RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **ZT-R02**

“Connecting the Dots” of NIST 800-207, TIC 3.0, and More Using SAFE

Chad Mitchell – CCIE #44090

US Public Sector Security Architect
Cisco

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

20.4M

Less miles on their trucks

350,000

More packages

20,000

Metric tons less in CO2 emissions

Unrealized Potential, Efficiency, & Security

- Nothing about how UPS trucks or package load changed
- Change of process rather than technology or tool
- Increased Safety - 61% of crashes that occur while turning or crossing traffic involve left turns (3.1% right turns)

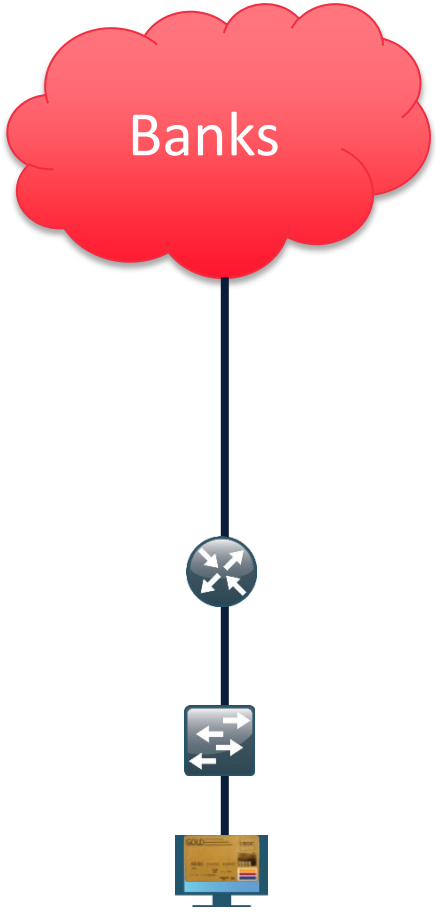
Session Agenda

- The Need for the SAFE Reference Architecture
- What is the SAFE Reference Architecture?
- How do we use the SAFE Reference Architecture? TIC 3.0, NIST 800-207, & CISA
- How can I **APPLY** the SAFE Reference Architecture in my environment?

RSAConference2022

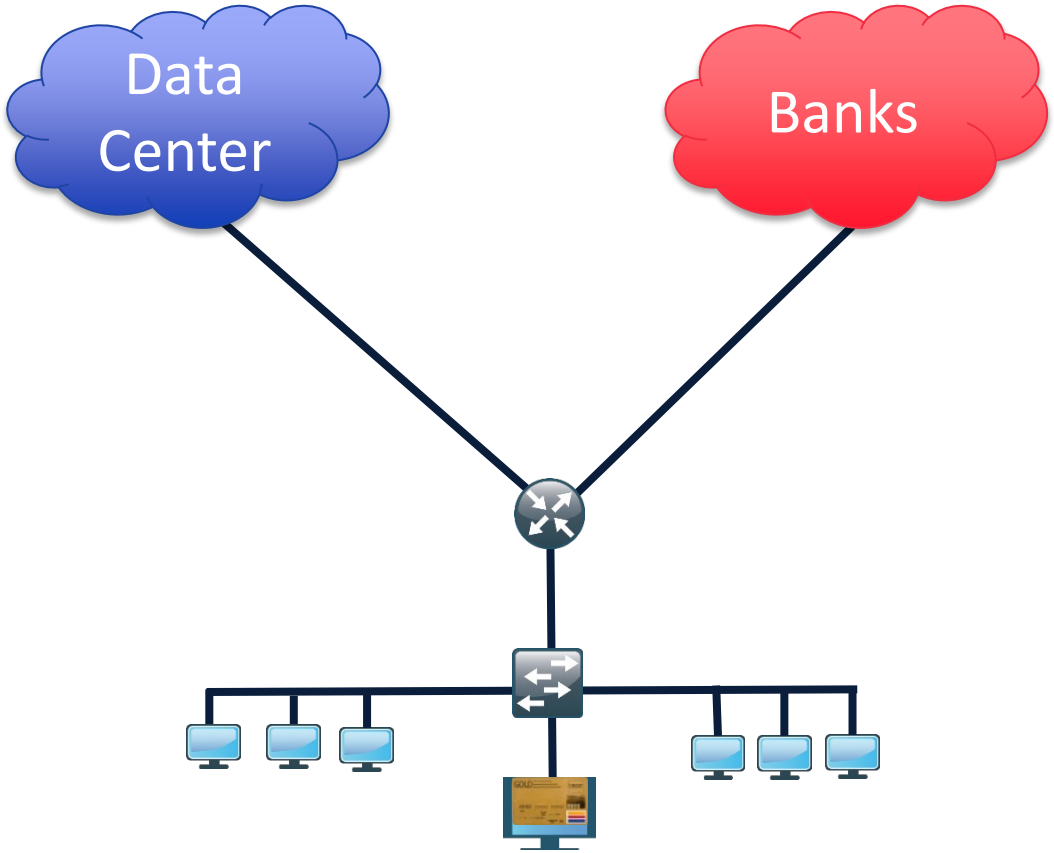
The Need for the SAFE Reference Architecture

The 80's Branch Networks



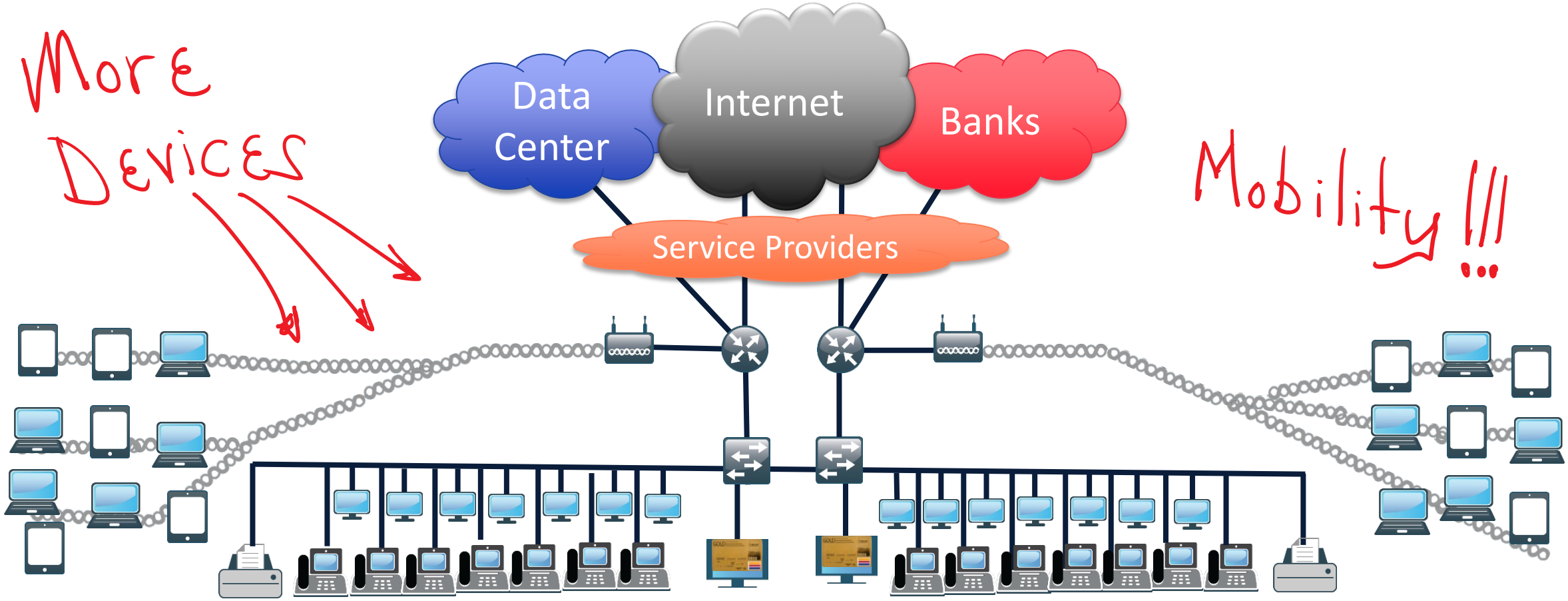
Way back
long time
Ago

Early 90's Branch Networks

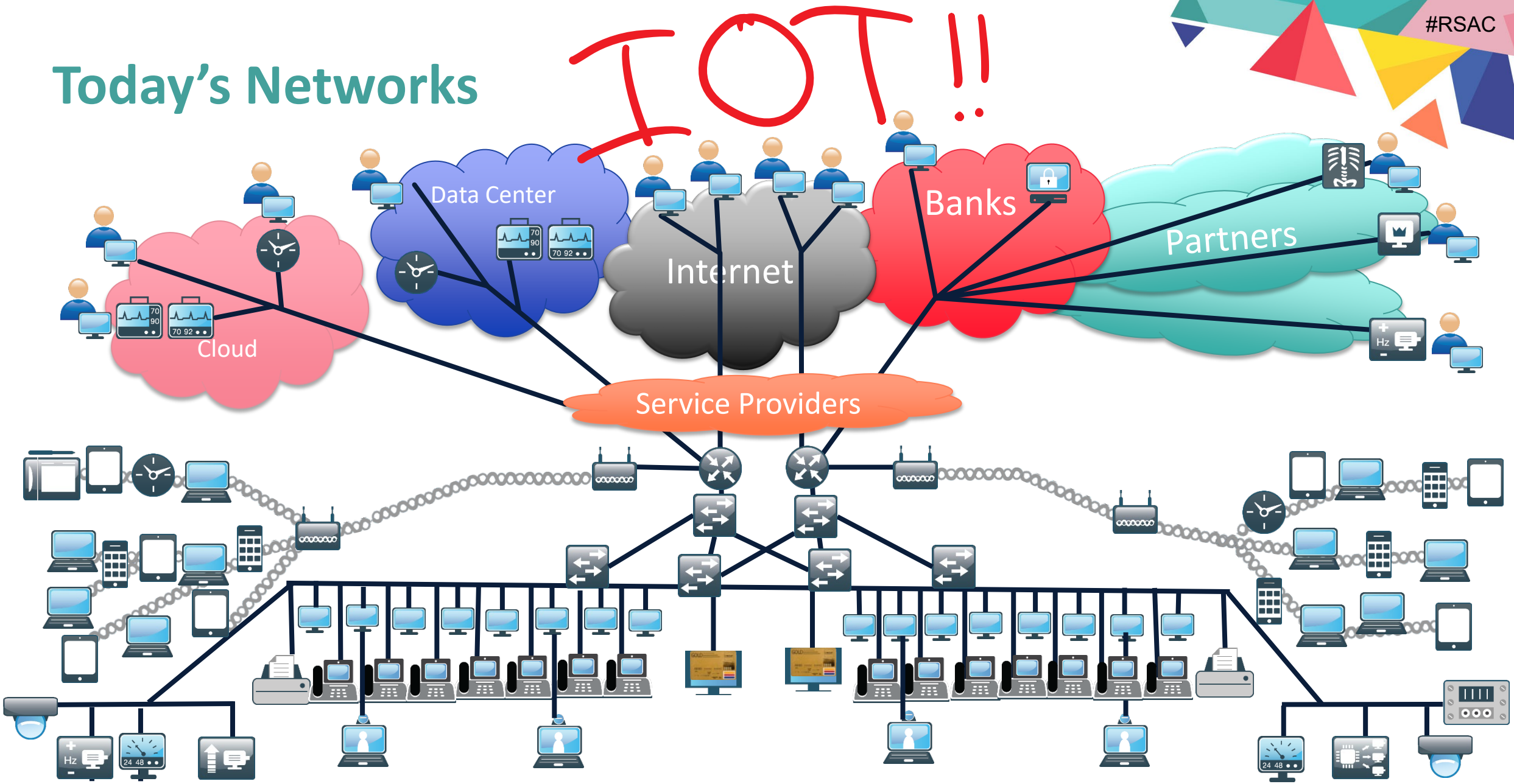


Simple Networks

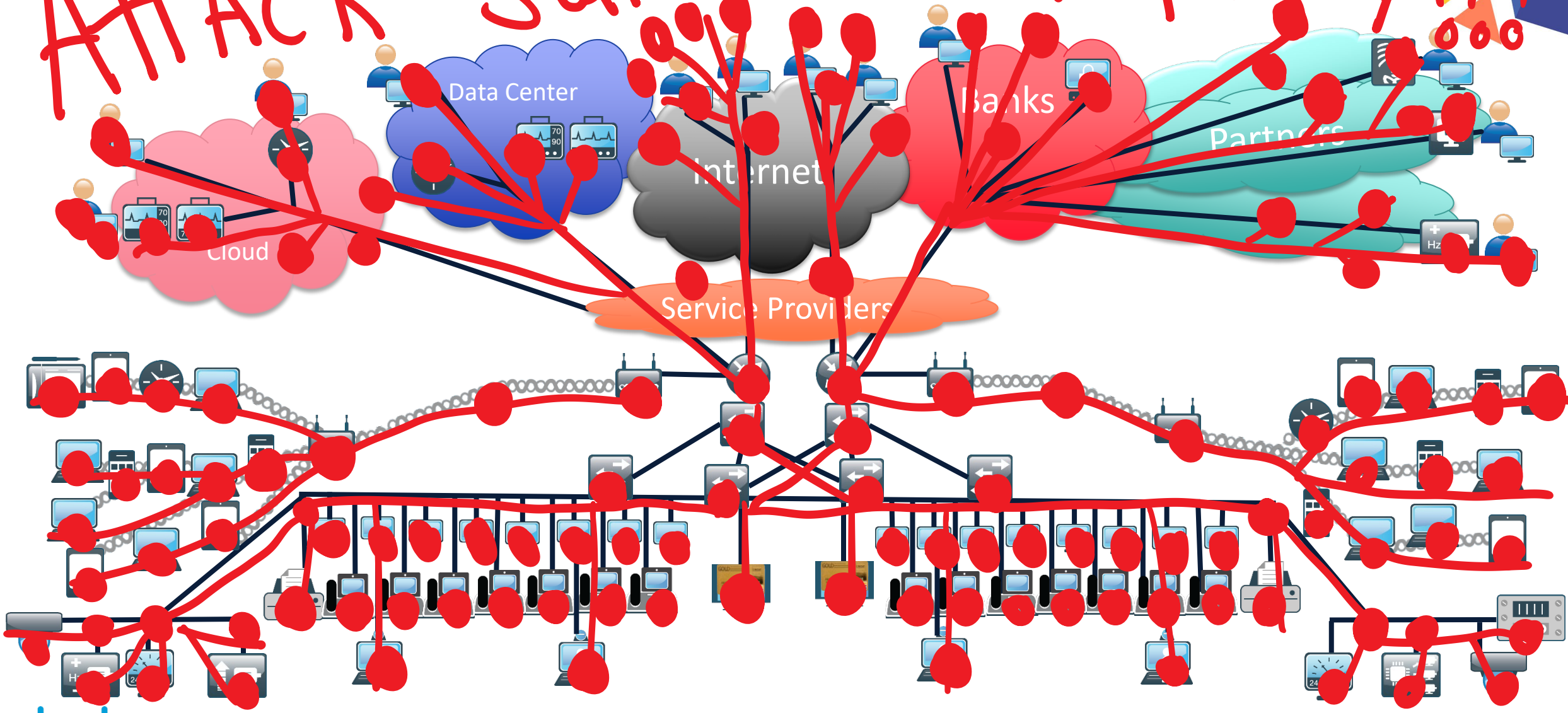
Early 2000's Networks



Today's Networks



Attack Surface of Today !!!



How did we get there?

SEKURITY

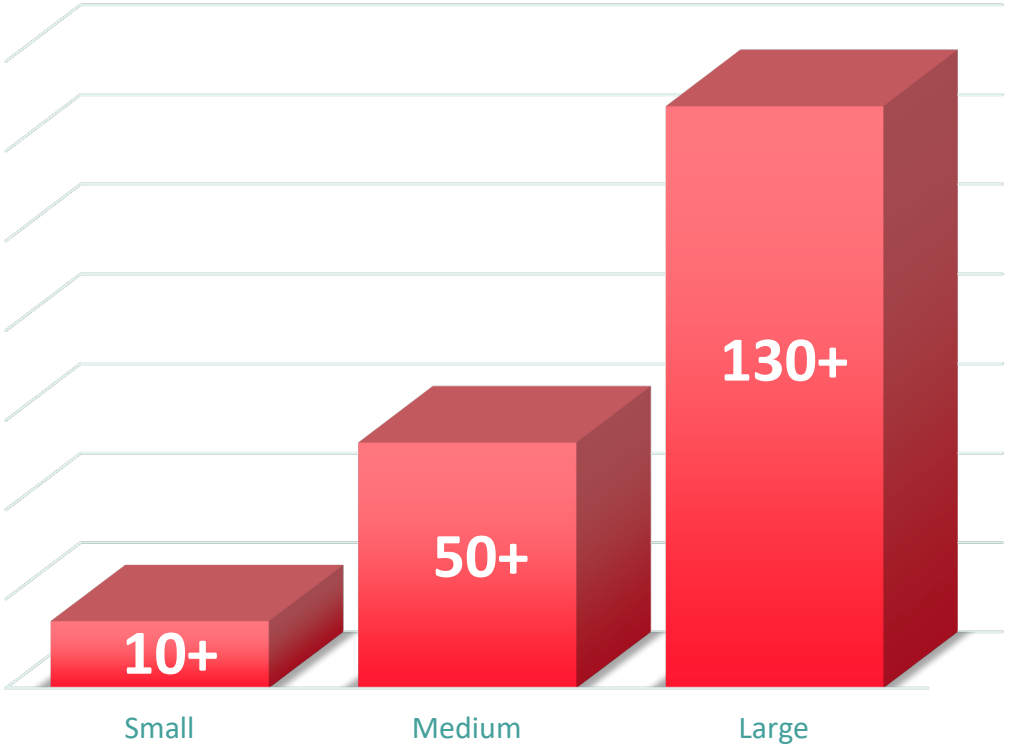
- No organization is exactly alike.
  - Operational Differences
  - Risk Profiles
  - Risk Tolerance
  - Governance / Executive Orders
- Hyper-focused on Prevention and not Reaction

Vendors sell solutions for a threat..

Not **ALL** of them

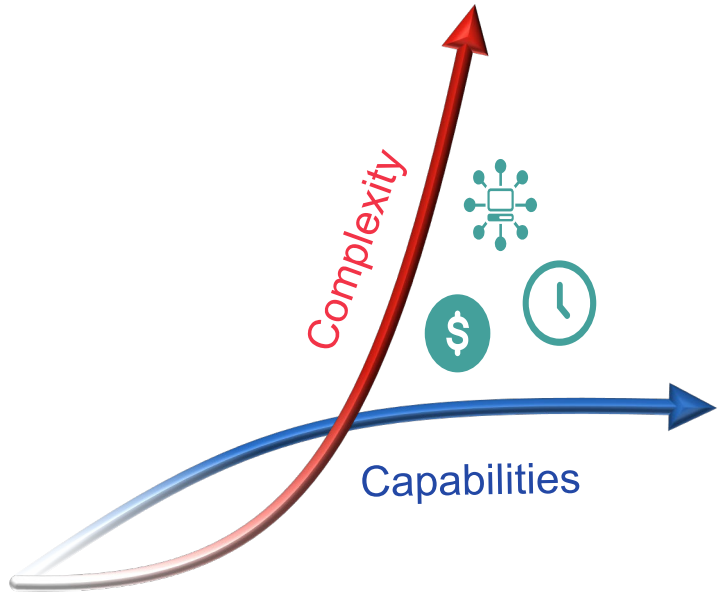
Too many tools!

Security Tools per Organization



=

Security Effectiveness Gap



Silos of Excellence

The tools work well on their own but……

- Narrow view of what's happening
- Input from other solutions is available but not commonly in same language or capability
- Duplicate efforts on same information
- Increase deployment and operational complexity

Mission: Integrated Architecture

ELIMINATE COMPLEXITY BY USING A MODEL AND METHOD BASED ON SECURITY BEST PRACTICE AND YOUR ENVIRONMENT

RSAConference2022

So… How do we get there?

Let’s take a high-level look at the SAFE Reference Architecture to get started

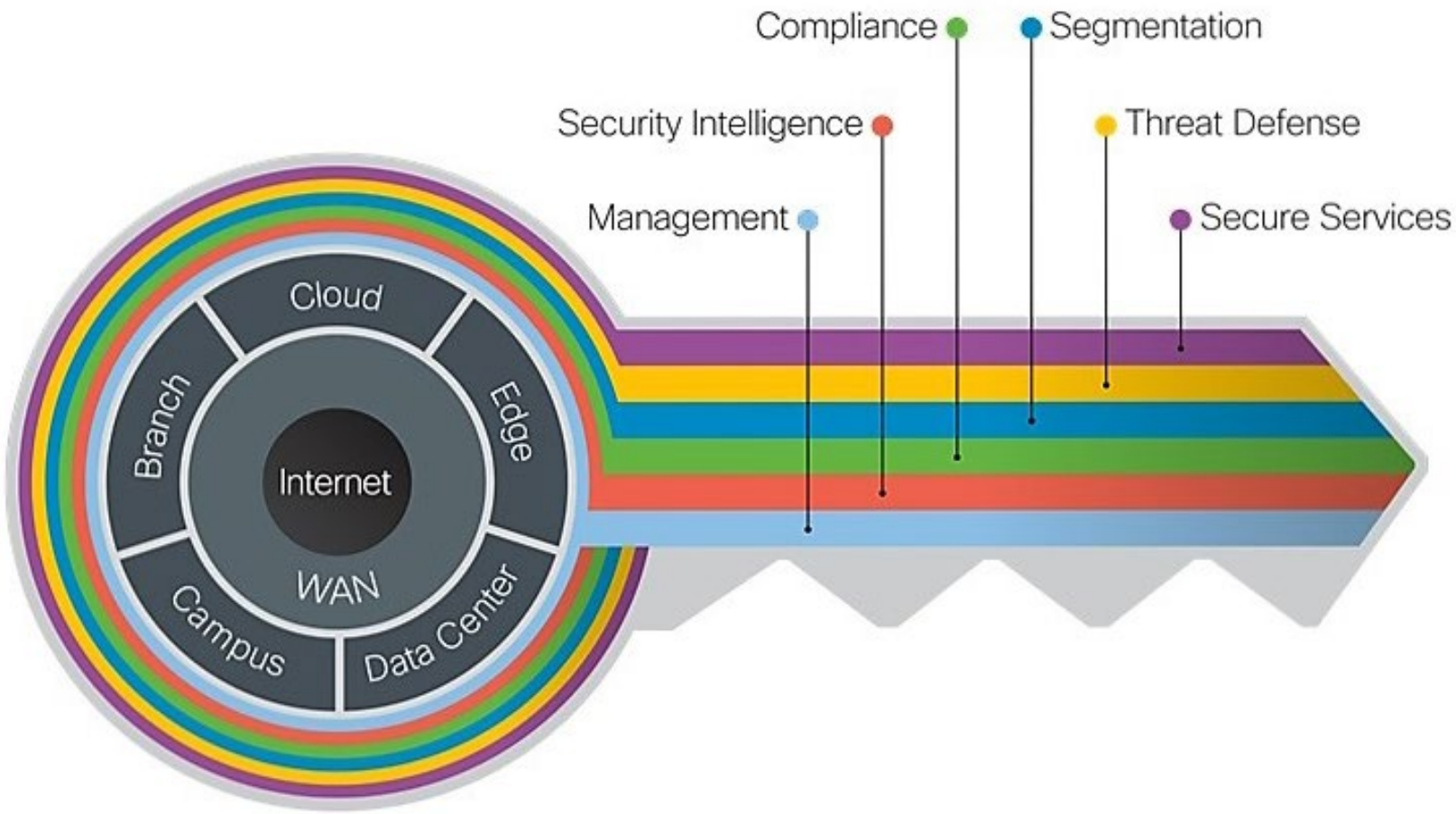
Proven Security with SAFE

A Security-Centric methodology and model for an effective Security Architecture

- Focuses on **Risks** and **Threats** by identifying required **Capabilities**
- **Architectural** guidance using **Capabilities**
- **Solution** guidance & best practice deployments tested in **Validated Designs**

The Key to SAFE

Domains



Places in the Network (PINs)

The 3 Phases of SAFE Reference Architecture

Capabilities for Threats

Architectures for Business

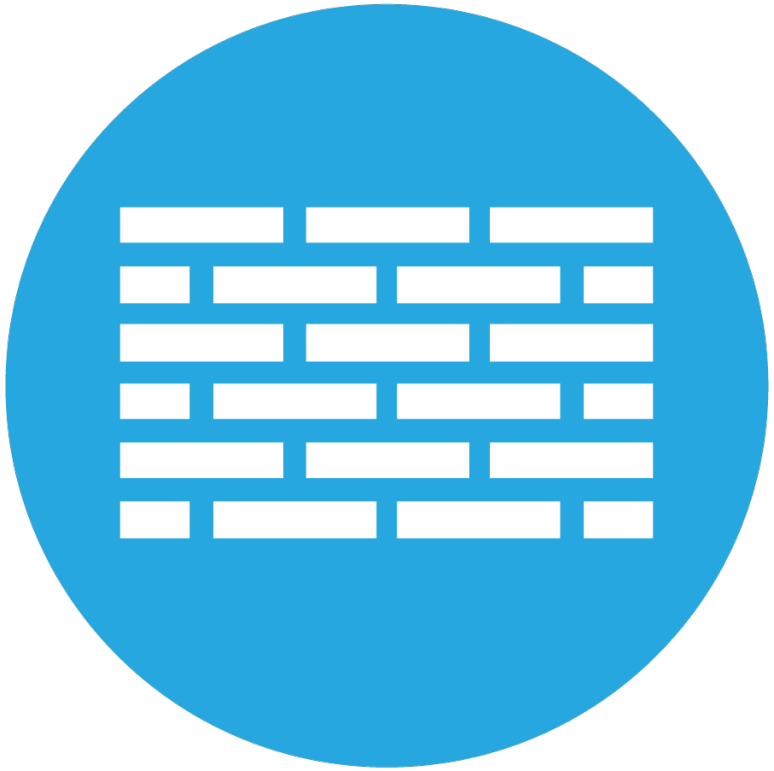
Designs for Security

The **business flows**
define the attack surface.

&

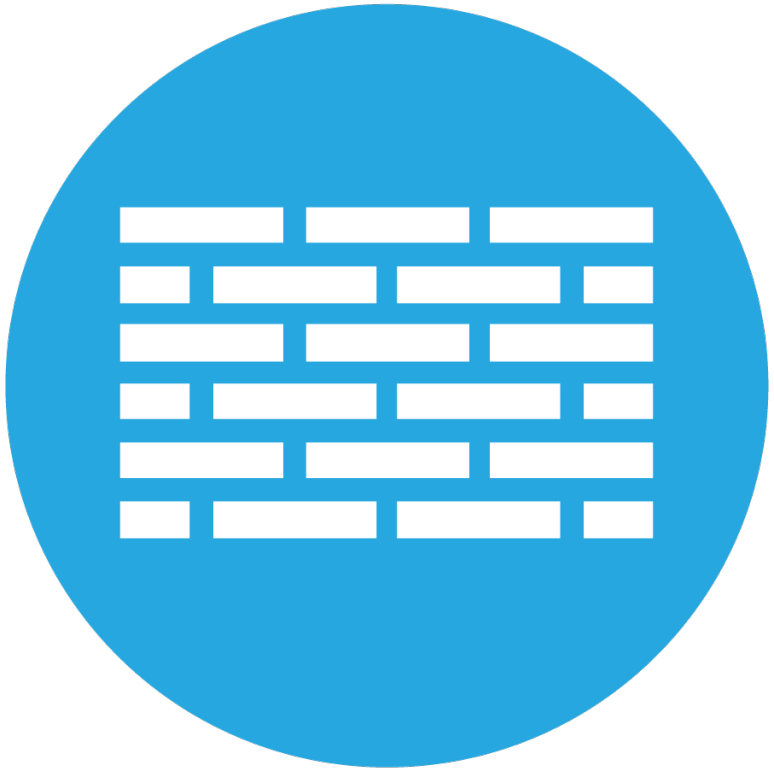
Capabilities
secure the attack surface.

Capability



Function rather than Product

I need a firewall **Capability** to **Segment** my network



Capabilities : The Security Alphabet

Firewall

Flow Analytics

Identity

Intrusion Prevention

DNS Security

Analysis/ Correlation

Anomaly Detection

Anti-Malware

Anti-Virus

Application Visibility Control (AVC)

CASB

Client-Based Security

Cloud Security

Disk Encryption

Distributed Denial of Service Protection

Vulnerability Management

Email Security

Web Security

Web Application Firewall

Web Reputation/ Filtering/DCS

Wireless Intrusion Prevention (WIPS)

Logging/ Reporting

Malware Sandbox

Mobile Device Management

Monitoring

Network Anti-Malware

Name Resolution

Policy/ Configuration

Posture Assessment

Server-Based Security

Tagging

Threat Intelligence

Time Synchronization

TLS Offload

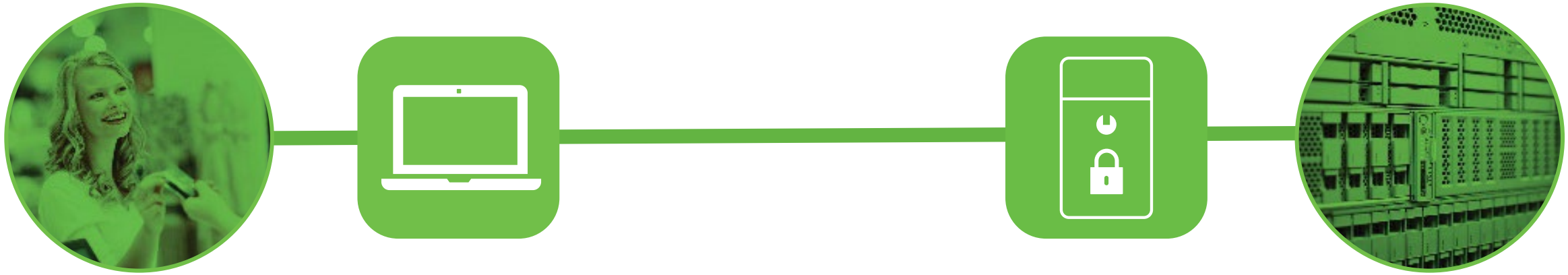
Virtual Private Network (VPN)

RSAConference2022

Understanding Business Flows

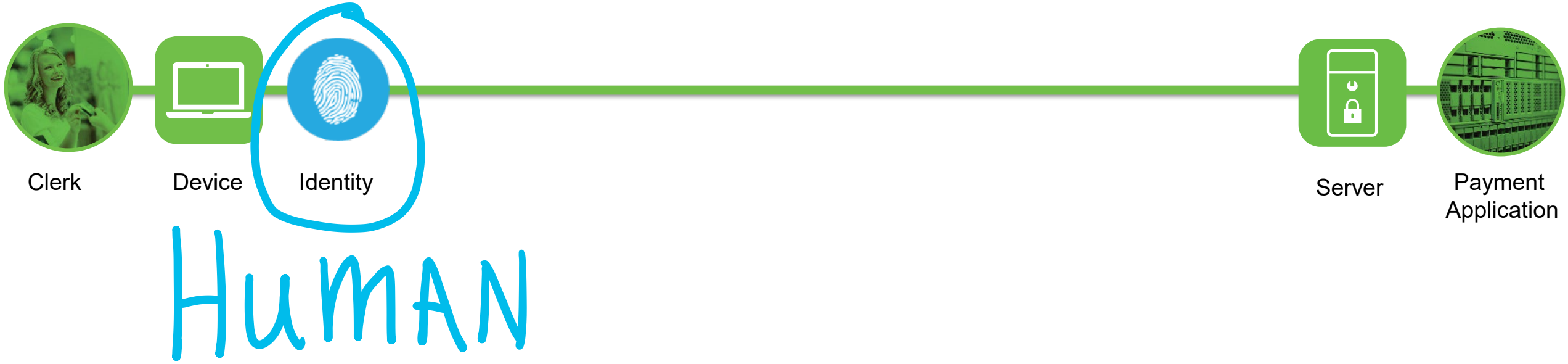
HUMAN | DEVICE | NETWORK | APPLICATION

Clerk Processing Credit Card

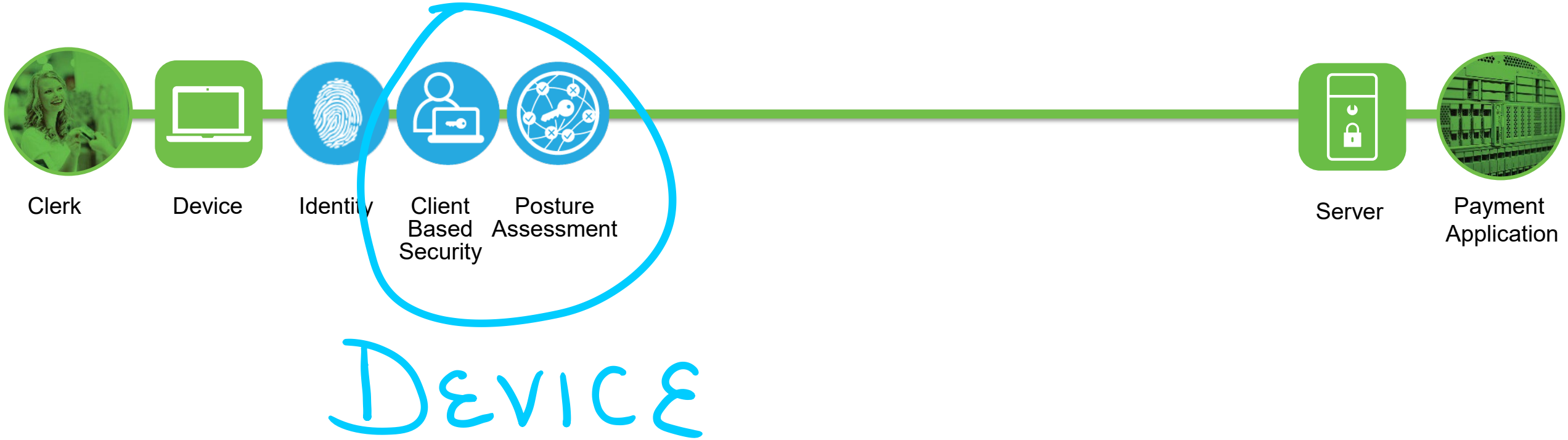


Business Flow for Payment Applications

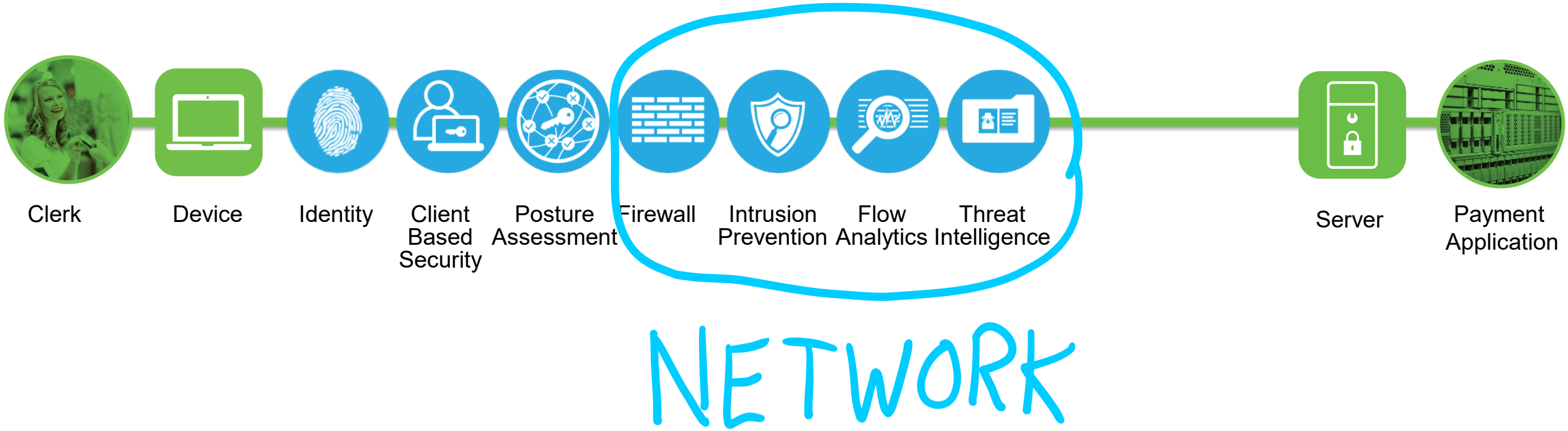
Secure the flow using Capabilities



Secure the flow using Capabilities



Secure the flow using Capabilities



Secure the flow using Capabilities

Example Business Flows

Secure web access for employees: Employee researching product information

Employee | Client-Based Security | Identity | Posture Assessment | Firewall | Intrusion Prevention | Flow Analytics | Threat Intelligence | Anti-Malware | Tagging | Application Visibility Control | Web Security | Website

Secure applications for PCI: Customer making purchase

Customer | Identity | Firewall | Intrusion Prevention | Flow Analytics | Threat Intelligence | Anti-Malware | Tagging | Distributed Denial of Service Protection | Application Visibility Control | Web Application Firewall | Server-Based Security | E-commerce

Architectures for Business

Designs for Security

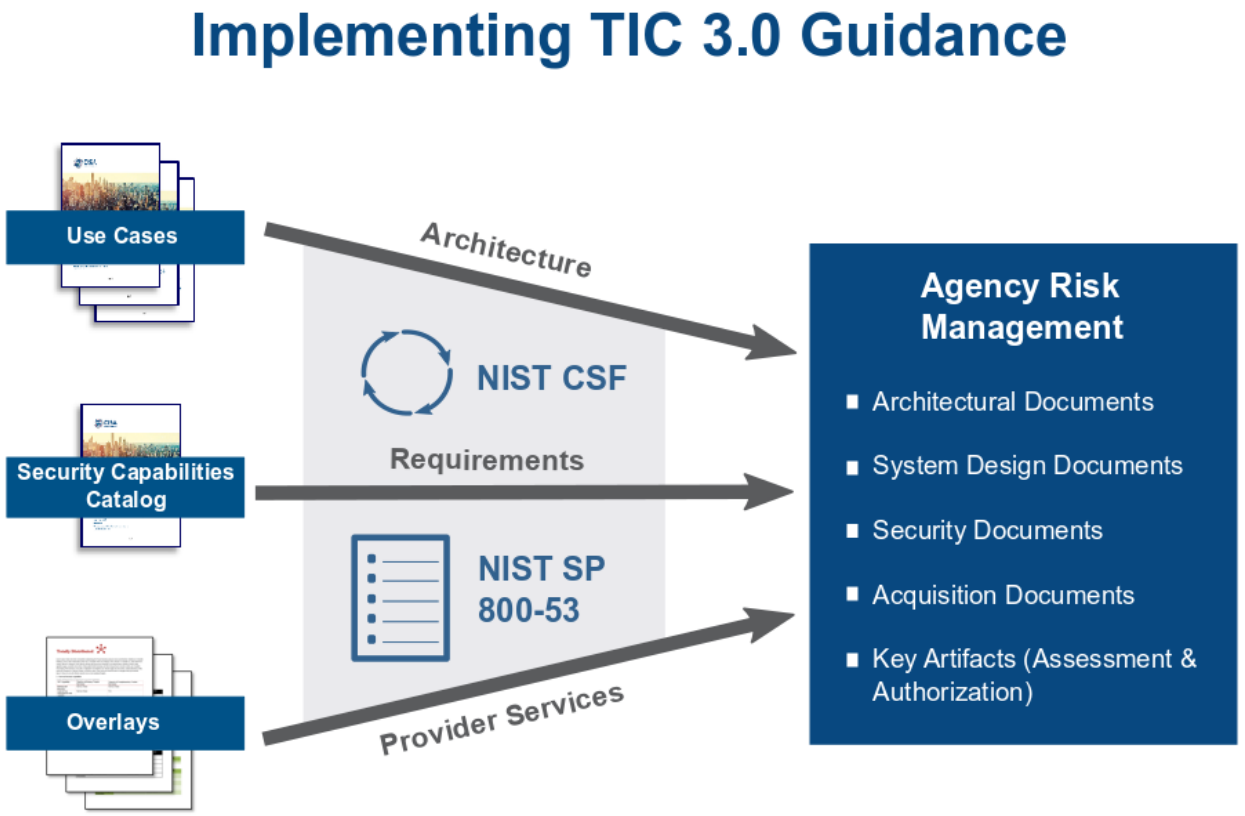
For more information on the next phases from what we have covered go here:
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf

RSAConference2022

SAFE Capabilities Flow for Trusted Internet Connections 3.0 (TIC 3.0)

What is TIC 3.0?

- Modern .gov IT environments and security **requirements vary based on each agency's mission, needs, and resources**.
- **TIC 3.0 guidance adopts a broader and less prescriptive tone** compared to earlier iterations to accommodate this wide variety of environments.



https://www.cisa.gov/tic-faq

“Agencies need to understand the flows that come out from the systems, where they are going and different users who will be using it, not just federal employees, but the public, system to system and hybrid or multi cloud”

Sean Connelly – DHS

Source: https://federalnewsnetwork-com.cdn.ampproject.org/c/s/federalnewsnetwork.com/ask-the-cio/2020/04/path-for-agencies-to-more-easily-use-cloud-services-paved-by-tic-pilots/amp/

CISA – Policy Enforcement Points w/ Segmentation and Trust Zones

Figure 8: Example Trust Zone Gradient

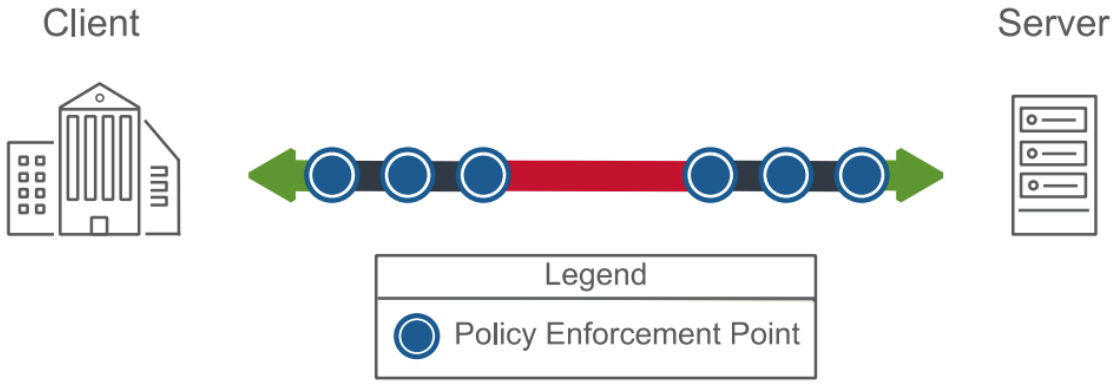


Figure 3: PEP Protections Affect Trust

Reference: CISA – TIC Core Guidance Volume 2: Reference Architecture
https://www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%202%20Reference%20Architecture.pdf

TIC 3.0 Universal Capabilities

- 18 Universal Capabilities that are broadly applicable
  - (should exist in all deployed solutions)

Secure Administration

Auditing & Accounting

Least Privilege

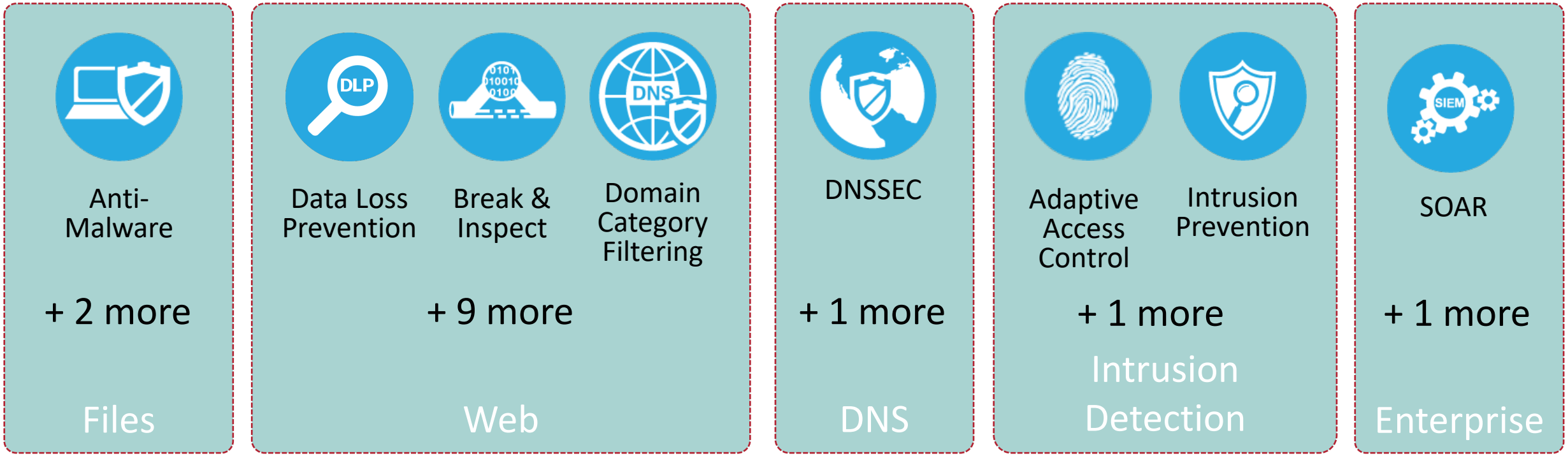
Configuration Management

Effective Use of Shared Services

Reference: https://www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%203%20Security%20Capabilities%20Catalog.pdf

TIC 3.0 Traditional TIC Capabilities

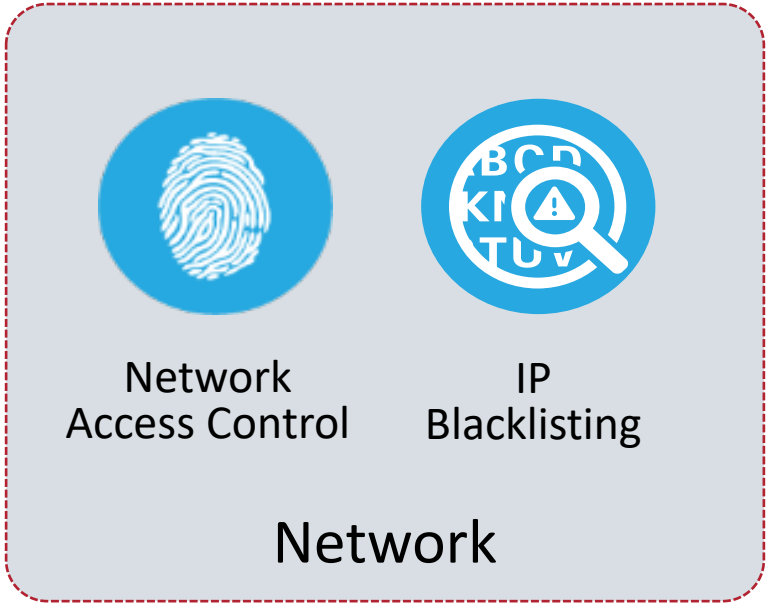
- Establishes 5 TIC Capability Groups with capabilities per group



Reference: CISA – TIC 3.0 Traditional TIC Use Case
https://www.cisa.gov/sites/default/files/publications/Draft%20TIC%203.0%20Traditional%20TIC%20Use%20Case.pdf

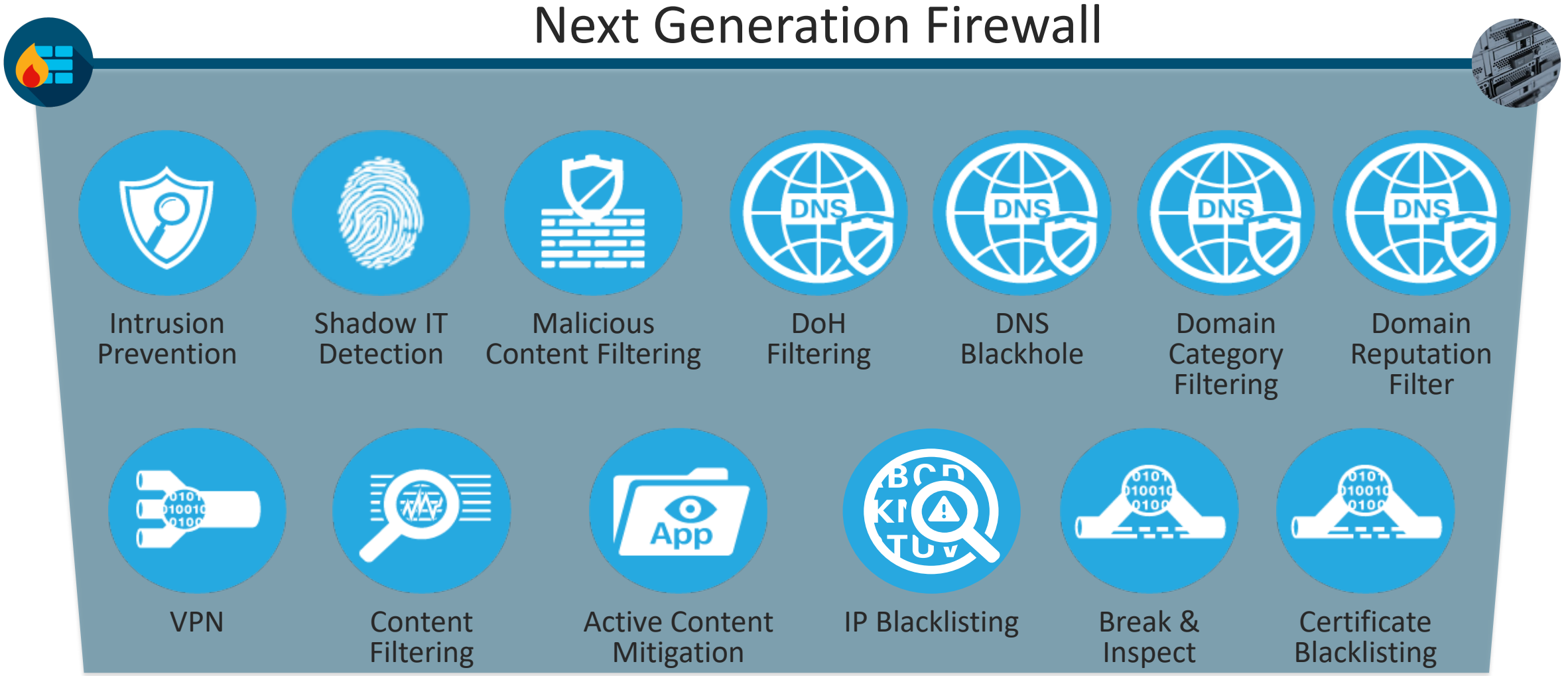
TIC 3.0 Branch Capabilities

- The Branch Use Case adds an additional group of Network
- It also removes some traditional TIC capabilities from other groups



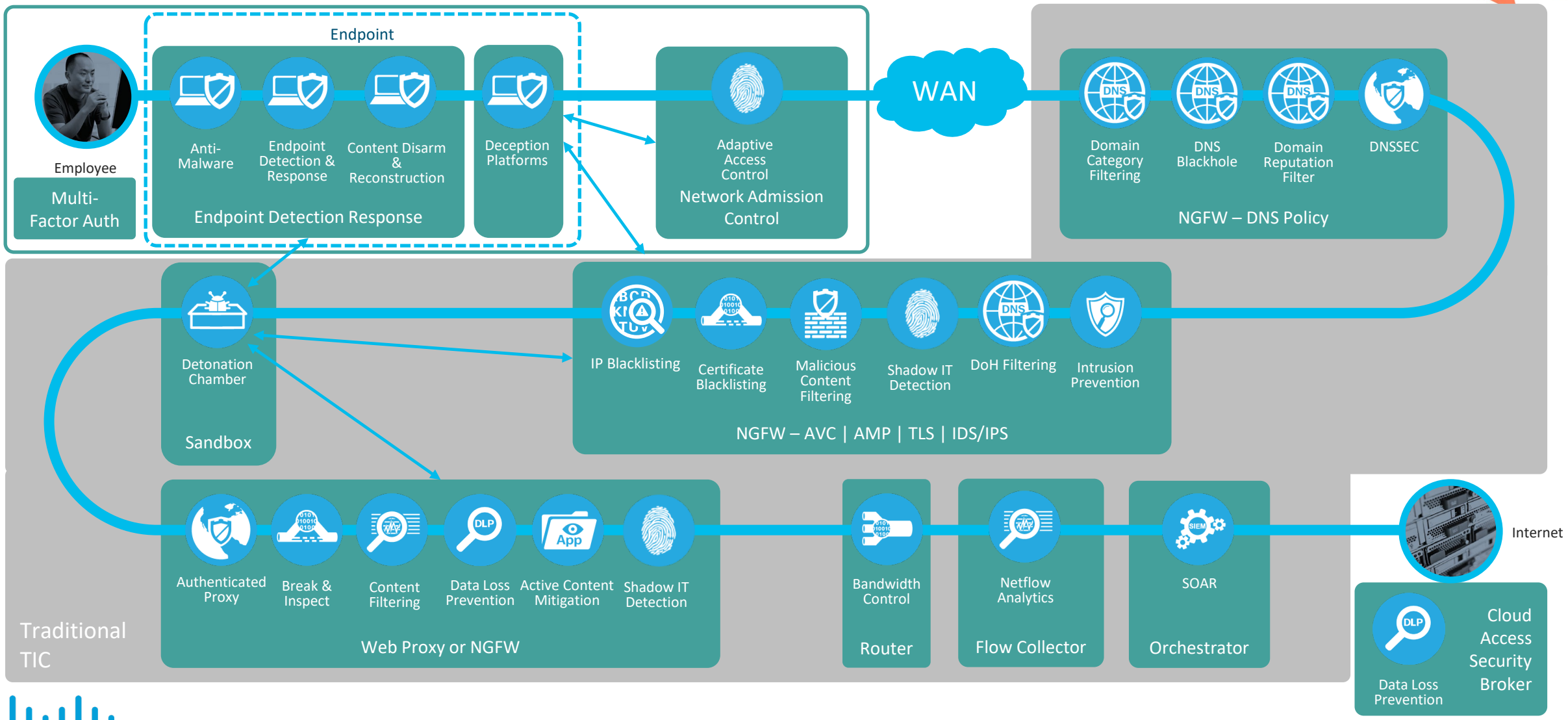
Reference: CISA – TIC 3.0 Branch Office Use Case
https://www.cisa.gov/sites/default/files/publications/Draft%20TIC%203.0%20Branch%20Office%20Use%20Case.pdf

Example Product to Capabilities Mapping



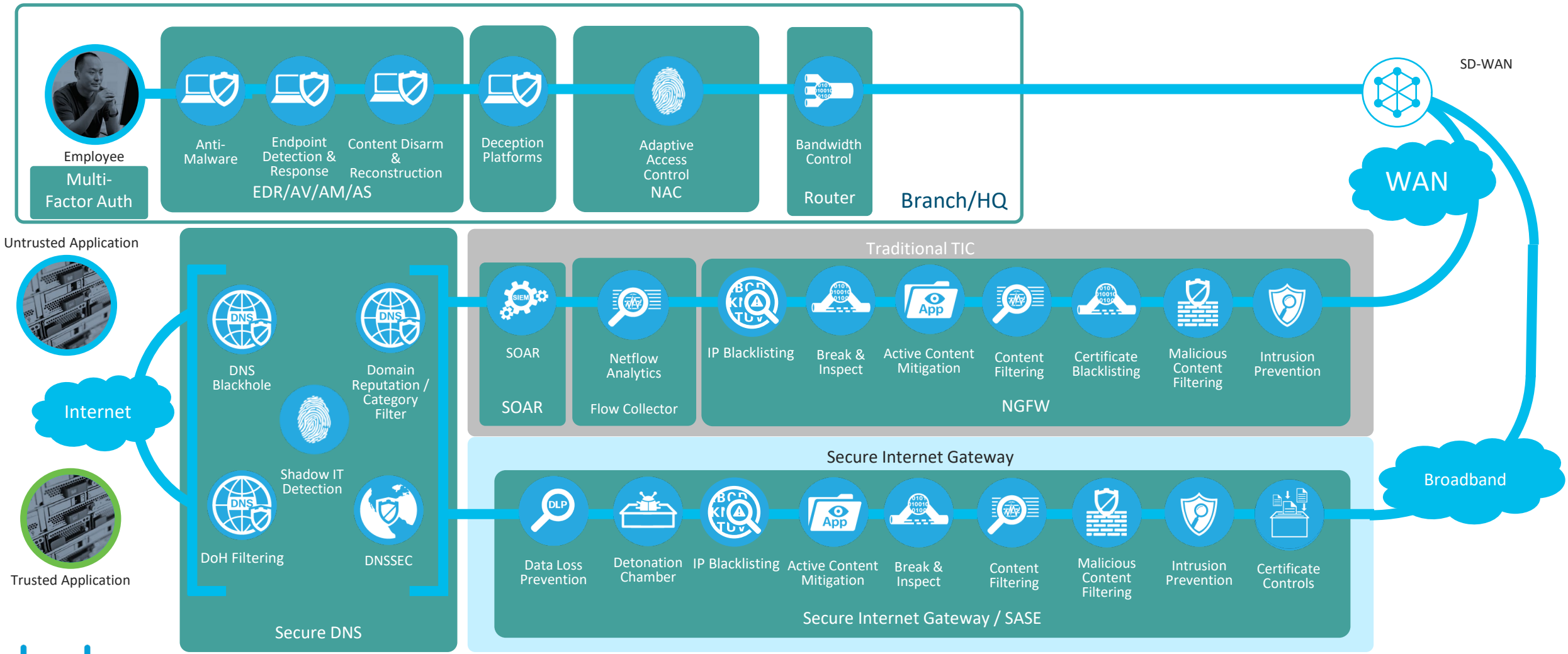
Example 1 – Traditional TIC (non-DIA)

Agency to TIC to Internet



Example 2 – Branch with DIA to External App

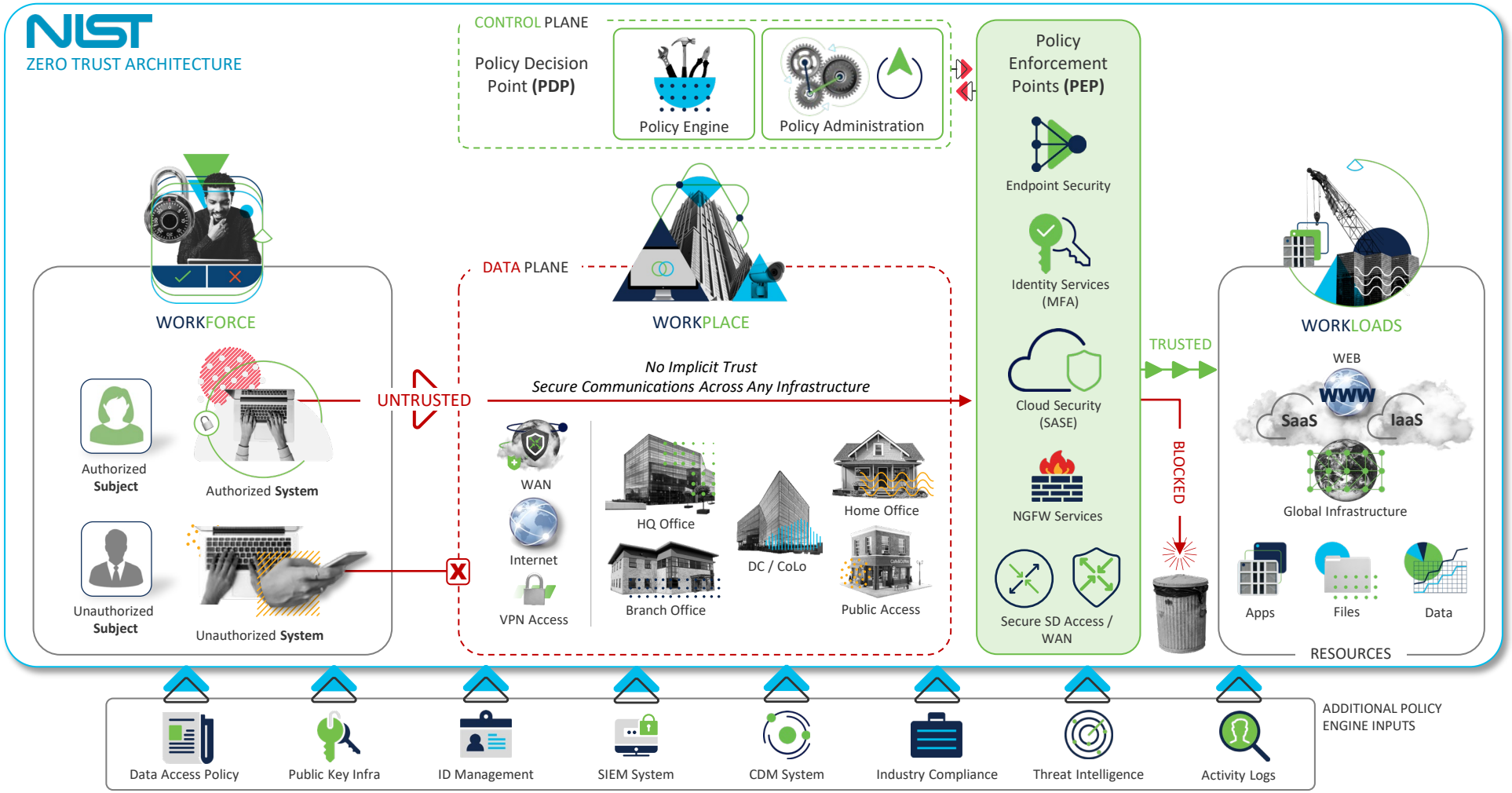
Branch Office to Sanctioned CSP Overlay Services



RSAConference2022

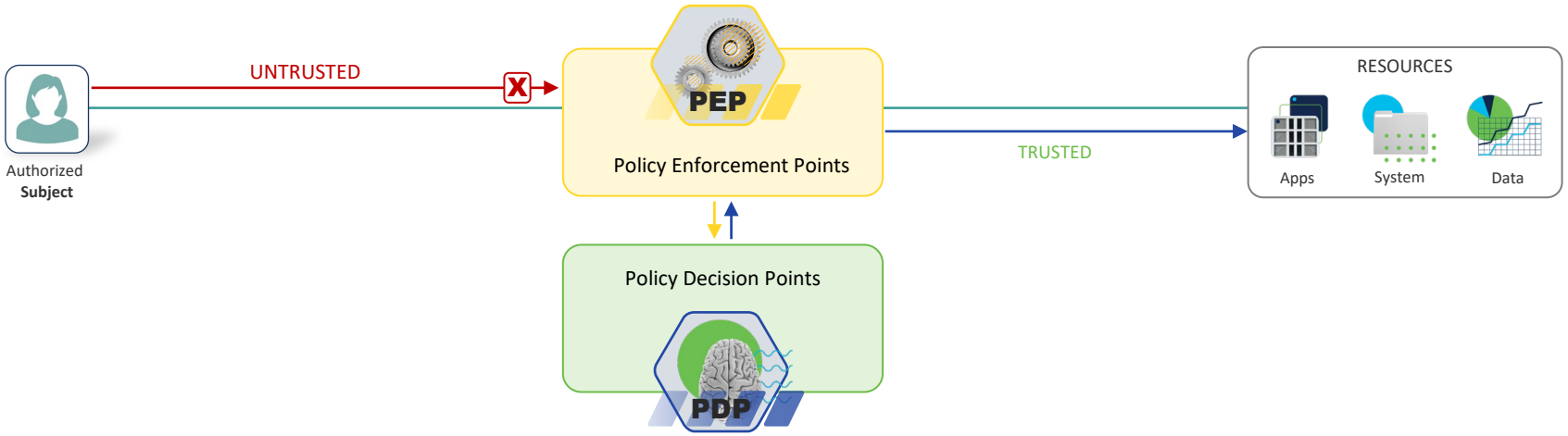
Applying SAFE Methodology to NIST 800-207 – Zero Trust & CISA Zero Trust Maturity Model

NIST 800-207 Basics – Logical Components



NIST 800-207 – Key Understanding

- ENFORCEMENT IS NOT REQUIRED TO EXIST ALL IN ONE PLACE!
- ENFORCEMENT CAN BE DONE ANYWHERE BETWEEN THE SUBJECT AND THE RESOURCE



Security Solution Domain Alignment

5 Pillars of Zero Trust

IDENTITY | DEVICES | NETWORK | APPLICATIONS | DATA

Security Capability Alignment

ZERO TRUST

USER & ENDPOINT PROTECTION

- MULTI-FACTOR AUTHENTICATION
- ENDPOINT DETECTION & RESPONSE
- VULNERABILITY MANAGEMENT
- MOBILE DEVICE MANAGEMENT

NETWORK SECURITY

- NETWORK ACCESS CONTROL
- NEXT-GEN FIREWALL / IPS
- SD-WAN / SASE
- SEGMENTATION

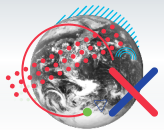
CLOUD EDGE

- SECURE INTERNET GATEWAY / SASE
- CLOUD APPLICATION SECURITY BROKER (CASB)
- CLOUD DETECTION & RESPONSE
- NEXT-GEN FIREWALL / IPS

APPLICATION SECURITY

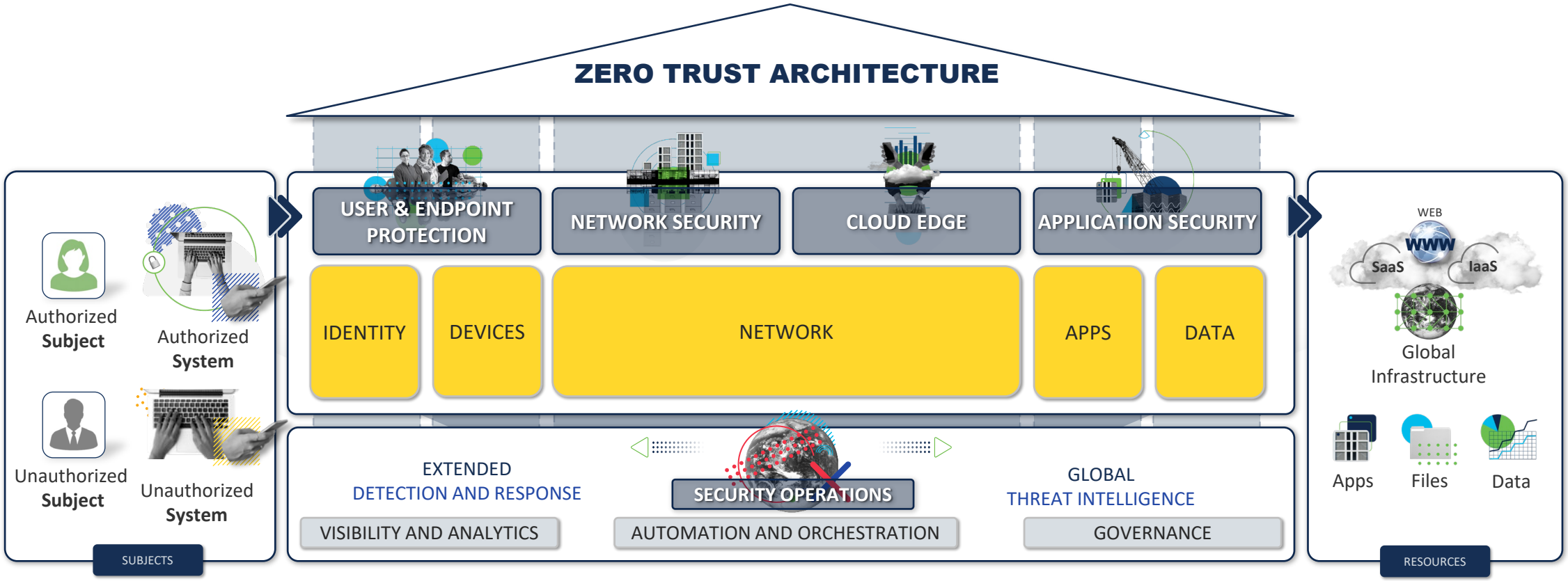
- APPLICATION & API SECURITY
- WORKLOAD PROTECTION / MICRO-SEGMENTATION
- CLOUD MALWARE DETECTION
- DATA LOST PREVENTION (DLP)

EXTENDED DETECTION AND RESPONSE

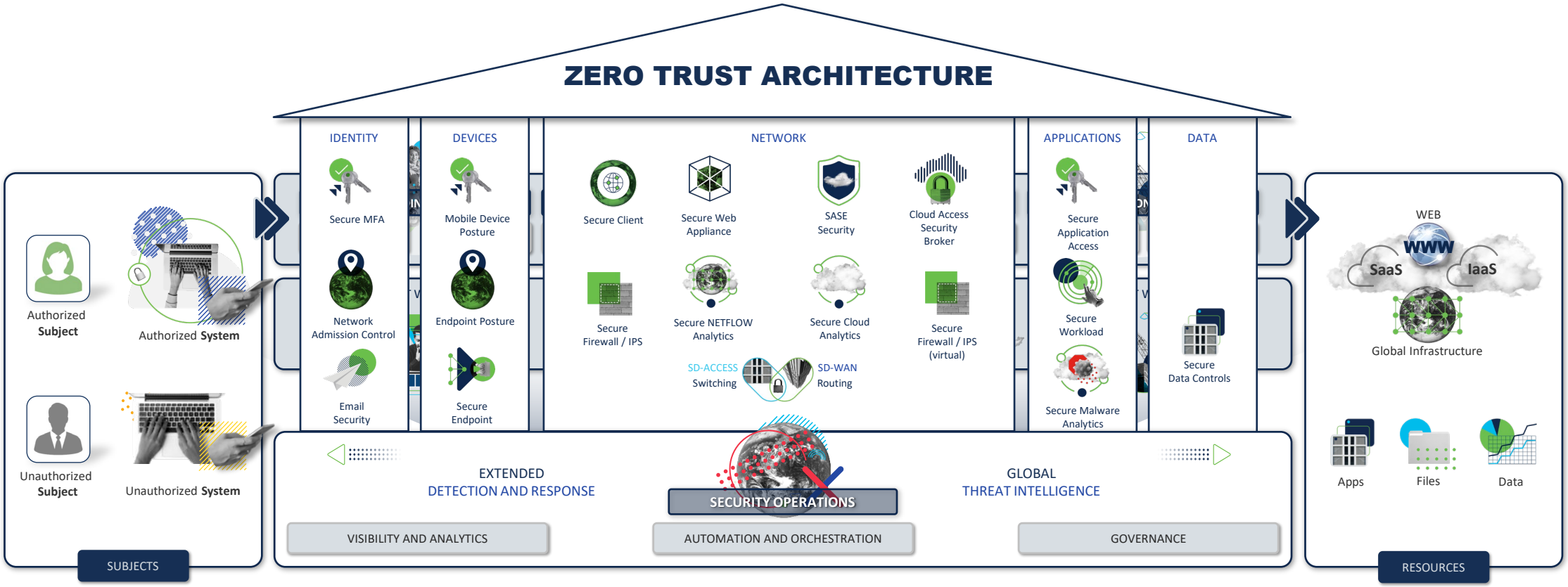


GLOBAL THREAT INTELLIGENCE

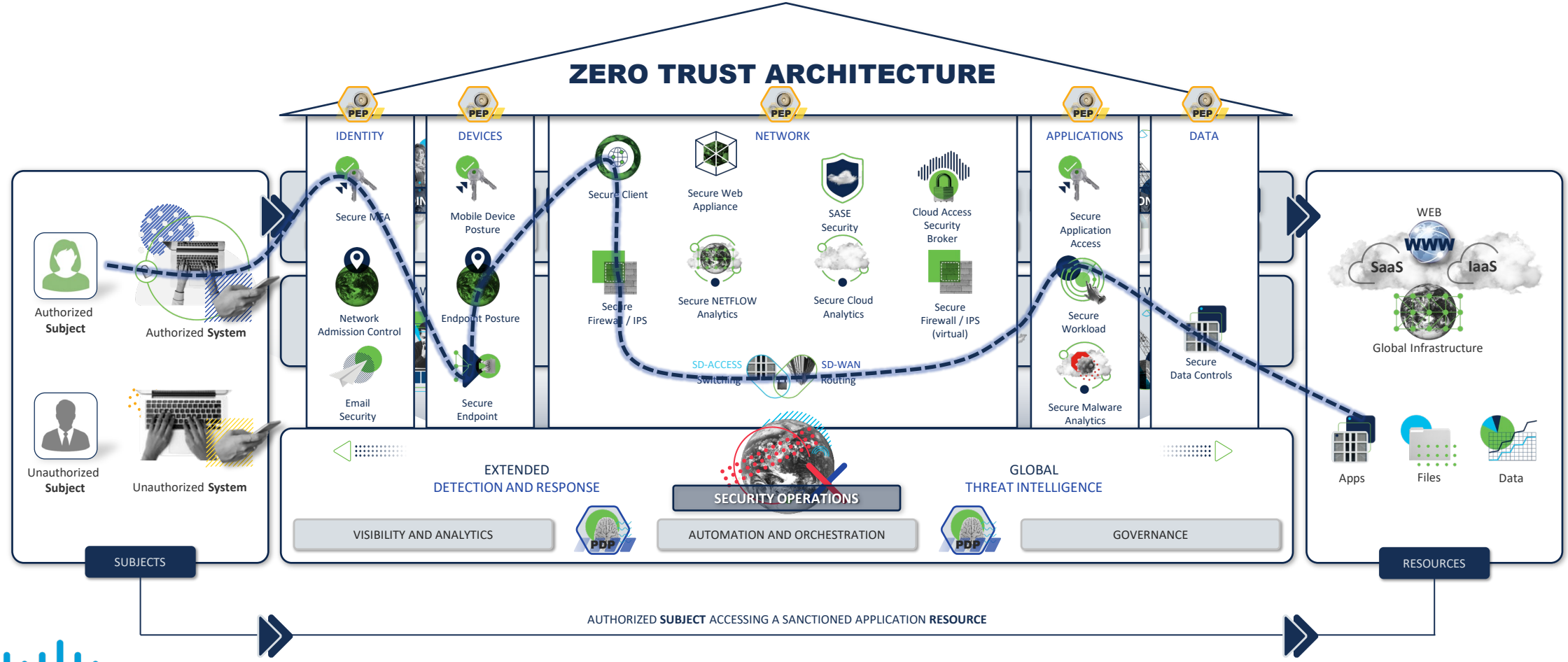
Building the flow based on 800-207 & CISA



Solution Alignment



Solution Alignment



CISA Zero Trust Maturity Model

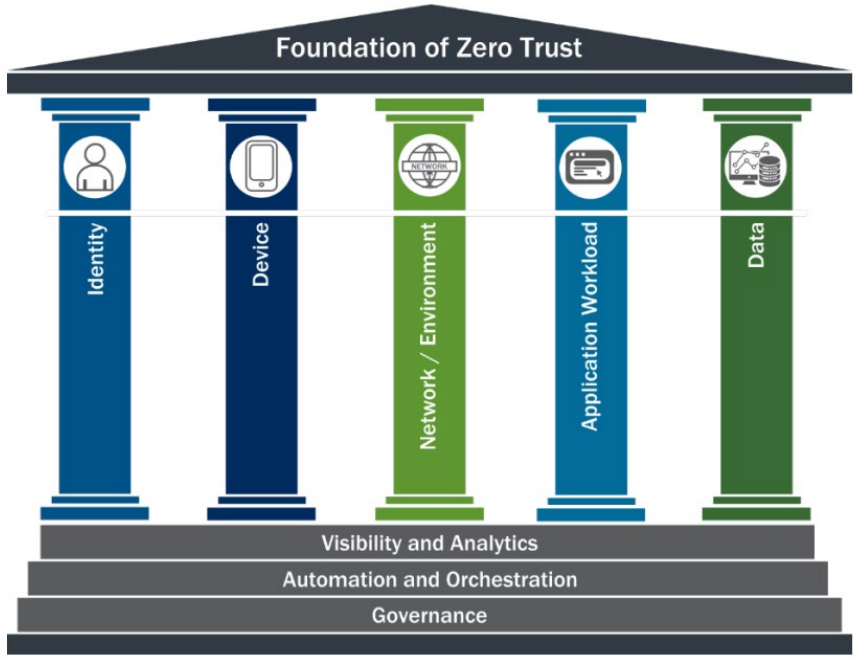


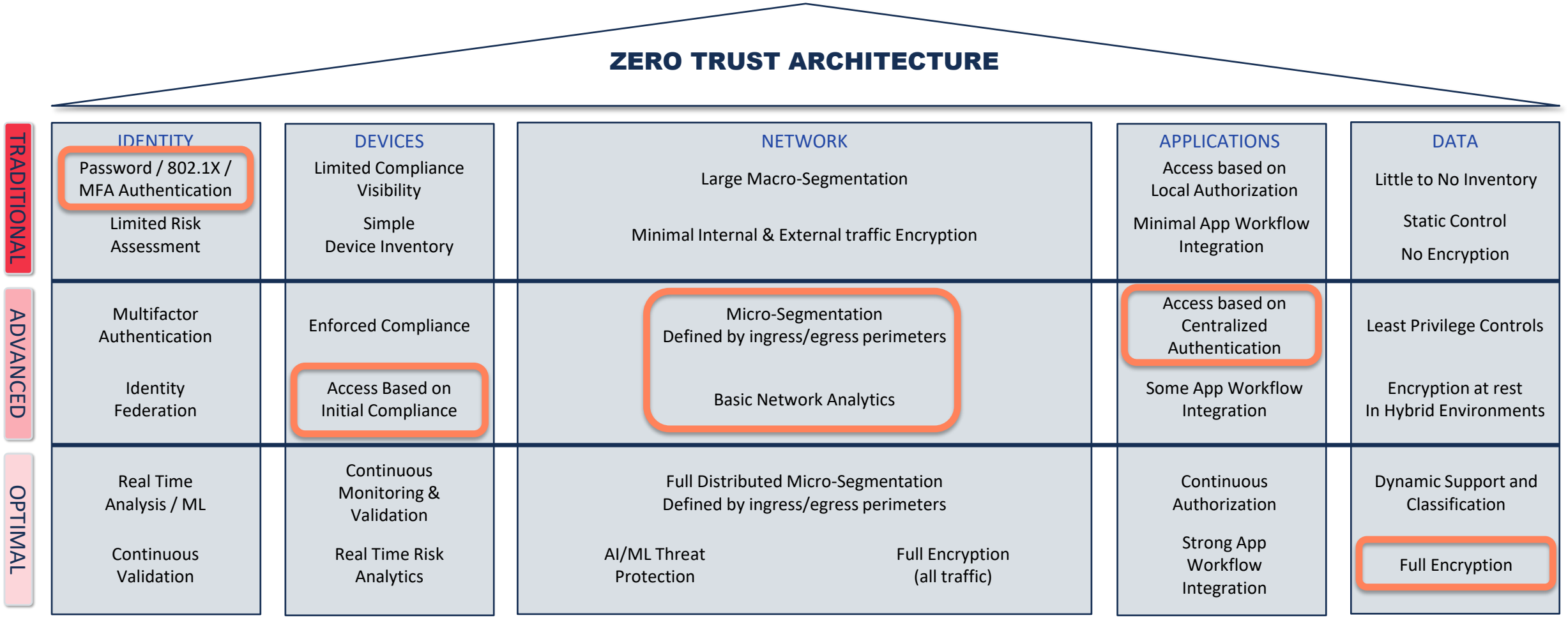
Figure 1: Foundation of Zero Trust[7]

	Identity	Device	Network / Environment	Application Workload	Data
Traditional	• Password or multifactor authentication (MFA) • Limited risk assessment	• Limited visibility into compliance • Simple inventory	• Large macro-segmentation • Minimal internal or external traffic encryption	• Access based on local authorization • Minimal integration with workflow • Some cloud accessibility	• Not well inventoried • Static control • Unencrypted
	Visibility and Analytics	*Automation and Orchestration*	*Governance*		
Advanced	• MFA • Some identity federation with cloud and on-premises systems	• Compliance enforcement employed • Data access depends on device posture on first access	• Defined by ingress/egress micro-perimeters • Basic analytics	• Access based on centralized authentication • Basic integration into application workflow	• Least privilege controls • Data stored in cloud or remote environments are encrypted at rest
	Visibility and Analytics	*Automation and Orchestration*	*Governance*		
Optimal	• Continuous validation • Real time machine learning analysis	• Constant device security monitor and validation • Data access depends on real-time risk analytics	• Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted	• Access is authorized continuously • Strong integration into application workflow	• Dynamic support • All data is encrypted
	Visibility and Analytics	*Automation and Orchestration*	*Governance*		

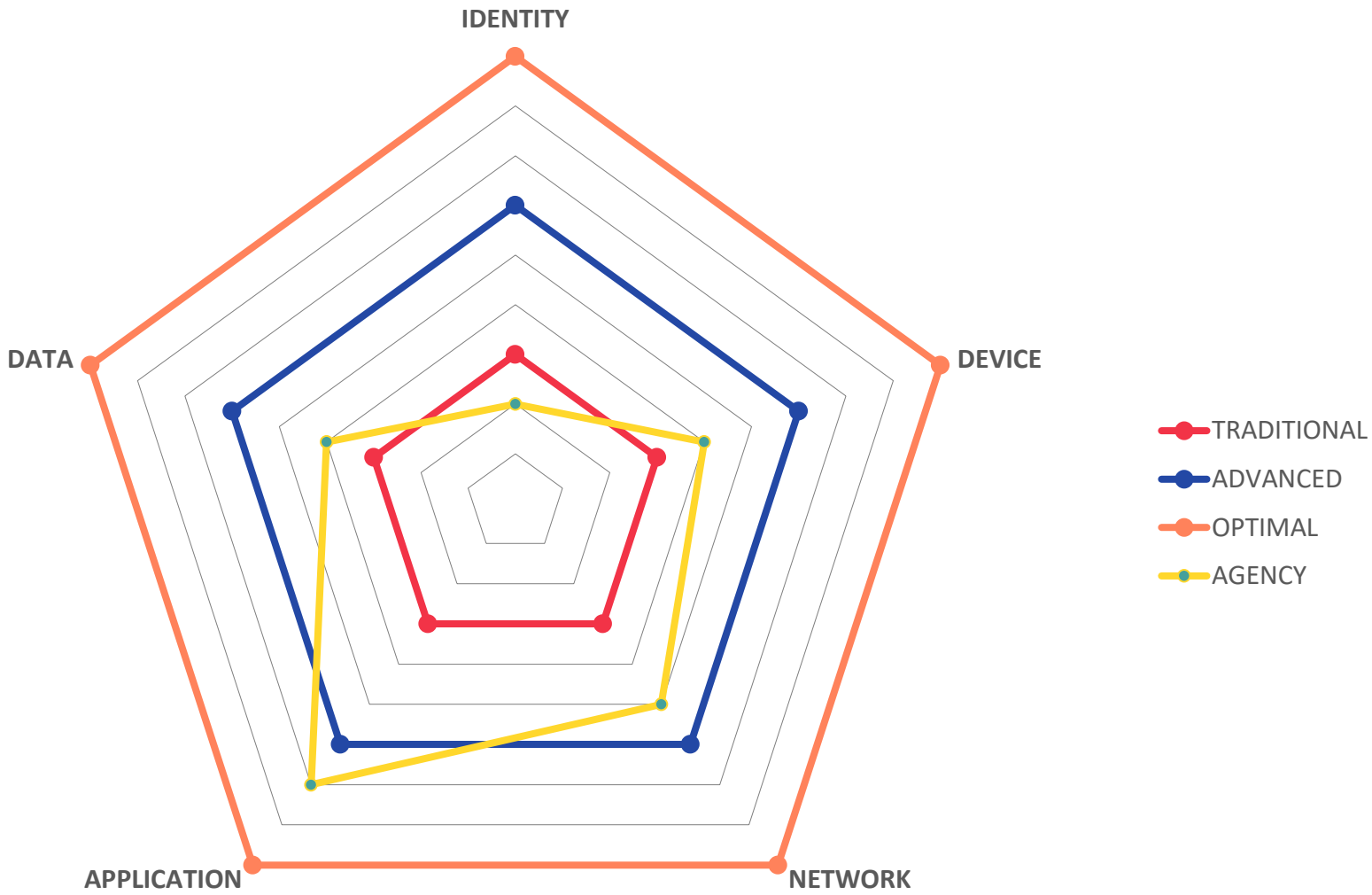
Figure 2: High-Level Zero Trust Maturity Model

https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

CISA Maturity Model Overlay



Assessing CISA Maturity based on Flows



RSAConference2022

How do I APPLY the SAFE Reference Architecture in my environment?

"APPLY"

- **IDENTIFY** the traffic flows that are critical to your environment and security posture goals
- Collect inventory of solutions and document your current **CURRENTLY AVAILABLE CAPABILITIES**
- Collect and document ALL needed or **REQUIRED CAPABILITIES** based on the mandate, framework, or regulation you are trying to satisfy
- **ALIGN** capabilities where needed in the flows gathered
- **IDENTIFY GAPS** between current and required capabilities
- **IMPLEMENT** where additional capabilities are needed
- Leverage Steps 2 & 3 of the SAFE Reference Architecture to document architecture for security