

CISCO *Connect* Toronto

October 30, 2019



You make **possible**



Cisco Connect Toronto 2019

Cisco SAFE - A Next Generation Architecture for Security

Jason Maynard

Senior Technical Solution Architect - Multi-Domain Cybersecurity

CCIE, CC[N|ID]P, SFCE, C|EH, RCSS, GICSP, GRID, GPEN



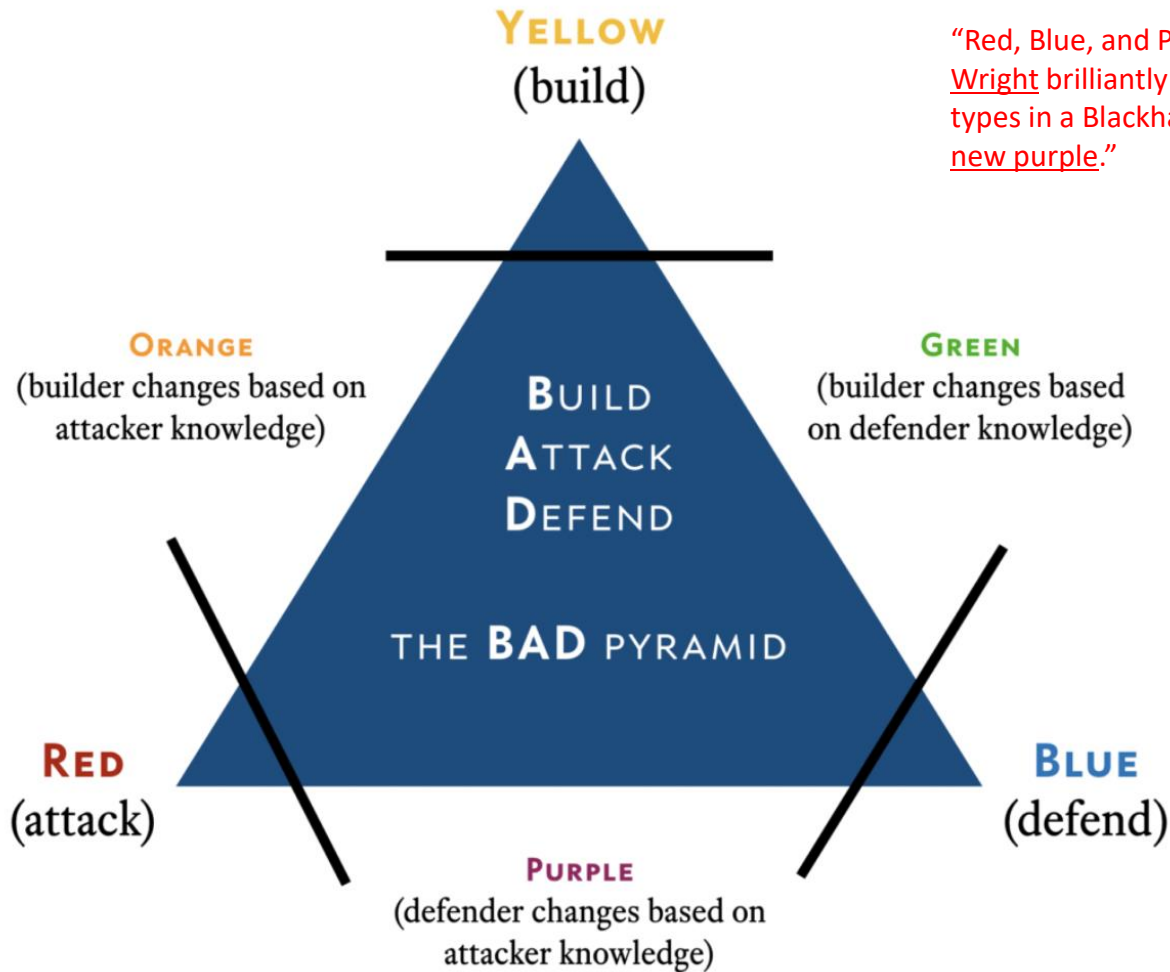
You make the power of data **possible**

Agenda

- Who can Benefit from this Session
- Industry Challenges
- The Point Product Approach
- Security as an Architectural Approach
- Security as an Architecture Walkthrough
- NIST/CIS and Cisco Capabilities Mapping
- Baseline Cyber Security Controls for Small and Medium Organizations



Who is on the Red Team?
Who is on the Blue Team?



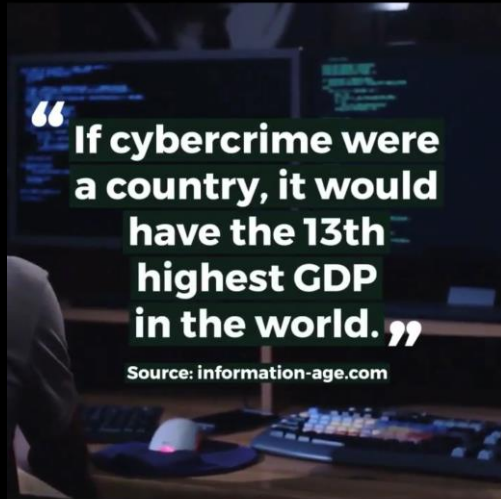
“Red, Blue, and Purple team concepts, [April Wright](#) brilliantly introduced a few other team types in a Blackhat talk called, [orange is the new purple.](#)”



You make the power of data **possible**

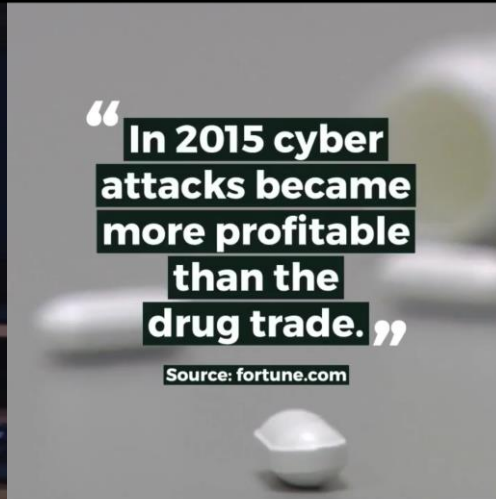
Industry Challenges

Interesting Statistics



“ If cybercrime were a country, it would have the 13th highest GDP in the world. ”

Source: information-age.com



“ In 2015 cyber attacks became more profitable than the drug trade. ”

Source: fortune.com



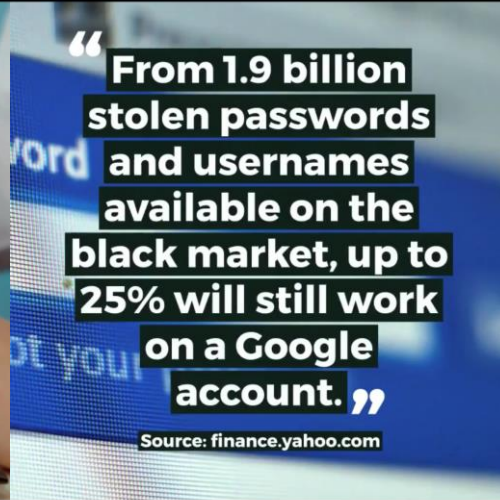
“ Sextortion, spam, phishing and crypto scams have increased 28% compared to 2017. ”

Source: fortune.com

Interesting Statistics



Interesting Statistics



Interesting Statistics

Canada is facing a **major shortage of cybersecurity workers**, with organizations across the country having about **8,000 roles to fill over the next few years**, according to a recent study. The situation is so urgent that Ryerson University has launched a 20-week bootcamp-style training program backed by the Royal Bank of Canada. Cybersecurity experts say colleges have fallen behind, and their existing programs take too long. Recent breaches, including Capital One's which affected six million Canadians, have thrust cybersecurity into the minds of many business leaders. • *Here's what people are saying.*



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

RSA® Conference Had - 100's and 100's and 100's of vendors! Over 43K attendees

Capability and Complexity



RSA Conference Had - 100's and 100's and 100's of vendors! Over 43K attendees

Capability and Complexity





Who is in Networking?

Can you name 10 vendors?

Who is in Systems?

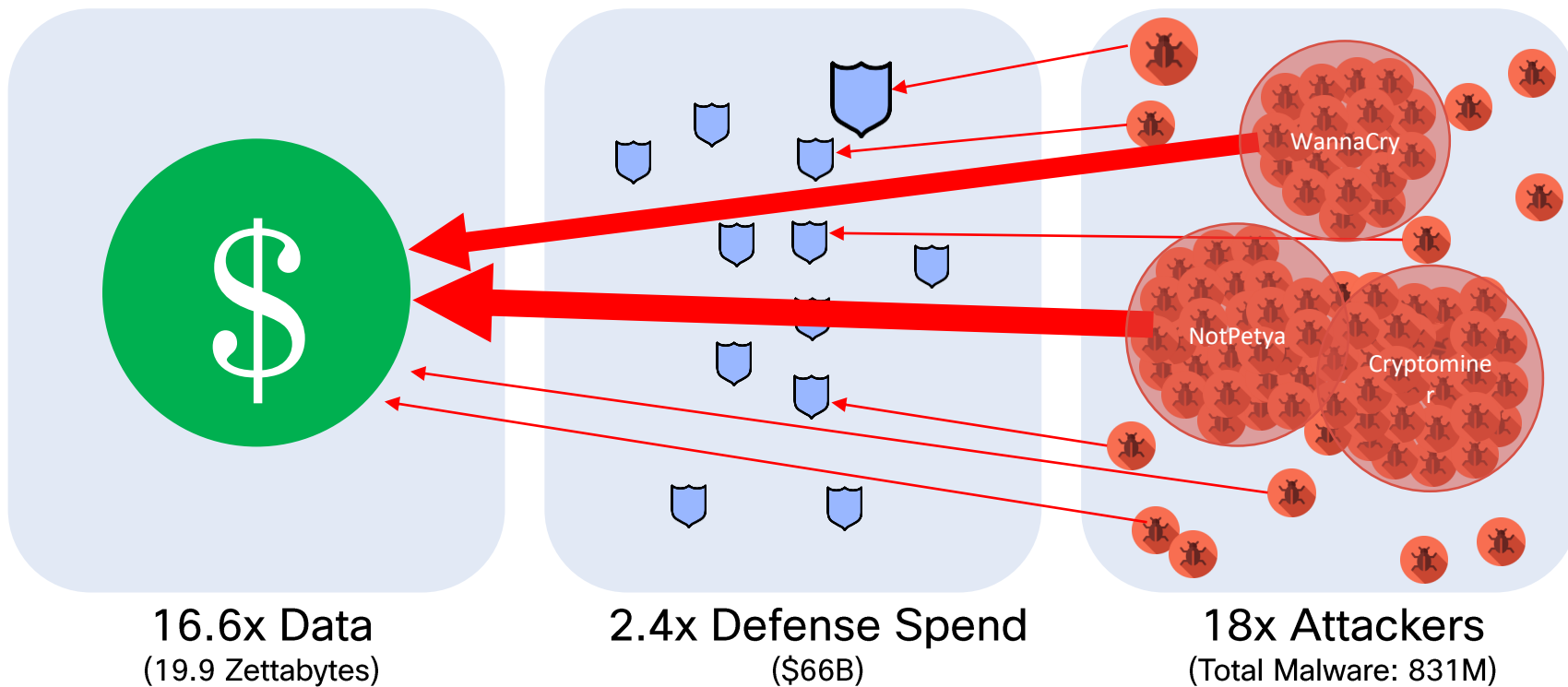
Can you name 10 vendors?

Who is in Storage?

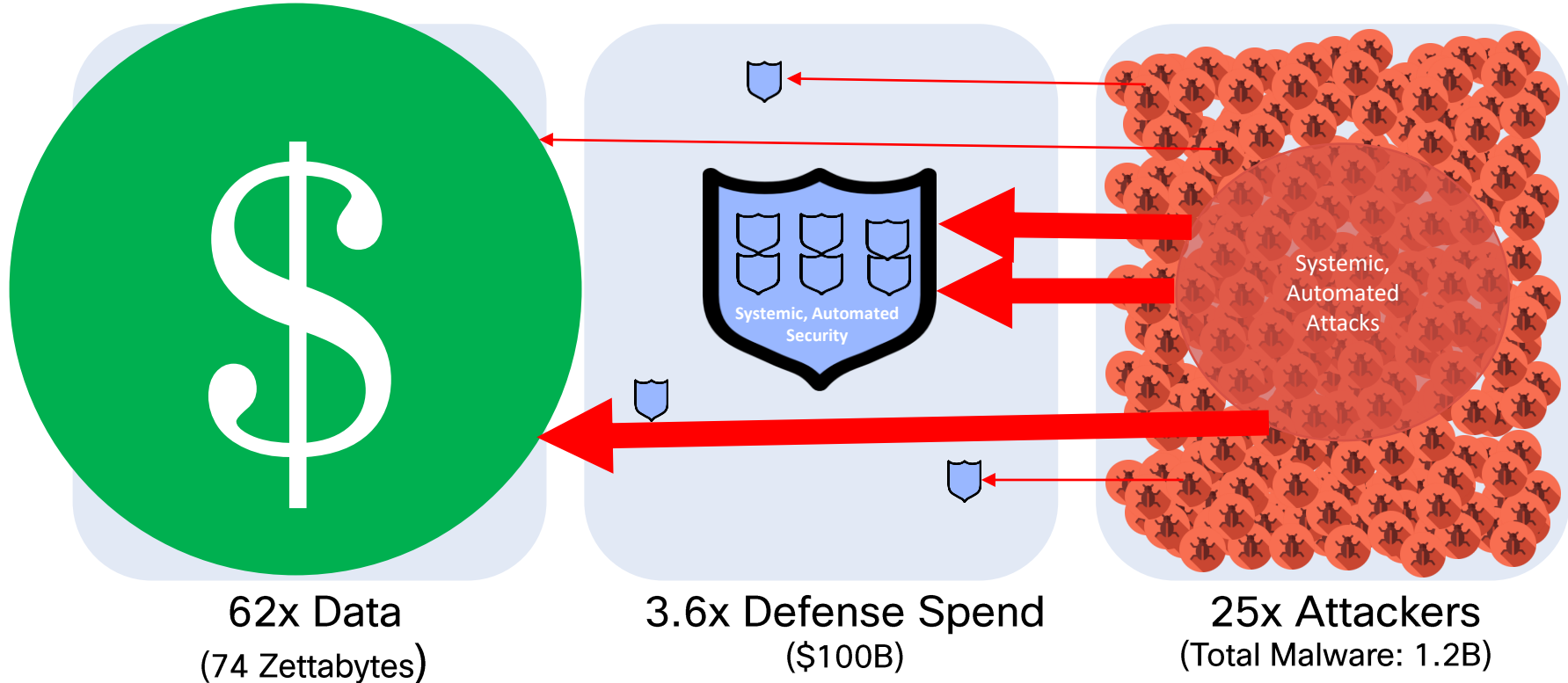
Can you name 10 vendors?

What about Security?

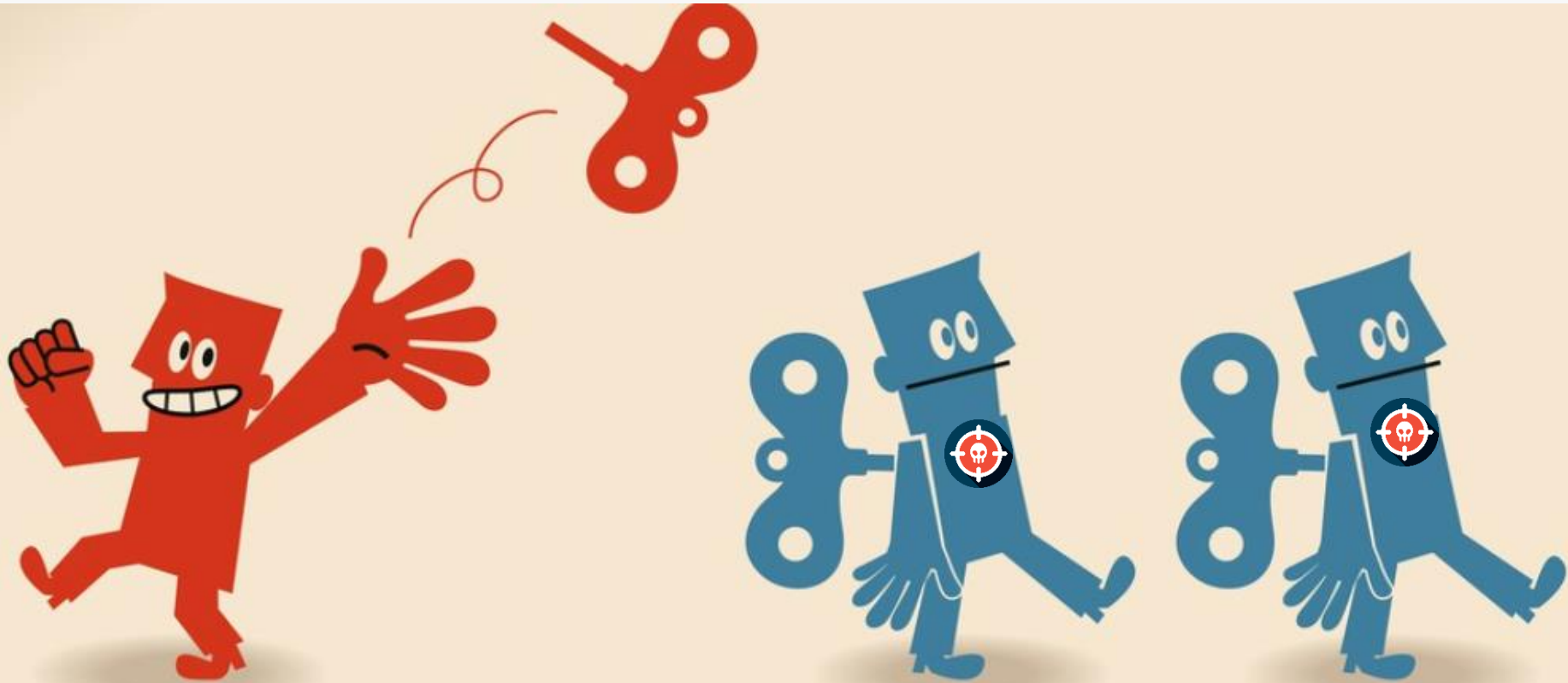
2019: Coordinated Attacks & Siloed Defense



2022: Integrated Defense Becomes a Necessity



What Are You Doing Different?



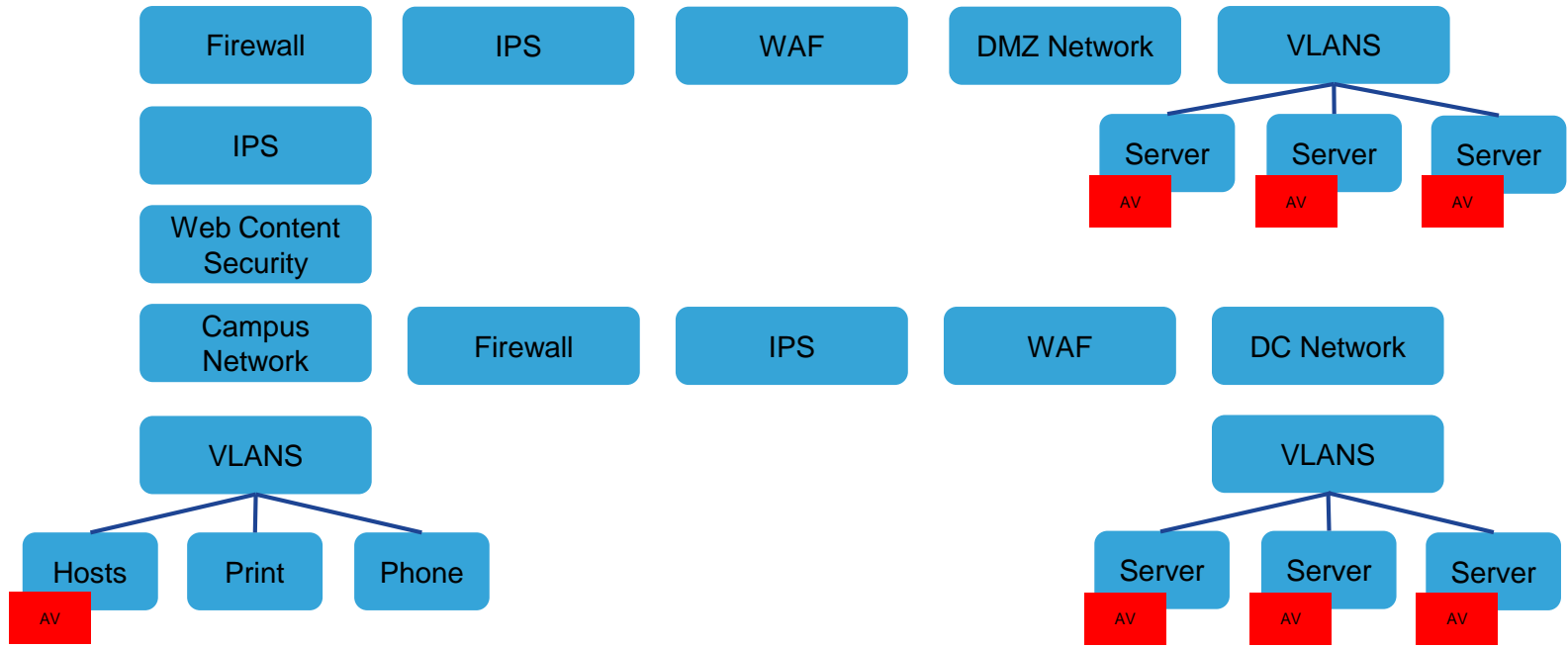
Time for a different approach!



You make the power of data **possible**

The Point Product Approach

Internet



DNS

Internet

Cloud Access Security Broker

Email Security

Firewall

IPS

WAF

DMZ Network

VLANS

IPS

Server

Server

Server

AV EDR

AV EDR

AV EDR

Web Content Security

Campus Network

Firewall

IPS

WAF

DC Network

VLANS

Hosts

Print

Phone

AV EDR

VLANS

Server

Server

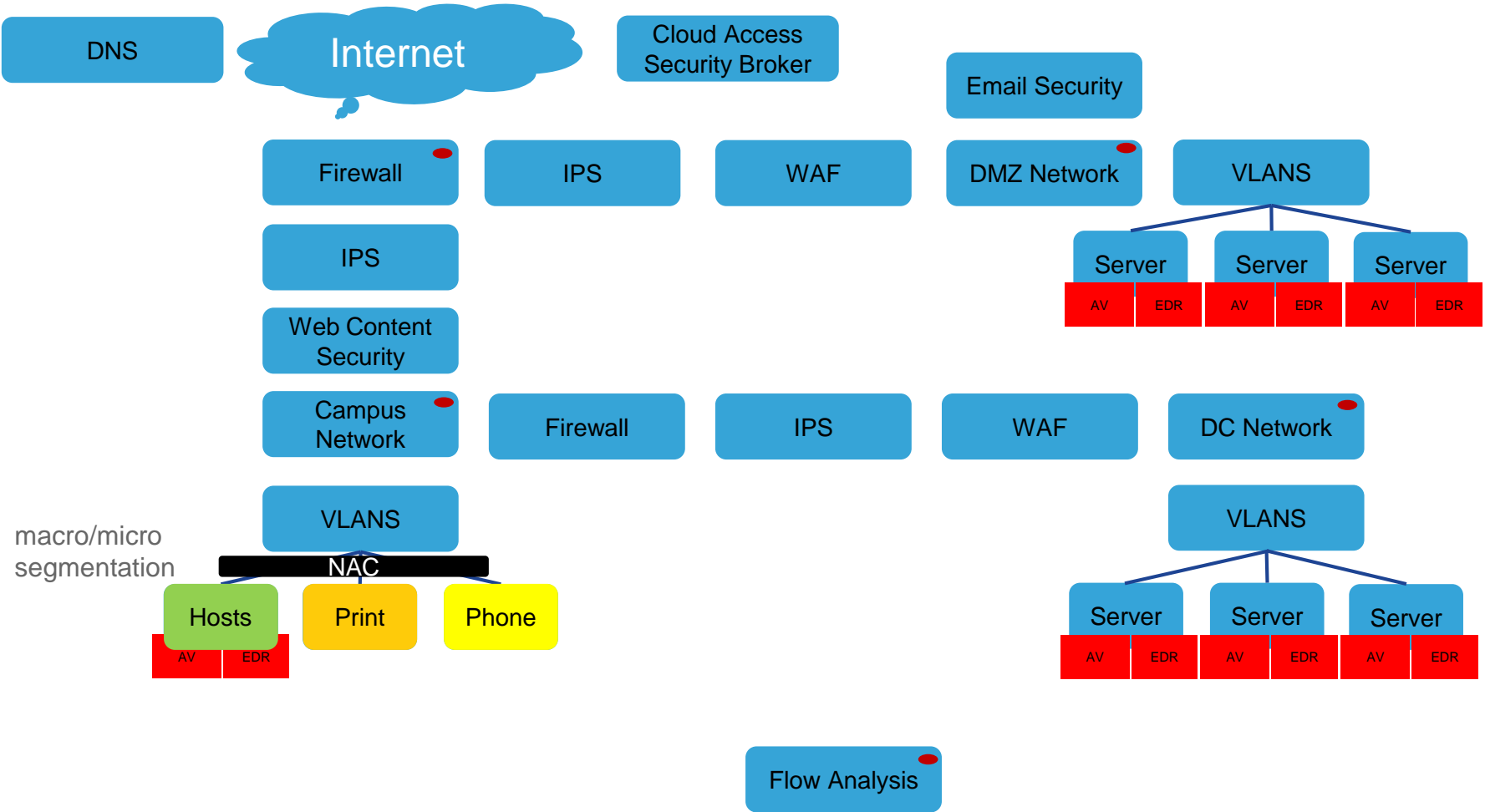
Server

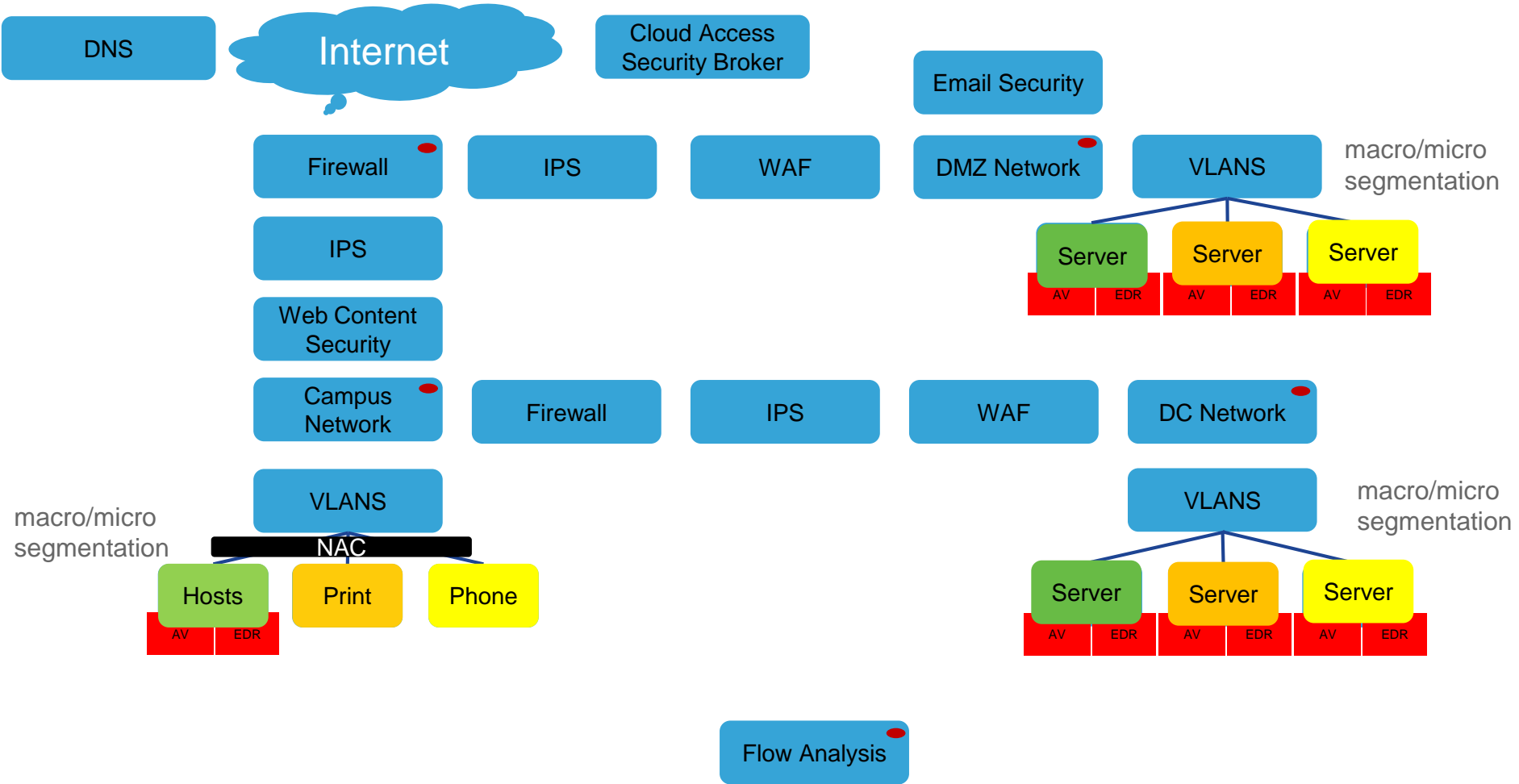
AV EDR

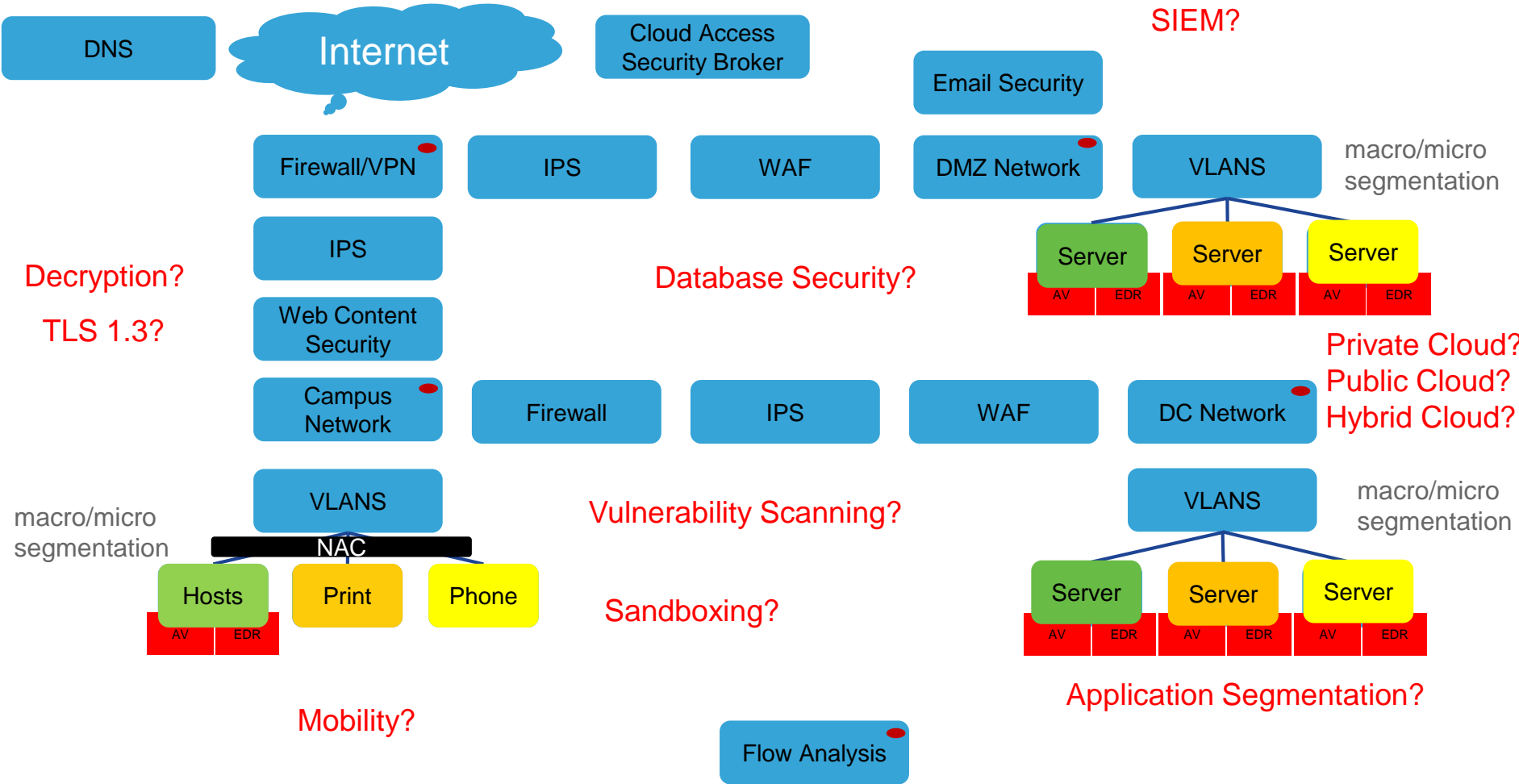
AV EDR

AV EDR

Flow Analysis







SIEM?

Email Security

Cloud Access Security Broker

Internet

DNS

Firewall/VPN

IPS

WAF

DMZ Network

VLANS

macro/micro segmentation

Server

Server

Server

AV

EDR

AV

EDR

AV

EDR

Decryption?

Database Security?

TLS 1.3?

IPS

Web Content Security

Campus Network

Firewall

IPS

WAF

DC Network

Private Cloud?

Public Cloud?

Hybrid Cloud?

macro/micro segmentation

VLANS

NAC

Hosts

Print

Phone

AV

EDR

Vulnerability Scanning?

Sandboxing?

VLANS

macro/micro segmentation

Server

Server

Server

AV

EDR

AV

EDR

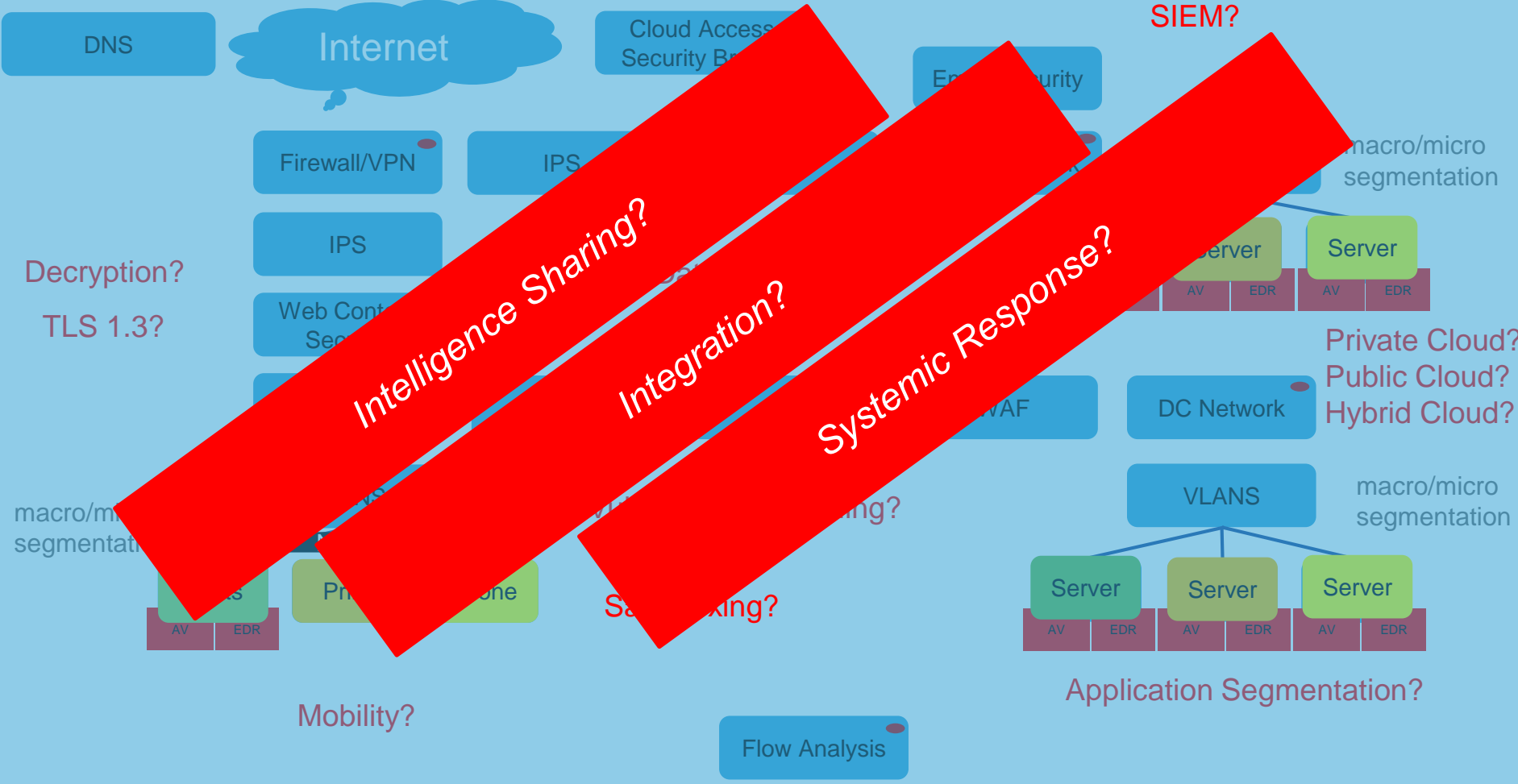
AV

EDR

Application Segmentation?

Mobility?

Flow Analysis



Intelligence Sharing?

Integration?

Systemic Response?

SIEM?

Decryption?
TLS 1.3?

Private Cloud?
Public Cloud?
Hybrid Cloud?

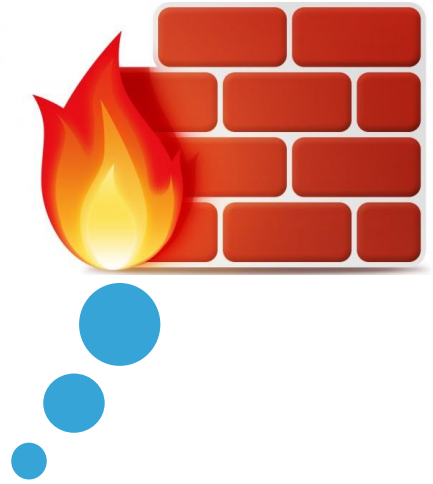
macro/micro
segmentation

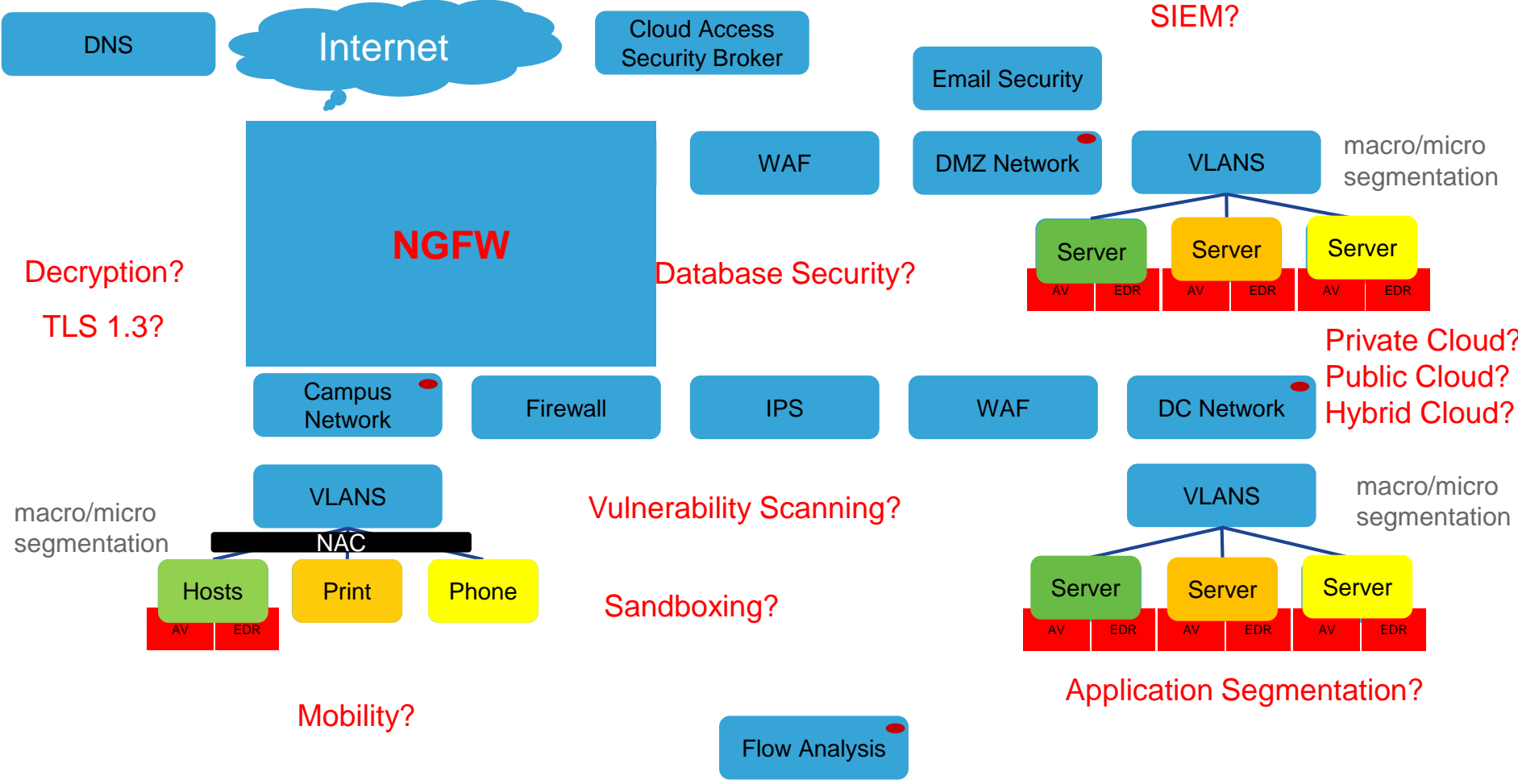
macro/micro
segmentation

Application Segmentation?

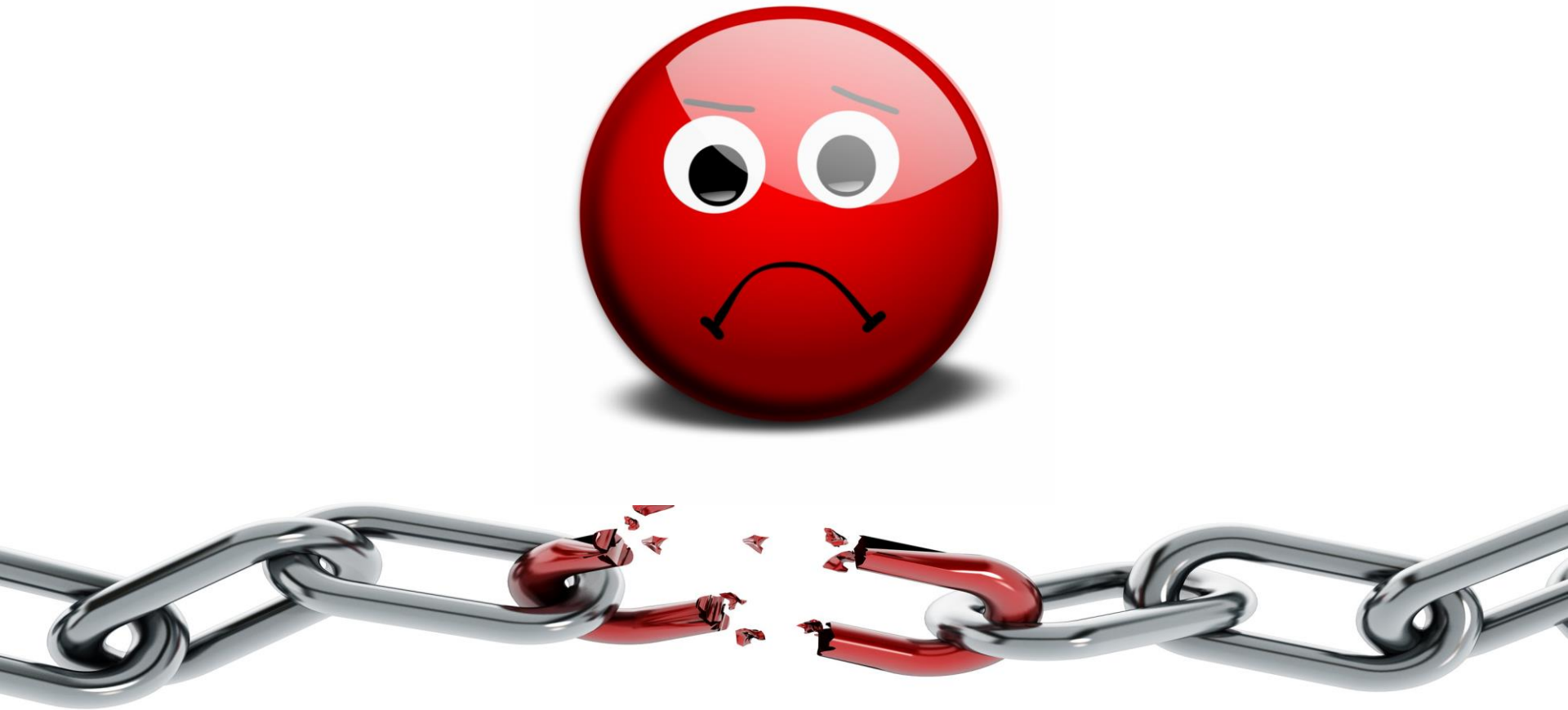
Mobility?

Flow Analysis









What is Broken!



You make the power of data **possible**

Security as an Architecture Overview

Building a Security Architecture: Executive Drivers



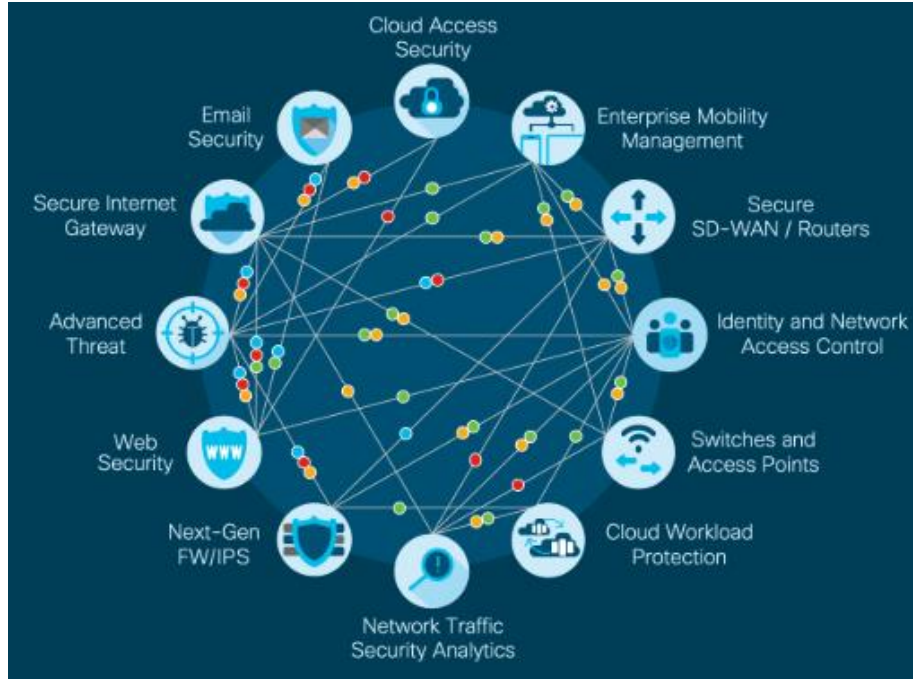
- Simplification of security stack
- Improve threat intelligence ingestion and consumption – reduce time to detect
- Reduce the number of vendors while increasing integration.
- Protect SaaS based applications
- Increase automated response action to threats in progress – reduce time to respond
- Simplified endpoint protection for advanced threat both on and off premise with architectural focus and integration.
- And more.....

Building a Security Architecture: Threats and Risks



- Compromise of customer data
- Credentials stolen and compromised accounts
- Lack of visibility on the network during an incident
- Risk of compromised assets off network
- IoT devices do not support agents
- Service impact due to breach
- And much more.....

Building a Security Architecture: Existing Tech



- Vendor A - Function
- Vendor B - Function
- Vendor C - Function
- Vendor D - Function
- Vendor E - Function
- Vendor F - Function
- Vendor G - Function
- Vendor H - Function
- Vendor I - Function
- Vendor J - Function
- Vendor K - Function
- Vendor L - Function



You make the power of data **possible**

Security as an Architecture

The Walkthrough

The Company!

ACME
CORPORATION

CEO



Acme Corporation

From Wikipedia, the free encyclopedia

This article is about the fictional Looney Tunes company. For other uses, see [Acme](#).

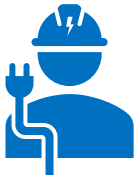
The **Acme Corporation** is a [fictional corporation](#) that features prominently in the *Road Runner/Wile E. Coyote* animated shorts as a [running gag](#) featuring outlandish products that fail or backfire catastrophically at the worst possible times. The name is also used as a generic title in many [cartoons](#), especially those made by [Warner Bros.](#), and [films](#), [TV series](#), [commercials](#) and [comic strips](#).

The company name in the *Road Runner* cartoons is [ironic](#), since the word *acme* is derived from [Greek](#) (ακμή; English transliteration: *akmē*) meaning *the peak, zenith or prime*,^[1] yet products from the fictional [Acme Corporation](#) are often [generic](#), [failure-prone](#), or [explosive](#).

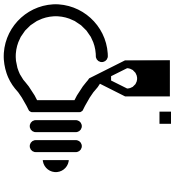
The Flow!



What Security Elements
Required to Secure the Flow



What Security Elements
Required to Secure the Flow



What Security Elements
Required to Secure the Flow

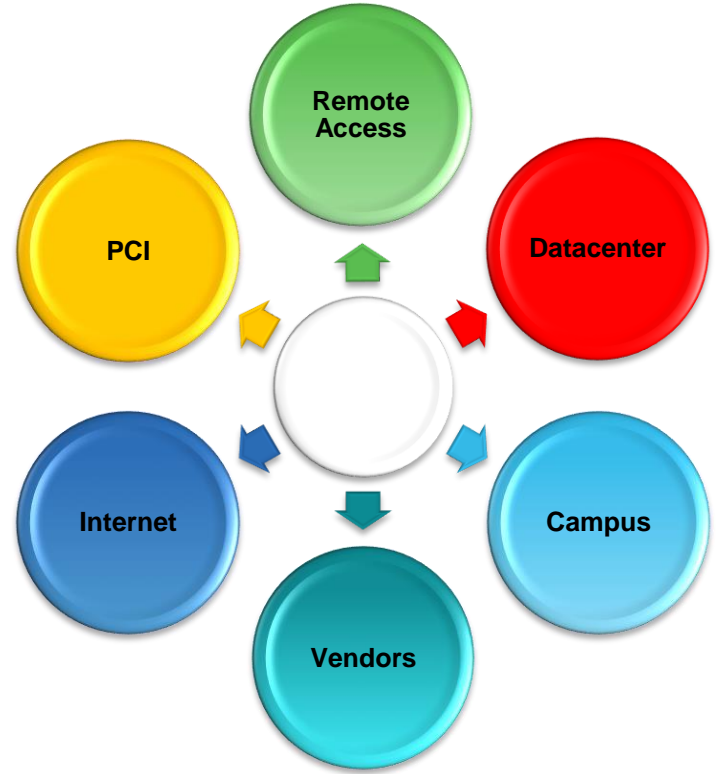


**Building
Management System**

Security Architectural Workshop

The workshop attendees suggested a focus on a couple of use cases..

Flows in this workshop:
1. Admin (on-premise) to Internet





You make the power of data **possible**

Security as an Architecture Capabilities Map

Legend



Capability is currently addressed.

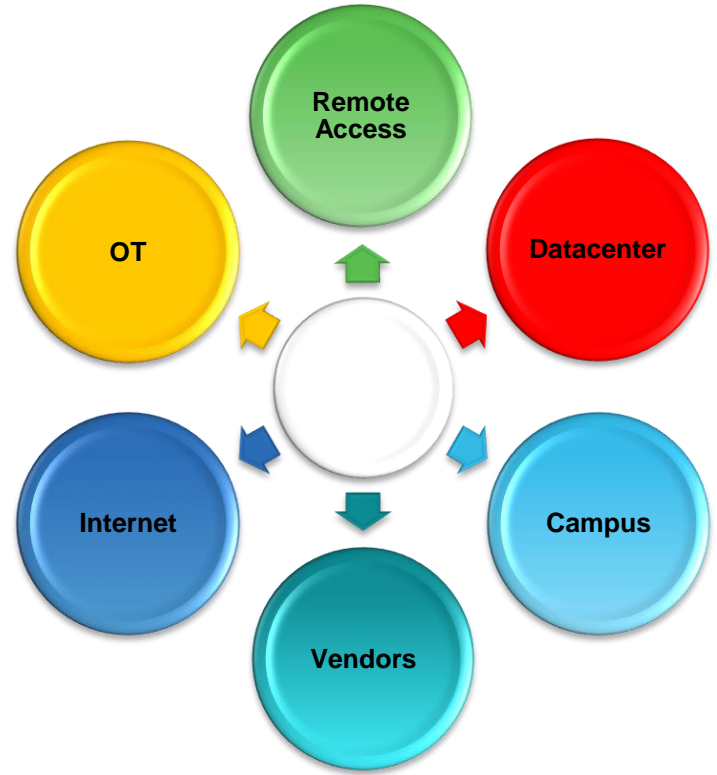


Capability is partially addressed, or purchased but not deployed.



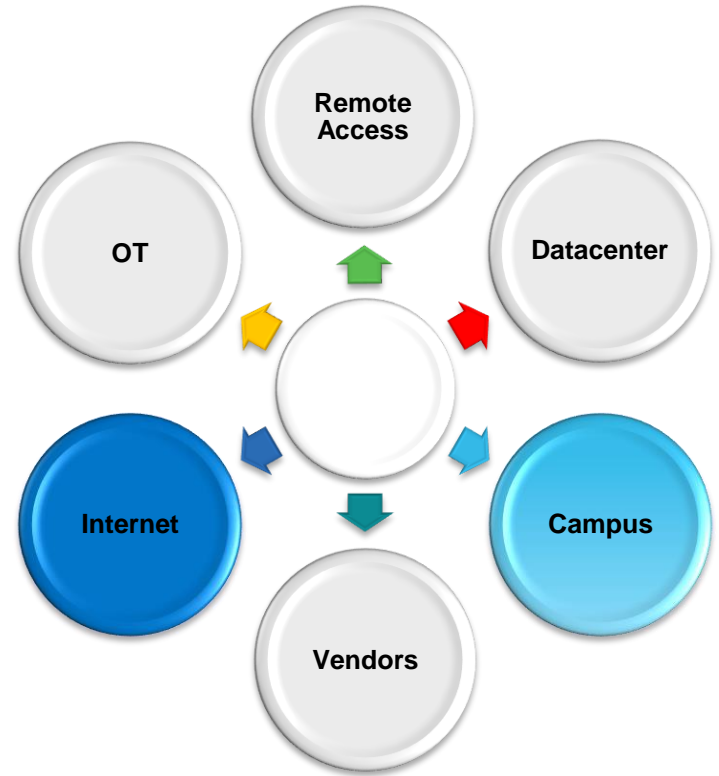
Capability is not addressed.

Internet



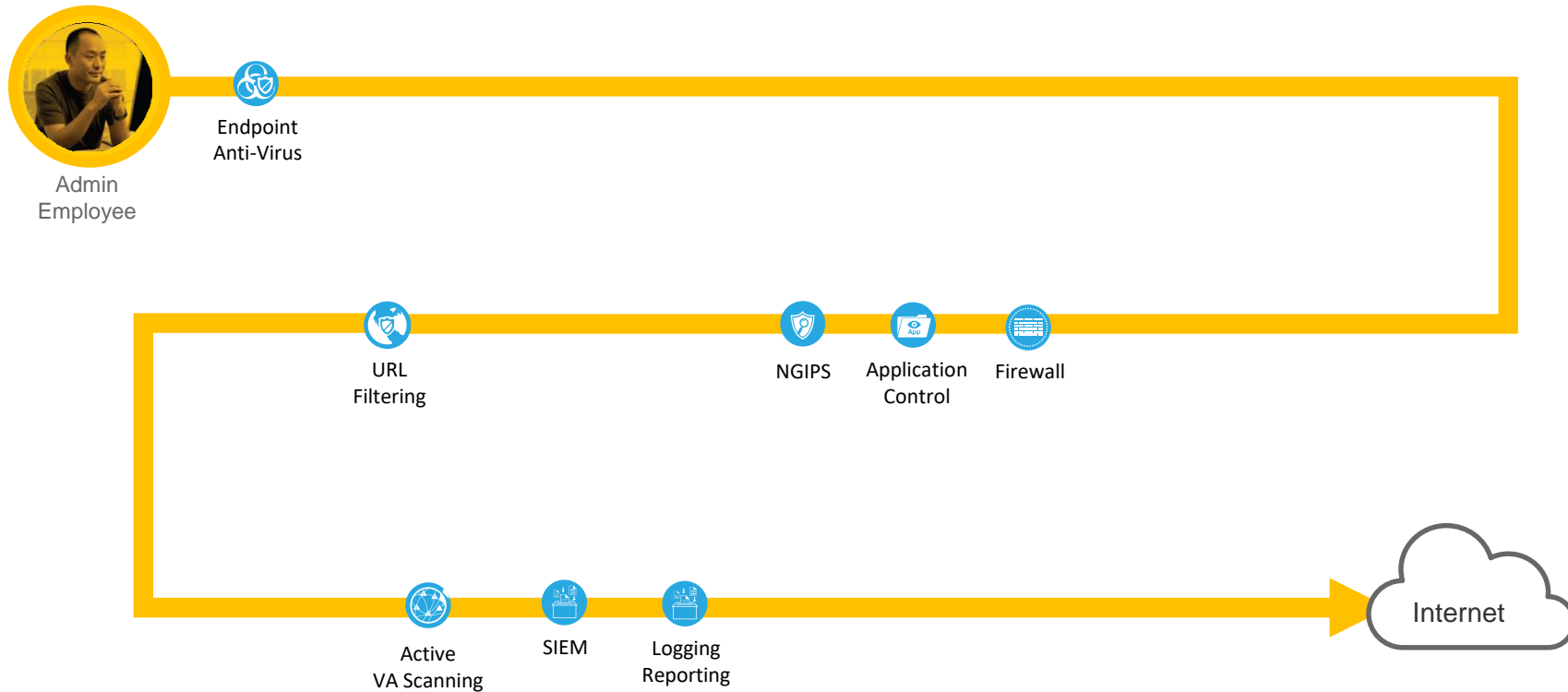
Internet

Campus (Admin on-premise) to
Internet



Campus to Internet

Flow: Admin (on-premise) to Internet



Campus to Internet

Flow: Admin (on-premise) to Internet



Admin Employee



Endpoint Anti-Virus



Identity Authorization



Device Profile and Posture



SDA / Segmentation / Dynamic Control

Should I be able to connect any asset and get access to the wired network?



URL Filtering



NGIPS



Application Control



Firewall

Do I need to understand the type and state of the asset?

Do I need dynamic Control based on the context of an asset?



Active VA Scanning



SIEM



Logging Reporting



Campus to Internet

Flow: Admin (on-premise) to Internet



Admin Employee



Endpoint Anti-Virus



Recursive DNS Security



Identity Authorization



Device Profile and Posture



SDA / Segmentation / Dynamic Control

What about DNS Security?



URL Filtering



NGIPS



Application Control



Firewall

Do I need Flow Analytics?



Flow Analytics



Active VA Scanning



SIEM



Logging Reporting



Campus to Internet

Flow: Admin (on-premise) to Internet



What Endpoint Detection and Response?



Admin Employee



Endpoint Anti-Virus



Endpoint Advanced Malware Protection (EDR)



Recursive DNS Security



Identity Authorization



Device Profile and Posture



SDA / Segmentation / Dynamic Control



URL Filtering



Network Anti-Malware



NGIPS



Application Control



Firewall

What network based malware detection?



Flow Analytics



Active VA Scanning



SIEM



Logging Reporting



Campus to Internet

Flow: Admin (on-premise) to Internet



Admin Employee



Endpoint Anti-Virus



Endpoint Advanced Malware Protection (EDR)



Recursive DNS Security



Identity Authorization



Device Profile and Posture



SDA / Segmentation / Dynamic Control

Does passive VA scanning add value?



SSL Decryption



URL Filtering



Network Anti-Malware



Passive VA Scanning



NGIPS



Application Control



Firewall

What about TLS and inspection?



Flow Analytics



Active VA Scanning



SIEM



Logging Reporting

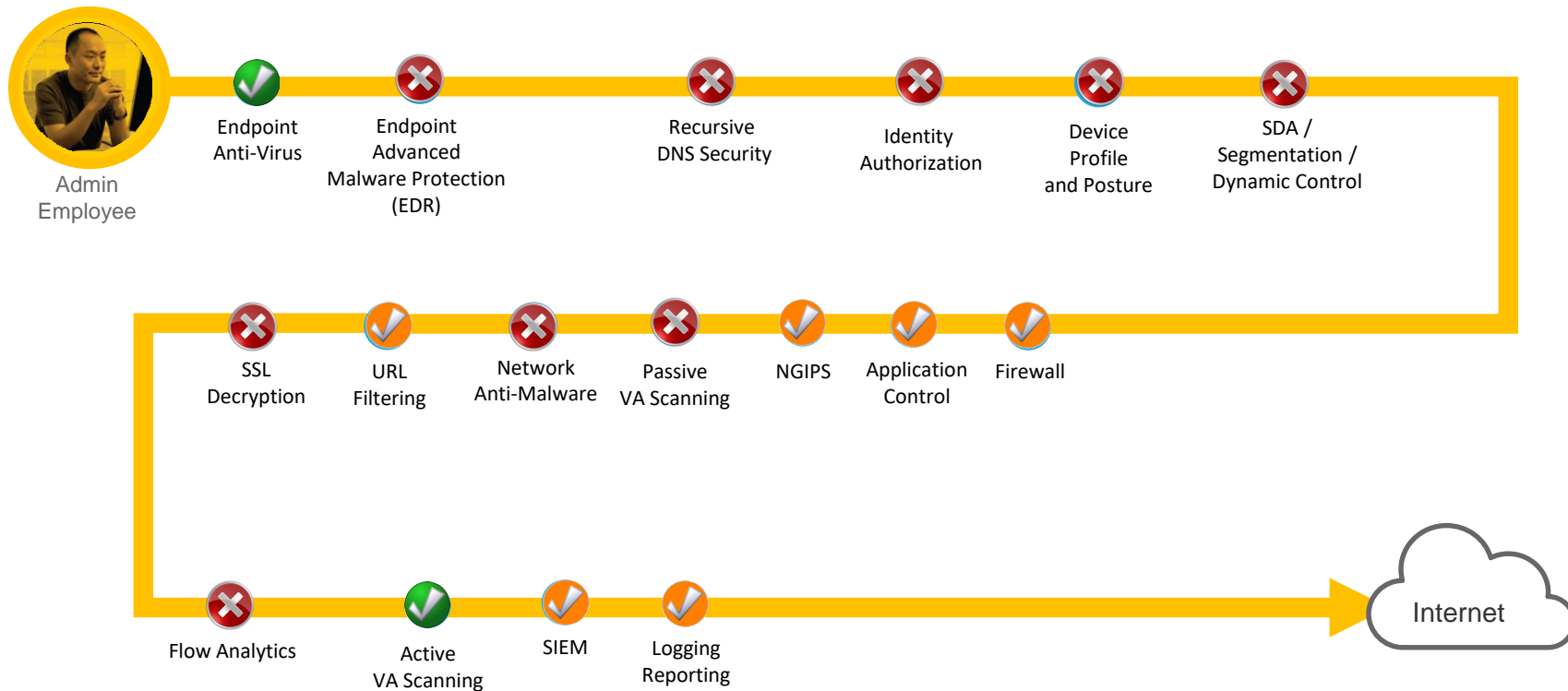


Campus to Internet

Flow: Admin (on-premise) to Internet

Summary:

- 3 Vendors
- 15 Gaps



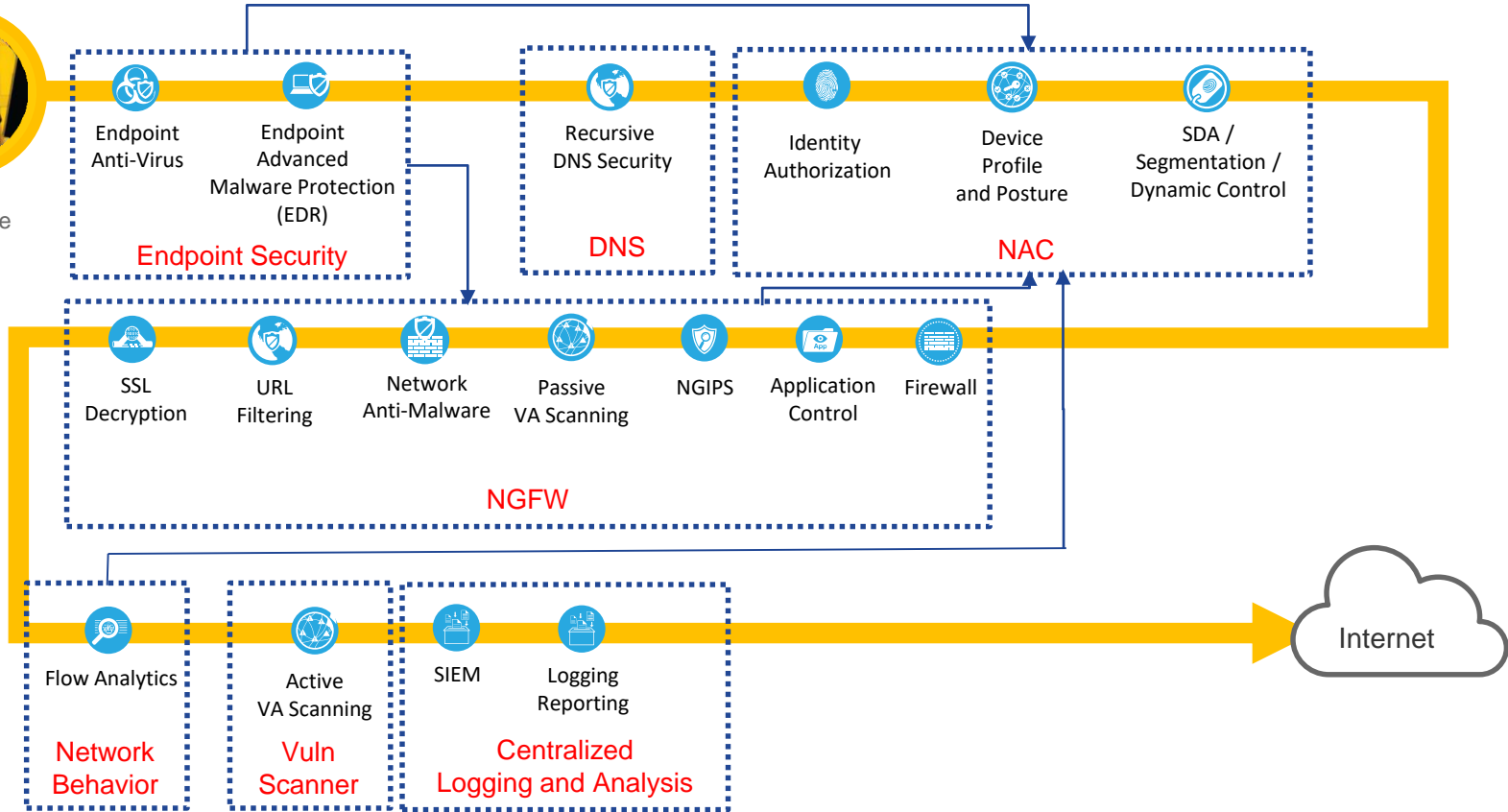
Campus to Internet

Flow: Admin (on-premise) to Internet

3 Vendors, 0 Gaps



Admin Employee



Campus to Internet

Flow: Admin (on-premise) to Internet



Admin Employee

3 Vendors, 0 Gaps



Endpoint Anti-Virus



Endpoint Advanced Malware Protection (EMAP)

Endpoint



Flow Analytics

Network Behavior



Active VA Scanning

Vuln Scanner

Logging Reporting

Centralized Logging and Analysis

How do I share intelligence?

How supported is the integration?

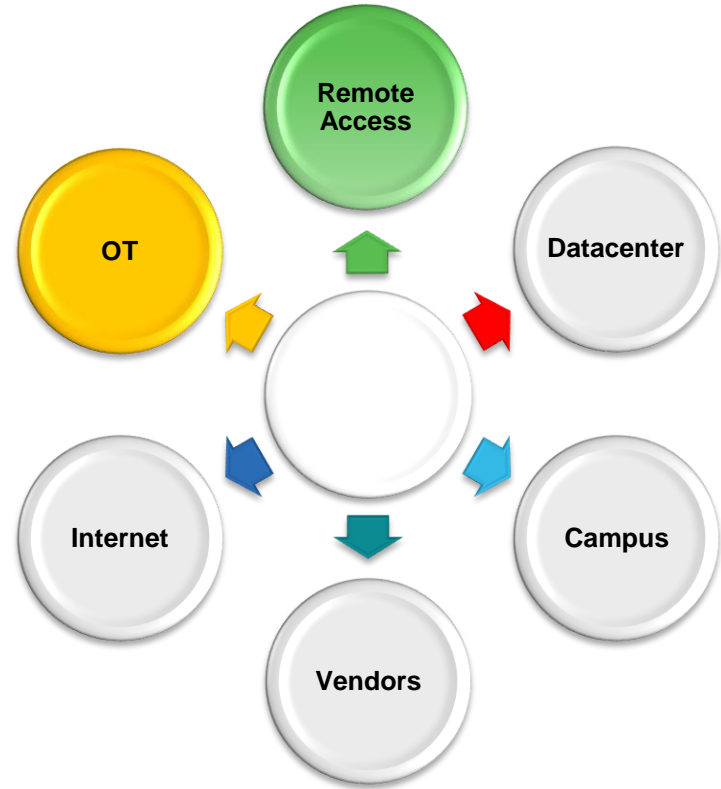
Do I get systemic response?

How much complexity did I introduce?



Internet

Operational Technologies



BMS Contractor/Support to BMS Access Management

Flow: Remote Access (Contractor/Support) to Jump Server



External Contractor /Support



RA VPN



Logging Reporting



Endpoint Anti-Virus



BMS Contractor/Support to BMS Access Management

Flow: Remote Access (Contractor/Support) to Jump Server



External Contractor /Support

Do we need identify, posture the device before giving access?



RA VPN



Identity Authentication and Authorization



Device Profile and Posture



TrustSec / Segmentation / Dynamic Control

What about dynamic control based on context of the asset?



Application Control



Firewall

Do we need firewall and what about application control?



Logging Reporting



Endpoint Anti-Virus



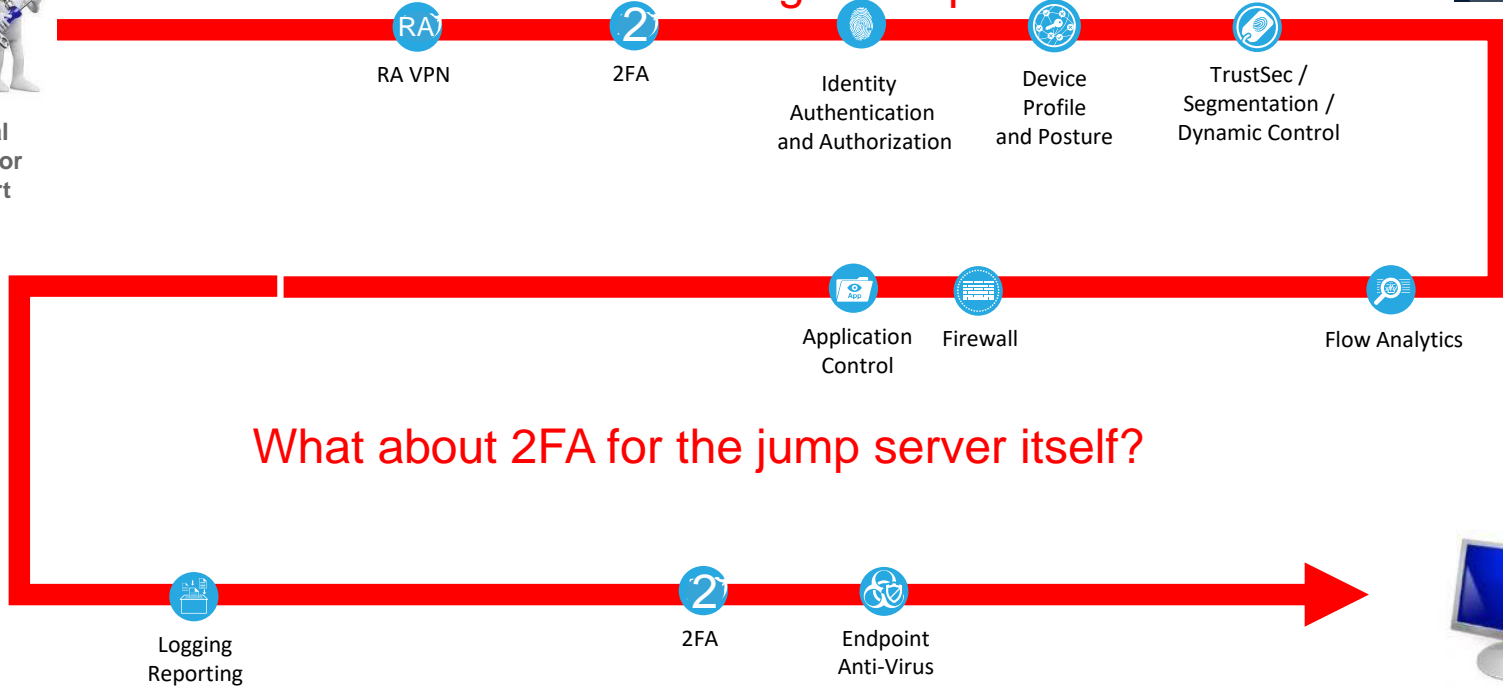
BMS Contractor/Support to BMS Access Management

Flow: Remote Access (Contractor/Support) to Jump Server



External Contractor /Support

What is the risk if the credentials get compromised?



What about 2FA for the jump server itself?

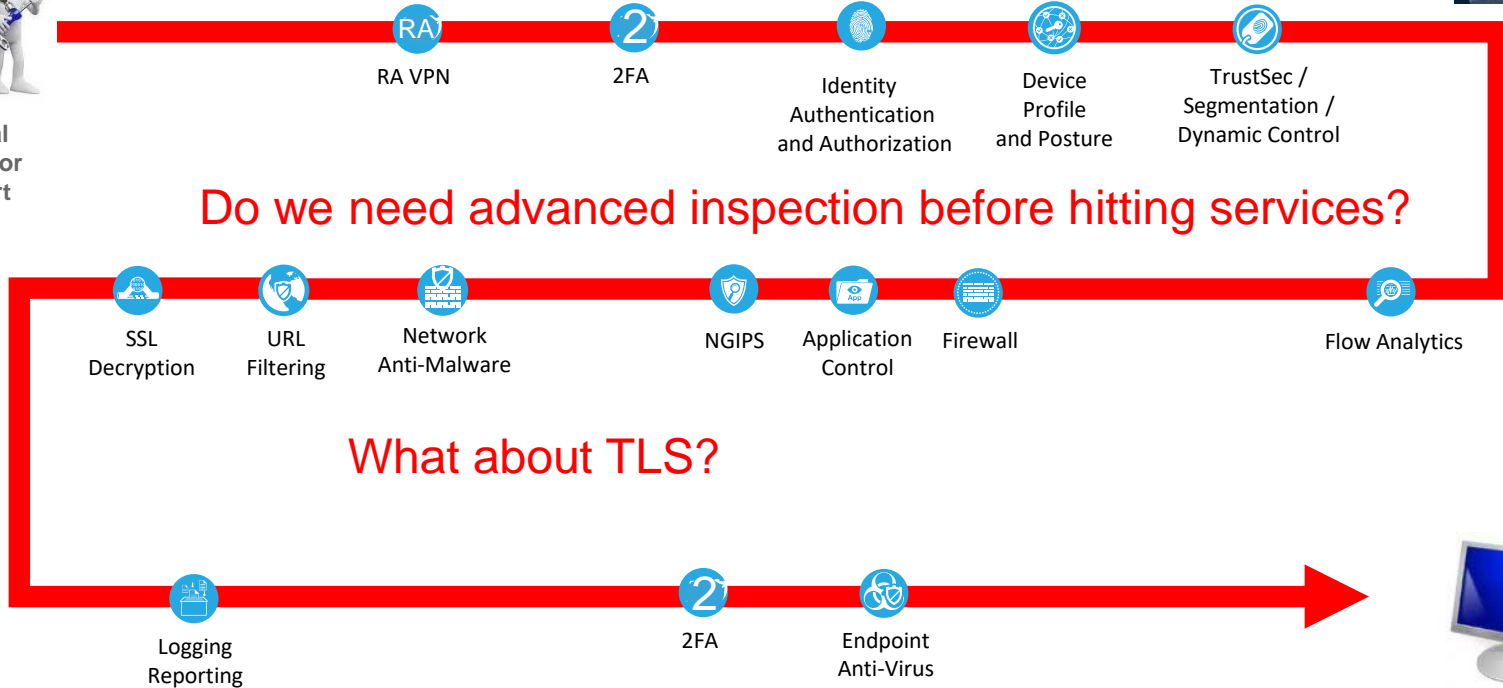


BMS Contractor/Support to BMS Access Management

Flow: Remote Access (Contractor/Support) to Jump Server



External Contractor /Support

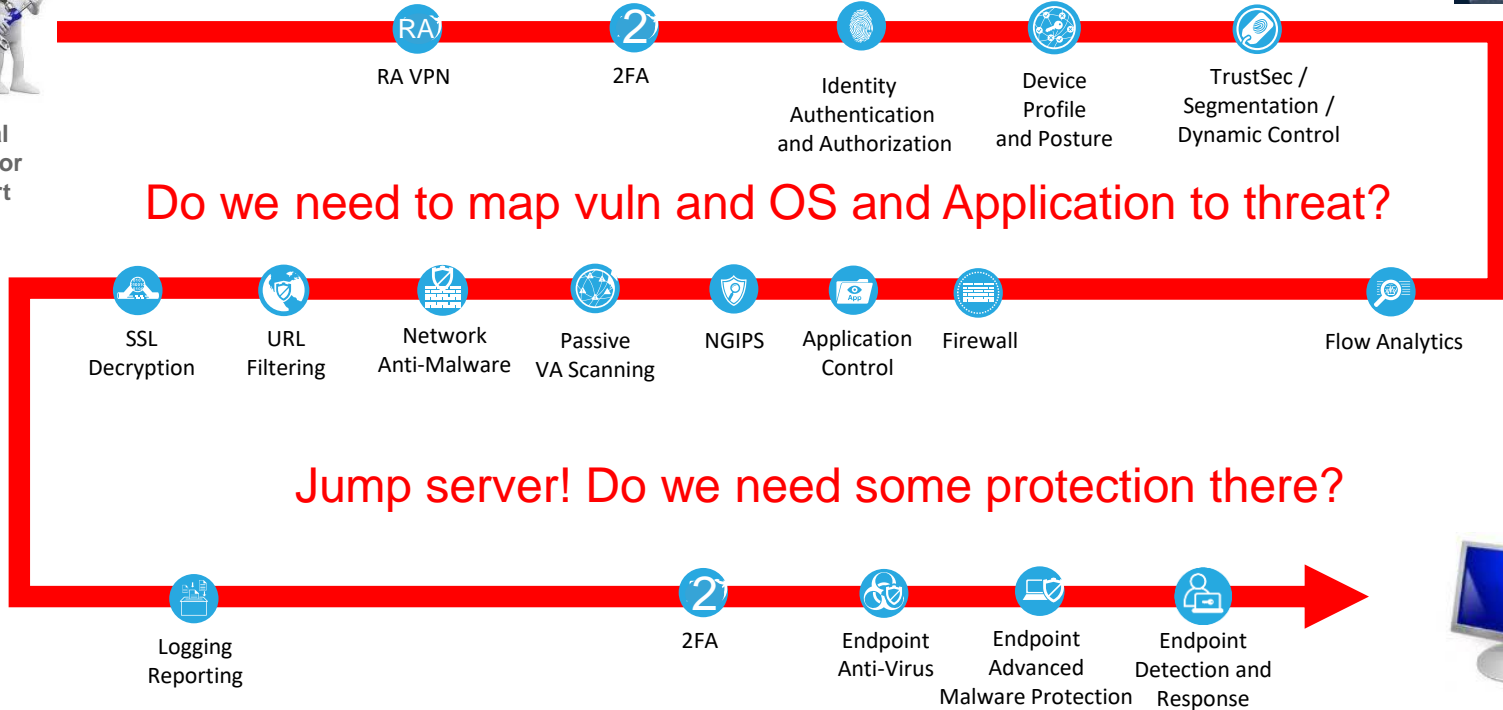


BMS Contractor/Support to BMS Access Management

Flow: Remote Access (Contractor/Support) to Jump Server



External Contractor /Support



BMS Contractor/Support to BMS Access Management

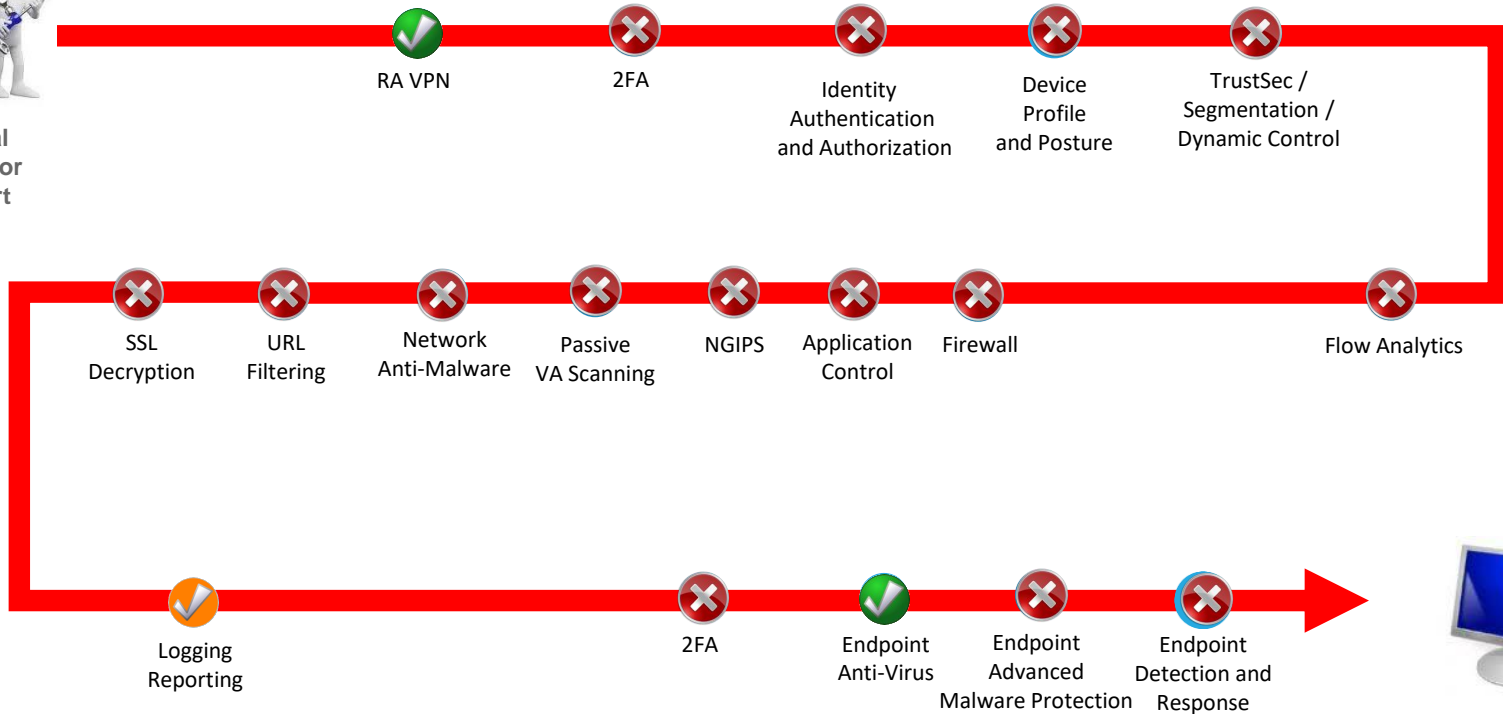
Flow: Remote Access (Contractor/Support) to Jump Server

Summary:

- 3 Vendors
- 16 Gaps



External Contractor /Support

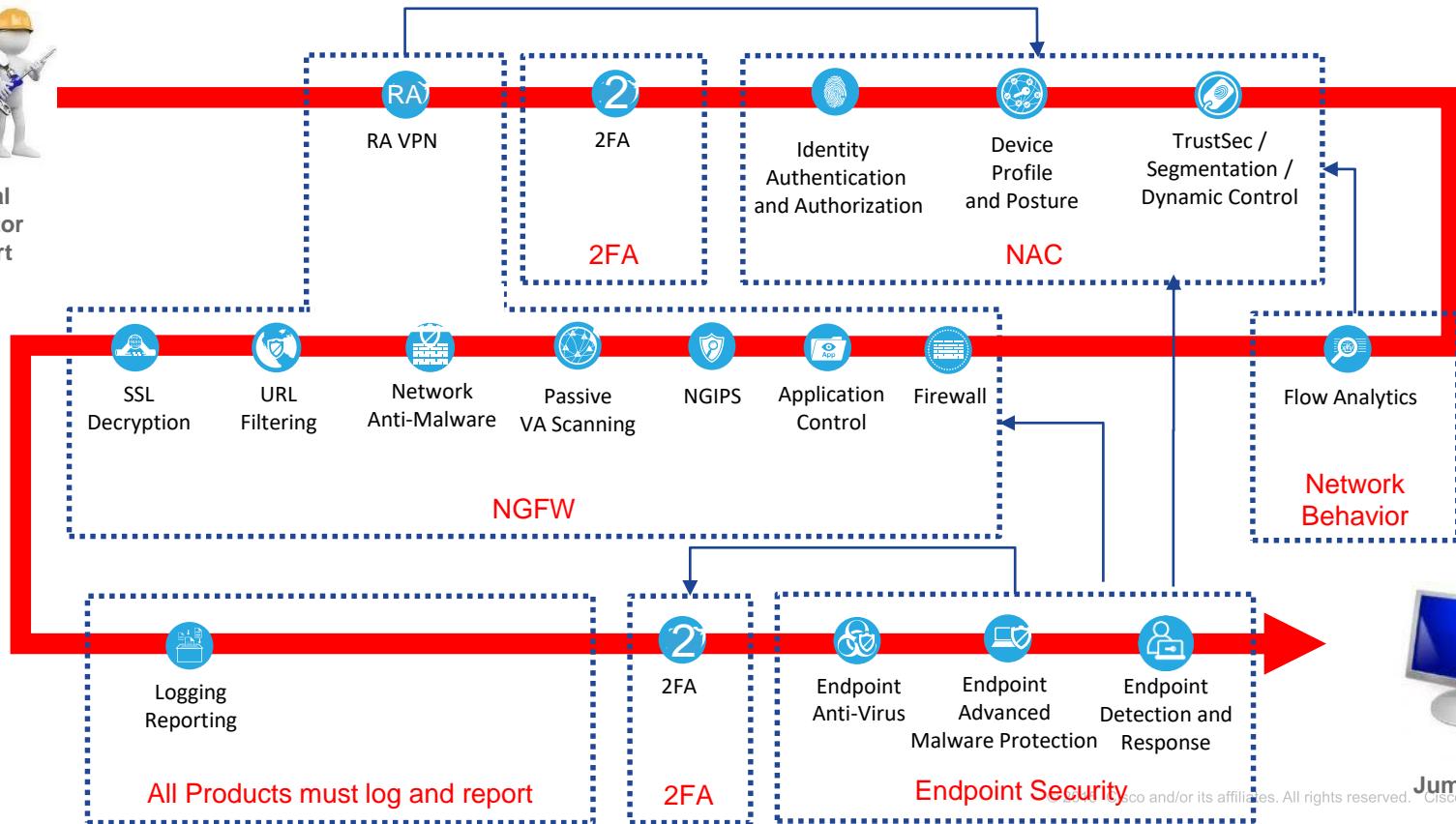


BMS Contractor/Support to BMS Access Management

Flow: Remote Access (Contractor/Support) to Jump Server



External Contractor /Support



Jump Server

BMS Contractor/Support to BMS Access Management

Flow: Direct Remote Access (Contractor/Support) Jump Server



External Contractor /Support

How do I share intelligence?

How supported is the integration?

Do I get systemic response?

How much complexity did I introduce?

Logging Reporting

All Products must log and report

2FA

Endpoint Anti-Virus

Endpoint Advanced Malware Protection

Endpoint Security

Endpoint Detection and Response

Flow Analytics

Network Behavior



Jump Server

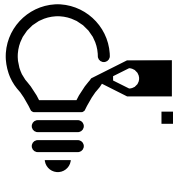
You would continue this effort for all major flows



What Security Elements
Required to Secure the Flow



What Security Elements
Required to Secure the Flow



What Security Elements
Required to Secure the Flow



Each flow may have similar capabilities some will require less or more capabilities

Building Management System

Top Mitigation Priorities (Gap Analysis)

Security Capability	Missing Capability (how often is this capability missing?)	Licensed or Partially Deployed
Network Segmentation (Dynamic Based Control and Segmentation)	10	Static deployment today
Next Generation Firewall (includes AMP, NGIPS, URL, AVC and SSL Decrypt)	10	Fully for the internet –not be deployed in all places of the network
Endpoint Advanced Malware Protection	9	
Malware Protection Data Leakage Protection (Email)	5	
Passive Vulnerability Scanning	10	
*Identity Based Control	8	
Recursive DNS Security	5	
DDoS	6	
Flow Analytics (Network and includes Encrypted Traffic Analytics)	10	
Cloud Access Security Broker	5	Sanctioned cloud applications

Top Mitigation Priorities Per Flow (Gap Analysis)

Security Capability	Missing Capability (how often is this capability missing?)	Admin On-Premise to Internet	Staff/Instructors On-Premise to internet	Researchers On-Premise to internet	Students (CORP Asset) On-Premise to Internet	Admin/Staff /Instructors Off-Premise to Internet	Admin/Staff /Instructors to Datacenter	BYoD to Datacenter	Contractor /Vendor (Non-CORP) to Datacenter	Remote Access VPN to Datacenter	WEB PCI to APP PCI	APP PCI to BD PCI
Network Segmentation (Dynamic Based Control and Segmentation)	10	Red	Red	Red	Red	Black	Red	Red	Red	Red	Red	Red
Next Generation Firewall	10	Yellow	Yellow	Yellow	Yellow	Black	Yellow	Red	Red	Red	Red	Red
Endpoint Advanced Malware Protection (includes AV and EDR)	9*	Red	Red	Red	Red	Red	Red	Black	Black	Red	Red	Red
Malware Protection & Data Loss Prevention (Email)	5	Red	Red	Red	Red	Red	Black	Black	Black	Red	Black	Black
Passive Vulnerability Scanning	10	Yellow	Yellow	Yellow	Yellow	Black	Red	Red	Red	Red	Red	Red
*Identity Based Control	8	Red	Red	Red	Red	Red	Red	Red	Red	Red	Black	Black
Recursive DNS Security	5	Red	Red	Red	Red	Red	Black	Black	Black	Black	Black	Black
DDoS	6	Black	Black	Red	Red	Black	Red	Red	Red	Red	Red	Red
Flow Analytics (Network includes Encrypted Traffic Analytics)	10	Red	Red	Red	Red	Black	Red	Red	Red	Red	Red	Red
Cloud Access Security Broker	5	Red	Red	Red	Red	Red	Black	Black	Black	Black	Black	Black

Company GAP

Company Owned Not Deployed

Company Not Required

This chart is calculated by adding the number of Red and Orange capabilities on each map.

Specific Recommendations

Priority	Description
1	Continue to rollout NGFW including NGIPS, URL, AVC, and Malware protection for internet based connections. Consider extending NGFW capabilities deeper into the network restricting access to protected networks from internal networks adding advanced inspection. NGIPS system should be able to utilize both active and passive vulnerability assessment tools and truly understand the assets being protected. These recommendations are most important in reducing risk and more specifically scope for PCI purposes (as an example), as well as for protecting CORP's internal network. DDoS mitigation capabilities will add additional protection capabilities when either volumetric or application layer attacks take place render the service useless. CORP has some static controls in place but really should consider dynamic control and more real-time automation.
2	CORP develop a strategy and implement identity-based access, with common controls across Wired, Wireless, and Remote Access networks. Dynamic controls should be in place for assets based on assessment of that asset and if the disposition changes automated response capabilities become critical when trying to reduce the overall exposure to CORP.
3	Implement DNS-based security to protect against Ransomware and other Malware, as well as Command & Control used in botnets. DNS also becomes critical when leveraging cloud based services and therefore the DNS solution should provide fallback resolution in case the recursive DNS provider cannot resolve an authoritative request. This should cover assets on and off premise
4	Email is the #1 vector for malware and CORP should consider advanced email security solution that provides a feature rich set of security capabilities with strong integration into cloud based email solutions. CORP should also consider leveraging cloud based access control solutions further protecting sanctioned cloud based applications.
5	CORP should consider adding Endpoint Advanced Malware Protection (eAMP) to corporately owned assets, and extend it to servers, as possible. Consolidating the eAMP which includes Endpoint Detection and Response with traditional AV is also advantageous when it comes to simplifying the number of vendors and reduces complexity while increasing automation and integration.
6	Enable automation and integration between products that support this, in order to enhance security and decrease operational burden. As an example, endpoint AMP, NGFW, Network Behavioral Analysis integration with NAC, you can enable powerful integration between these products to realize things such as rapid threat containment.
7	CORP requires network visibility into all areas of the network including PCI (known or unknown environments). This should leverage netflow data and provide insight into what is taking place of the network and generate alarms when certain behaviors reach a certain threshold. CORP should consider to host lock the PCI environment (or like environments) and trigger alarms if non-approved assets attempt to communicate to the controlled PCI environment; this also ensures controls are working as expected.

Specific Recommendations

(ordered by Ease/Time of Deployment)

Order	Description
1	Implement DNS-based security to protect against Ransomware and other Malware, as well as Command & Control used in botnets. Centralize all DNS requests externally for all ports and protocols which maximizes visibility for both on and off premise use cases.
2	Continue to rollout NGFW including NGIPS, URL, AVC, and Malware protection for internet based connections.
3	Rollout Endpoint Advanced Malware Protection and consider consolidating AV function, and extend it to servers, as possible.
4	Implement strong email security capabilities to reduce the overall risk and improve productivity. Feature rich set of security capabilities should include SPAM, Graymail, Phishing, Forged Email, Advanced Malware, Retrospection, DLP, and encryption with strong integration into cloud based email solutions. CORP should also consider leveraging cloud based access control solutions further protecting sanctioned cloud based applications. (perhaps start with Email). Note: CORP should consider integrations to ensure that the CASB has the ability to provide API based capabilities and can enforce security on and off premise.
5	Consider extending NGFW capabilities deeper into the network restricting access to protected networks from internal networks adding advanced inspection. NGIPS system should be able to utilize both active and passive vulnerability assessment tools and truly understand the assets being protected. These recommendations are most important in reducing risk and more specifically scope for PCI purposes (as an example), as well as for protecting CORP's internal network. DDoS mitigation capabilities will add additional protection capabilities when either volumetric or application layer attacks take place render the service useless. CORP has some static controls in place but really should consider dynamic control and more real-time automation.
6	Develop a strategy and implement identity-based access, with common controls across Wired, Wireless, and Remote Access networks. Dynamic controls should be in place for assets based on assessment of that asset and if the disposition changes automated response capabilities become critical when trying to reduce the overall exposure to CORP. This should also include BYoD, and Guest access improving security and user experience.
7	CORP requires network visibility into all areas of the network including PCI (known or unknown environments). This should leverage netflow data and provide insight into what is taking place of the network and generate alarms when certain behaviors reach a certain threshold. CORP should consider to host lock the PCI environment (or like environments) and trigger alarms if non-approved assets attempt to communicate to the controlled PCI environment; this also ensures controls are working as expected.
8	Enable automation and integration between products that support this, in order to enhance security and decrease operational burden. As an example, endpoint AMP, NGFW, Network Behavioral Analysis integration with NAC, you can enable powerful integration between these products to realize things such as rapid threat containment.



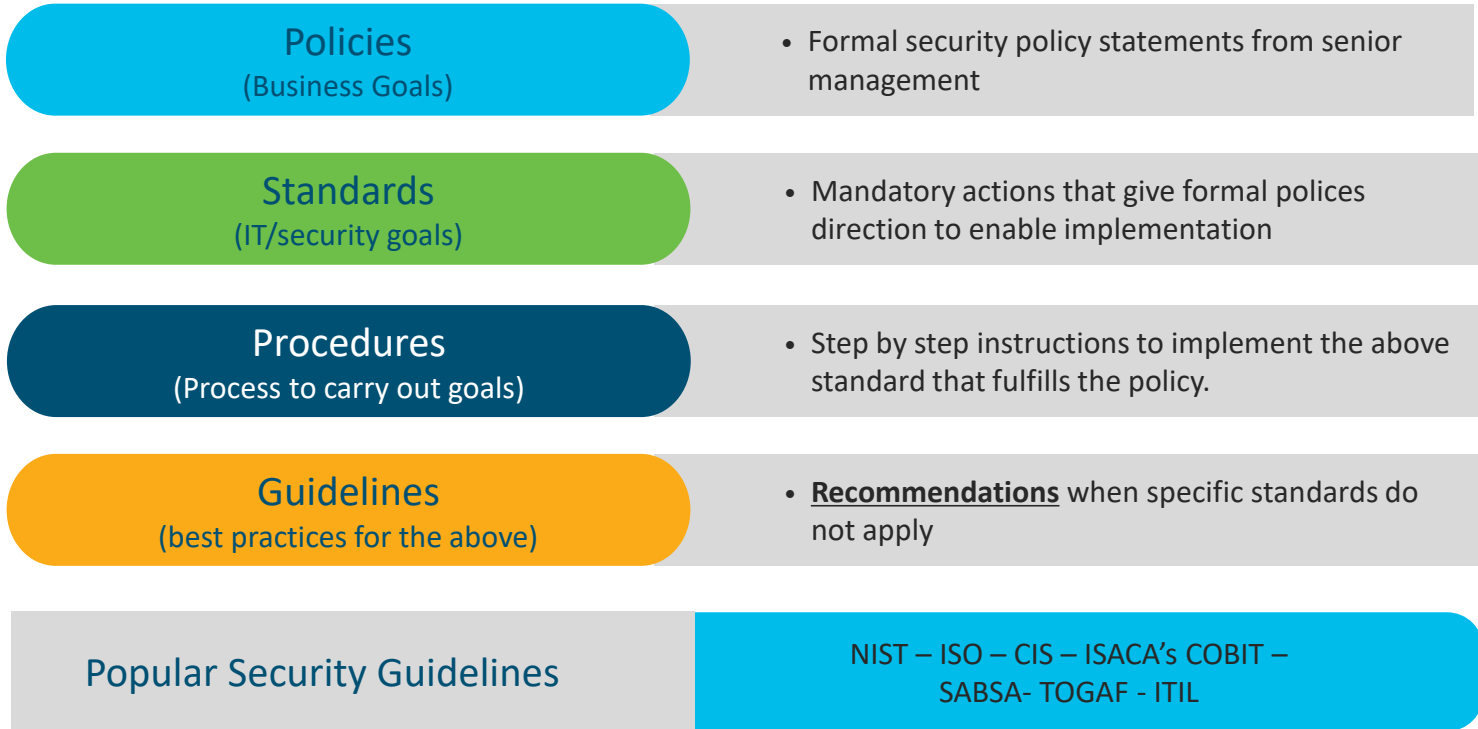
You make the power of data **possible**

Cisco Security and NIST/CIS

Mapping Cisco Security to Security Controls

Security Requirement Basics

Required



What is NIST National Institute of Standards and Technology

- Group within the U.S. Commerce Department.
- Develops cybersecurity standards, guidelines, tests and metrics for protection.

NIST Published framework: **Cybersecurity Framework (CSF)**

- Follows U.S. President's executive order Improving Critical Infrastructure Cybersecurity from 2013.
- NIST CSF has five core functions (next slide)

Five Core NIST CSF Functions

Framework Functions

Identify ID

Organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities

Protect PR

Safeguards that ensure delivery of critical services

Detect DE

Activities that identify the occurrence of a cybersecurity event

Respond RS

Take action regarding a detected cybersecurity incident

Recover RC

Maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity incident



		Tetration	AMP/Threat Grid	Stealthwatch	CloudLock	Web/Email Security	Cognitive Threat Analytics (CTA)	Umbrella	Firepower	Identity Services Engine (ISE)	TrustSec	AnyConnect	Advisory Services	Integration Services	Managed Services
ID	Asset Management	Green		Green	Green				Green	Green				Green	Green
	Business Environment	Non-technical control area											Green		
	Governance	Non-technical control area											Green		
	Risk Assessment	Green					Green		Green					Green	Green
	Risk Mgmt. Strategy	Non-technical control area											Green		
PR	Access Control	Green		Green			Green	Green	Green	Green	Green	Green	Green	Green	Green
	Awareness/Training	Non-technical control area													Green
	Data Security	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green			Green
	Info Protection Process	Non-technical control area											Green		Green
	Maintenance											Green			Green
	Protective Technology	Green	Green						Green	Green	Green	Green			Green
DE	Anomalies and Events	Green	Green	Green	Green	Green	Green	Green					Green	Green	Green
	Continuous Monitoring	Green	Green	Green		Green	Green		Green				Green	Green	Green
	Detection Processes	Non-technical control area													Green
RS	Response Planning	Non-technical control area											Green		Green
	Communications	Non-technical control area											Green		Green
	Analysis	Green	Green	Green	Green	Green	Green	Green	Green					Green	Green
	Mitigation	Green	Green	Green	Green		Green	Green	Green	Green	Green			Green	Green
	Improvements	Non-technical control area											Green		Green
RC	Recovery Planning	Non-technical control area											Green		Green
	Improvements	Non-technical control area													Green
	Communications	Non-technical control area													Green

NIST 800-53

NIST published framework: Recommended Security Controls for Federal Information Systems and Organizations.

Summary: Catalog of security and privacy controls for federal information systems and organizations

Provides a process for selecting controls to protect organizational operations, organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors (both intentional and unintentional).

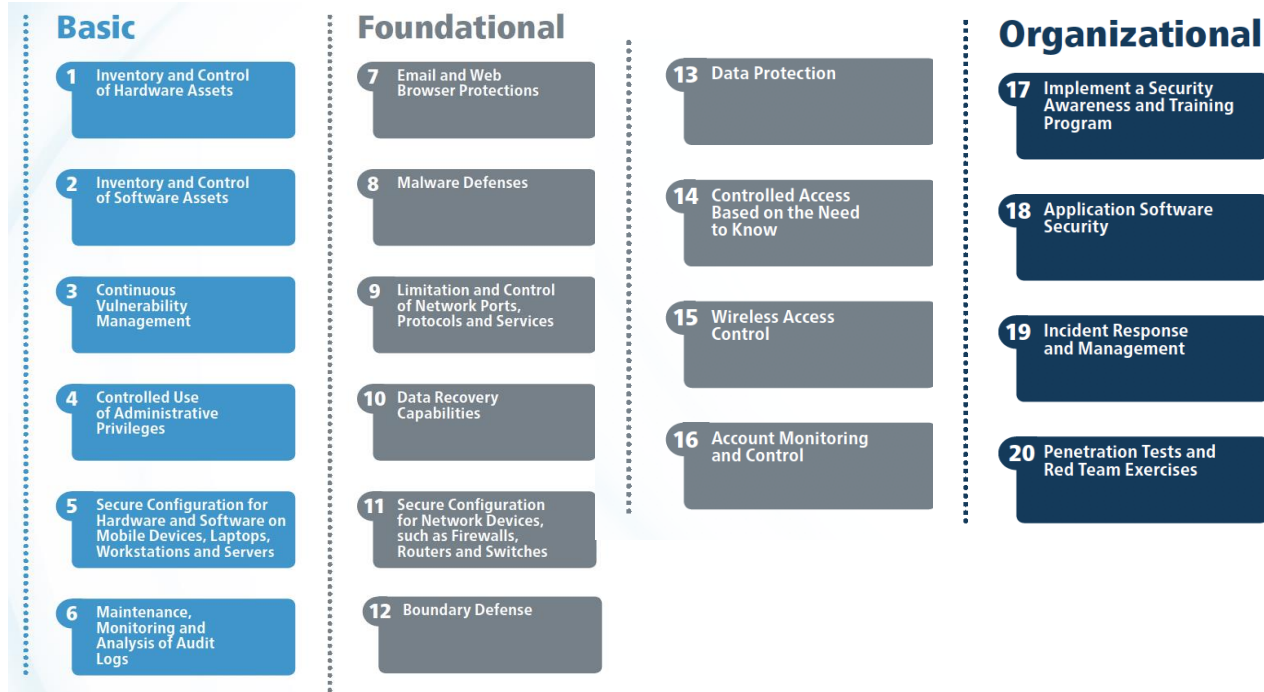
Center for Internet Security CIS

CIS Controls™ and CIS Benchmarks™ are global industry best practices endorsed by leading IT security vendors and governing bodies.

CIS Cyber Security Controls (CSC)

Recommendations for protections using a series of 20 foundational and advanced cybersecurity actions, where the most common attacks can be eliminated.

Center for Internet Security Top 20 Controls



CIS CSC Cisco Alignment Summary by Critical Security Control (CSC)



■ Product fulfills control
 ■ Non-technical control
 ■ Product does not fulfill control

			AMP/Threat Grid	Stealthwatch (with CTA)	Cloudlock	Web/Email Security	Umbrella	ASA/Firepower	Duo	Identity Services Engine (ISE)	TrustSec	AnyConnect	Meraki SM	
Basic	CSC1	Hardware Inventory												
	CSC2	Software Inventory												
	CSC3	Vulnerability Assessment	Cisco Technology Partners											
	CSC4	Admin Privileges Control	Cisco Security Services: non-technical control											
	CSC5	Secure Endpoint Configuration												
	CSC6	Audit Log Analysis	Cisco Technology Partners											
Foundational	CSC7	Email/Web Protections												
	CSC8	Malware Defenses												
	CSC9	Port/Protocol/Service Control												
	CSC10	Data Recovery Capability	Cisco Technology Partners											
	CSC11	Secure Network Configuration	Cisco DNA Network											
	CSC12	Boundary Defense												
	CSC13	Data Protection												
	CSC14	Access controls (least privilege)												
	CSC15	Wireless Access Control	Cisco Wireless Controllers											
	CSC16	Account Monitor/Control												
Organizational	CSC17	Skills Awareness/Training	Cisco Security Services: non-technical control											
	CSC18	Application Security	Cisco Security Services: non-technical control											
	CSC19	Incident Response/Mgmt	Cisco Security Services: non-technical control											
	CSC20	Pen Test / Red Team	Cisco Security Services: non-technical control											

Baseline Cyber Security Controls for Small and Medium Organizations

Mapping Cisco Security to Security Controls



You make the power of data **possible**

Introduction to Baseline Cyber Security Controls

The Problem

Small and medium sized organizations will face a cyber threat at some point causing financial or privacy impact.

Canadian businesses are at risk of a cyber threat compromising data about customers, partners and suppliers, financial and payment systems, and intellectual and proprietary information.

Cyber threats cause a wide range of damage to Canadian businesses which include reputational damage, productivity loss, intellectual property theft, operational disruptions, and recovery expenses.

Following traditional cyber security frameworks (NIST Cyber Security Framework or ISO/IEC 27001:2013) can be expensive to implement for small to medium sized businesses

Introduction to Baseline Cyber Security Controls

The Solution

The Canadian government believes that organizations can mitigate most cyber threats through awareness and best practices in cyber security and business continuity. As such, the Canadian government believes we can successfully apply the 80/20 rule (achieve 80% of the benefit from 20% of the effort) in the domain of cyber security and achieve concrete gains for the cyber security of Canadians

The goal is to implement as many of these baseline controls as possible. Please note that your business may require additional controls that go beyond what is outlined within this document.

Cisco Security and Baseline Security Controls

The Cisco Security Value

Cisco security experts have reviewed the baseline controls and aligned them to Cisco security products and services to either meet the control fully or provide a supporting role.

The purpose of aligning the baseline control with a product and/or services from Cisco is to simplify vendor relationships, increase security effectiveness, improve integration and support, and provide a cost effective consumption model.

Cisco Security Products

Baseline Cyber Security Controls for SMB → Cisco Mappings



Product or Service meets or supports the control



Non-technical control



Product or service not required to fulfill the control



No capability

	AMP/ Threat Grid	Stealthwatch (with Cognitive)	Cloudlock	Web/Email	Umbrella	Firepower / Maraki	ISE/ Trustsec	Duo	AnyConnect	Meraki SM	Cisco Threat Response	Cisco Services
3.1 Develop an IR Plan	Non Technical Control (1*)											BC 1,1, 1.2, 1.3
3.2 Auto Patch OS and Applications	BC2.1(2*)	BC2.1(2*)	BC2.1(2*)	BC2.1(2*)	BC2.1(2*)	BC2.1(2*)	BC2.1(2*)	BC2.1(2*)	BC2.1(2*)	BC2.1(2*)	BC2.1(2*)	BC 2.2
3.3 Enable Security Software	BC 3.1	Product or services not required to fulfill the control										
3.4 Securely Configure Devices	BC 4.1	BC 4.1	BC 4.1	BC 4.1	BC 4.1	BC 4.1	BC 4.1	BC 4.1	BC 4.1	BC 4.1	BC 4.1	
3.5 Use Strong User Auth								BC 5.1				
3.6 Provide Emp Awareness Training	Non Technical Control							BC6.1	Non Technical Control			BC6.1
3.7 Backup and Encrypt Data	BC7.1, 7.2 (3*)	BC7.1, 7.2 (3*)	BC7.1, 7.2 (3*)	BC7.1, 7.2 (3*)	BC7.1, 7.2 (3*)	BC7.1, 7.2 (3*)	BC7.1, 7.2 (3*)	BC7.1, 7.2 (3*)	BC7.1, 7.2 (3*)	BC7.1, 7.2 (3*)	BC7.1, 7.2 (3*)	
3.8 Secure Mobility						BC8.6	BC8.6		BC8.6	BC8.3,8.4,8.5,8.6		
3.9 Establish Basic Perimeter Defences			BC9.7	BC9.7	BC9.2,9.6	BC9.1,9.4,9.6	BC9.3,9.5,9.6	BC9.4	BC9.3			
3.10 Secure Cloud and Outsourced IT Services						BC10.4		BC10.5	BC10.4	BC10.4		
3.11 Secure Websites	BC11.1(4*)	BC11.1(4*)				BC11.1(4*)		BC11.1(4*)				BC11.1
3.12 Implement Access Control and Authorization	BC12.1,12.2	BC12.1,12.2	BC12.1,12.2	BC12.1,12.2	BC12.1,12.2	BC12.1,12.2	BC12.1,2,3	BC12.1,12.2	BC12.1,12.2	BC12.1,12.2	BC12.1,12.2	
3.13 Secure Portable Media	No Capability	No Capability	No Capability	No Capability	No Capability	No Capability	No Capability	No Capability	No Capability	No Capability	No Capability	

Review supporting slides

- (1*) Cisco Security products can be supportive during incident and response and send logging data to information and event monitoring systems (BC1.4).
- (2*) Cisco Security products can support patching helping achieve. Cisco Security products can asset with identifying vulnerable software and enable controls to mitigate the risk. (BC 2.1)
- (3*) Products support backup and restore and can be stored on external encrypted disks (BC 7.2)
- (4*) Cisco security helps address web security with the following capabilities Firepower (NGIPs, NGFW, WAF), Endpoint AMP, DUO (2FA), Stealthwatch (BC11.1)

3.1 Develop an Incident Response Plan

Base Control

- **BC.1.1** Organizations should have a basic plan for how to respond to incidents of varying severity. If an organization is unable to manage some types of incidents on its own, the organization should have a plan for what it will do.
- **BC.1.2** Organizations should have a written incident response plan that details who is responsible for handling incidents including any relevant contact information for communicating to external parties, stakeholders and regulators. Organizations should have an up-to-date hard copy version of this plan available for situations where soft copies are not available.
- **BC.1.3** Organizations should consider purchasing a cyber security insurance policy that includes coverage for incident response and recovery activities.
- **BC.1.4** Organizations should consider implementing a monitoring capability (e.g. a security information and event management system) or document why they decided not to.

Cisco Addressing Capabilities

- **BC 1.1, 1.2** - Cisco IR services <https://www.cisco.com/c/en/us/products/security/sas-incident-response.html>
- **BC 1.3** - Cisco program around cyber security insurance <https://www.cisco.com/c/en/us/solutions/security/cyber-insurance/index.html#~:stickynav=1>
- **BC 1.4** – Note: we do not provide the SIEM but Cisco security products can send logging to information and monitoring systems

3.2 Auto Patch OS and Applications

Base Control

- **BC.2.1** Organizations should enable automatic patching for all software and hardware OR establish full vulnerability and patch management solutions.
- **BC.2.2** Organizations should conduct risk assessment activities as to whether to replace any software and hardware that are not capable of automatic updates. If the organization chooses to keep such devices, they should have a business process to ensure regular manual updates.

Cisco Addressing Capabilities

- **BC 2.1-** Cisco Security products can support patching helping achieve this guideline – Cloud based technologies further reduces the effort as this is managed by Cisco. Cisco Security products can assist with identifying vulnerable software and enable controls to mitigate the risk. Technologies supporting identification of vulnerabilities include endpoint AMP, Firepower (passively), and DUO. Controls in place may include Firepower preventing asset from communicating, endpoint AMP blocking vulnerable software, DUO blocking access to system based on vulnerable software.
- **BC 2.2 -** Cisco provides assessments – this includes risk management assessment services (ex: Vulnerability, patch, change, and asset management) and security infrastructure assessments (Inc. perform gap analysis). Scoping is required to ensure services aligns with outcomes desired.

3.3 Enable Security Software

Base Control

- **BC.3.1** Organizations should enable anti-malware solutions that update and scan automatically

Cisco Addressing Capabilities

- **BC 3.1** - Cisco Endpoint AMP can provide advanced malware protection

3.4 Securely Configure Devices

Base Control

- **BC.4.1** Organizations should implement secure configurations for all their devices changing all default passwords, turning off unnecessary features, and enabling all relevant security features.

Cisco Addressing Capabilities

- **BC 4.1** – All Cisco products have the ability to change default password, hardened in regards to unnecessary services and security. This includes both on-premise and cloud.

3.5 Use Strong User Authentication

Base Control

- **BC.5.1** Organizations should implement two-factor authentication wherever possible, and document all instances where they make the business decision not to do so. Organizations should require two-factor authentication for important accounts such as financial accounts, system administrators, cloud administration, privileged users, and senior executives.
- **BC.5.2** Organizations should only enforce password changes on suspicion or evidence of compromise.
- **BC.5.3** Organizations should have clear policies on password length and reuse, the use of password managers and if, when, and how users can physically write down and securely store a password.

Cisco Addressing Capabilities

- **BC 5.1** - Cisco DUO provides 2FA
-

3.6 Provide Employee Awareness Training

Base Control

- **BC.6.1** Organizations should invest in cyber security awareness and training for their employees.

Cisco Addressing Capabilities

- **BC 6.1** –Cisco DUO can provide phishing education and awareness campaigns. Cisco also provides Awareness and education under risk management assessment services
-

3.7 Backup and Encrypt Data

Base Control

- **BC.7.1** Organizations should backup systems that contain essential business information, and ensure that recovery mechanisms effectively and efficiently restore these systems from backups. Organizations should consider storing backups at a secure offsite location.
- **BC.7.2** Organizations should securely store backups in an encrypted state, and restrict access to them to those who must access them for the testing or use of restoration activities.

Cisco Addressing Capabilities

- **BC 7.1** – Cisco Products support backup and restore and can be stored (Indirectly supporting the baseline control)
- **BC 7.2** – Cisco Backups can be stored on encrypted media (Indirectly supporting the baseline control)

3.8 Secure Mobility

Base Control

- **BC.8.1** Organizations should decide on an ownership model for mobile devices and document the rationale and associated risks.
- **BC.8.2** Organizations should enforce separation between work and personal data on mobile devices with access to corporate IT resources, and document the details of this separation.
- **BC.8.3** Organizations should ensure that employees only download mobile device apps from the organization's list of trusted sources.
- **BC.8.4** Organizations should require that all mobile devices store all sensitive information in a secure, encrypted state.
- **BC.8.5** Organizations should implement an enterprise mobility management solution for all mobile devices OR document the risks assumed to the audit, management, and security functionality of mobile devices by not implementing such a solution.
- **BC.8.6** Organizations should enforce or educate users to: (1) disable automatic connections to open networks, (2) avoid connecting to unknown Wi-Fi networks, (3) limit the use of Bluetooth and NFC for the exchange of sensitive information, and (4) use corporate Wi-Fi or cellular data network connectivity rather than public Wi-Fi.

Cisco Addressing Capabilities

BC 8.3 – Meraki SM can have a whitelist of apps (with trusted installation locations) and if the device has something outside of that list then you can make the device non-compliant and they can't access the network. If the company has ownership of the device then they can actually prevent the installation of the app or remove it as well.

BC 8.4 - Meraki SM can force encryption on the device. This is systemwide so you really can't pick and choose the data but encrypt the entire device.

BC 8.5 –Meraki SM provides enterprise mobility management (EMM)

BC 8.6 –Meraki SM can do some of this through policy but it is device dependent and whether in supervisory mode. (1) Meraki SM can disable automatic connections to open networks and (2) avoid connecting to unknown Wi-Fi networks. (3) can be done BUT there will some usability issues with the device if the end user wants to use Bluetooth and we start playing around with it. (4) an be done but usually we leave it up to the device to decide which is the best network to use. You can do some things like geofencing where you can force a specific wireless to be used in a specific area but it is a management nightmare. Also (1) Cisco Anyconnect and Firepower can limit the risk of connecting to open networks by enforcing always-on VPN connection. This ensures all communications is secured and encrypted over the open network. (4) Cisco ISE can prevent corporate users from connecting to public (guest) wifi connections.

3.9 Establish Basic Perimeter Defences

Base Control

- **BC.9.1** Organizations should have a dedicated firewall at the boundaries between its corporate network and the Internet.
- **BC.9.2** Organizations should implement a DNS firewall for outbound DNS requests to the Internet.
- **BC.9.3** Organizations should activate any software firewalls included on devices within their networks or document the alternative measures in place instead of these firewalls.
- **BC 9.4** Organizations should require secure connectivity to all corporate IT resources, and require VPN connectivity with two-factor authentication for all remote access into corporate networks.
- **BC 9.5** Organizations should only use secure Wi-Fi, preferably WPA2-Enterprise. BC.9.6 Organizations should never connect public Wi-Fi networks to their corporate networks.
- **BC 9.6** Organizations should follow the Payment Card Industry Data Security Standard (PCI DSS) for all point-of-sale terminals and financial systems and further isolate these systems from the Internet.
- **BC 9.7** Organizations should ensure the implementation of DMARC on all of the organization's email services.

Cisco Addressing Capabilities

- **BC 9.1** - Cisco Firepower or Meraki can provide advanced Firewalling capabilities
- **BC 9.2** – Cisco Umbrella provides DNS protection for recursive lookup
- **BC 9.3** – Cisco ISE/Anyconnect support posturing can ensure that assets have firewalling enabled before connecting to the network
- **BC 9.4** – Cisco ASA, Firepower, and Meraki can provide RA-VPN, DUO can provide 2FA
- **BC 9.5** – Cisco ISE can enforce this setting for corporate wifi and restrict access to guest connections
- **BC 9.6** – Cisco ISE can provide segmentation control and Cisco Firepower or Meraki and Umbrella can restrict access outbound to the internet.
- **BC 9.7** – Cisco Email Security provides robust security measures for email including DMARC

3.10 Secure Cloud and Outsourced IT Services

Base Control

- **BC.10.1** Organizations should require that all their cloud service providers share an SSAE 16 SOC 3 report that states that they achieved Trust Service Principles compliance.
- **BC.10.2** Organizations should evaluate their comfort level with how their outsourced IT providers handle and access their sensitive information.
- **BC.10.3** Organizations should evaluate their comfort level with the legal jurisdictions where their outsourced providers store or use their sensitive information.
- **BC.10.4** Organizations should ensure that their IT infrastructure and users communicate securely with all cloud services and applications.
- **BC.10.5** Organizations should ensure that administrative accounts for cloud services use two-factor authentication and differ from internal administrator accounts.

Cisco Addressing Capabilities

- **BC 10.4** – Cisco cloud based services leverage secured channels such as TLS or Firepower can provide the secured VPN channel to cloud based datacenters (S2S or RA VPN).
- **BC 10.5** – Cisco DUO provides 2FA

3.11 Secure Websites

Base Control

- **BC.11.1** Organizations should ensure that their websites meet the OWASP ASVS guidelines.

Cisco Addressing Capabilities

- **BC 11.1** –Cisco security helps address web security with the following capabilities Firepower (NGIPs, NGFW, WAF), Endpoint AMP, DUO (2FA), Stealthwatch (Indirectly supporting the baseline control). Note: Cisco provides assessments – this includes risk management assessment services (ex: Vulnerability, patch, change, and asset management) and security infrastructure assessments (Inc. perform gap analysis). Scoping is required to ensure services aligns with outcomes desired. (check out comment on BC 2.2 – need to engage services)

3.12 Implement Access Control and Authorization

Base Control

- **BC.12.1** Organizations should provision accounts with the minimum functionality necessary for tasks and in particular should restrict administrator privileges to an as-required basis. Organizations should remove accounts and/or functionality when employees no longer require these for their tasks.
- **BC.12.2** Organizations should only permit administrator accounts to perform administrative activities (and not user-level activities such as accessing email or browsing the web).
- **BC.12.3** Organizations should consider the implementation of a centralized authorization control system

Cisco Addressing Capabilities

BC 12.1 – Cisco products support the use of least privilege and support RBAC

BC 12.2 – Cisco product support restricted access and user level activities such as accessing email or browsing the web is not available within the technologies being offered.

BC 12.3 – Cisco ISE can support Radius and TACACS for central authorization control

3.13 Secure Portable Media

Base Control

- **BC.13.1** Organizations should mandate the sole use of organization-owned secure portable media, have strong asset controls for these devices, and require the use of encryption on all of these devices.
- **BC.13.2** Organizations should have processes for the sanitization or destruction of portable media prior to disposal.

Cisco Addressing Capabilities

No Cisco capabilities today

Cisco Product Summary

Cisco Product	Baseline Controls
AMP / Threatgrid	BC 2.1, 3.1, 4.1, 7.1, 7.2, 11.1, 12.1, 12.2
Stealthwatch (with Cognitive)	BC 2.1, 4.1, 7.1, 7.2, 11.1, 12.1, 12.2
Cloud Lock	BC 2.1, 4.1, 7.1, 7.2, 9.7, 12.1, 12.2
Web / Email	BC 2.1, 4.1, 7.1, 7.2, 9.7,12.1, 12.2
Umbrella	BC 2.1, 4.1, 7.1, 7.2, 9.2, 9.6, 12.1, 12.2
Firepower / Meraki MX	BC 2.1, 4.1, 7.1, 7.2, 8.6, 9.1, 9.4, 9.6, 10.4, 11.1, 12.1, 12.2
ISE / Trustsec	BC 2.1, 4.1, 7.1, 7.2, 8.6, 9.3, 9.5, 9.6, 12.1, 12.2
DUO	BC 2.1, 4.1, 7.1, 7.2, 8.6, 9.4, 10.5, 11.1, 12.1, 12.2
Anyconnect	BC 2.1, 4.1, 7.1, 7.2, 8.6, 9.3, 10.4, 12.1, 12.2
Meraki SM	BC 2.1, 4.1, 7.1, 7.2, 8.3, 8.4, 8.5, 8.6, 10.4, 12.1, 12.2
Cisco Threat Response	BC 2.1, 4.1, 7.1, 7.2, 12.1, 12.2

Note: ensure to work with a qualified Cisco Cyber Security Engineer as some technologies are complementary while others may overlap. Cisco security solutions either meet or provide supportive capabilities of the baseline control.

Cisco Services Example

Security risk management assessment services:

- Perform analysis of areas that may include, where relevant:
 - Information security governance and oversight.
 - Information security policies, standards, and procedures.
 - Information classification and handling.
 - Compliance processes.
 - Risk assessment and management.
 - Enterprise security architecture.
 - Security metrics, measurement, and performance management.
 - Awareness and education.
 - Vulnerability, patch, change, and asset management.
 - Security monitoring and instrumentation.
 - Incident management.
 - Software acquisition, development, and maintenance.
 - System resiliency and disaster recovery.
 - Third-party risk management.
 - Identity and access management.
 - Human resources security.
 - Physical and environmental security.
 - Network security.
 - System security.
 - Data security and encryption.
 - Mobile devices and media security.
 - Malicious code protection

Security Infrastructure Assessment Services:

- Perform gap analysis of key secure network components, such as:
 - Identity and access management.
 - Key management system.
 - Multi-factor authentication.
 - Secure remote access (such as VPN).
 - Network access control.
 - Wireless security configuration and appliances.
 - Network intrusion prevention systems.
 - Mobile device management.
 - Data leakage prevention.
 - Application layer gateways (e.g., web and e-mail gateways).
 - Endpoint protection.
 - Security and information event management.
 - File integrity monitoring.
 - Availability monitoring.
 - Load-balancing, high availability, and virtualization.
 - DDoS protection.
 - Network segmentation.
 - System backup.
 - Incident response.
 - System inventory.
 - System provisioning.
 - Patch management.
 - Configuration management.
 - Change management.
 - Vulnerability management.

