TechVision RESEARCH

Zero Trust Networking

Webinar
Feb 21, 2019

Sorell Slaymaker
Principal Consulting Analyst
TechVision Research
sorell@techvisionresearch.com

TechVision Research at a glance

Our model is built around industry experts with strong track records of execution.

We go beyond the trends. Our deliverables-based engagements give you the action plans you need to get the job done.

We offer tested templates, tools and reference architectures to assist your decision making.

Founded in 2015 by veterans of the research industry to bridge the gap between enterprise board-level strategy and technical solutions through cutting-edge research and pragmatic consulting.

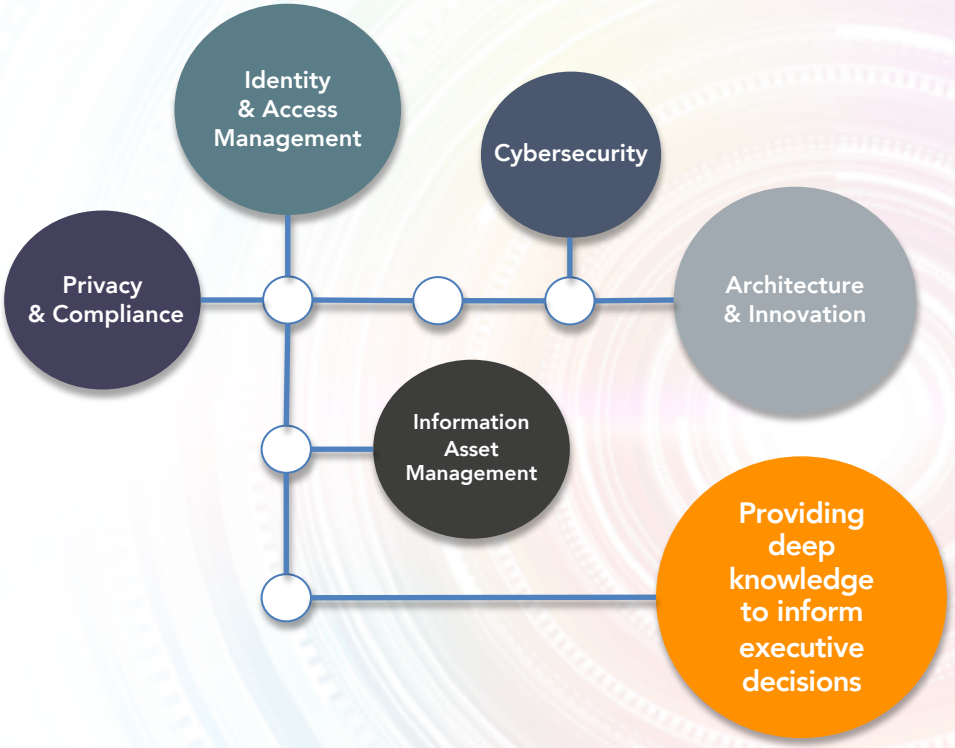
TechVision RESEARCH

What we do

Take a client theme

- Zero Trust Networking
- Microservices Level Set
- Identity of Things
- Evolving against Vulnerabilities, Breaches and the next Cyber Attack
- AI Executive Level Set—The Three Waves of AI
- Innovation Reference Architecture
- Customer Identity and Access Management (CIAM)
- Multi-Factor Authentication (MFA)
- Developing an Enterprise Blockchain Strategy
- Future of Identity Management (2019-2024)
- Developing an Enterprise DevOps Strategy
- The Future of Work
- Robotic Process Automation (RPA)
- Consent Management
- Best Practices in Securing Unified Communication
- An Emerging Decentralized Identity/Verifiable Claims Ecosystem
- Developing a Digital Transformation Reference Architecture

and Connect the Dots



Research

- ✓ Enterprise-focused research with unlimited access
- ✓ Answers the hardest technology questions
- ✓ Research agenda driven by disruptive and emerging technologies

Consulting

- ✓ Deliverables-based engagement model using proven techniques
- ✓ Performed by one or more of our Principal Consulting Analysts
- ✓ Tailored to your specific situation

TechVision RESEARCH

Today's Presenters

Gary Rowe is a seasoned technology analyst, consultant, advisor, executive and entrepreneur. Mr. Rowe helped architect, build and sell two companies and has been on the forefront the standardization and business application of core infrastructure technologies over the past 35 years. Core areas of focus include identity and access management, blockchain, Internet of Things, cloud computing, security/risk management, privacy, innovation, AI, new IT/business models and organizational strategies.

He was President of Burton Group from 1999 to 2010, the leading technology infrastructure research and consulting firm. Mr. Rowe grew Burton to over $30+ million in revenue on a self-funded basis, sold Burton to Gartner in 2010 and supported the acquisition as Burton President at Gartner.

Sorell Slaymaker has 30 years of experience designing, building, securing, and operating IP networks and the communication services that run across them. His mission is to help make communication easier, cheaper and more secure since he believes that the more we communicate, the better we are. Prior to joining TechVision Research, Sorell was an Evangelist for 128 Technology which is a routing and security software company. Prior to that, Sorell was a Gartner analyst covering enterprise networking, security, and communications.

Sorell is an IT Architect with a focus on network, security, and communications architecture. He specializes in IT Architecture – Network Architecture, SIP Trunking, Contact Centers, Unified Communications, and Security Architecture.

TechVision RESEARCH

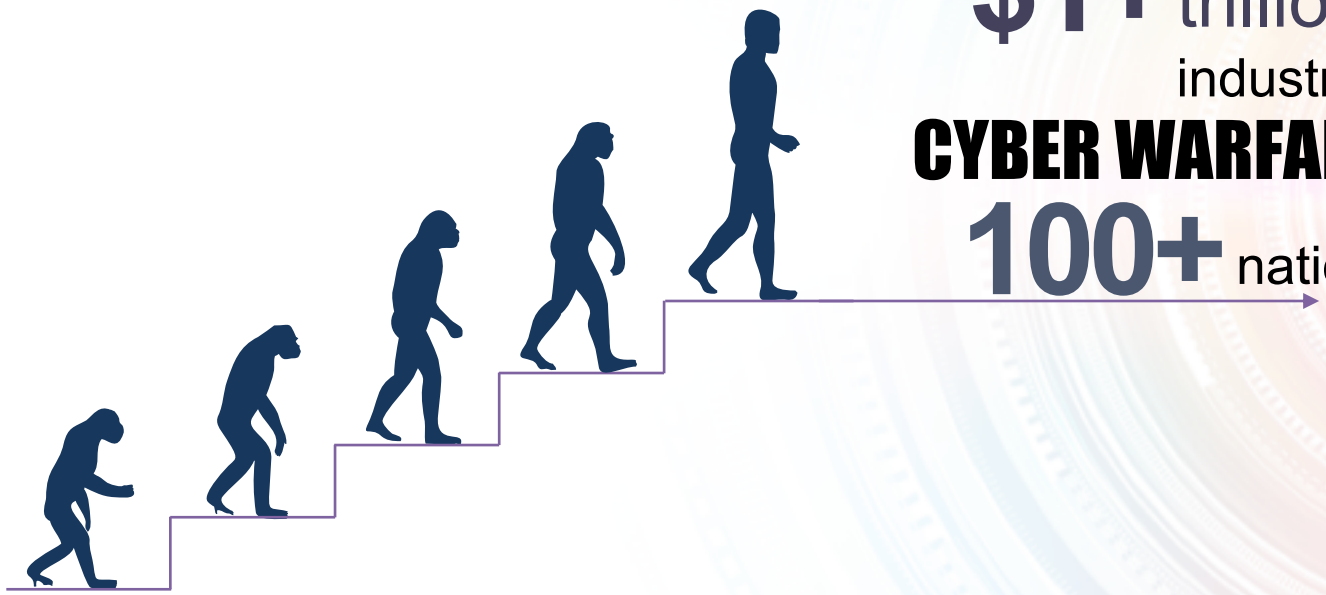
ZTN Agenda

- 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

TechVision RESEARCH

Threats Will Continue To Grow

THE EVOLUTION OF THE **ATTACKER**



CYBERCRIME NOW

$1+ trillion industry

CYBER WARFARE

100+ nations

We Must Evolve Quicker!

TechVision RESEARCH

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)

TechVision RESEARCH

Understanding An Attack Vector

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

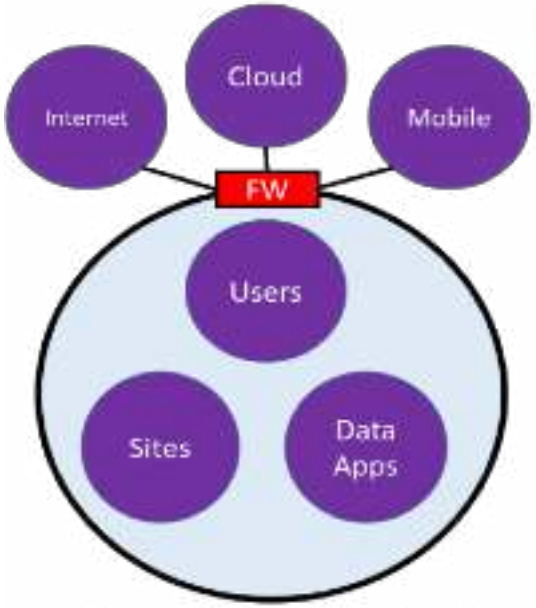
TechVision RESEARCH

Agenda

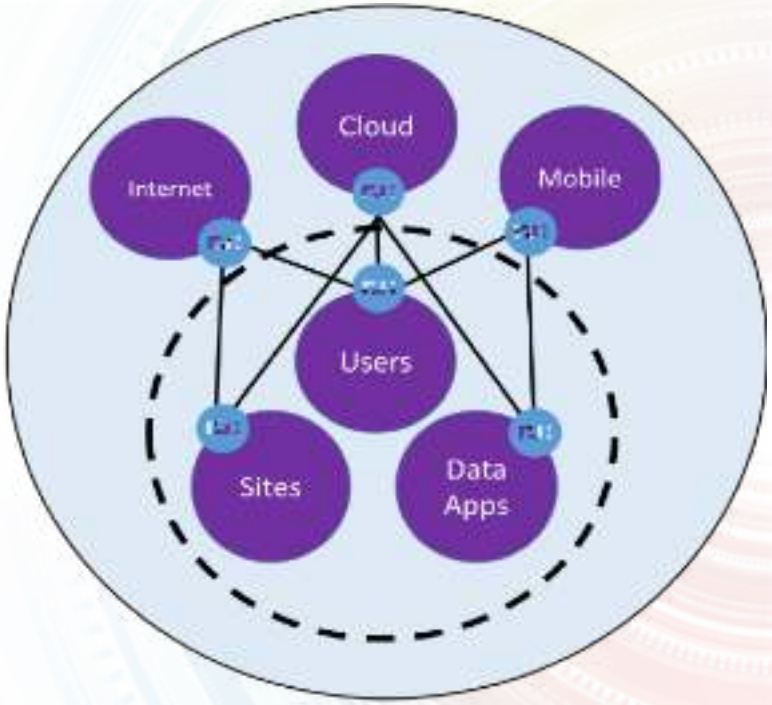
- The Evolving & Increasing Threat
- Why Today's Networks Are Not Secure
- Creating A New Security Model
- How Zero Trust Networking Works
- Measuring Network Risks
- Moving To A Zero Trust Network
- Q&A

TechVision RESEARCH

Gone Is The Secure Network Perimeter



Secure Network Perimeter
With Clear Demarcation Point

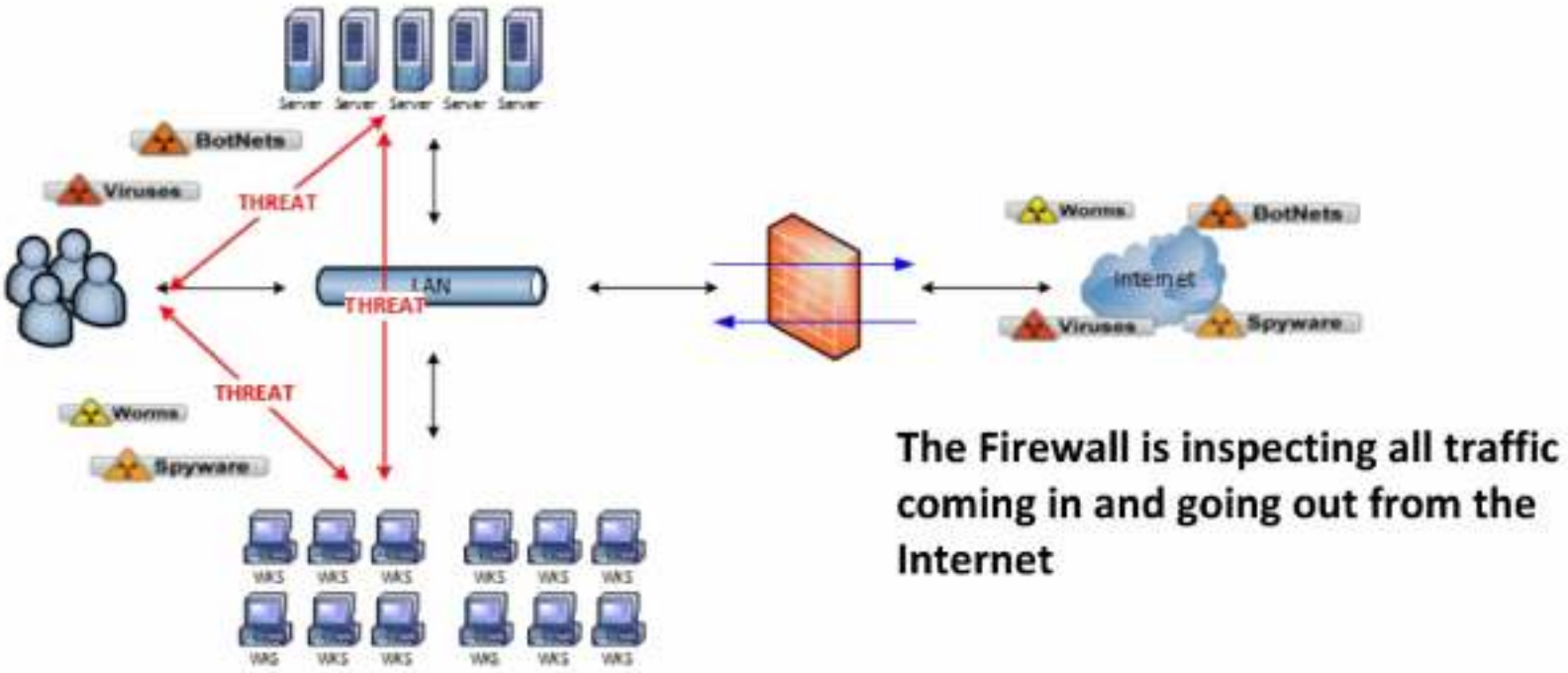


Fluid Network Perimeter

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

TechVision RESEARCH

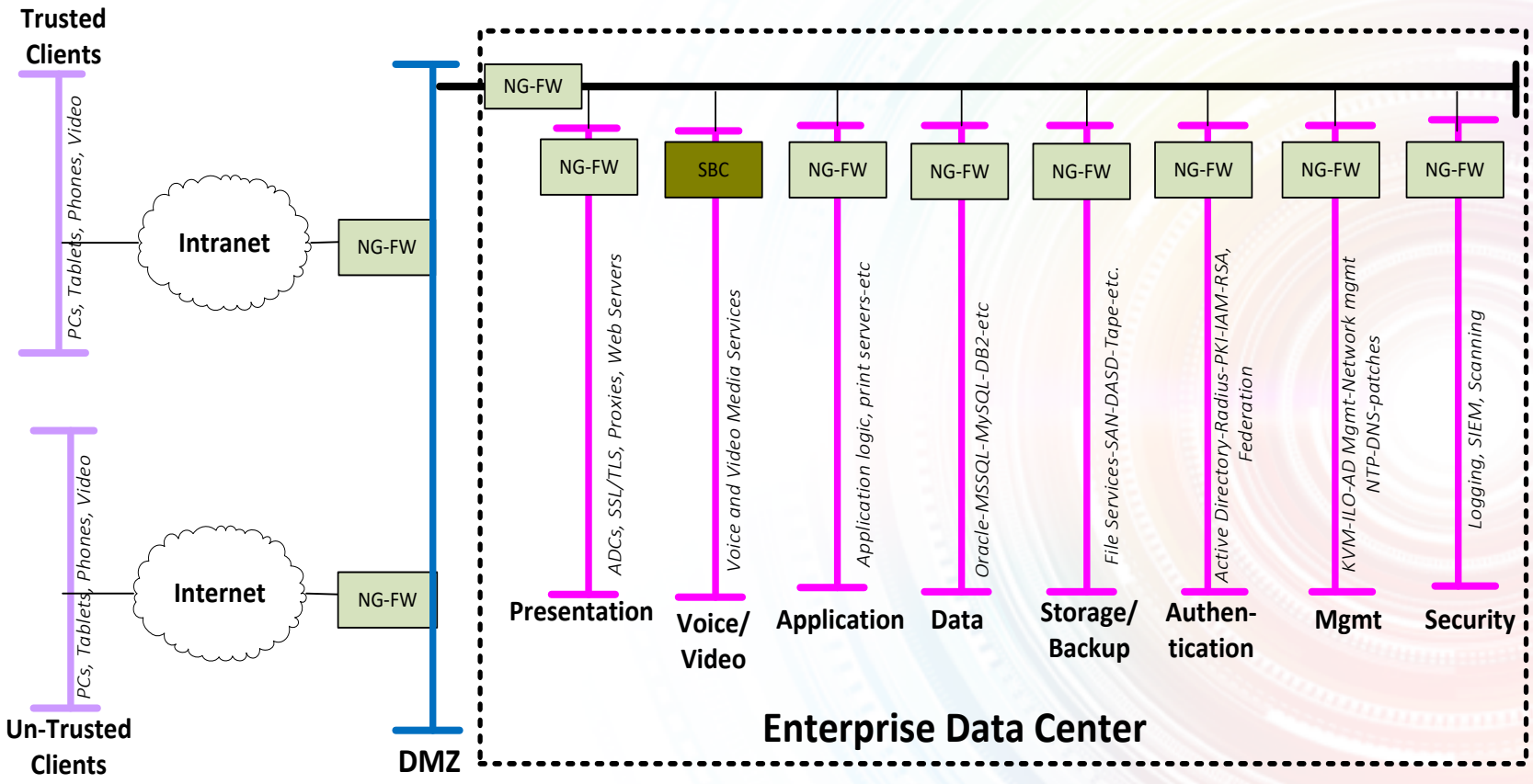
Threats Are Internal & External



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

TechVision RESEARCH

North/South Security Does Not Cut It

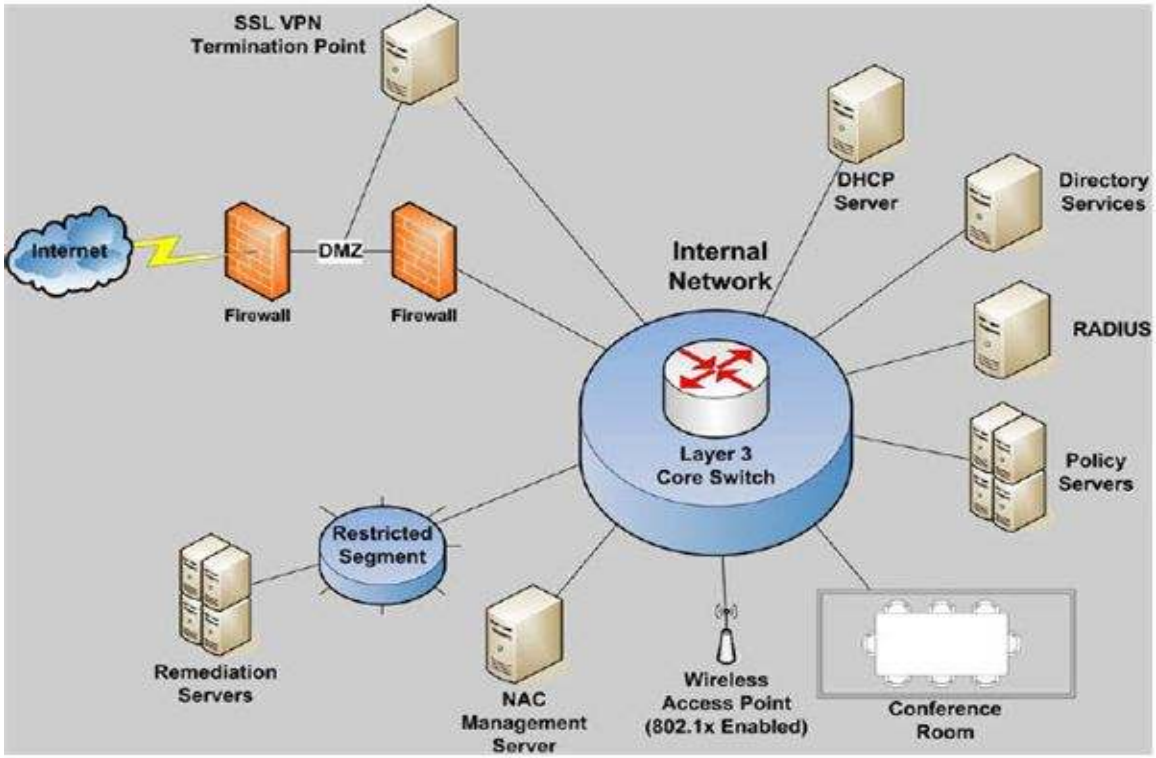


Physical zones are the old way of data center network security which does not work in a virtualized world

TechVision RESEARCH

The Problems With NAC

- Assumes a trusted interior network
- Requires a device to have a common operating system to run NAC client
- Requires control of all devices and applications accessing the network



Printers, IoT, BYOD, Cloud, Partners plus users who want instant access are all challenges for VPNs and NAC

TechVision RESEARCH

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

TLS 1.3 with Server Name Indication and DNS over TLS makes the network and proxies blind

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 Security Risks
- Moving To A Zero Trust Network
- Q&A

TechVision RESEARCH

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

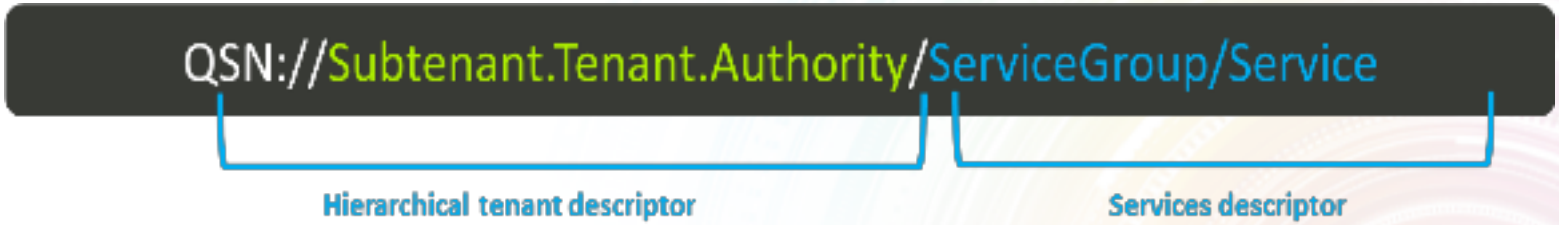
TechVision RESEARCH

4 Steps in Creating New Network Security Model Based on Zero Trust

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

TechVision RESEARCH

#1 Using Names, Not IP Addresses

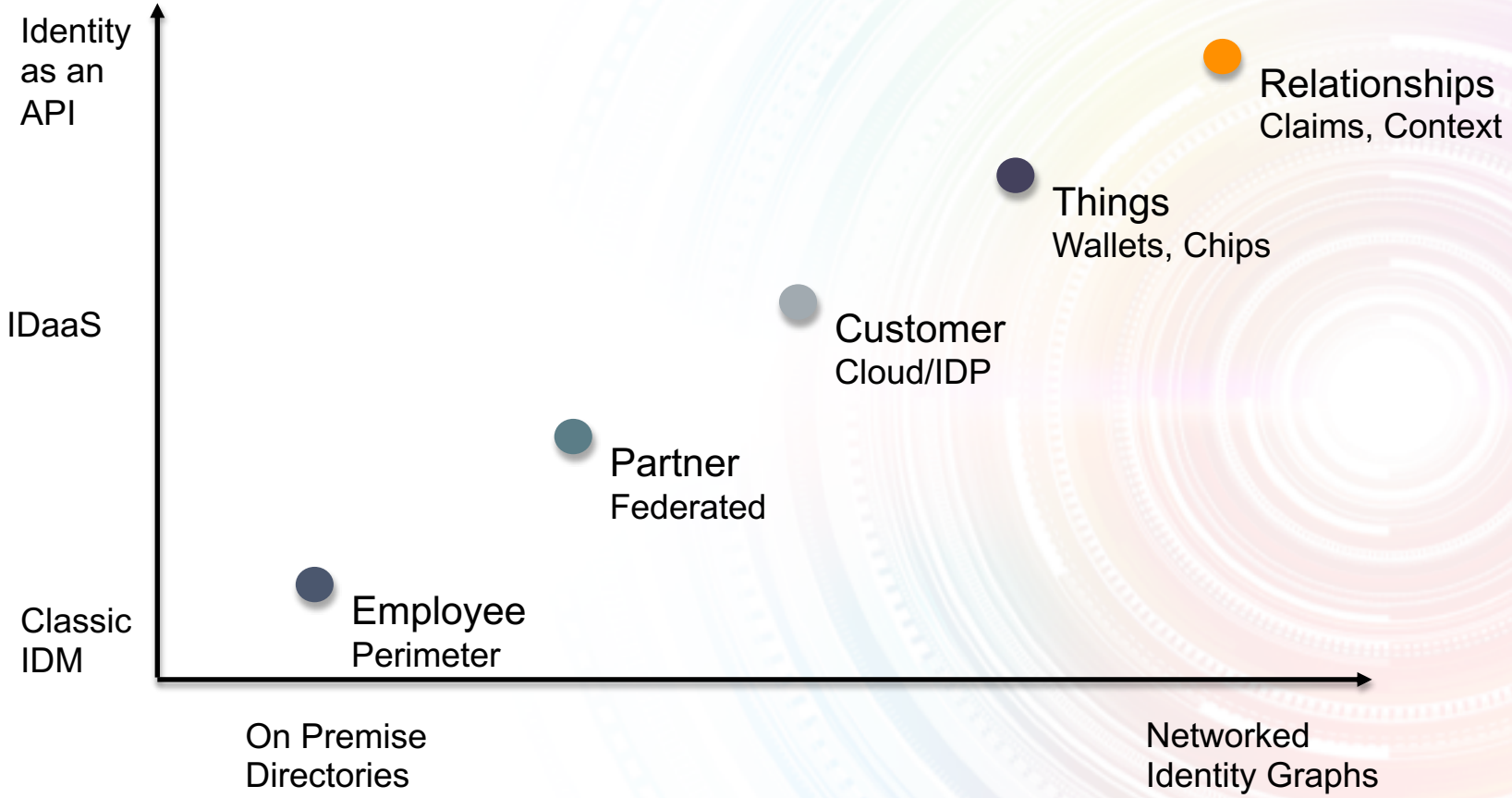


- **Named Data Networking** – NSF project to replace IPv4/6 addressing and encrypt data to the user
- **Common Naming** is the foundation for integration and simplicity, but IP addresses are not going away for a long time, so IP abstraction will evolve as a way to link addresses and names
- **Complexity** - 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**

https://blogs.cisco.com/sp/cisco-announces-important-steps-toward-adoption-of-information-centric-networking

TechVision RESEARCH

#2 Evolution of Identity



TechVision RESEARCH

#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.

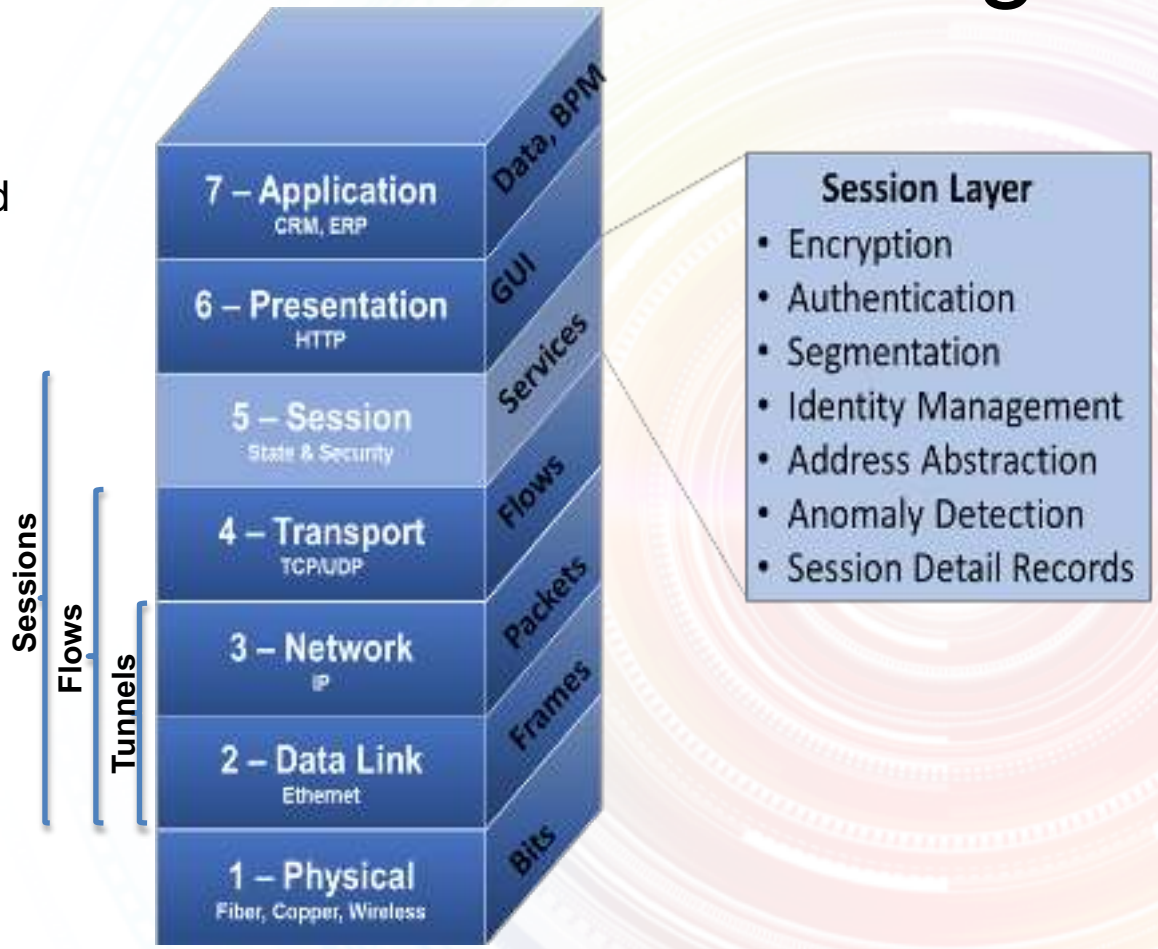
TechVision RESEARCH

#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

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

TechVision RESEARCH

Defining Zero Trust Networking

- **A Zero Trust Architecture** means that 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 must first 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.

TechVision RESEARCH

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

TechVision RESEARCH

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.

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

TechVision RESEARCH

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.

TechVision RESEARCH

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**

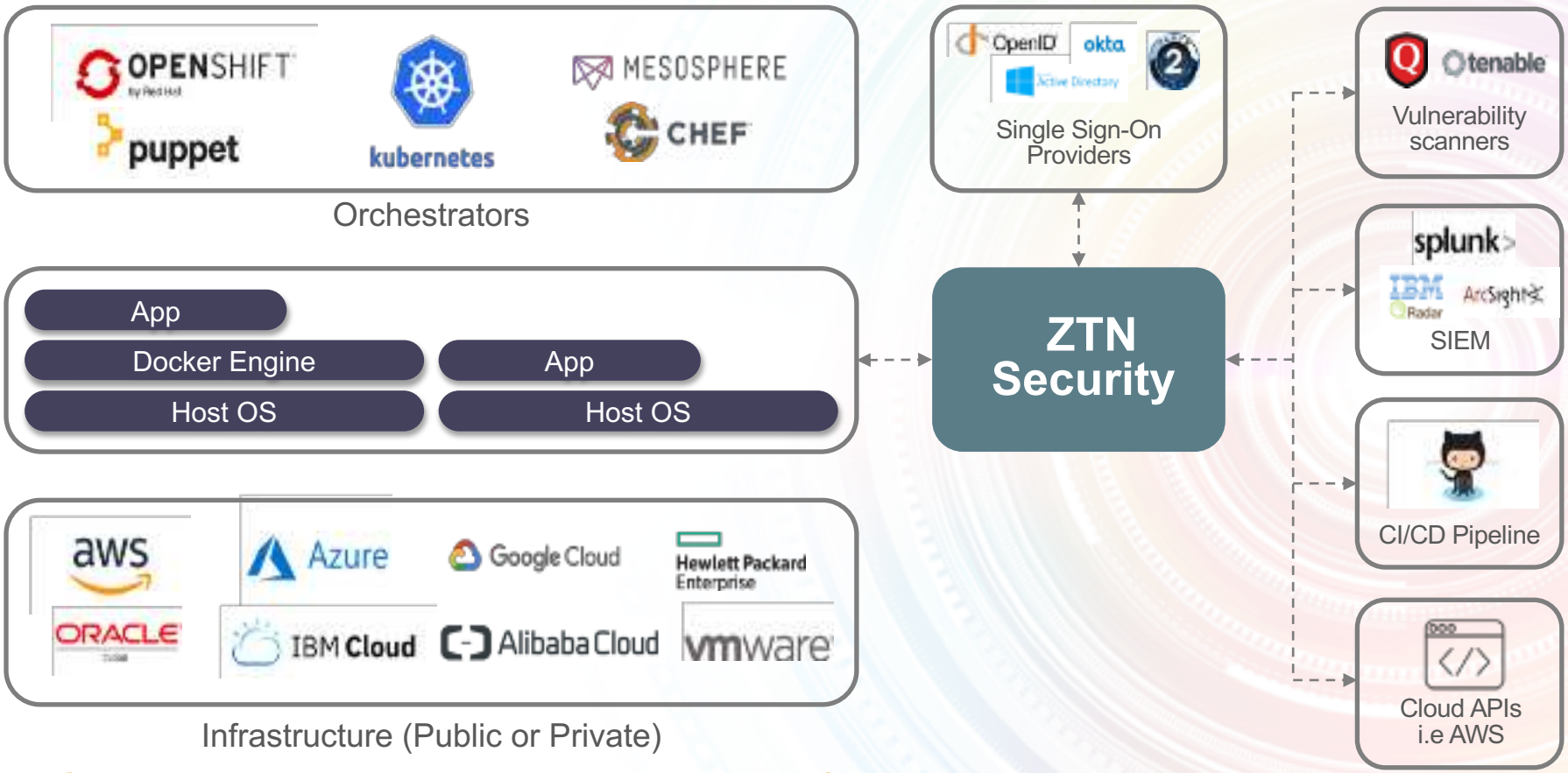
TechVision RESEARCH

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

TechVision RESEARCH

Example #1 Hybrid/Multi-Cloud



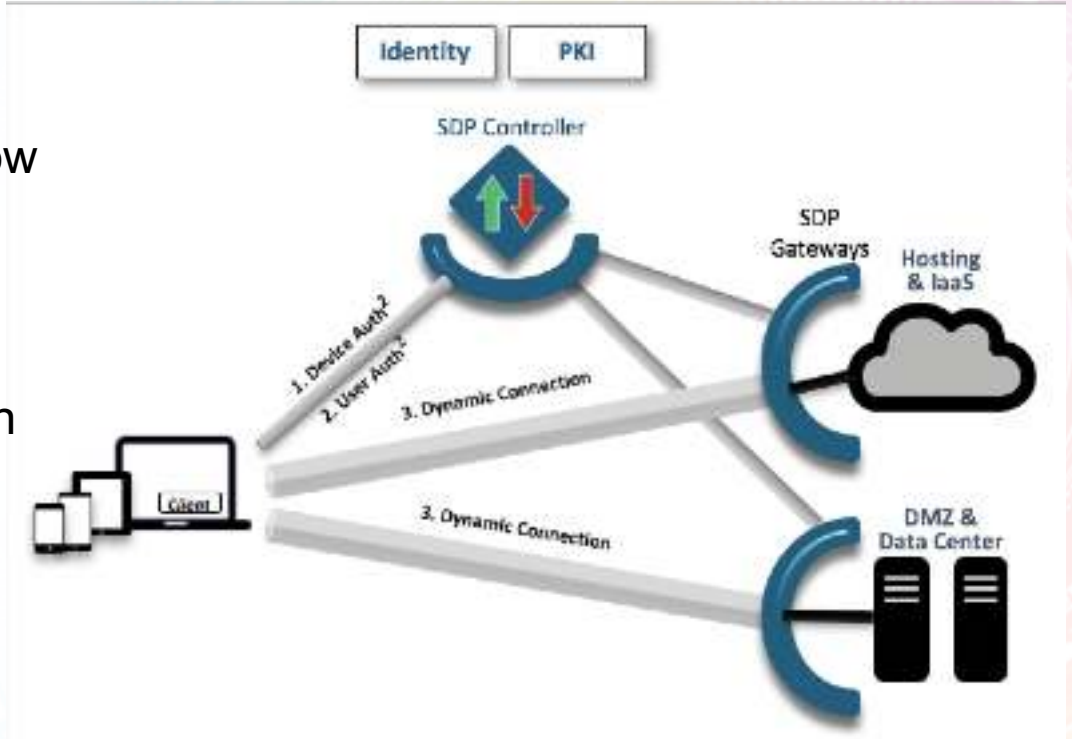
Overlay providing a 1:1 mapping of containers, microservices, and applications to IAM - *www.aporeto.com*

TechVision RESEARCH

Ex. #2 – Intelligent & Dynamic VPN

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

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
https://www.cyxtera.com/secure-access/appgate-sdp

TechVision RESEARCH

Ex. #3 – Point of Sale Segmentation

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

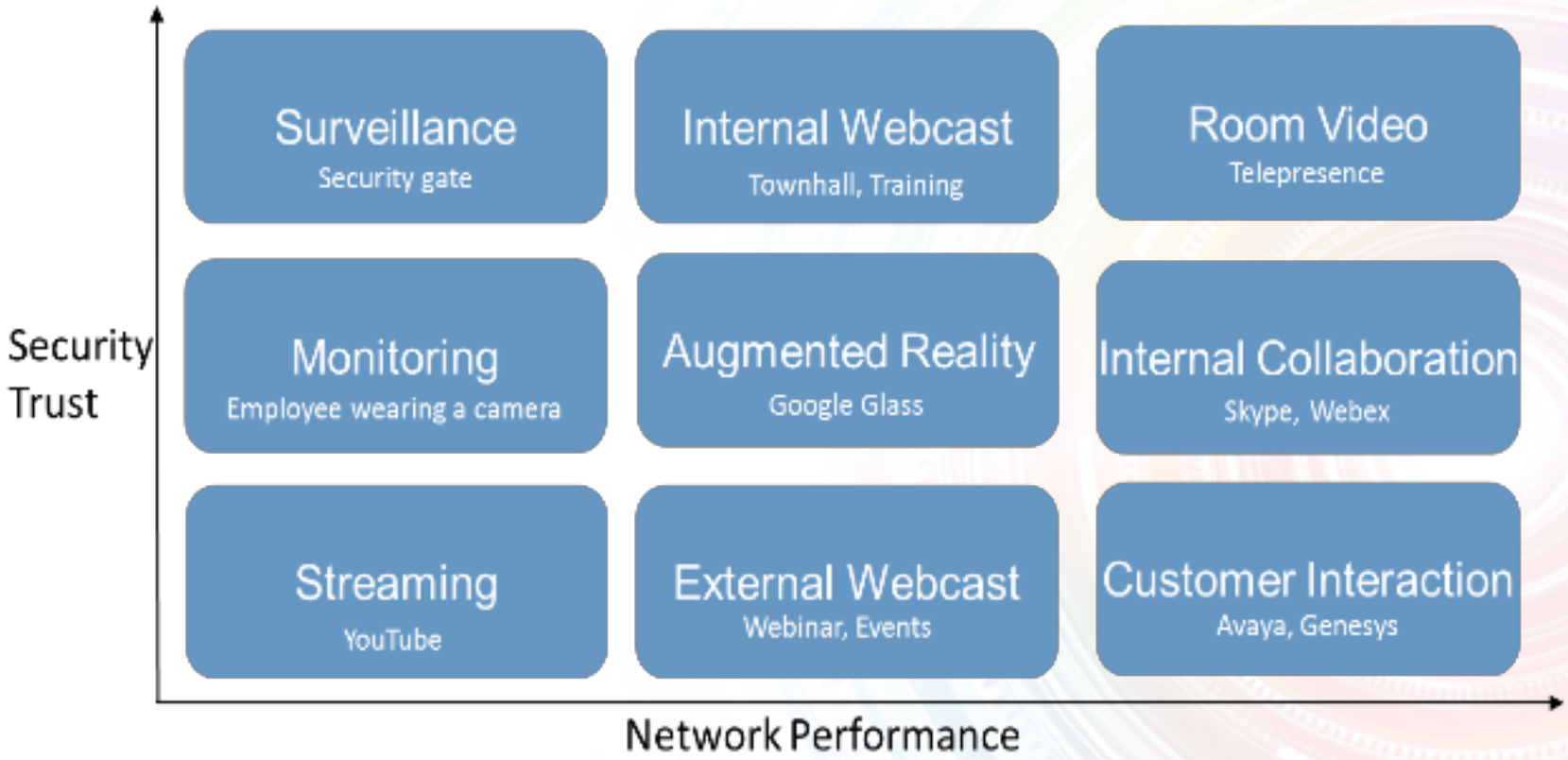
ZTN takes segmentation to the services and applications running on an endpoint

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

TechVision RESEARCH

Ex. #4 – SD-WAN Video Segmentation

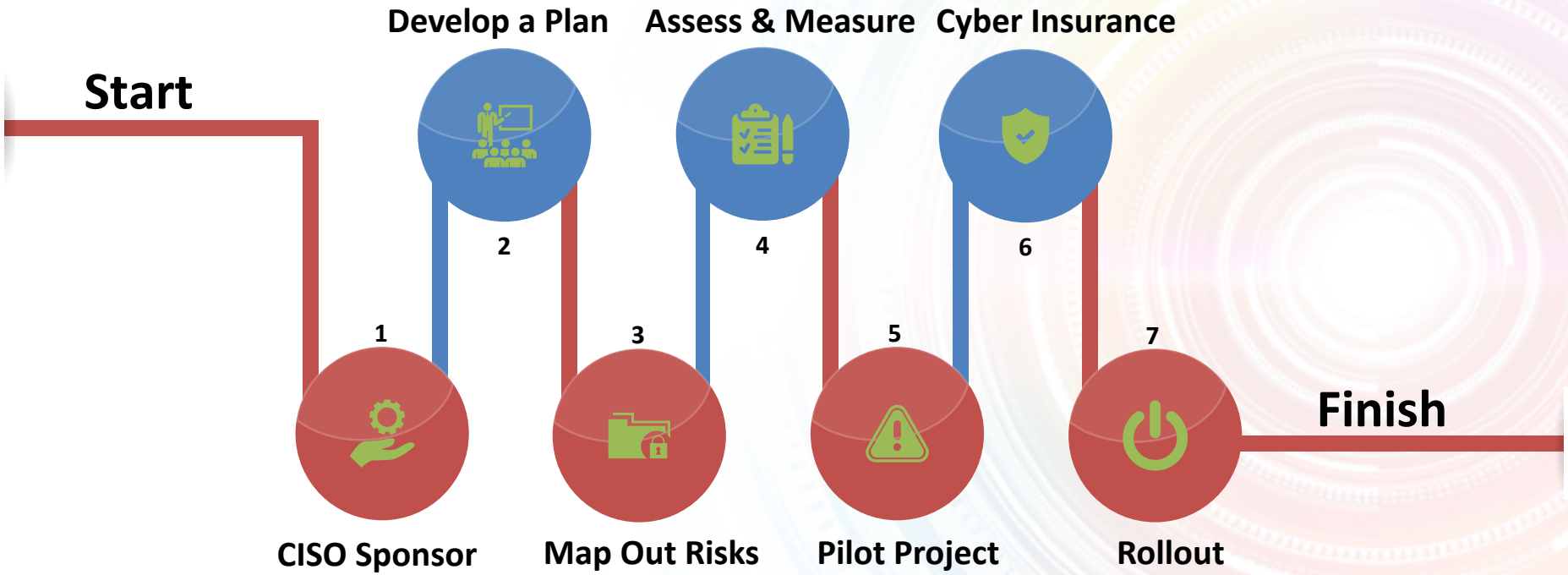


Segmenting traffic based on security and performance to go across different WAN links (MPLS, Internet, LTE)

www.128Technology.com

TechVision RESEARCH

ZTN Seven Step Plan



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

TechVision RESEARCH

Key Take-Aways

1) ZTN is a subset of an overall enterprise Zero Trust security strategy
2) 80% of breaches have an internal component driving enterprises to re-think their security strategy
3) 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.
4) It is more secure to define whitelists of access versus blacklists of denial
5) Integrating IAM directories with routing empowers enterprises to build zero trust networks, but this will require session stateful routing which some of the new software defined network solutions are providing.

TechVision RESEARCH

More from Sorell

Research

- UC Security Best Practices
- Inter-Networking vs. Inter-Connecting Your Clouds & Apps
- Master Naming Models

Workshops

- Zero Trust Network Security
- Contact Center Infrastructure
- Unified Communications

Events

- Featured Consulting Analyst at the TechVision Chrysalis Conference this November in San Diego, CA

TechVision RESEARCH

Questions?

TechVision RESEARCH