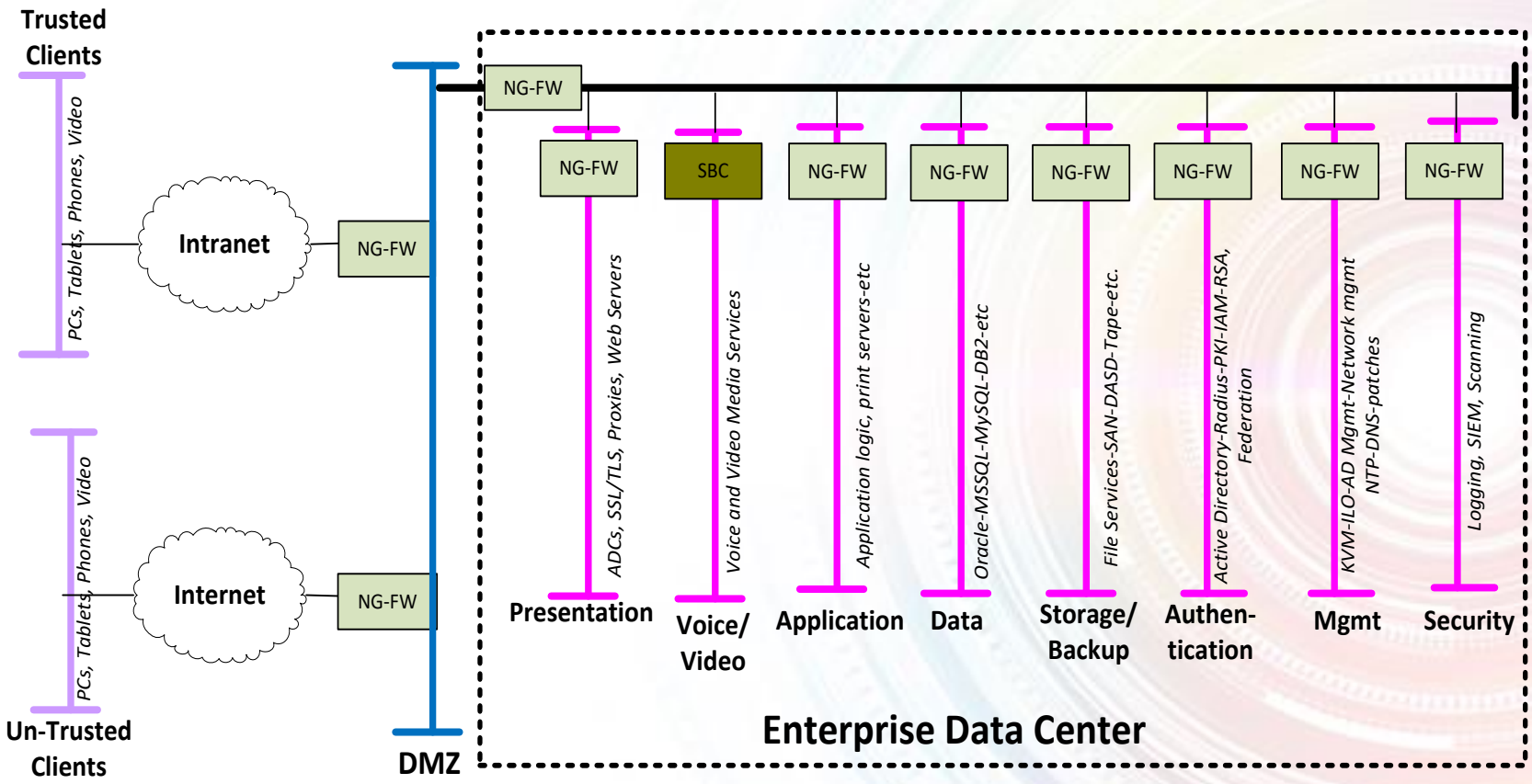
The Digital Economy blends customers, suppliers, organizations. Cloud, Mobile, BYOD, IoT, Social create a fluid network perimeter.

Threats Are Internal & External



Upwards of 80% of breeches have an internal security component, whether it is malware or a malicious employee

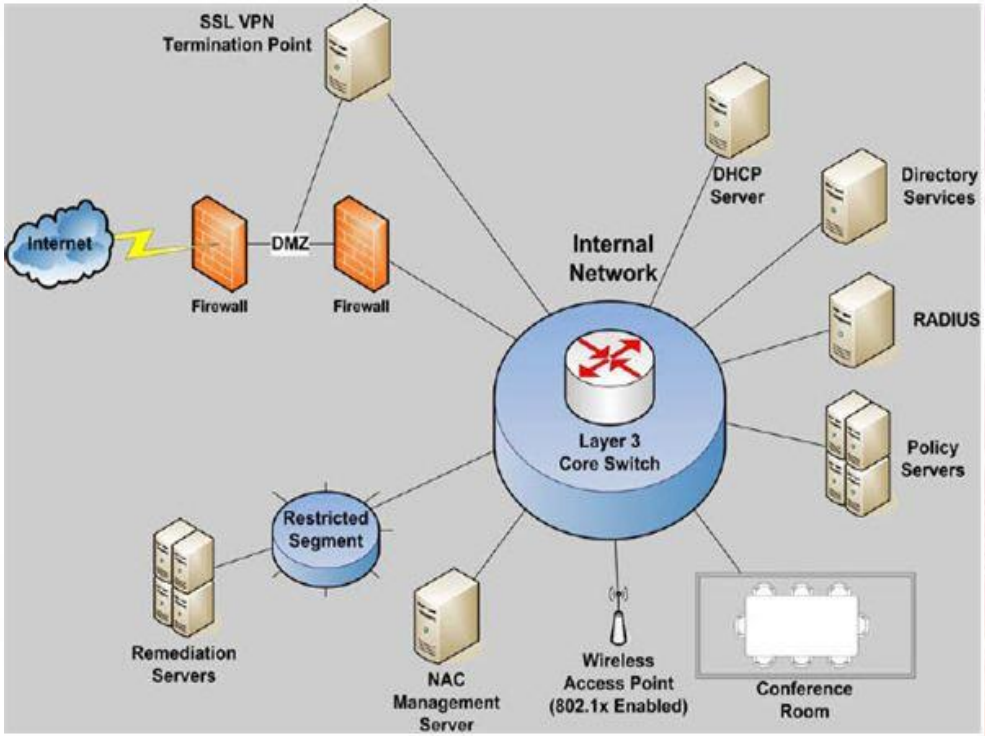
North/South Security Does Not Cut It



This architecture is good on paper, but does not account for East/West lateral movement nor operational backdoors

The Problems With NAC

- Assumes a trusted interior network
- Requires a device to have a common operating system to run NAC client (No BYOD or IoT)
- Requires control of all devices and applications accessing the network



Network Admission Control has many false positives which isolate and frustrates users.

Network Security Is Blind

- All new applications are using TLS, with keys that are not shared
- After the first 5 packets in a session setup, Firewalls & IDS are blind
- Most breeches are TLS encrypted too
- Future security will further compound this – DNS encryption, certificate encryption

Everything on the network will be encrypted at the application layer with no enterprise shared keys

Agenda

- The Evolving & Increasing Threat
- Why Today's Networks Are Not Secure
- Creating A New Security Model
- How Zero Trust Networking Works
- Measuring Network Security Risks
- Moving To A Zero Trust Network
- Q&A

Technology and Business Trends

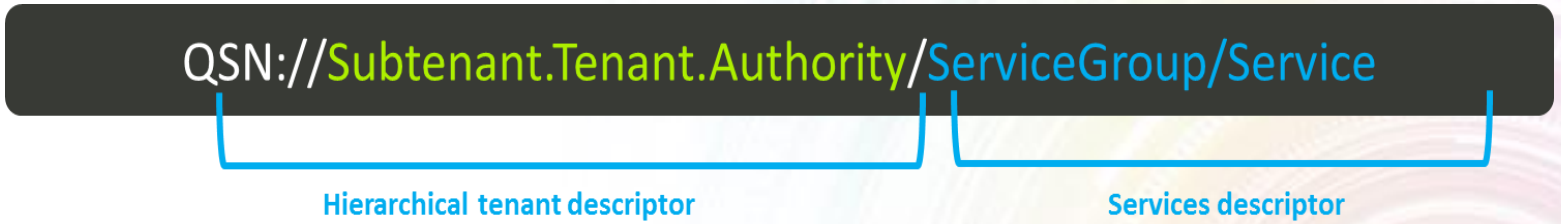
1. DevOps and microservices are the standard
2. Privacy and data protection are in the forefront
3. Enterprise security is proactive and user friendly
4. Disruption, innovation and change are the new normal
5. Every person, thing, service, application, and data are connected
6. AR/VR apps change the way we interact including how we work

The network still glues everything together, end-to-end

Driving New Security Models

1) Common Naming – Master integrated data model at all layers (Data, API, IAM Directory, Network)
2) More Sophisticated Identity and Access Management that is integrated at all layers including routing (layer 3)
3) Intelligent & Secure Edge – Stop malicious traffic at the edge versus in the middle of the network
4) Session & Stateful Networks – Move IP routing further up the technology stack

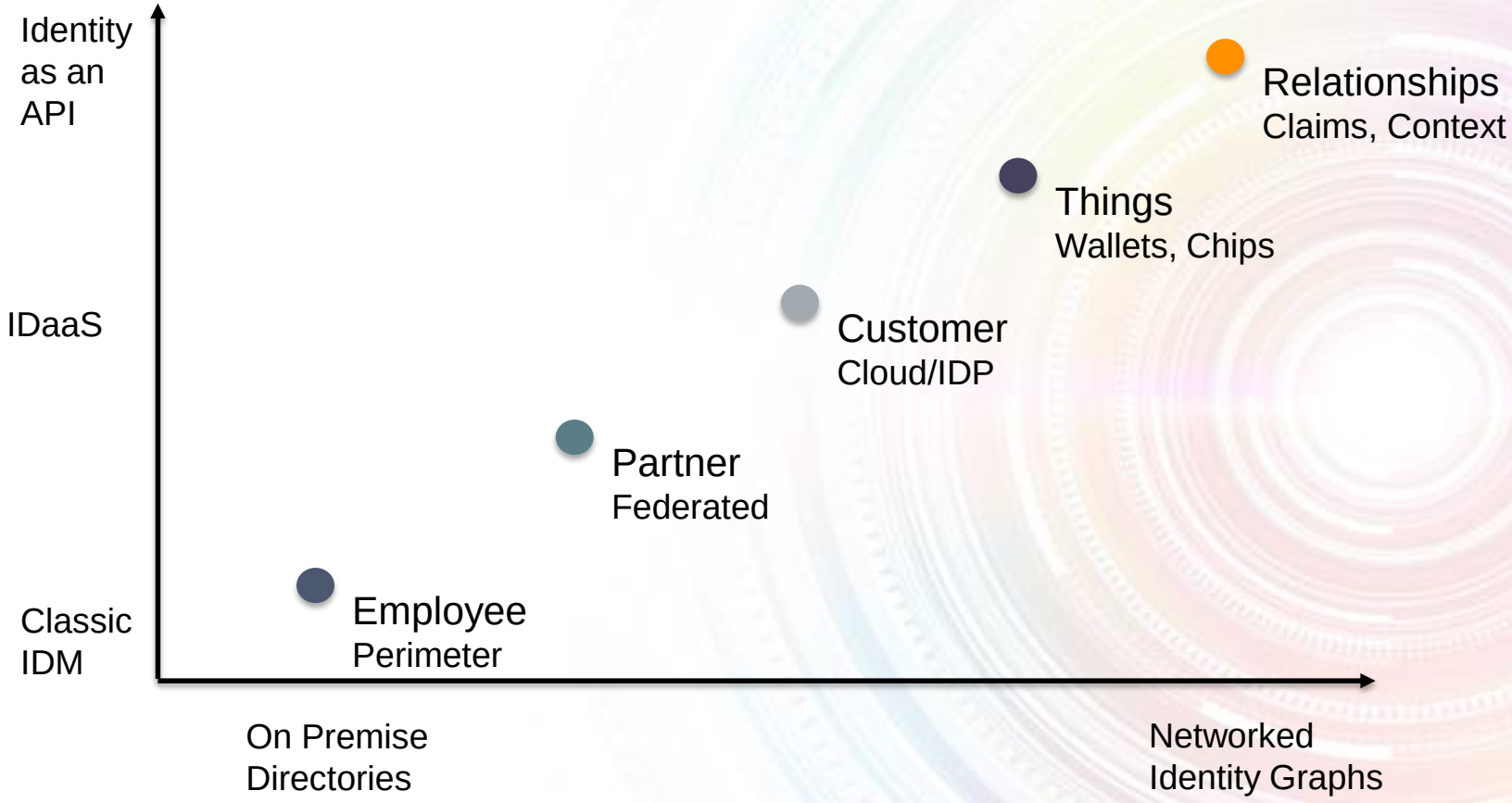
#1 Using Names, Not IP Addresses



- **Named Data Networking** – NSF project to replace IPv4/6 addressing and encrypt data to the user
- **Common Naming** is the foundation for integration and simplicity, but IP addresses are not going away for a long time, so IP abstraction will evolve as a way to link addresses and names
- **Complexity** - Today's routing and firewall rules based on access control lists using IP addresses and port numbers are static and complex and provide binary security rules of allow or deny
- **A Master Data Model** that connects meta-data of data -> API's -> Security -> Network is an **area of research that I would like to further explore and am seeking volunteers to help**

Routing needs to be integrated with IAM

#2 Evolution of Identity



Great IAM is the foundation of great security

#3 Intelligent Edge

Stop putting middleboxes and software at boundaries and drive intelligence to the edge.

- **Platform Sprawl -** many different security elements with different specialties required. You become the SI
- **Rule Management—**as applications or policies change, rules don't get uniformly updated across all platforms, leaving rules that are no longer relevant or that might create new vulnerabilities
- **Malware detection -** becomes another piece of product sprawl
- **Fast Identity & Isolation** - Very difficult to move from detection to prevention with so many dissimilar security products in the network

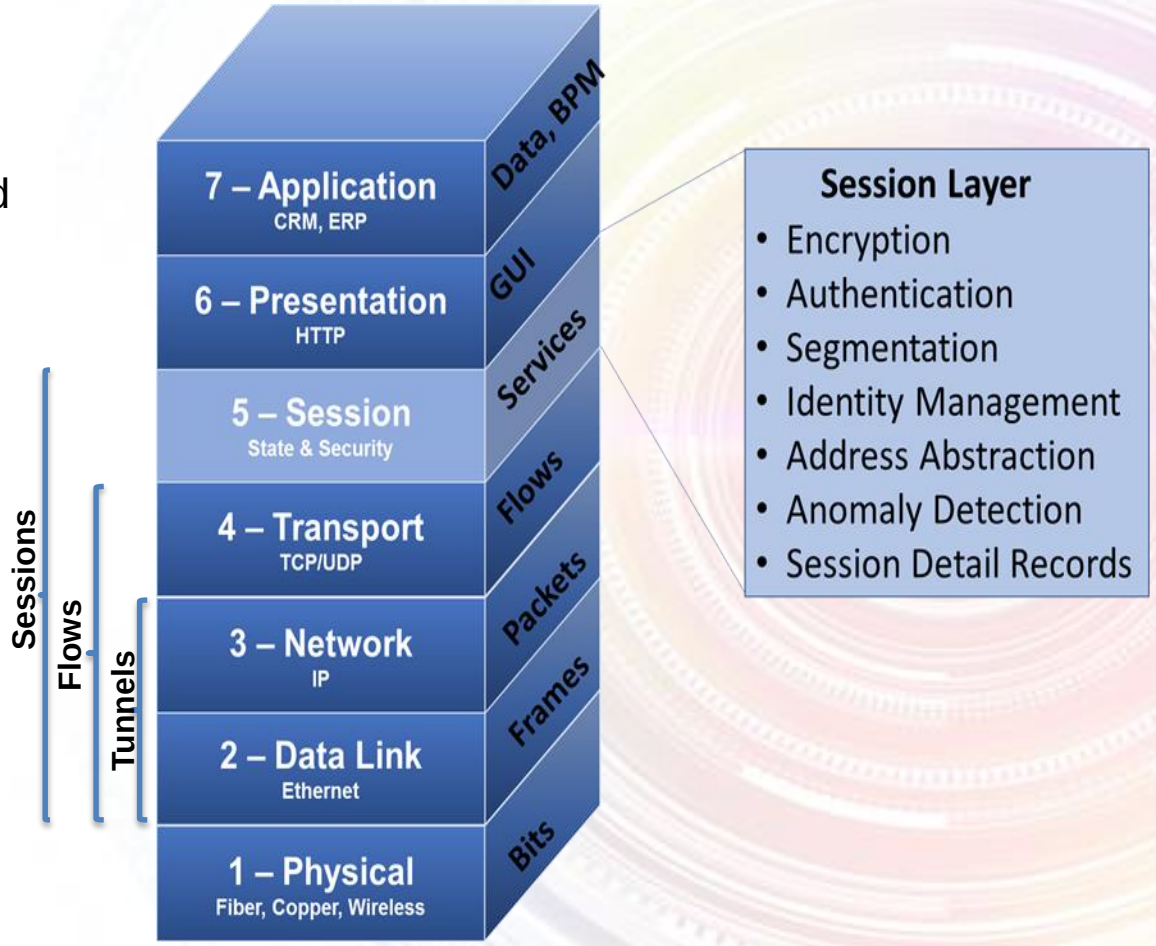
As networking & firewalls move to pure software, it is economically feasible to place them on the edge.

#4 Session & Stateful Networking

The Session layer provides the mechanism for opening, closing, and managing a session between end users and applications.

Sessions are stateful and end-to-end, which provides more granular network and security controls for application services.

Firewalls, proxies, SBCs, WAN op, load balancers, manage network state and provide higher-level networking and security functions.



Networking needs to move up to layer 5 to provide full suite of security functions

Agenda

- The Evolving & Increasing Threat
- Why Today's Networks Are Not Secure
- Creating A New Security Model
- How Zero Trust Networking Works
- Measuring Network Risks
- Moving To A Zero Trust Network
- Q&A

Defining Zero Trust Networking

- **A Zero Trust Architecture** means every user, device, service, or application is implicitly untrusted and must go through an identity and access management process to gain a least privileged level of trust and associated access privileges.
- **Zero Trust Networking, ZTN**, is a subset of this architecture focused on the IP network where all network traffic is considered untrusted.
- **In ZTN every TCP/UDP session that must be Authenticated, Authorized, and Accounted (AAA)** for before a communication session is allowed to be established.
- **ZTN enforces security policies at the edge of networks** and stops malicious traffic at its origin, not in the middle of the network or at the front door to an endpoint or application.

Changing Face of Network Security

- Legacy Blacklist Based Security Policies
  - Block known bad traffic (IP address, Port, URL, Signature)
  - Pass rest of traffic as good with static rules
  - Trust the secure internal perimeter
- Zero Trust Networking is Whitelist Based
  - Start with a zero trust model for everything (Internal & External). Do not trust any one/thing and only grant least privileged access
  - Only allow that which is pre-authenticated and authorized
  - Unknown traffic must be investigated and classified within a sandbox and create feedback loop to map unknown to known
  - Use anomaly detection to quickly identify and isolate compromised devices, services, or applications and dynamically update rules

Driveway Analogy to ZTN

- Today, someone can leave their house and come up your driveway and knock on your door.
- In a Zero Trust Networking world, someone would need prior authentication and authorization in order to leave their house to come to yours.

Agenda

- The Evolving & Increasing Threat
- Why Today's Networks Are Not Secure
- Creating A New Security Model
- How Zero Trust Networking Works
- Measuring Network Risks
- Moving To A Zero Trust Network
- Q&A

Defining The Network Attack Surface

The 4 variables used to calculate the network attack surface:

1) **Number of devices with access** – Number of devices that have network access to said device. On the LAN, this is all devices within the broadcast domain of a VLAN. On the WAN, it is all devices that have an IP address that can route to said device.

2) **Number of services** – Number of ports that are open on said device for communication. Common ones are HTTP (port 80), HTTPS (port 443), SSH (port 22), and the list goes on.

3) **Directionality** – Who can initiate a TCP/UDP session (1=yes, 10=no)

4) **Application Encryption** – A TLS 1.2 (with 1.3 on its way) session that validates the certificate for a session and provides 256bit AES encryption and a SHA-256 authentication, mitigating man in the middle attacks (1 = yes, 10 = no)

Enterprises should strive for a network attack surface of 1.

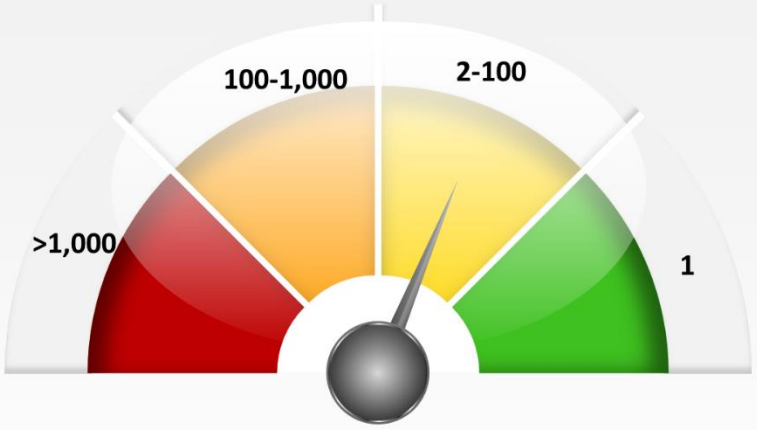
Example NAS Calculation

Scenario 1 – IoT surveillance camera that is on its own network VLAN by itself, using a private IP address, that sets up a HTTPS connection to a server and firewall and routing rules do not allow the camera to talk to anything else and the server initiates the conversation.

Number of IP devices with Access	1
Number of TCP/UDP Ports Open	1
Session Directionality Controls	1
TLS Encryption Used	1
Total - Network Attack Surface	**1**

Scenario 2 – IoT surveillance camera at the entrance of a remote warehouse. The warehouse has router/firewall that only allows sessions to be initiated to the Internet from within that network. There are 50 computers and systems on the LAN at this warehouse. The camera can be accessed through 40 different ports/services.

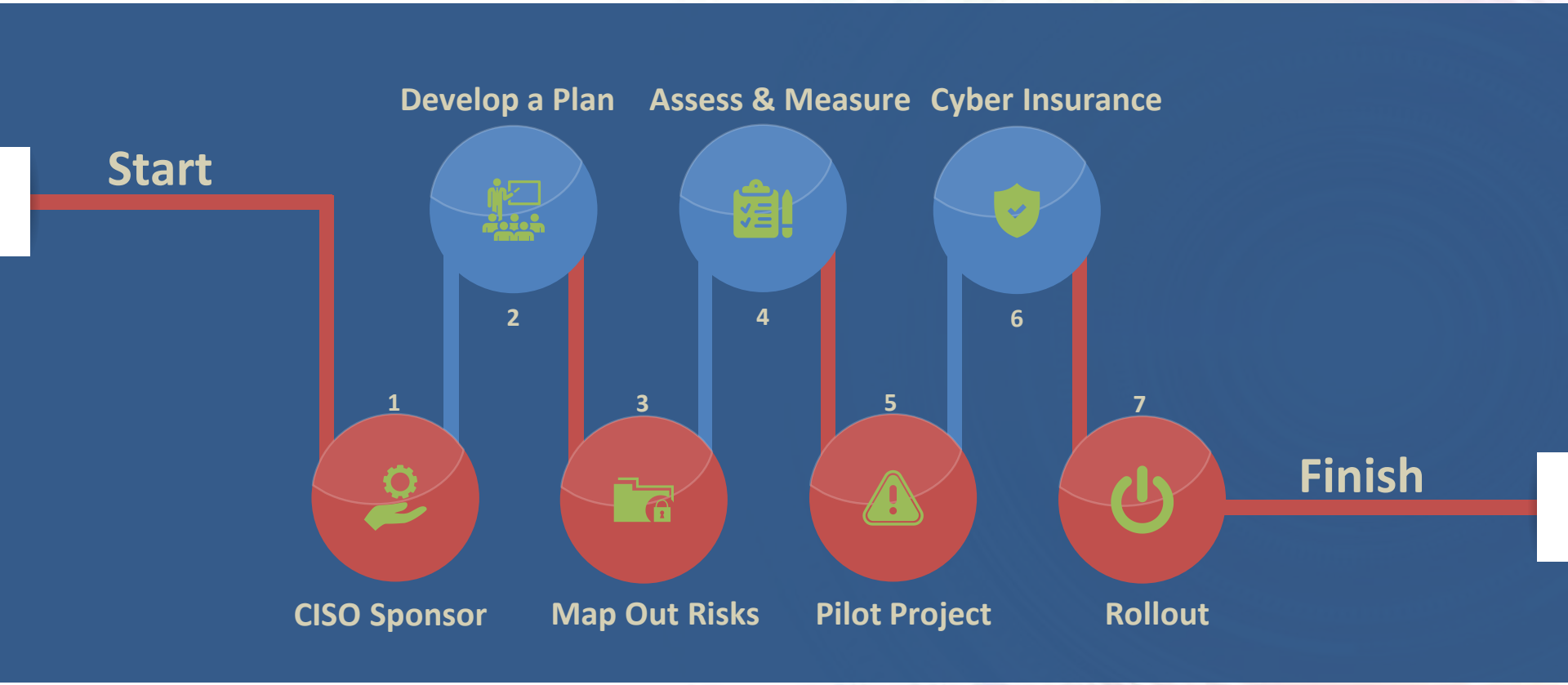
Number of IP devices with Access	50
Number of TCP/UDP Ports Open	40
Session Directionality Controls	10
TLS Encryption Used	10
Total - Network Attack Surface	**200,000**



Agenda

- The Evolving & Increasing Threat
- Why Today's Networks Are Not Secure
- Creating A New Security Model
- How Zero Trust Networking Works
- Measuring Network Risks
- Moving To A Zero Trust Network
- Q&A

ZTN Seven Step Plan

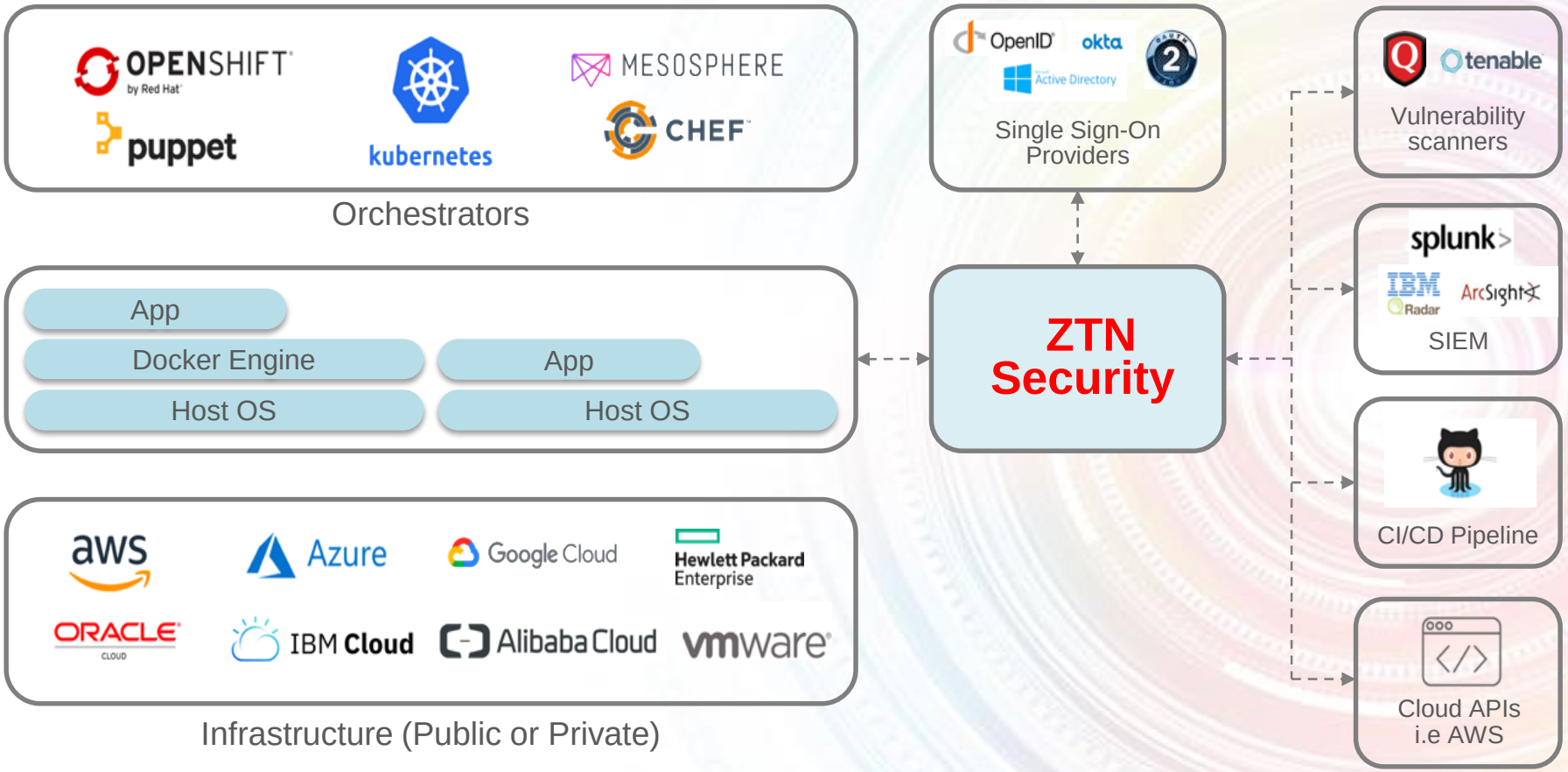


Moving to Zero Trust Networking will be an evolution, and one you should start today

Key ZTN Success Criteria

1) **Leverage IAM –** Use existing directories to define who has access to what. Great IAM is the source of truth.
2) **Track Anomalies** – The best way of finding malicious users or malware that has been activated is to track network anomalies when a user, device, server, or application has multiple attempts to try and communicate with something it does not have permission for.
3) **Intelligent & Dynamic –** Access rules should have many different variables and criteria – time of day, previous access, current security threats, level of authentication, location, device used, …
4) **Ensure Encryption In Motion –** While most applications will be TLS encrypted, ensure that which is not, is encrypted at the network layer such as printers, CTI, Voice, some Internet traffic, …
5) **Start With Specific Project** – Get a win and then move on, some examples are on the next few slides

Example #1 Hybrid/Multi-Cloud

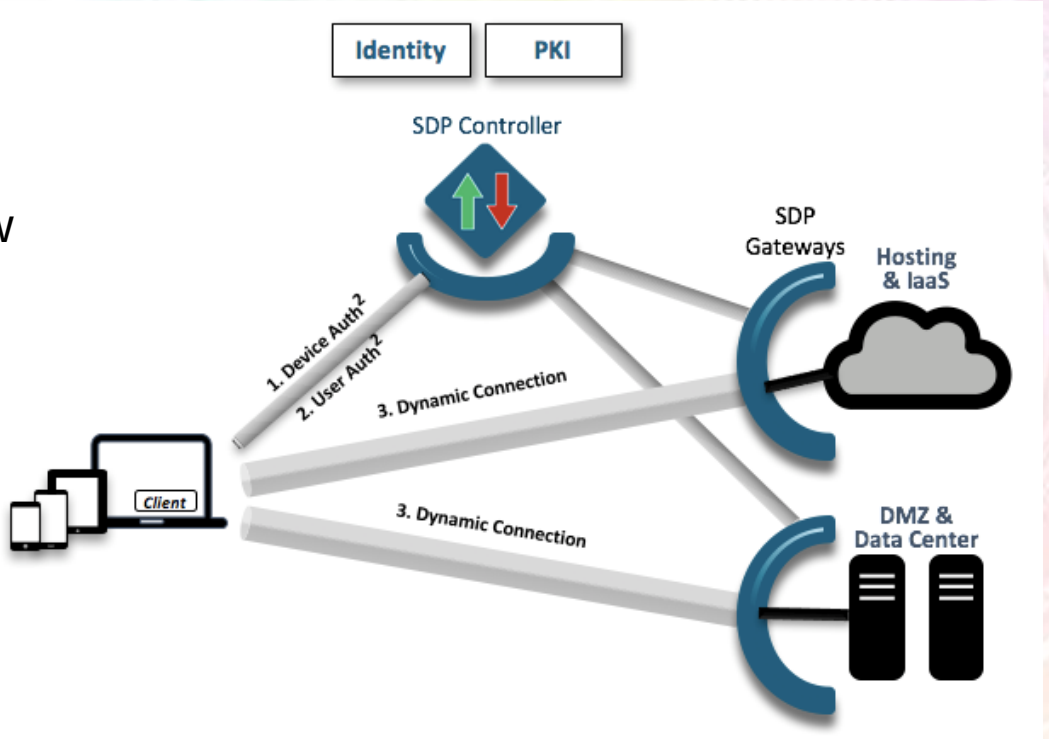


Overlay providing a 1:1 mapping of containers, microservices, and applications to IAM

Ex. #2 – Intelligent & Dynamic VPN

3rd party technical support needs access to a server to apply a patch. Create a trouble ticket

1) Create a maintenance window
2) Allow specific technician access to only one specific server
3) Technician multi-factor log-on
4) Create 1:1 VPN tunnel from technician to server
5) Technician cannot see or access anything else in data center.



1:1 mapping of user to another device, service, or app

Ex. #3 – Point of Sale Segmentation

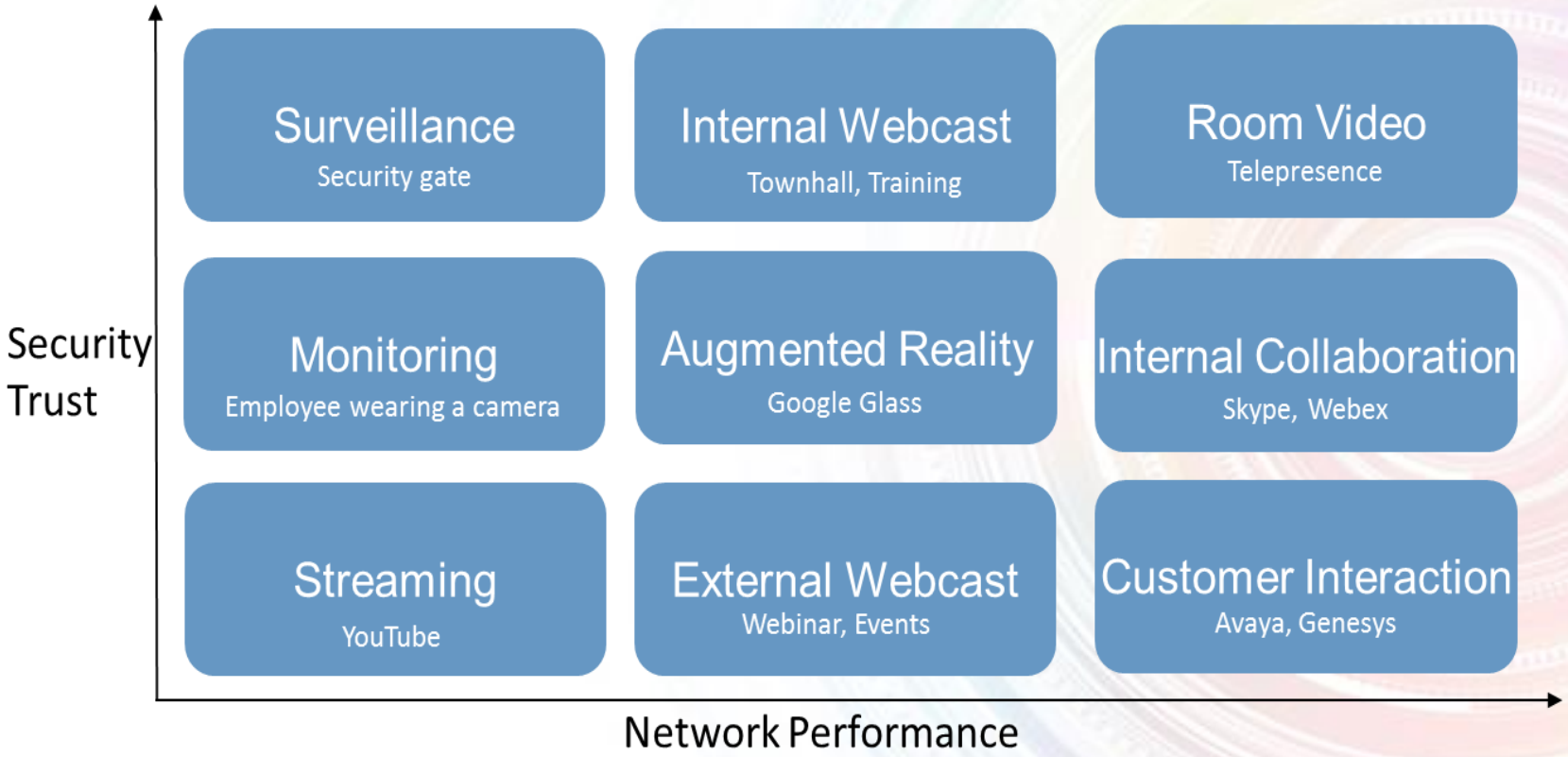
The problem with today's segmentation is that it only goes down to the specific endpoint

ZTN takes segmentation to the services and applications running on an endpoint

Example, credit card PCI authorization can be on a separate logical segment with its own unique encryption from other applications and services running on the device.

Logical segmentation within a physical device

Ex. #4 – SD-WAN Segmentation



Segmenting traffic based on security and performance to go across different WAN links (MPLS, Internet, LTE)

Key Take-Aways

1) ZTN is the 1:1 mapping of users, devices, services, and applications such that no TCP/UDP session is allowed to be established without prior authentication and authorization.
2) It is more secure to define whitelists of access versus blacklists of denial
3) Integrating IAM directories with routing empowers enterprises to build zero trust networks, but this will require session stateful routing

Q&A

TechVision RESEARCH

Thank You

TechVision RESEARCH