Beyond the Pandemic

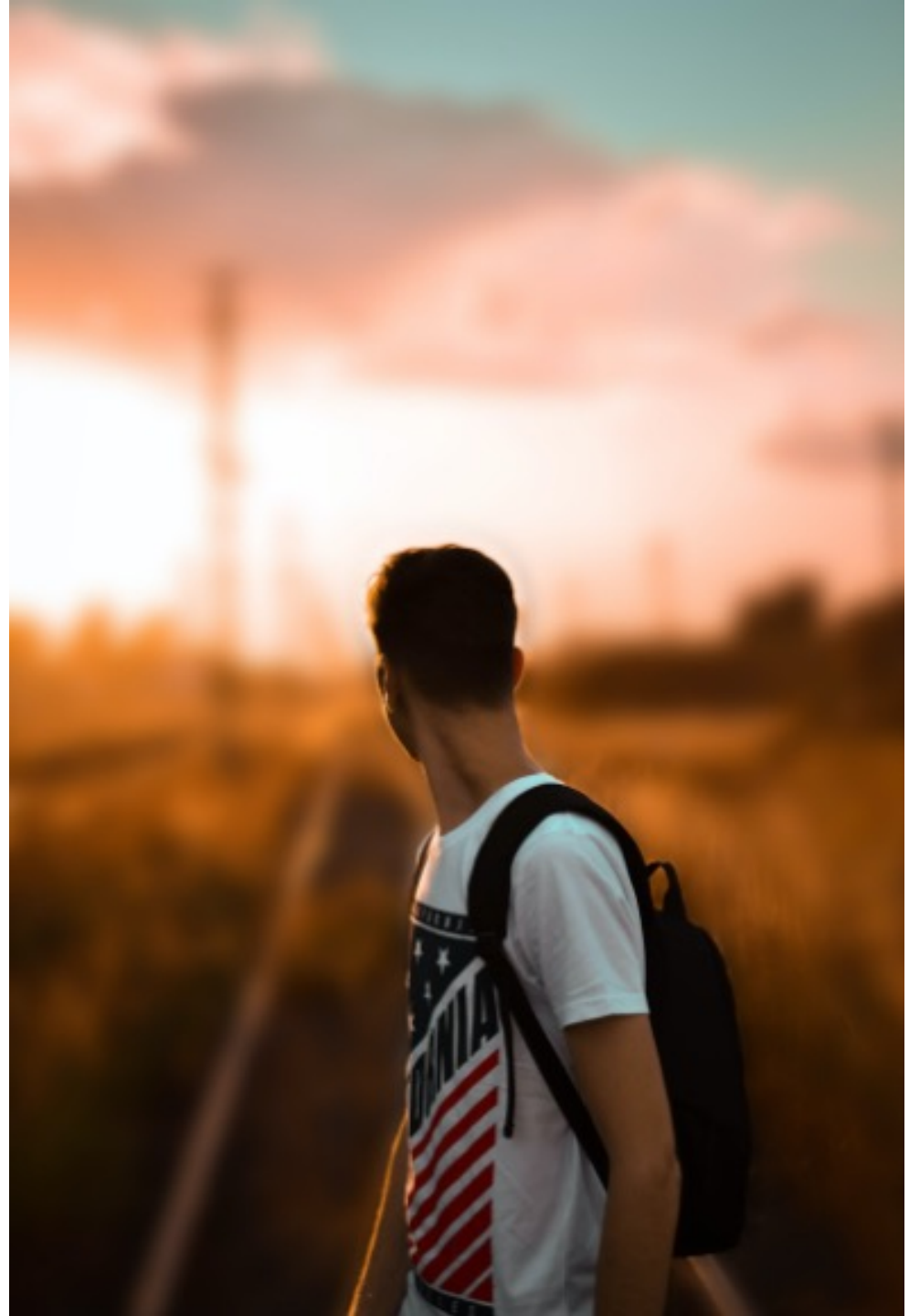
How The Pandemic Shaped Organizations and Their Security Architecture

Dan Han

Virginia Commonwealth University

A little about me

- Grew up in RVA
- Served as the CISO for VCU since 2011
- Worked in IT and information security for over 20 years now
- Technophile who loves gadgets, coding, and technology overall



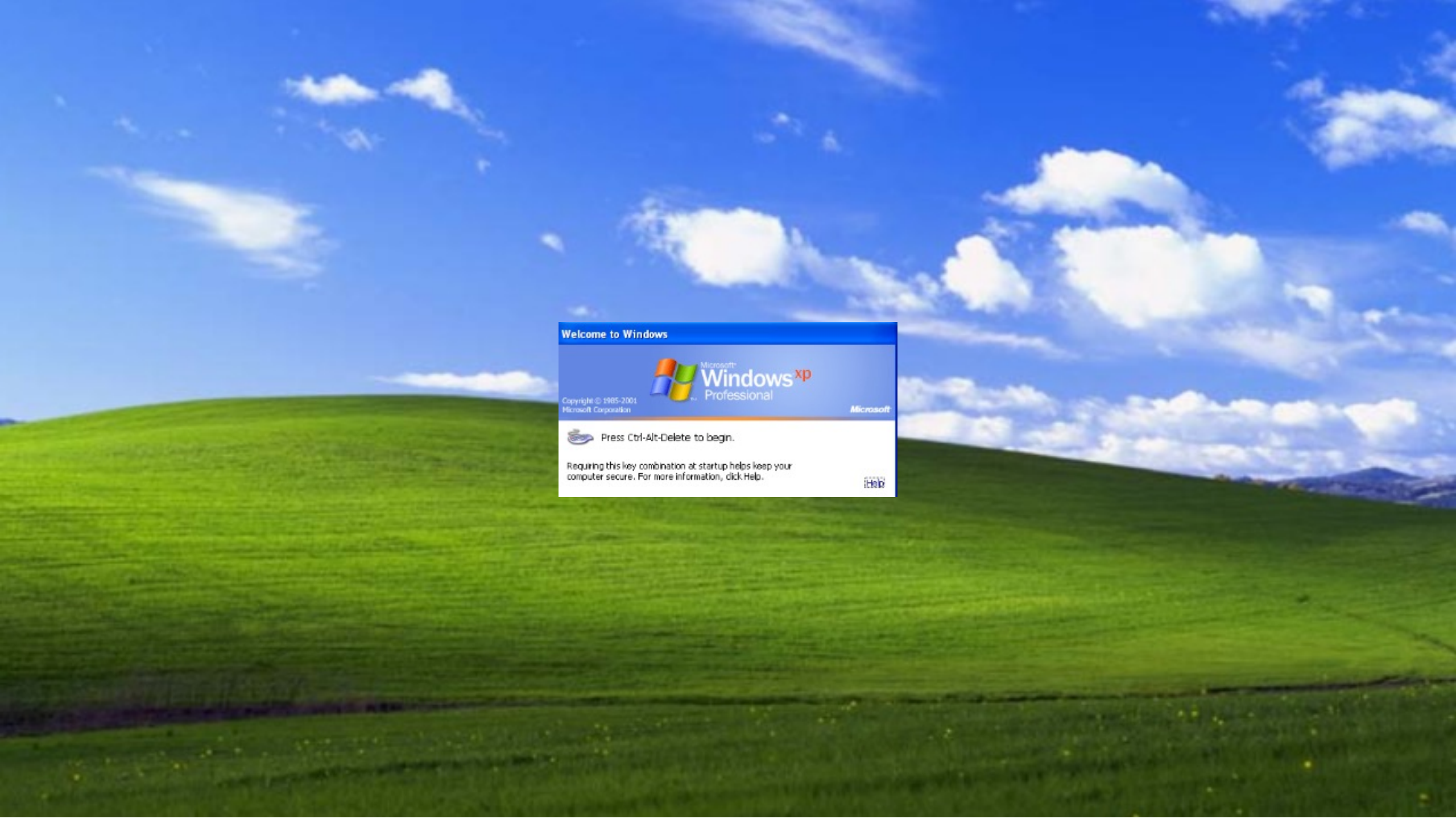
20 Years ago…


Playlists
Favorites
Monday Morning
Party Mix
Road Trip
Top 5 Break-Up Songs
Workout Tunes
menu


WIKIPEDIA
The Free Encyclopedia


ADSL
Ethernet


Sony Ericsson
Sony Ericsson


Welcome to Windows
Microsoft
Windows xp
Professional
Copyright © 1985-2001
Microsoft Corporation
Microsoft
Press Ctrl-Alt-Delete to begin.
Requiring this key combination at startup helps keep your
computer secure. For more information, click Help.
Help

A problem has been detected and Windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

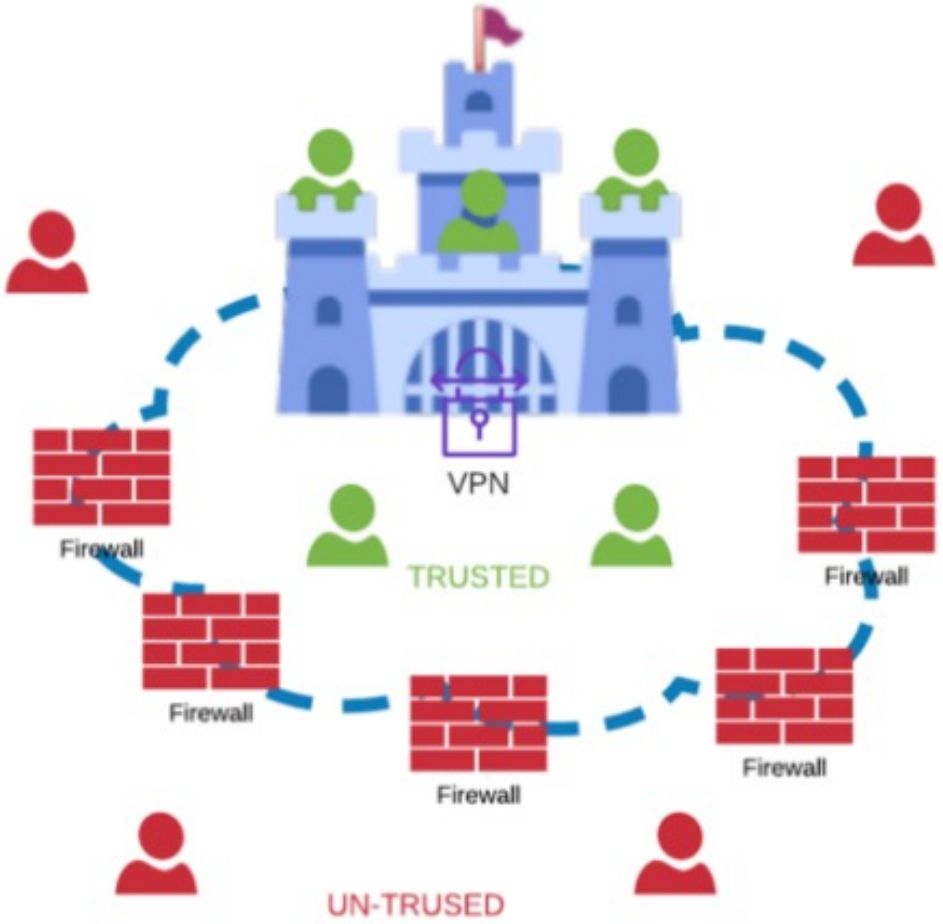
*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c


4210 ½ GRA
4210 ½ GRA

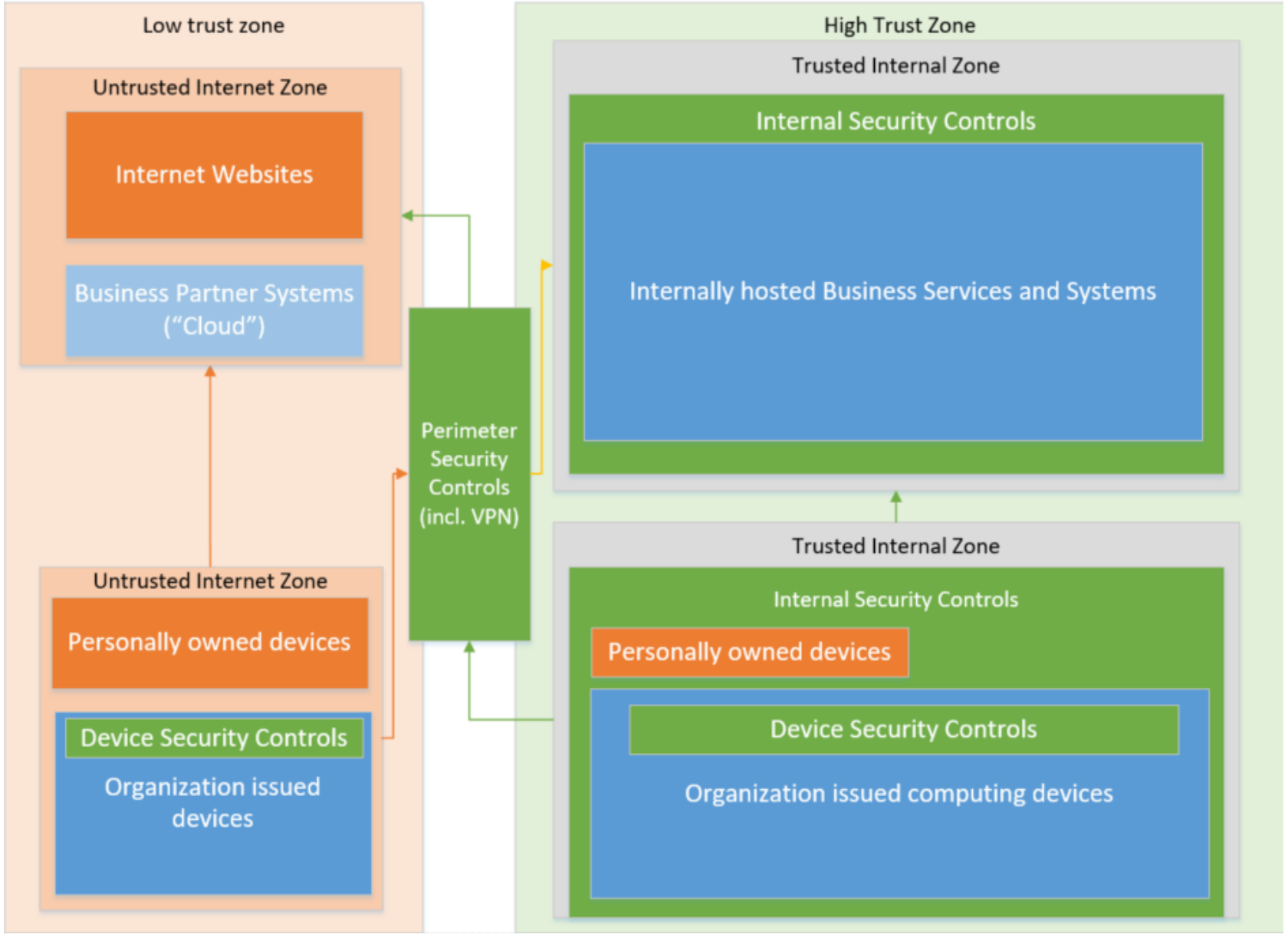
Before 2010

- Aside from the policies and procedures, we focused on
  - Antivirus
  - SPI Firewalls
  - IDS/IPS on plaintext traffic
  - QoS throttling
  - Some configuration management
  - VPNs
  - Saying “No” to users

For the most part, we spent the 2000's building moats around our castle



The IT environment from 2000 - 2010



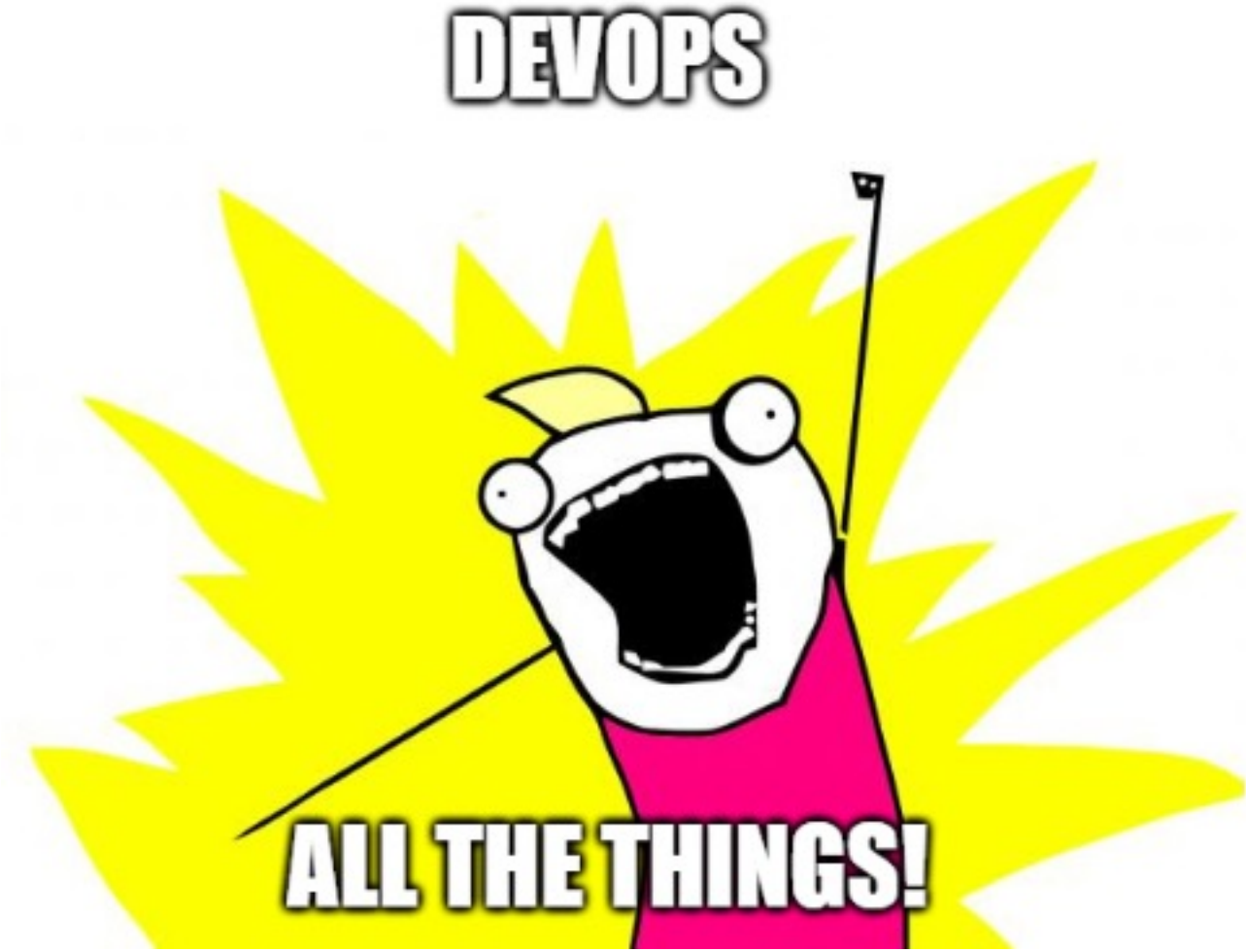
Early 2010s


SECURITY

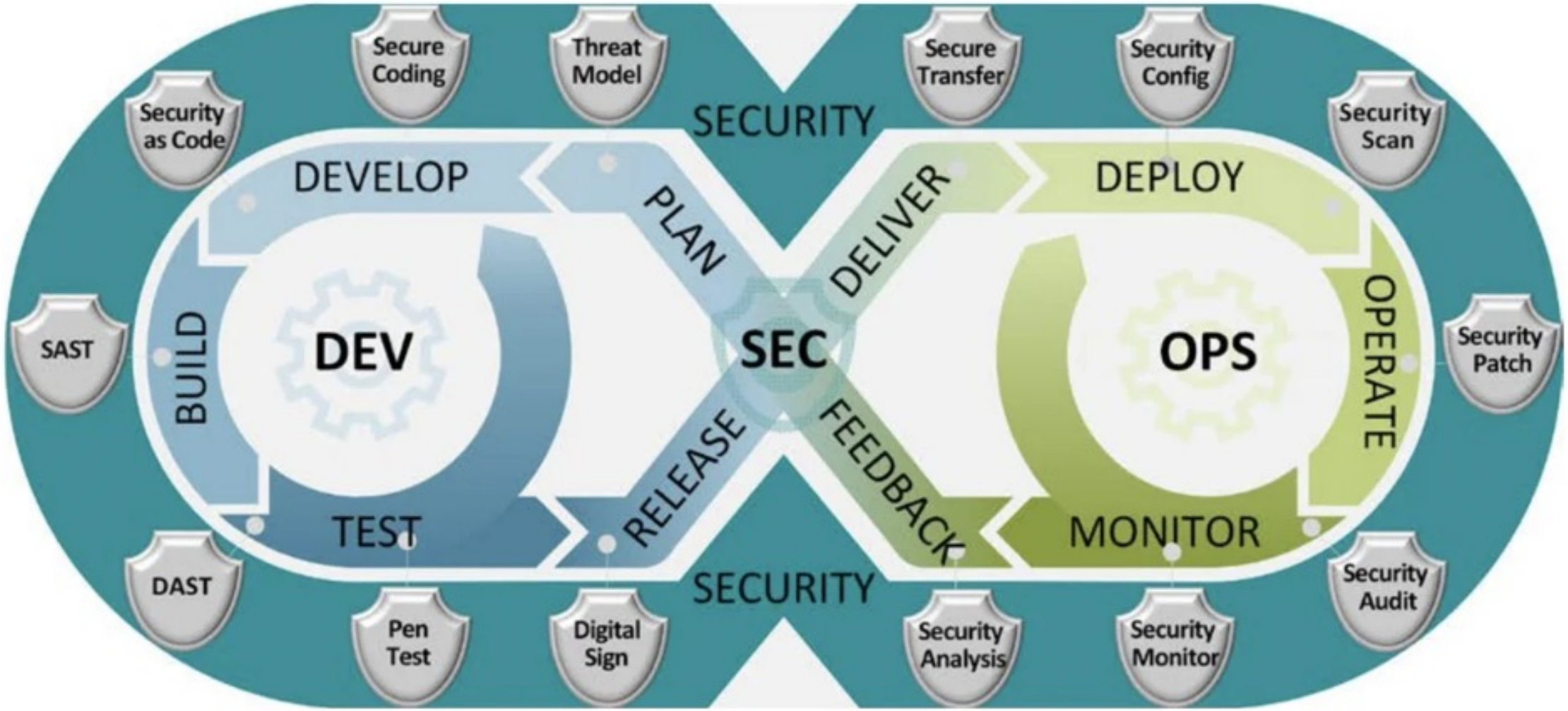
As such…

- The additional focus of security in the past 10 years
  - Mobile Device Management
  - Third-Party Risk Assessments
  - Enterprise Governance, Risk, and Compliance platforms
  - Advanced SIEM with UEBA
  - Layer 7 Firewalls with SSL/TLS inspection
  - Web App and workload protection
  - Cloud Access Service Brokers
  - Data Loss Prevention technologies

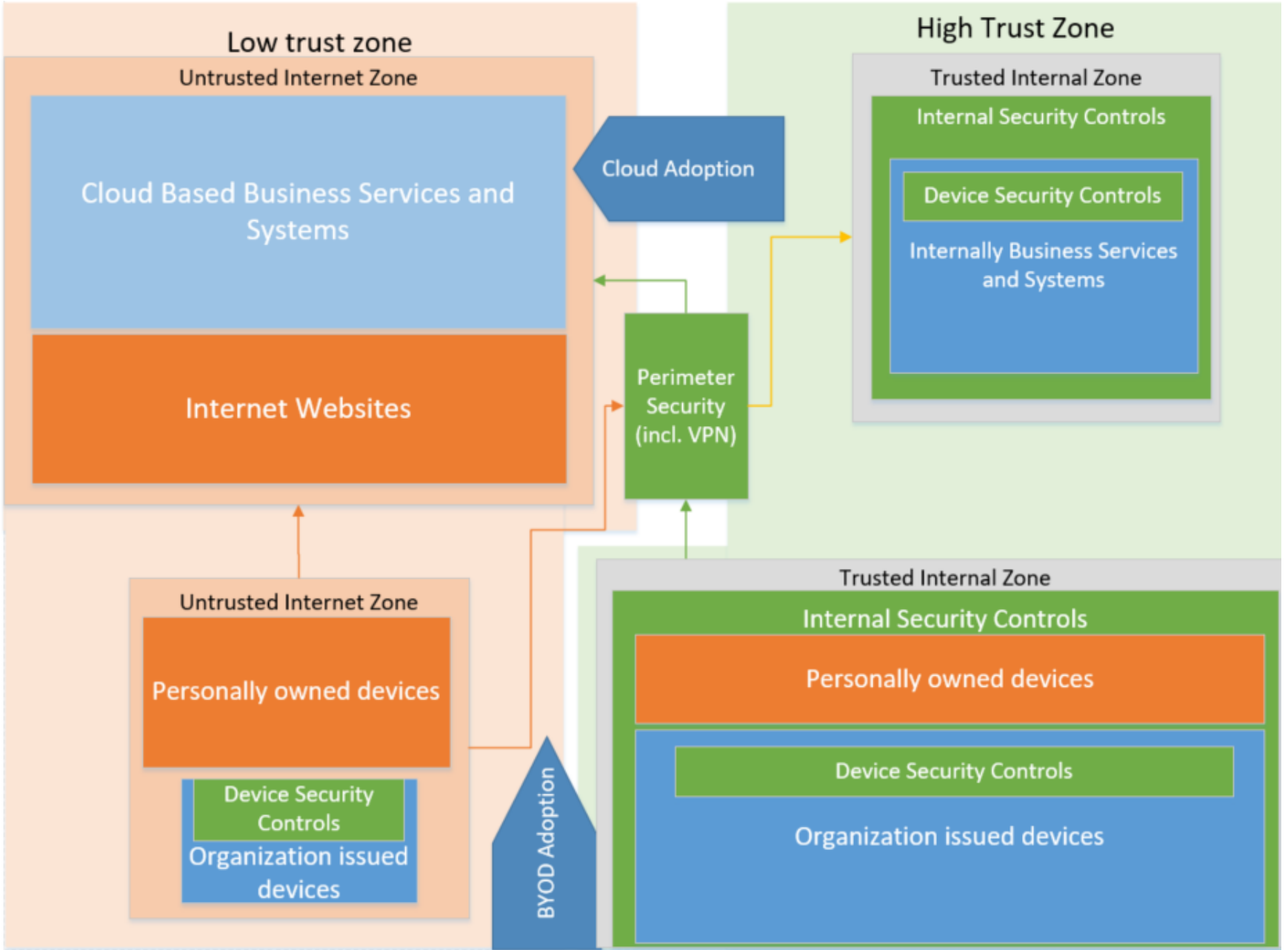
Mid-2010s



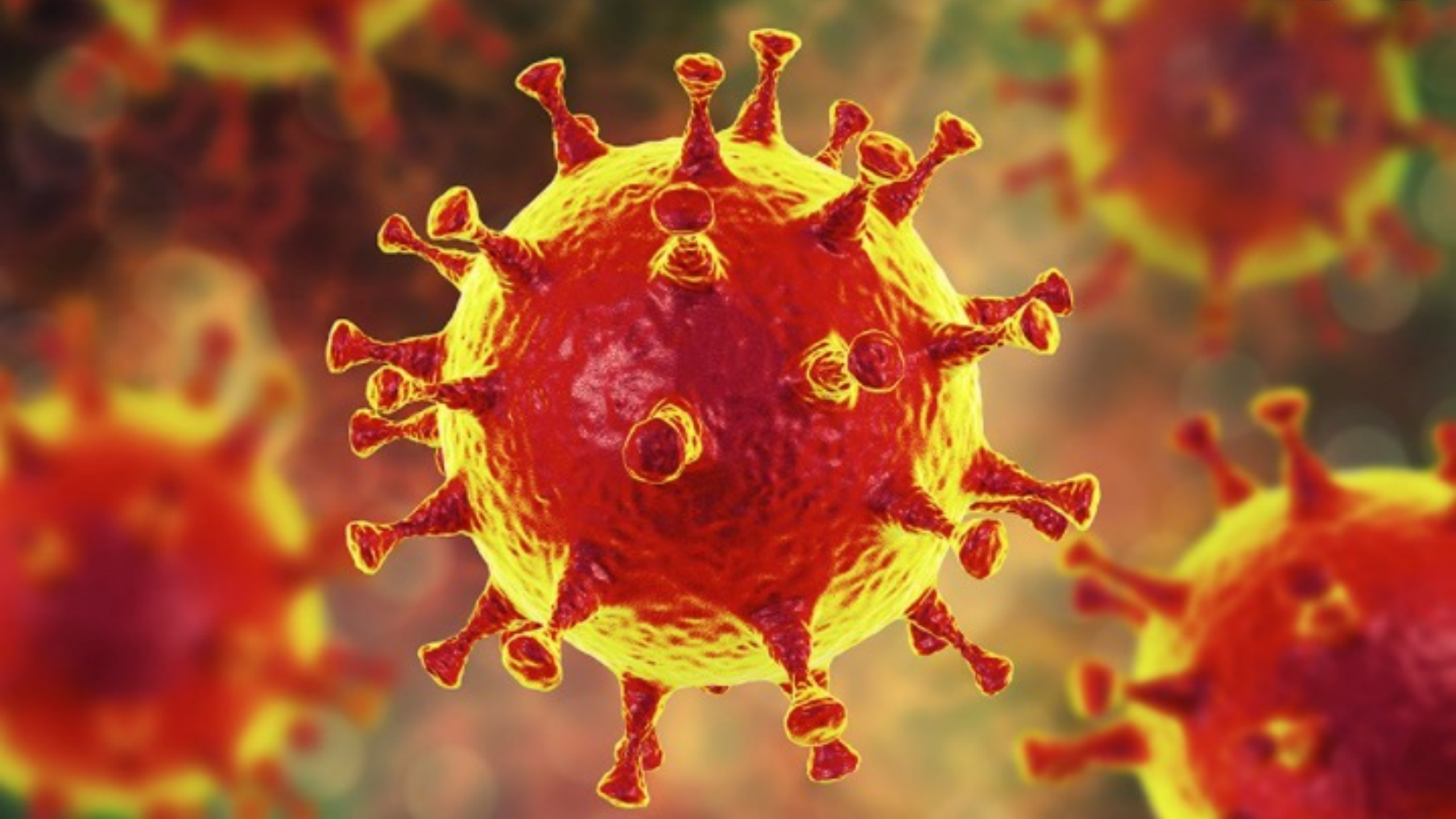

SECURITY


Secure Coding
Threat Model
Secure Transfer
Security Config
Security as Code
SECURITY
Security Scan
DEVELOP
PLAN
DELIVER
DEPLOY
SAST
BUILD
DEV
SEC
OPS
OPERATE
Security Patch
RELEASE
FEEDBACK
TEST
MONITOR
DAST
SECURITY
Security Audit
Pen Test
Digital Sign
Security Analysis
Security Monitor

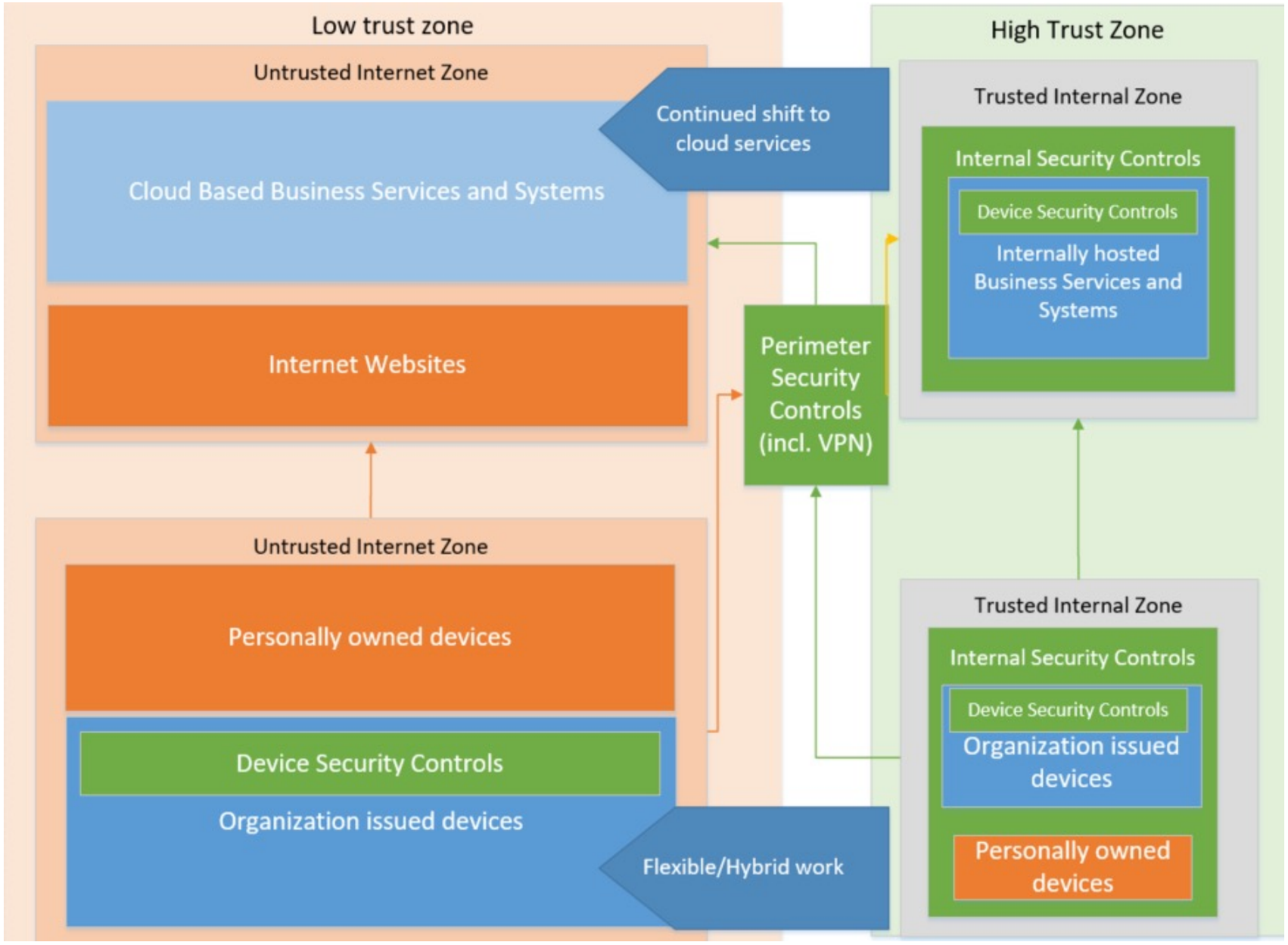
The IT environment from 2010 - 2020



And then, between late 2019 to early 2020…



The IT environment from 2020 on…



Pandemic came and then what?

- Remote work
- Off-site equipment

- Where are our assets?
- Can we manage them remotely?
- Hostile adjacent devices
- Unknown users
- r/Overemployed

LastPass Hack: Engineer's Failure to Update Plex Software Led to Massive Data Breach

Mar 07, 2023 Ravie Lakshmanan

The massive breach at LastPass was the result of one of its engineers failing to update Plex on their home computer, in what's a sobering reminder of the dangers of failing to keep software up-to-date.

Stop using your work laptop or phone for personal stuff, because I know you are

A former IT pro turned end user explains why blending your work and personal tech was, is and always will be a bad idea for you and your employer.

Will remote/hybrid work really go away?

Organizations must again change and adapt

- Work from anywhere
- Work at any time
- Work from any device

Anywhere

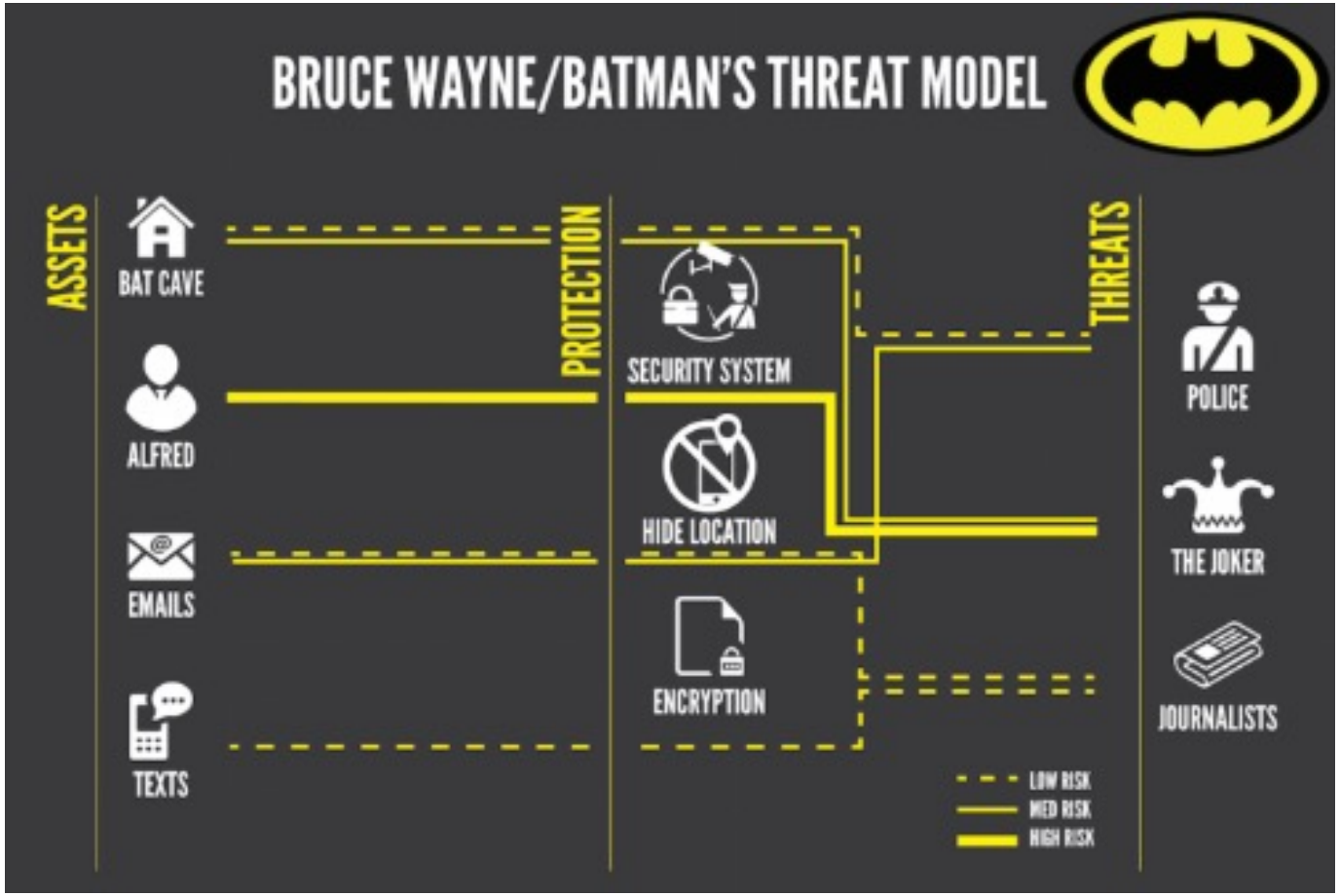
Anytime

Ease

Secure

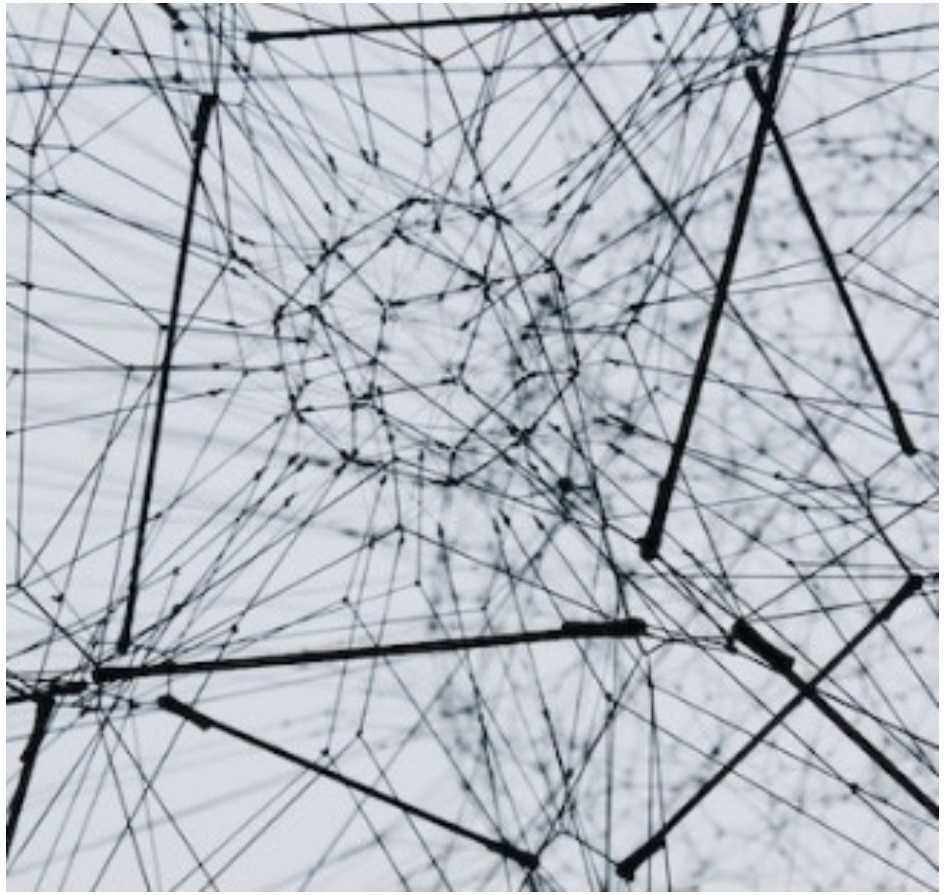
Back to the basics

- What do we need to protect?
- How do the transactions work?
- Who are our adversaries?
- What are their TTPs?
- Have we classified our assets?
- Have we mapped our data flow?
- How about threat modeling?



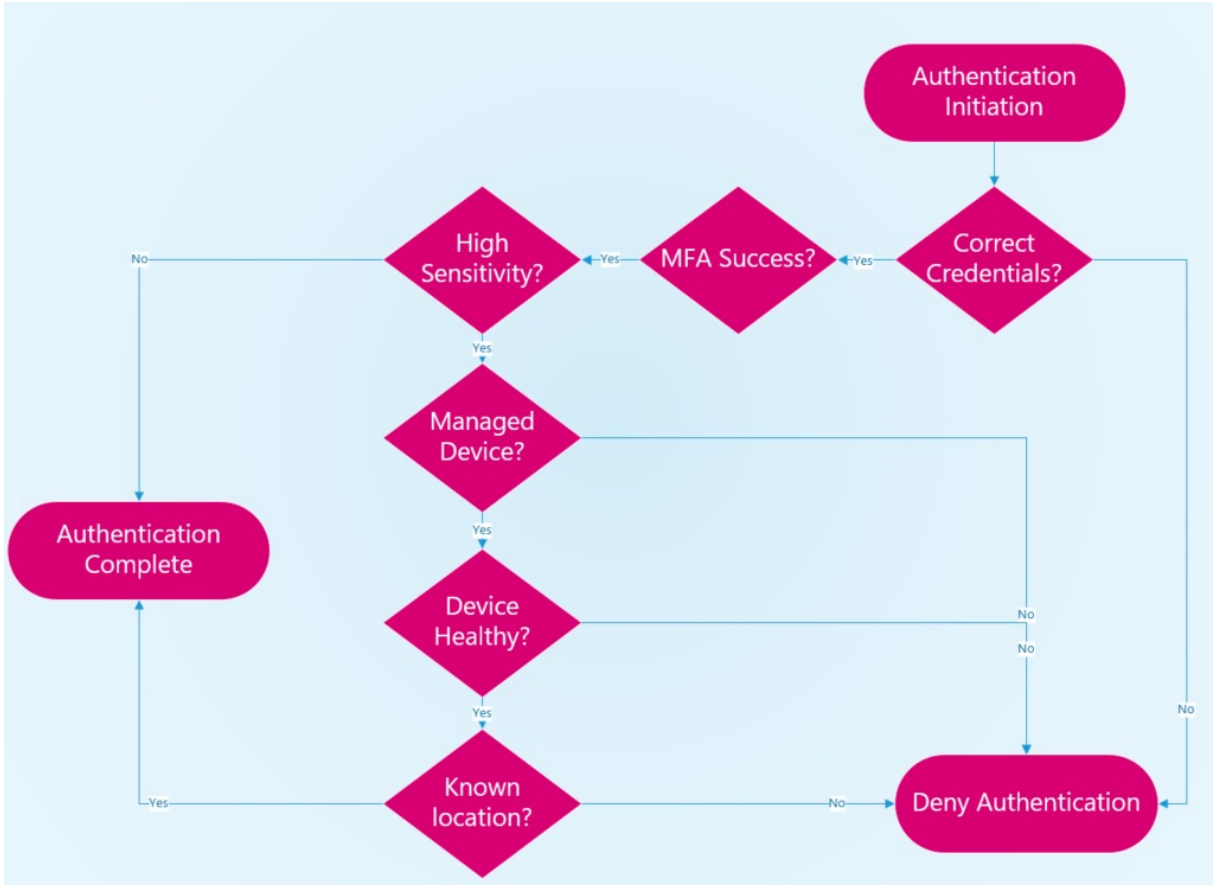
Identity is the new perimeter?

- Not any longer
- Identity is an important component of a modern perimeter
- Components of the perimeter
  - Identity
  - Device
  - Location
  - Workload
  - Behavioral signals
  - Proximity signals



Risk-based authentication

- Start from data and business processes
- Map to IT systems
- Determine tolerable level of validation
- Function between **sensitivity** (*of assets*) and **confidence** (*of signals*)



Continuous authorization

- Examine interactions as frequently as possible
  - Identity
  - Device
  - Location
  - Behavior
  - Proximity
- Make dynamic and automated decisions based on changes in signals

Zero-Trust

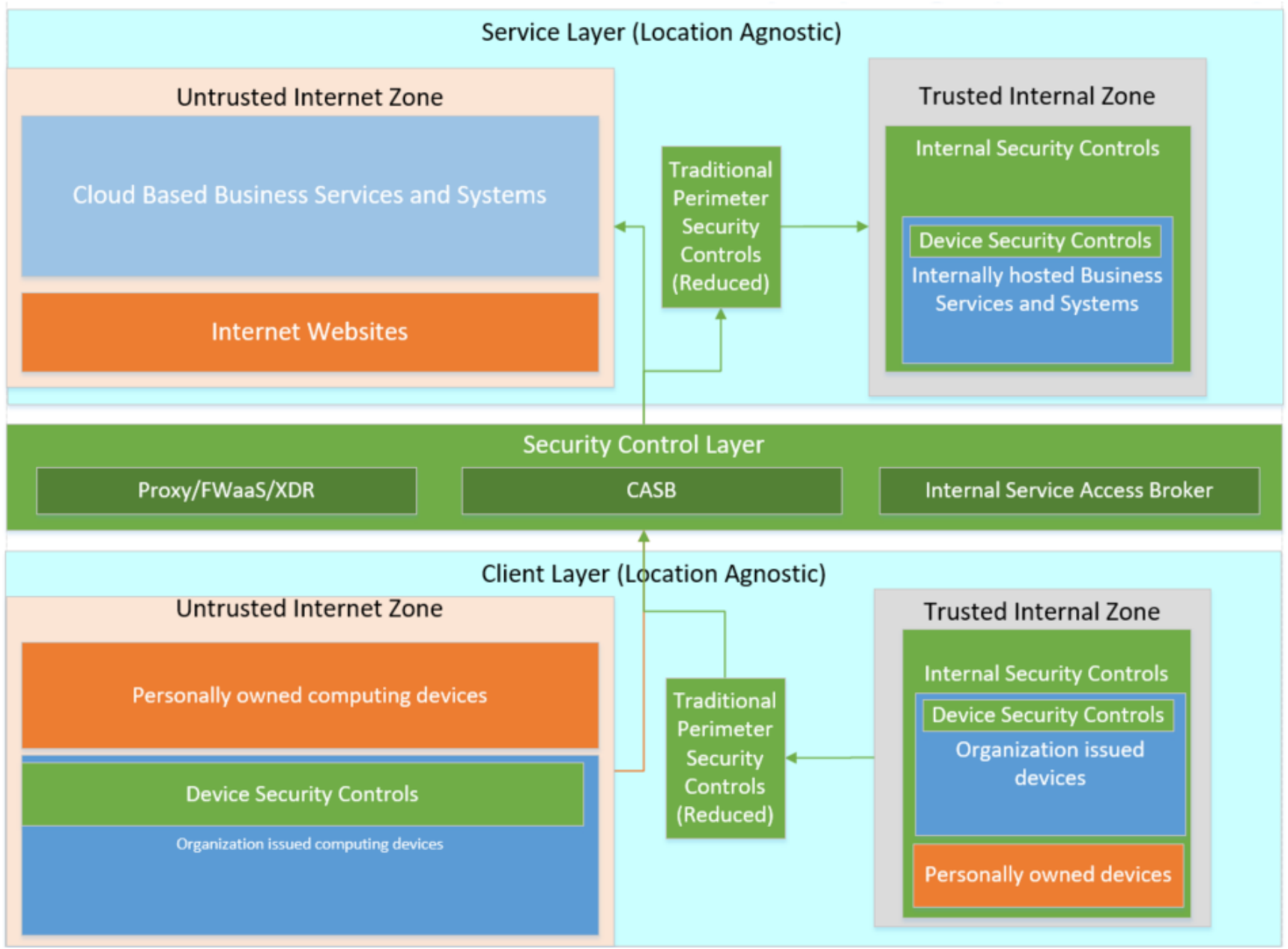
- The continuous examination of interactions between a subject (client) and an object (service) based on various signals
- The dynamic provisioning of access based on the measurement of these signals
- Implement controls around workloads to minimize the blast radius

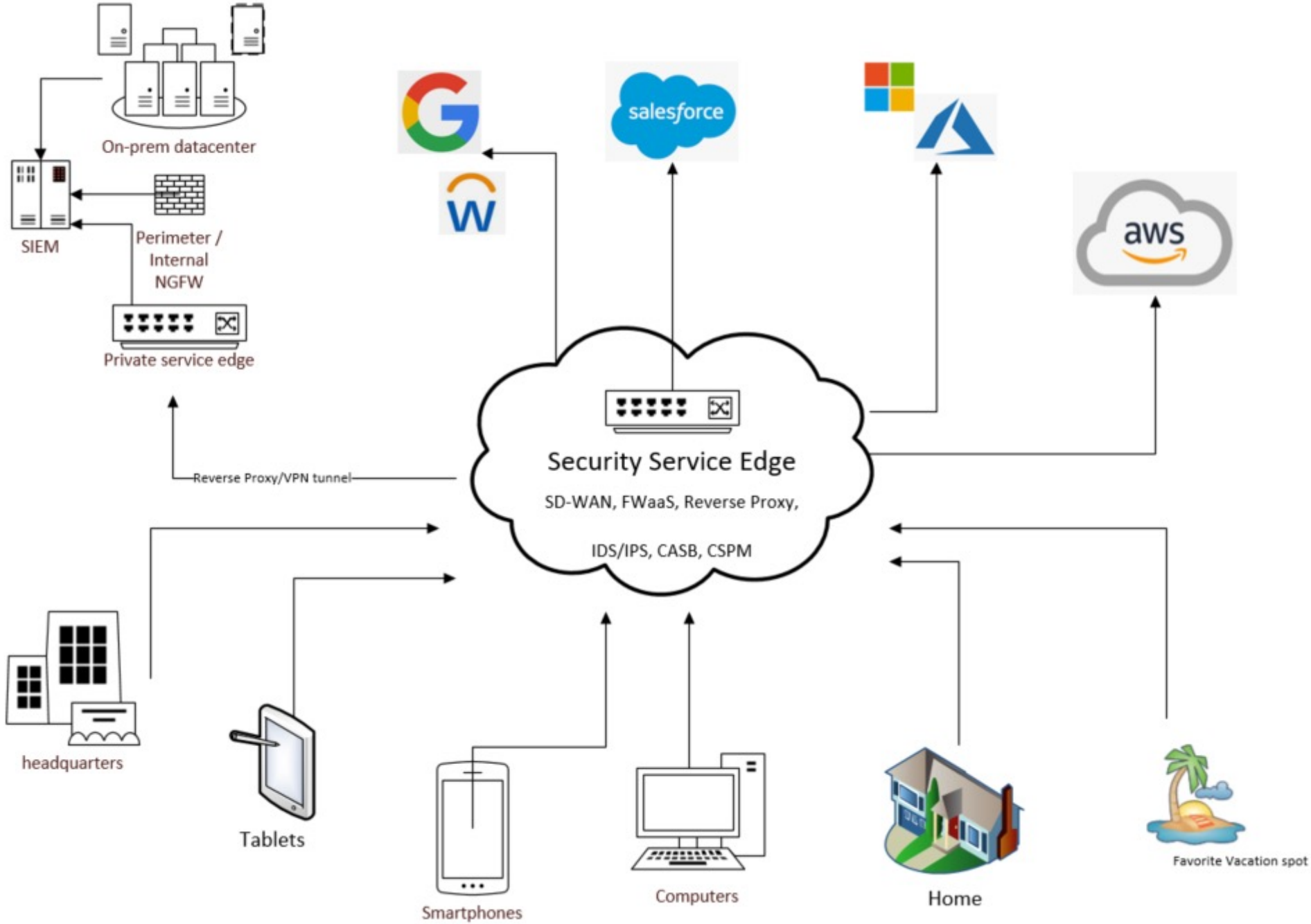
A risk-based and location-agnostic approach

- To protect a borderless organization, we need to build our security architecture that is not focused on borders, but rather on the continuous evaluation of **a collection of signals that provides the authenticity of a session**
  - Provide consistent protection from anywhere
  - Provide consistent experience to end users
  - Minimize visibility of security
  - Minimize blast radius
  - Provides / ingest high-fidelity signals

Conceptually… a page can be taken out of the Software-Defined Anything playbook

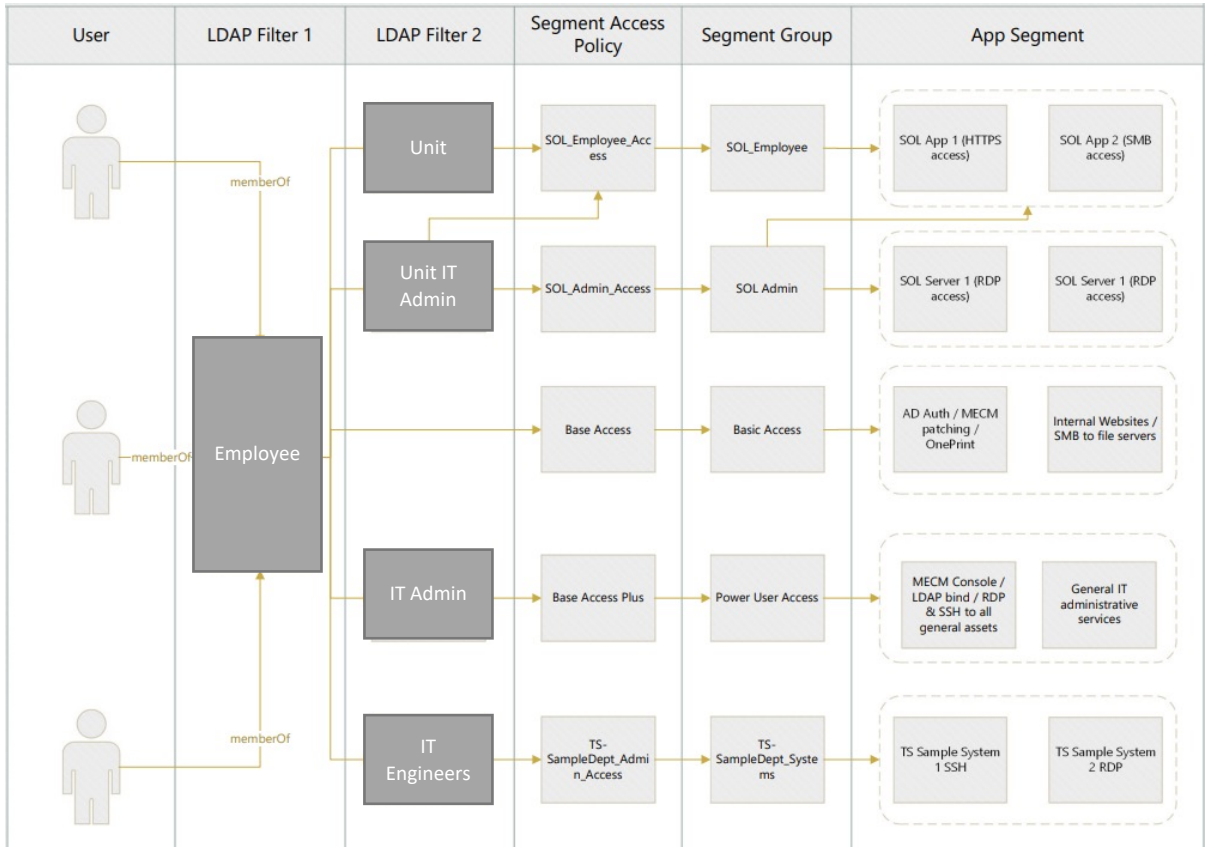
Moving beyond the castle and moat model




On-prem datacenter
SIEM
Perimeter / Internal NGFW
Private service edge
salesforce
aws
Reverse Proxy/VPN tunnel
Security Service Edge
SD-WAN, FWaaS, Reverse Proxy,
IDS/IPS, CASB, CSPM
headquarters
Tablets
Smartphones
Computers
Home
Favorite Vacation spot

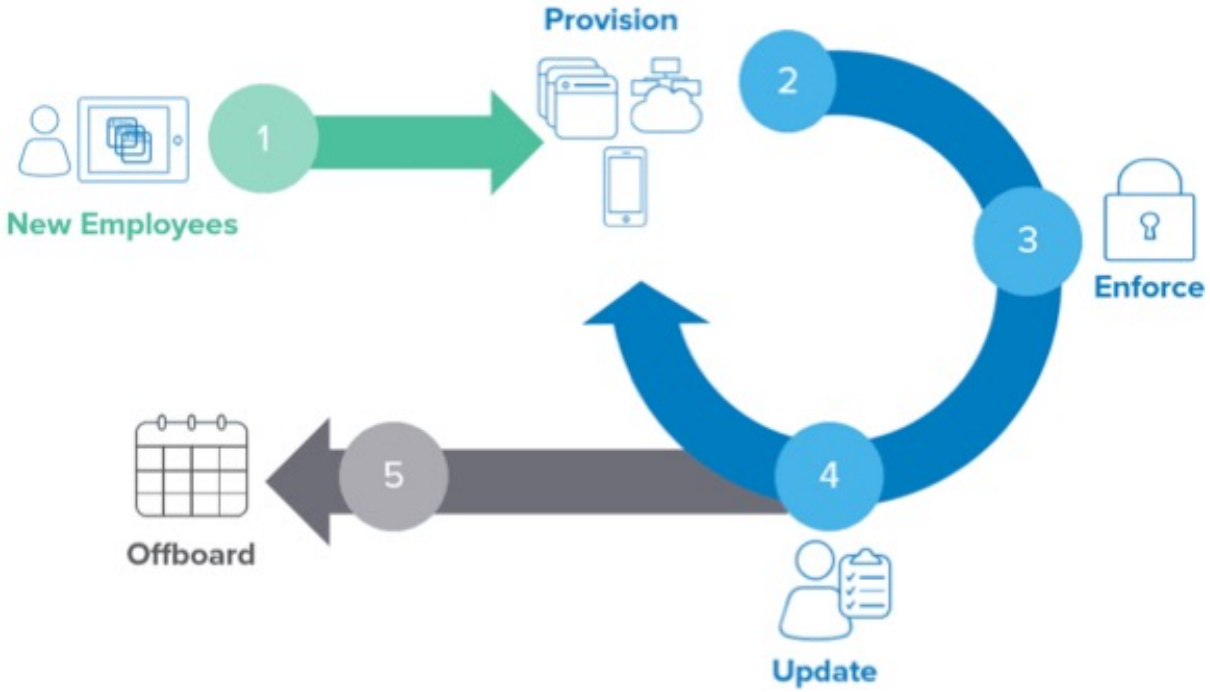
Define protection requirements

- System-based or Role-based: Classification of assets and units based on criticality
- Define interaction measurement requirements based on classification
- Define acceptable criteria for continued interaction based on parameters and classification



Dynamic role-based access provisioning

- Driven by your authoritative data source (e.g., HR/ERP)
- Orchestrated by Identity and Access Management systems
- Granularity of each layer of controls
  - Network
  - Device
  - Application
  - Workload
  - Storage
  - Data
- With control layers, the goal is to collectively minimize blast radius



Limiting the blast radius

- Segmentation
  - Network
  - Device
  - Access
- Granularity in controls can lead to complexity
- **Complexity can threaten sustainability**
- Focus on what is the most important
- Minimize exceptions to the norm

Operationalizing – Know yourself and know your enemy

- Understand the business mission and supporting assets
  - Classify assets based on sensitivity and risk (3 or 5-tier classification)
- Threat modeling for top tiers assets
  - Include hostile threats in remote environment
- Catalog available controls
  - Authentication (Traditional UN/PW, MFA, Passwordless)
  - Authorization (IAM workflows, groups)
  - Device (AV/EDR/XDR, Certificates, Domain Membership, Device health posture, Focus on host-based controls such as **Host-based FW**)
  - Behavior (UEBA data, SIEM data, and SOAR response)

Operationalizing - Control selection

	TIER 1 ASSET	TIER 2 ASSET	TIER 3 ASSET
ACCESS FROM PERSONAL DEVICE	No	Yes	Yes
REQUIRE DEVICE POSTURE CHECK	Yes, Enhanced Security required	Yes	No
ACCESS FROM KNOWN LOCATION	MFA Enforced	MFA Enforced	Not Required
ACCESS FROM UNKNOWN LOCATION	MFA Enforced	MFA Enforced	MFA Enforced
ACCESS PROVISIONING	Dedicated Group SCIM provisoned	Unit Group SCIM provisioned	Unit Group SCIM provisioned
MONITORING & RESPONSE	Auth / System /App / UEBA / Auto-containment	Auth / System / App / UEBA / Alert Only	Auth / System / App / Alert Only

Operationalizing - Control Layer extraction

- Secure Service Edge
  - L7 FWaaS
  - SWG
  - Sandbox
  - IDS/IPS
  - DLP
  - Internal System Access
- Always on full-tunnel VPN
  - Route all traffic from organization-issued devices through the VPN
- VDIs and App Virtualization
- **Real-time access provisioning**

Operationalizing - The device

- Aside from your EDRs, XDRs, and MDR clients what else?
  - Configuration baselines
  - **Bi-directional Host-based firewall by central policy**
  - Remote patching and management (InTune/JAMF)
  - Disable legacy protocols (NTLM anyone?)
  - Enable security features (e.g., SMB Signing)

Operationalizing – The people

- UEBA signals for high value targets
- Scenario-based training
- Driving adoption of the new security architecture
  - Simplicity and user experience is the key
  - Consistent and location-agnostic experience
  - Enticement related to reduced complexity in authentication experience

Summary

- Security controls must be implemented between a client layer and service layer and zones will be less significant in a new security model
- Controls should be consistent and location agnostic
- Organizations should strive to ingest more telemetry data to help facilitate risk-based authentication and continuous authorization
- Control granularity at each layer must be carefully managed to avoid support issues
- A more device focused control set that allows adequate remote management should be pursued

Thank you