CSCI E-117A SPRING 2025

Lecture 7
Mar 11, 2025

SECURE APPLICATIONS: MANAGING THE DEPLOYMENT INFRASTRUCTURE

LECTURE 6 AGENDA

- *Assignment 1*
  - *Marks*
- *Assignment 2, 3*
  - *Office Hours*
- *DEVICES : In the News*

QUICK ANNOUNCEMENTS

Assignment 3: March 16 (pushed back one week)

Assignment 4: April 6 (pushing back one week from March 30)

Capstone: (Still) Saturday May 3

ASSIGNMENT 2 FEEDBACK

Network Segmentation | Network Traffic Management | Traffic Encryption | Network Resilience

Brute Force - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1110/	3 respondents	8 %
Browser Session Hijacking - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1185/	5 respondents	13 %
Active Scanning / IP Blocks - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1595/001/		0 %
Adversary-in-the-Middle - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1557/	30 respondents	**77 %**
Compromise Infrastructure: Botnet - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1584/005/		0 %
Network Boundary Bridging - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1599/	1 respondent	3 %

77% answered correctly

Network Segmentation | Network Traffic Management | Traffic Encryption | Network Resilience

Brute Force - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1110/	3 respondents	8 %
Browser Session Hijacking - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1185/	2 respondents	5 %
Active Scanning / IP Blocks - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1595/001/	19 respondents	**49 %**
Adversary-in-the-Middle - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1557/	8 respondents	21 %
Compromise Infrastructure: Botnet - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1584/005/	3 respondents	8 %
Network Boundary Bridging - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1599/	4 respondents	10 %

9% answered correctly

Network Segmentation | Network T | Traffic Encryption | Network Resili

Brute Force - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1110/	1 respondent	3 %
Browser Session Hijacking - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1185/	1 respondent	3 %
Active Scanning / IP Blocks - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1595/001/	10 respondents	26 %
Adversary-in-the-Middle - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1557/		0 %
Compromise Infrastructure: Botnet - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1584/005/		0 %
Network Boundary Bridging - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1599/	27 respondents	**69 %**

69% answered correctly

Network Segmentation | Network Traffic Management | Traffic Encryption | Network Resilience

Brute Force - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1110/	7 respondents	18 %
Browser Session Hijacking - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1185/	2 respondents	5 %
Active Scanning / IP Blocks - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1595/001/	1 respondent	3 %
Adversary-in-the-Middle - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1557/		0 %
Compromise Infrastructure: Botnet - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1584/005/	28 respondents	**72 %**
Network Boundary Bridging - MITRE TECHNIQUE REFERENCE: https://attack.mitre.org/techniques/T1599/	1 respondent	3 %

% answered correctly

DETAILS

- Attack Technique: Adversary-in-the-Middle
  - https://attack.mitre.org/techniques/T1557/
  - Traffic encryption helps prevent adversary in the middle
- Attack Technique: Network Boundary Bridging
  - https://attack.mitre.org/techniques/T1599/
  - Network segmentation makes it harder to cross (bridge) network boundaries
- Attack Technique: Active Scanning of IP Blocks
  - https://attack.mitre.org/techniques/T1595/001/
  - Network traffic management helps identify scanning of IP blocks
- Attack Technique: Compromise Infrastructure: Botnet
  - https://attack.mitre.org/techniques/T1584/005/
  - Network resilience helps limit the impact of botnet/DDoS (whether hosted or impacted by)

Network segmentation

priority1 | priority2 | priority3 | priority4

1	18 respondents	46 %
2	10 respondents	26 %
3	7 respondents	18 %
4	4 respondents	10 %

Network Traffic Management

priority1 | priority2 | priority3 | priority4

1	1 respondent	3 %
2	14 respondents	36 %
3	18 respondents	46 %
4	6 respondents	15 %

Traffic Encryption

priority1 | priority2 | priority3 | priority4

1	17 respondents	44 %
2	14 respondents	36 %
3	4 respondents	10 %
4	4 respondents	10 %

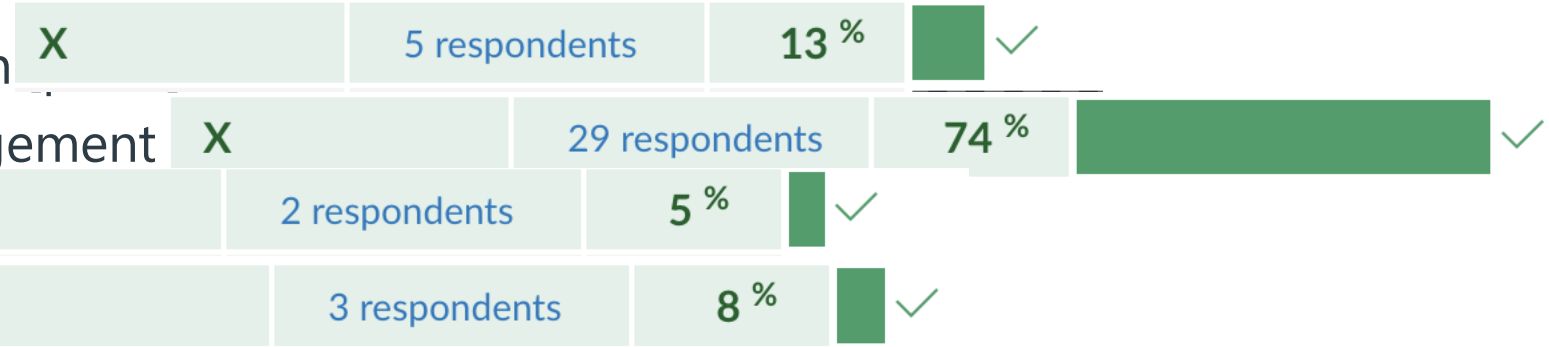
Network Resilience

priority1 | priority2 | priority3 | priority4

1	3 respondents	8 %
2	1 respondent	3 %
3	10 respondents	26 %
4	25 respondents	64 %

Most likely to benefit from Generative AI based DEFEND capabilities.

- Network Segmentation
- Network Traffic Management
- Traffic Encryption
- Network Resilience



Most likely to benefit from Generative AI based ATTACK capabilities.

- Network Segmentation [pick1]
- Network Traffic Management [pick2]
- Traffic Encryption [pick3]
- Network Resilience [pick4]

GOOD ANSWER (TOP NETWORK ZTA FUNCTION):

- *Your justification should mention / include threats, likelihood of compromise due to unprotected/poorly protected network architecture, severity of compromise, intrusiveness & cost of the program to implement the network architecture controls in terms of dollars, people, time.*
- Network segmentation is my top priority and first line of defense for the protection of my entire environment. With (effective) network segmentation in place, we are able to limit the movement of bad actors (including malicious or unintentional insider threats) to segments, making lateral movement harder to accomplish and giving us more time to detect and respond to bad actors trying to move through our networks. Strong network segmentation also allows us to enforce policies that unauthorized users cannot access important resources, including applications and data, providing assurance to customers that their data is not accessed by unauthorized users.
- Moving from a flat (not segmented) network to a robust network segmentation architecture will be time consuming and will require skilled network engineering focus to ensure that the implementation has a minimal impact on development and operations (the teams who will be primarily impacted).
- With a robust network segmentation-based architecture we can provide fit-for-purpose protection for different network segments. For example, we can put more resources towards the protection of Internet-facing segments and segments hosting critical applications and customer data. We believe that increasing the maturity of our network segmentation will also increase customer trust and will help towards sales (less time explaining how we protect a flat network by relying on segmentation means less time defending security during sales cycle, and faster response to customer's security questionnaires).

GOOD ANSWER (2ND NETWORK ZTA FUNCTION):

- This was a difficult decision. I would have normally had “Traffic Monitoring” as my second priority, but we have not been given any information on the state of encryption/key management. Given this, while I HOPE that network traffic to our Internet-facing resources is encrypted, I cannot make any assumptions about how, and how the keys used (are they rotate-able?) and so on, and so I must pick Traffic Encryption over Network Monitoring.
- As I roll out Traffic Encryption, I will focus on the individual network segments based on their mission criticality (how important are they to the business), starting with robust encryption and key management (including the ability to rotate keys/certificates) for Internet facing, development and production environments and a focus on robust network encryption for all of my third-party applications that the business uses.
- My top priority within Traffic Encryption is to encrypt all Internet facing traffic. Because I have put network segmentation in place, I can focus on adding encryption on environments that need it, such as my production environment where customer data is hosted to limit the ability of bad actors to eavesdrop on / compromise my network traffic.
- Like network segmentation, I believe that increasing the maturity of our traffic encryption rollout will also increase customer trust and will help towards sales (less time explaining how we protect a flat network by relying on segmentation means less time defending security during sales cycle, and faster response to customer’s security questionnaires).

GOOD ANSWER: PROVISIONALLY ADDING #3

- My third priority is to add network traffic monitoring disciplines to the environment. With NTM we can monitor for anomalous traffic and behavior, reducing the time it takes us to identify potential bad actors attempting to move across our environment (which is protected with strong network segmentation).
- We will require additional tooling / licenses to roll out a robust NTM discipline and will focus on the most critical network segments (Internet facing and mission critical) first. The rollout of the tooling and overall NTM discipline will be handled by the same team building out the maturity of our network segments.
- Adding a NTM discipline will also help position us for overall network resilience – by monitoring and learning our traffic patterns we will be able to understand our overall network resilience needs as part of our overall business continuity and availability.

GOOD ANSWER: OPTIONS

1. Drop priority 3, complete the programs for priority 1 and 2 but three (3) months later
2. Drop priority 3, keep priority 1 on track and slip priority 2 by six (6) months
3. Keep all three programs but slip the delivery date of all three by nine (9) months.

This was a very difficult decision. Based on my assumed risk profile, I am going with Option 1 to to drop priority 3 and keep 1 and 2 with a three-month delay. While I very much wanted to select option 3 (keep all three but slip by nine months), I believe that the risk to the business based on attacks that are “enabled” by a flat network and the customer risks related to a lack of a robust encryption discipline are such that we must get both of those in place.

Note that I did not pick option 2 because I believe that it will be more effective for the business to roll out a robust traffic encryption discipline as part of the network segmentation rollout and so slipping one but not the other did not make sense. The risks associated with a three-month delay in the network segmentation project are offset by the efficiency of rollout out network segmentation + encryption as part of a single program and timeline.

GREAT ANSWER

- A high-level strategy for security objectives is more effective with executive leaders because it positions cybersecurity not as a reactive expense but as an investment that supports business continuity, regulatory compliance, and risk management. While scary stories about assaults are engaging, they create short-term, fear-driven decisions rather than enduring security measures, and by focusing on certain security objectives such as protecting critical assets, reducing operational risk, and gaining compliance, executives can envision the necessity for an effective managed security program and how it actively supports enduring business resilience and success.

UPCOMING ASSIGNMENTS

ASSIGNMENT 3

Due Date: March 16 ~~March 9~~

Purpose: As we move to Devices, there are LOTS of vulnerabilities to consider. This is made worse as we consider the "variety" of devices we have to protect and how different Servers, Workstations and IoT are.

The protection and detection of vulnerabilities and compromises of devices includes people, process and technology; vendor solutions often cover both protect/detect and the CISA Zero Trust Maturity Model (ZTMM) assumes least maturity relies on people based solutions and most mature is full automated, technology based solutions.

The purpose of this assignment is to start to focus on the prioritization of Protection/Detection of devices, the ZTMM, and how Generative AI will impact our ability to move up (or down) the ZTMM.

ASSIGNMENT 4

Due Date: ~~Mar 30~~ April 6

Purpose: To look at the Applications category in more detail, from a zero trust point of view, a threat point of view and a protection point of view.

CAPSTONE ASSIGNMENT

Due Date: SATURDAY MAY 3

Purpose: To reflect on the intersection and benefits of a zero trust versus a secure be design versus a threat and risk point of view, given that ”you can’t have it all, but still have to protect an environment”.

REMINDERS

DEVICES & NETWORKS WRAP UP

DEVICES

End User Devices

(Fixed) Workstations

Laptops

Tablets

Mobile Devices

SOHO Routers

Office IT & IOT

Network

- ISP Termination
- WiFi Routers

Surveillance

- Cameras
- Recordings

Collab Equip

- Phones / Speaker
- TV / Display

“Data Center”
OnPrem or Cloud Hosted

Physical Compute

Physical Network

- Firewalls
- Routers
- Switches

PaaS

PaaS Storage

PaaS Database

PaaS “Networks”

PaaS Compute

- Containers
- Microservices
- ”PaaS Mgmt”

NETWORKS

Home
(Home Office)

Third Party BizApps
SaaS & Self Managed

Third Party Tools
SaaS & Self Managed

Office
I/T & IoT

Product
Dev/Test/Production

DEVICES: Zero Trust Maturity Levels

A device refers to any asset (including its hardware, software, firmware, etc.) that can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, **IoT devices**, networking equipment, and more.			
Traditional	**Initial**	**Advanced**	**Optimized**
• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics
• *No configuration standards, manufacturer recommended*	• *Locally defined configuration*	• *Industry standards for configuration*	• *Federal/Regulatory standards*

Figure 4: High Level Zero Trust Maturity Model Overview

DEVICES

DEVICES	Traditional	Initial	Advanced	Optimized
Inventory	Manually tracking of device inventory	All physical assets tracked	All physical, most virtual tracked (start to introduce automation to assist)	Continuous (automated) identification of physical, virtual asset inventory
(Config & Patch) Compliance	Limited visibility into device compliance posture	Limited enforcement of device compliance	Enforced compliance + integrated threat protection	Continuous (automated) enforced compliance + integrated threat protection
Resource Access	No defined criteria enforced for access	Limited device-based access control	Initial resource access depends on device posture	Resource access depends on real-time device risk analytics
Protection	Manual deployment of protections to some devices	Some protections delivered via automation	Enforced compliance + integrated threat protection	Continuous (automated) enforced compliance + integrated threat protection

DEVICES ZTM THINGS TO THINK ABOUT

- How are you creating, maintaining your inventory
  - Do you allow for BYOD devices for laptops/mobile devices?
- What standards are you using to define baseline configuration
- How you are handling patching / updates
- How do you monitor for vulnerabilities / things that must be patched or otherwise addressed
- How are you protecting devices
- Do you have a discipline that prevents unmanaged / non-compliant devices from accessing “stuff”

NETWORKS: Zero Trust Maturity Levels

A network refers to an open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages.			
Traditional	**Initial**	**Advanced**	**Optimized**
• Large perimeter / macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware applications profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility

Figure 4: High Level Zero Trust Maturity Model Overview

NETWORKS

	Traditional	Initial	Advanced	Optimized
Network Segmentation	Flat network / limited segmentation, manually managed network architecture; minimal restrictions on reachability within network segments	Begin to deploy network architecture with the isolation of critical workloads, constrain connectivity to least function principles, and a transition toward service-specific management	Expand deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress micro- perimeters and service- specific interconnections.	Fully distributed ingress/egress micro- perimeters and extensive micro-segmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific Distributed micro-perimeters, just-in-time and just-enough access control
Traffic Encryption	Minimal traffic encryption, ad hoc key management	Increased encryption, formalized key management	Encrypt application traffic, key management & rotation	Best practice crypto management including quantum aware
Network Traffic Management	Static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities	Application profiles with distinct traffic management Features; begin to map all apps to profiles	Dynamic network rules and configurations for resource optimization	Dynamic network rules and configurations that continuously evolve to meet application profile needs
Network Resilience	Configures network capabilities on a case-by-case basis, manually managed	begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms	Dynamically manage network capabilities for availability demands and resilience mechanisms for the majority of applications.	Holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.

NETWORK ZTM THINGS TO THINK ABOUT

- Do you have a network segmentation strategy?
- How do you control movement across network segments?
- How wide is your encryption in transit coverage?
- Do you have a robust encryption discipline, including key management, rotation, quantum aware?
- How do you monitor for vulnerabilities / things that must be patched or otherwise addressed with protocols (eg TLS/Heartbleed?)
- How do you monitor for anomalous behaviour
  - How do you define “not anomalous” behaviour?
- How and what do you have resilience strategies
  - How do you protect against DDoS?

DEVICES

End User Devices

(Fixed) Workstations

Laptops

Tablets

Mobile Devices

SOHO Routers

Office IT & IOT

Network

- ISP Termination
- WiFi Routers

Surveillance

- Cameras
- Recordings

Collab Equip

- Phones / Speaker
- TV / Display

“Data Center”
OnPrem or Cloud Hosted

Physical Compute

Physical Network

- Firewalls
- Routers
- Switches

PaaS

PaaS Storage

PaaS Database

PaaS “Networks”

PaaS Compute

- Containers
- Microservices
- ”PaaS Mgmt”

NETWORKS

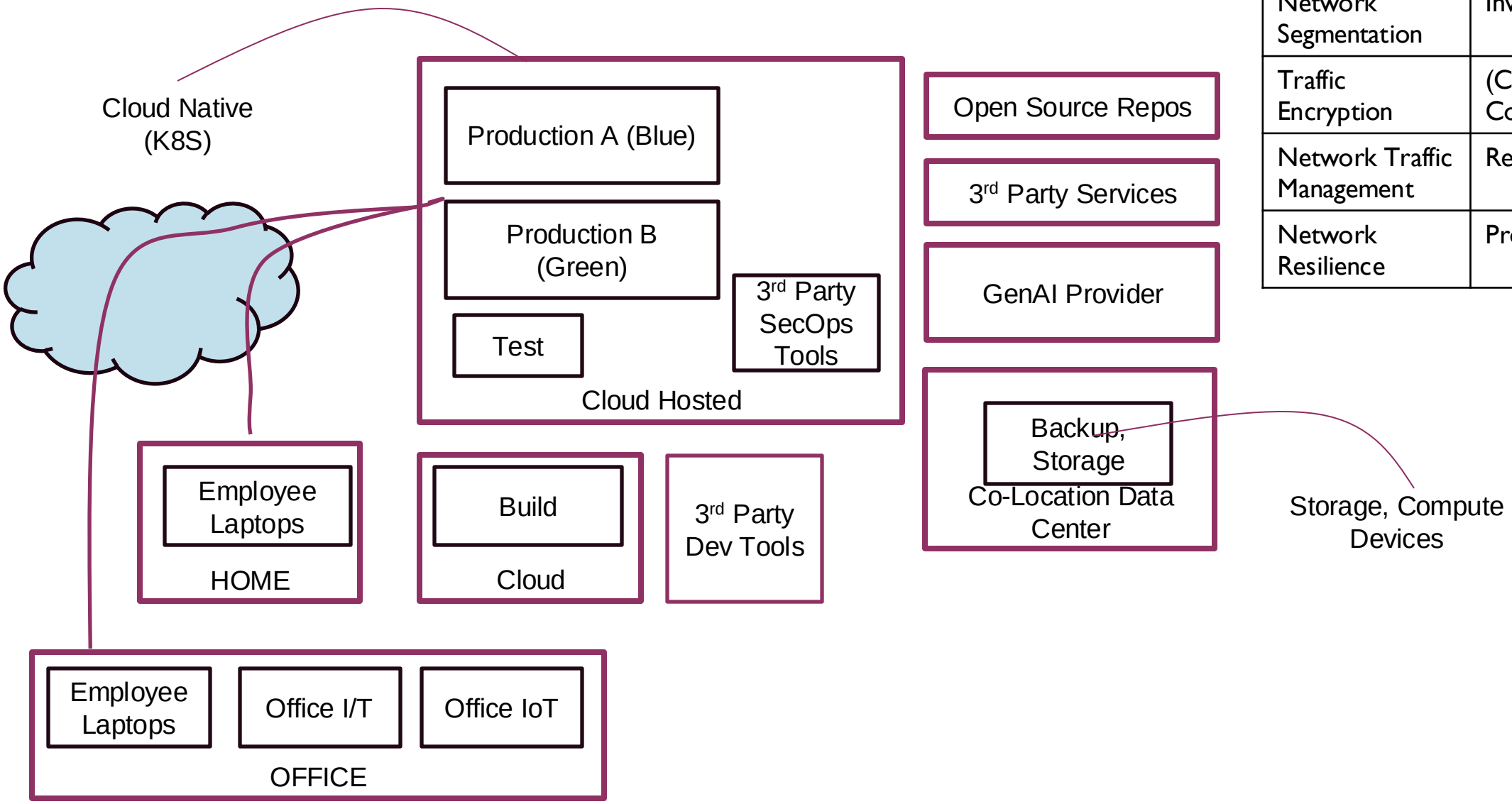
Home
(Home Office)

Third Party BizApps
SaaS & Self Managed

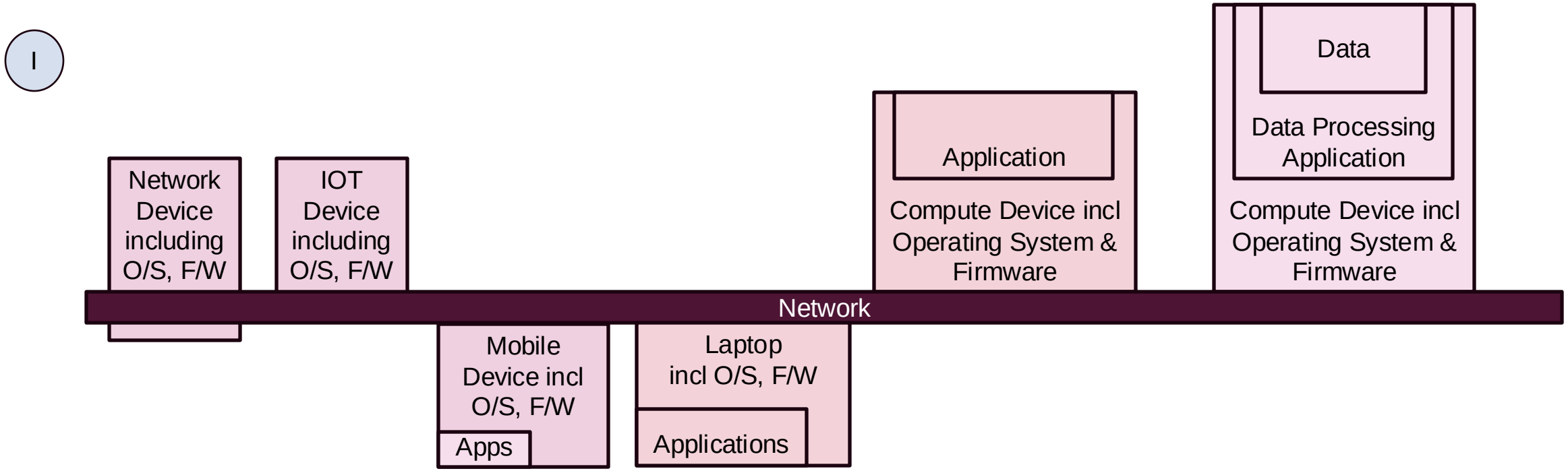
Third Party Tools
SaaS & Self Managed

Office
I/T & IoT

Product
Dev/Test/Production



NETWORKS	DEVICES
Network Segmentation	Inventory
Traffic Encryption	(Config & Patch) Compliance
Network Traffic Management	Resource Access
Network Resilience	Protection



O/S – Operating System
F/W – Firmware

NETWORKS	DEVICES	APPLICATIONS	DATA	IDENTITY
Network Segmentation	Inventory			
Traffic Encryption	(Config & Patch) Compliance			
Network Traffic Management	Resource Access			
Network Resilience	Protection			

IOT & (SOHO) NETWORK DEVICES

- These (often overlooked) devices play an important role in the security posture of an organization
- Unfortunately, it is often difficult to protect these in terms of patching and MFA

IOT & SOHO ROUTERS – NATION STATE ACTIVITY TIMELINE

- September 2016, Mirai-based DDoS attack against a French technology company, OVH. Mirai's attack peaked at an unprecedented 1Tbps and is estimated to have used about 145,000 (IOT/DVR) devices within the assault.
- September 2016, Mirai-based DDoS attack against Krebs on Security was flooded with over 600 GB of data
- October 2016, Mirai-variant based DDosS believed to be behind the massive attack that brought down the domain registration services provider, Dyn.
- In 2018, researchers reported that more than 500,000 SOHO routers had been compromised by sophisticated malware dubbed VPNFilter.
- In 2021, hackers compromised Internet-facing DVR and IP cameras for use as command-and-control nodes from malware tracked as Shadowpad, according to security firm Recorded Future.
- In 2024, the FBI surreptitiously sent commands to hundreds of infected small office and home office routers to remove malware China state-sponsored hackers were using to wage attacks on critical infrastructure.
- In 2024, Russian hackers gained control of devices after they were already infected with Moobot.
  - Threat actors had already compromised and installed Moobot after first exploiting publicly known default administrator credentials that hadn't been removed from the devices by the people who owned them.

RECOMMENDATIONS TO PROTECT AGAINST MIRAI/IOT COMPROMISE https://www.cisecurity.org/insights/blog/the-mirai-botnet-threats-and-mitigations

- Segment your network – Ensure that all IoT devices are on a separate network from systems critical for daily operations [NETWORKS]
- Update IoT devices – Always keep IoT devices up to date to ensure there is less of a chance for infection [DEVICES]
- Where possible, use and maintain anti-virus software or anti-malware tools – Using a legitimate program that identifies and removes malware can help eliminate an infection [DEVICES, maybe APPLICATIONS]
- Have an official password policy – Reset passwords as (original and in-place) passwords may have been compromised [DEVICES]
- Keep operating systems and application software up-to-date – Set up automatic updates and install software patches [DEVICES]

MIRAI BOTNET: DVR/SURVEILLANCE DEVICES

https://www.een.com/blog/importance-cyber-security-driven-home-145000-dvrs-compromised/
September 30, 2016 Eagle Eye Networks

- According to Level3, of the identifiable devices participating in these attacks, almost 96 percent were IoT devices, of which 95 percent were cameras and DVRs.
- Security camera DVRs often come configured with telnet and web interfaces enabled, allowing users to configure the devices and view their security footage over the Internet making them vulnerable to attacks. This compromise can be used by hackers to get access to the customers' local network and obtain sensitive corporate information, which is a potentially dangerous liability for the Reseller or VAR. In order to patch or upgrade these DVRs they will have to be manually upgraded or replaced.
- Detecting and determining if a DVR is comprised can be accomplished with some network investigation or the application of security appliances that analyze all the Internet traffic.
- The infection that was identified was labeled "MIRAI". The MIRAI code has built into it a large number of default cameras and DVR passwords. If you are using DVR's from one of these manufacturers and didn't change the passwords it is likely that you are infected.

MIRAI BOTNET
https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/
https://www.cisecurity.org/insights/blog/the-mirai-botnet-threats-and-mitigations

- Mirai scans the Internet for IoT devices that run on the ARC processor. This processor runs a stripped-down version of the Linux operating system. If the default username-and-password combo is not changed, Mirai is able to log into the device and infect it.
- Mirai's first large-scale attack was in September 2016 against a French technology company, OVH. Mirai's attack peaked at an unprecedented 1Tbps and is estimated to have used about 145,000 devices within the assault. This attack set the scale for how massive the botnet had become, with the second largest attack peaking around 400 Gbps. After the attack on OVH, Krebs on Security, created by the journalist Brian Krebs, was flooded with over 600 GB of data in late September 2016.
- A week later they released the source code into the world … and [it] is believed to be behind the massive attack that brought down the domain registration services provider, Dyn, in October 2016.

(NETWORK) DEVICES IN THE NEWS: UBIQUITY EDGE ROUTERS

https://arstechnica.com/security/2024/02/kremlin-backed-hackers-are-infecting-ubiquity-edgerouters-fbi-warns/

- How compromised
  - Routers have publicly known, default admin (root) credentials and Internet facing admin access
    - → "Owners" did not reset credentials
  - Routers were discovered and infected with Moobot (botnet malware) by "actor A" (financially motivated threat actors)
  - APT28 used (inventory of devices and) admin access to install custom scripts, tooling (malware)
- What happened
  - APT28 has used the routers to collect credentials (which in turn were on unprotected comms), proxy malicious traffic, and host spoofed landing pages and custom post-exploit malware.
- APT28 has used the routers to
  - Collect credentials and proxy malicious traffic,
  - Host spoofed landing pages and custom post-exploit malware,
  - Created Python scripts in attacks for collecting account credentials for webmail accounts of interest
  - Used the routers to exploit CVE-2023-23397, a critical zero-day in Microsoft's Outlook email app that allowed the group to harvest cryptographic hashes that gave access to user accounts.

(NETWORK) DEVICES IN THE NEWS: UBIQUITY EDGE ROUTERS

https://arstechnica.com/security/2024/02/kremlin-backed-hackers-are-infecting-ubiquity-edgerouters-fbi-warns/

- … Owners of Ubiquiti EdgeRouters [should] check their gear for signs they've been hacked and are being used to conceal ongoing malicious operations by Russian state hackers.
- With root access to compromised Ubiquiti EdgeRouters, APT28 actors have unfettered access to Linux-based operating systems to install tooling and to obfuscate their identity while conducting malicious campaigns," FBI officials
- The Ubiquiti EdgeRouters make an ideal hideout for hackers. The inexpensive gear, used in homes and small offices, runs a version of Linux that can host malware that surreptitiously runs behind the scenes. The hackers then use the routers to conduct their malicious activities. Rather than using infrastructure and IP addresses that are known to be hostile, the connections come from benign-appearing devices hosted by addresses with trustworthy reputations, allowing them to receive a green light from security defenses.

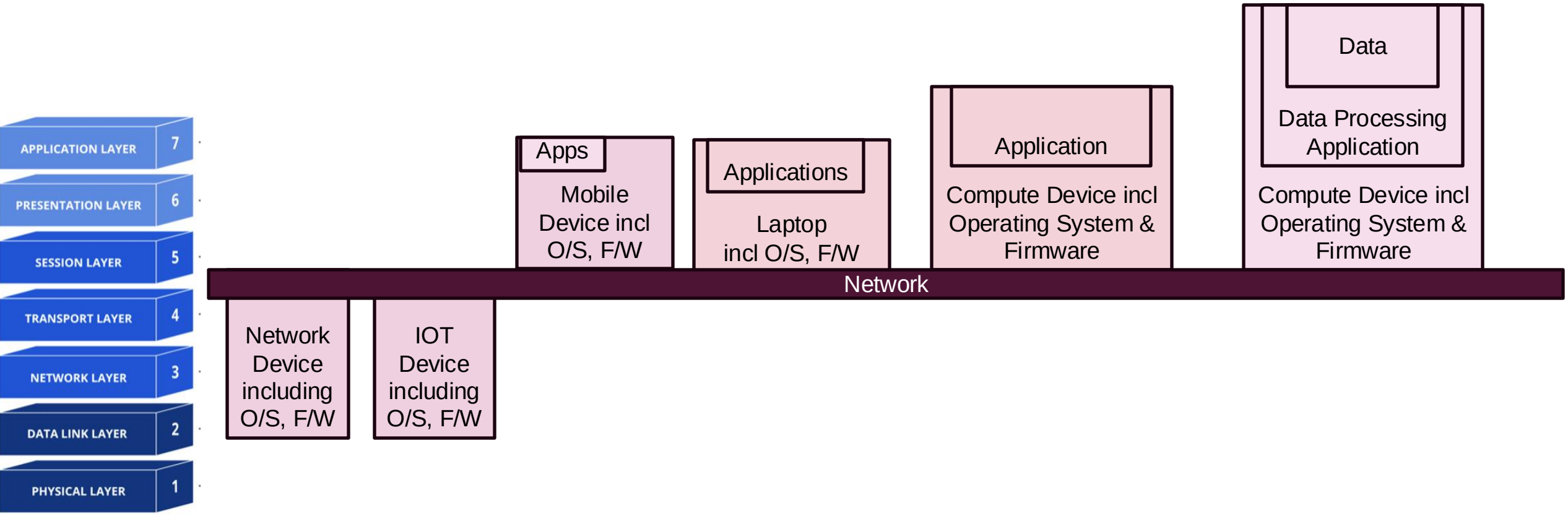
HOME NETWORK DEVICES / EDGE ROUTERS

- The Russian hackers gained control of devices after they were already infected with Moobot, which is botnet malware (based on Mirai) used by financially motivated threat actors not affiliated with the GRU. These threat actors installed Moobot after first exploiting publicly known default administrator credentials that hadn't been removed from the devices by the people who owned them. APT28 then used the Moobot malware to install custom scripts and malware that turned the botnet into a global cyber espionage platform.
- The actions against APT28 and its use of Ubiquiti EdgeRouters comes one month after authorities conducted a similar operation against a China state group's commandeering of small office and home office routers, which were mainly Cisco and Netgear devices that had reached their end of life. A group backed by the Chinese government and tracked as Volt Typhoon used the routers to connect to the networks of US critical infrastructure organizations to establish covert posts that could be used in future cyberattacks.

(NETWORK) DEVICES IN THE NEWS: CISCO & NETGEAR DEVICES

https://arstechnica.com/security/2024/01/chinese-malware-removed-from-soho-routers-after-fbi-issues-covert-commands/

- The US Justice Department said Wednesday that the FBI surreptitiously sent commands to hundreds of infected small office and home office routers to remove malware China state-sponsored hackers were using to wage attacks on critical infrastructure.
- The routers—mainly Cisco and Netgear devices that had reached their end of life—were infected with what's known as KV Botnet malware, Justice Department officials said. Chinese hackers from a group tracked as Volt Typhoon used the malware to wrangle the routers into a network they could control. Traffic passing between the hackers and the compromised devices was encrypted using a VPN module KV Botnet installed. From there, the campaign operators connected to the networks of US critical infrastructure organizations to establish posts that could be used in future cyberattacks. The arrangement caused traffic to appear as originating from US IP addresses with trustworthy reputations rather than suspicious regions in China.
- In 2018, researchers reported that more than 500,000 SOHO routers had been compromised by sophisticated malware dubbed VPNFilter. The mass hack was later revealed to be an operation by a Russian-state group tracked as Sofacy. In that event, the FBI issued an advisory urging people to restart their routers to remove any possible infections. The agency also seized a domain used to control VPNFilter.
- The compromise of SOHO routers for use in state-sponsored attacks underscores a growing problem with legacy devices that no longer receive security patches from their manufacturers. These permanently vulnerable devices pose a threat not just to the owners but also to the public at large. Users with the means should replace them with new routers and check for and install available patches as they become available. Another measure is to reboot routers every day or two since most infections of these devices cannot survive them.


APPLICATION LAYER 7
PRESENTATION LAYER 6
SESSION LAYER 5
TRANSPORT LAYER 4
NETWORK LAYER 3
DATA LINK LAYER 2
PHYSICAL LAYER 1
Apps
Mobile Device incl O/S, F/W
Applications
Laptop incl O/S, F/W
Application
Compute Device incl Operating System & Firmware
Data
Data Processing Application
Compute Device incl Operating System & Firmware
Network
Network Device including O/S, F/W
IOT Device including O/S, F/W

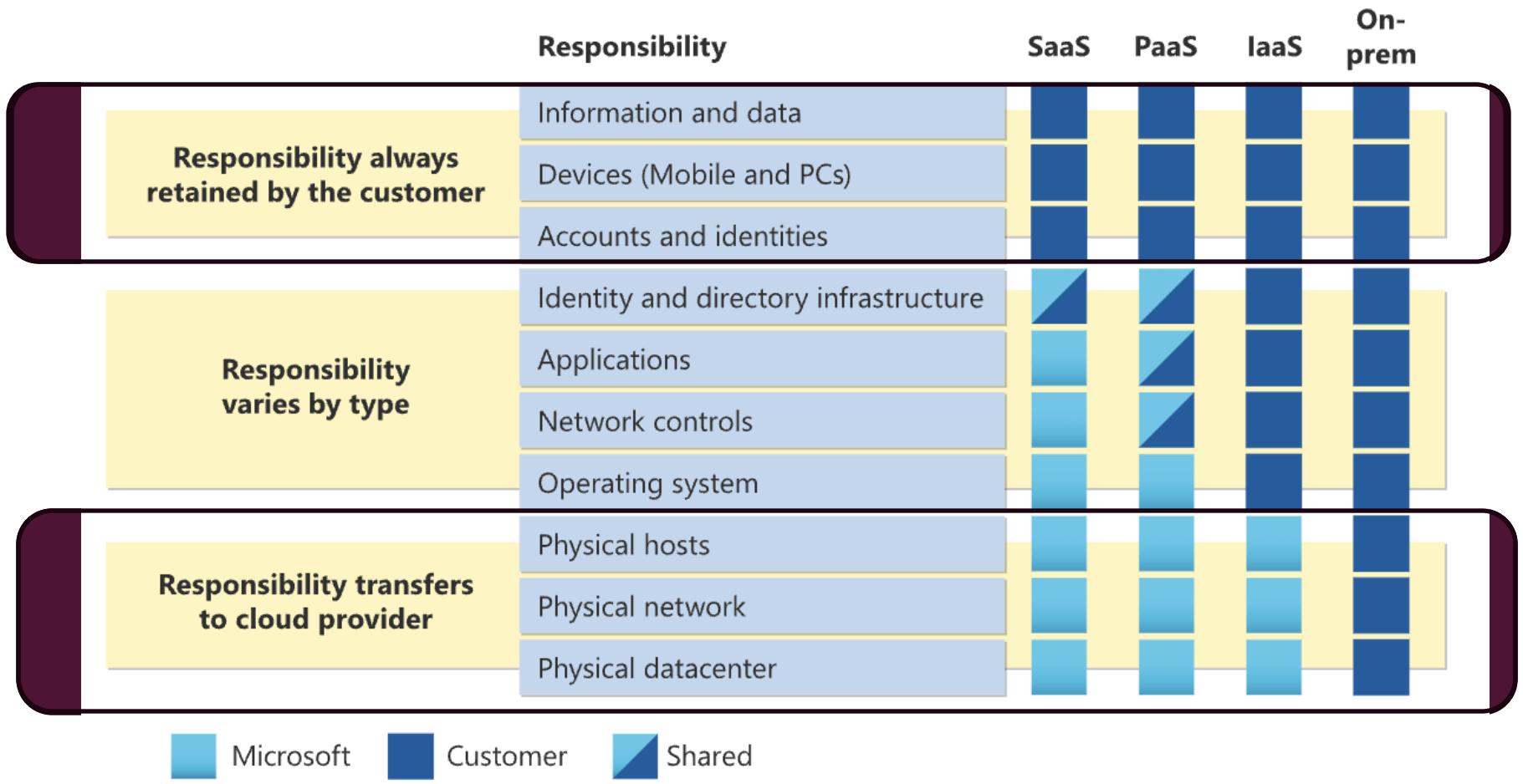
SHARED RESPONSIBILITY AND APPLICATIONS/WORKLOADS

https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

- DATA
- IDENTITIES
- APPLICATIONS
- DEVICES

- DATA
- IDENTITIES
- APPLICATIONS
- DEVICES
- NETWORKS

- DEVICES
- NETWORKS



DISCUSSION/POLL

Question 1: You are responsible for security for your WFH employees and you have the following control options for protection of their SoHo routers. You are not 100% SaaS based – you have applications/environments that you host, manage and patch (IaaS and OnPrem). If you had to choose from the following sets of controls that magically your employees will happily comply with, which would you chose?

- *Option I:*
  - *Reset all default passwords, Remove Internet facing administration (must be local network based only), Require (at least) monthly patch and restart (power cycle) of the devices*
- *Option II:*
  - *Remotely trigger a restart (power cycle) of the devices on a daily basis*
- *Option III:*
  - *Require employees to use only "in support" devices (no EOL/EOS routers allowed), Report/register/manage employee's home network device manufacturer, version*

Question 2: If you could not do any of the above options, would you want to allow them onto your corporate network?

Question 3: Even if you COULD do all of the above, would this be sufficient controls in your mind to allow them on to your corporate network?

CLASS BREAKOUT PROMPT: PROTECTING DEVICES & NETWORKS

- *SoHo routers (whether they are part of network or device class) are a critical part of environment security*
- *[In office IOT devices (especially DVR) are also critical part of (physical) security oversight]*
- *As someone held accountable for your employer's security does it seems reasonable to "require" that your employees protect their ENITRE work-from-home set up with the same controls as enforced for your office? Regardless of reasonableness, what about practicality?*

- *Set up for next section (Applications):*
- *Would you rather*
  - *Use the political capital to enforce security controls on the employee's (personally owned) router OR*
  - *Disallow access to anything other than SaaS-hosted apps from a laptop that accesses (any) network from a personally owned & managed router OR*
  - *Enforce controls on their laptops/workstations/mobile devices to prevent lateral movement from a compromised device to a local laptop/workstation?*

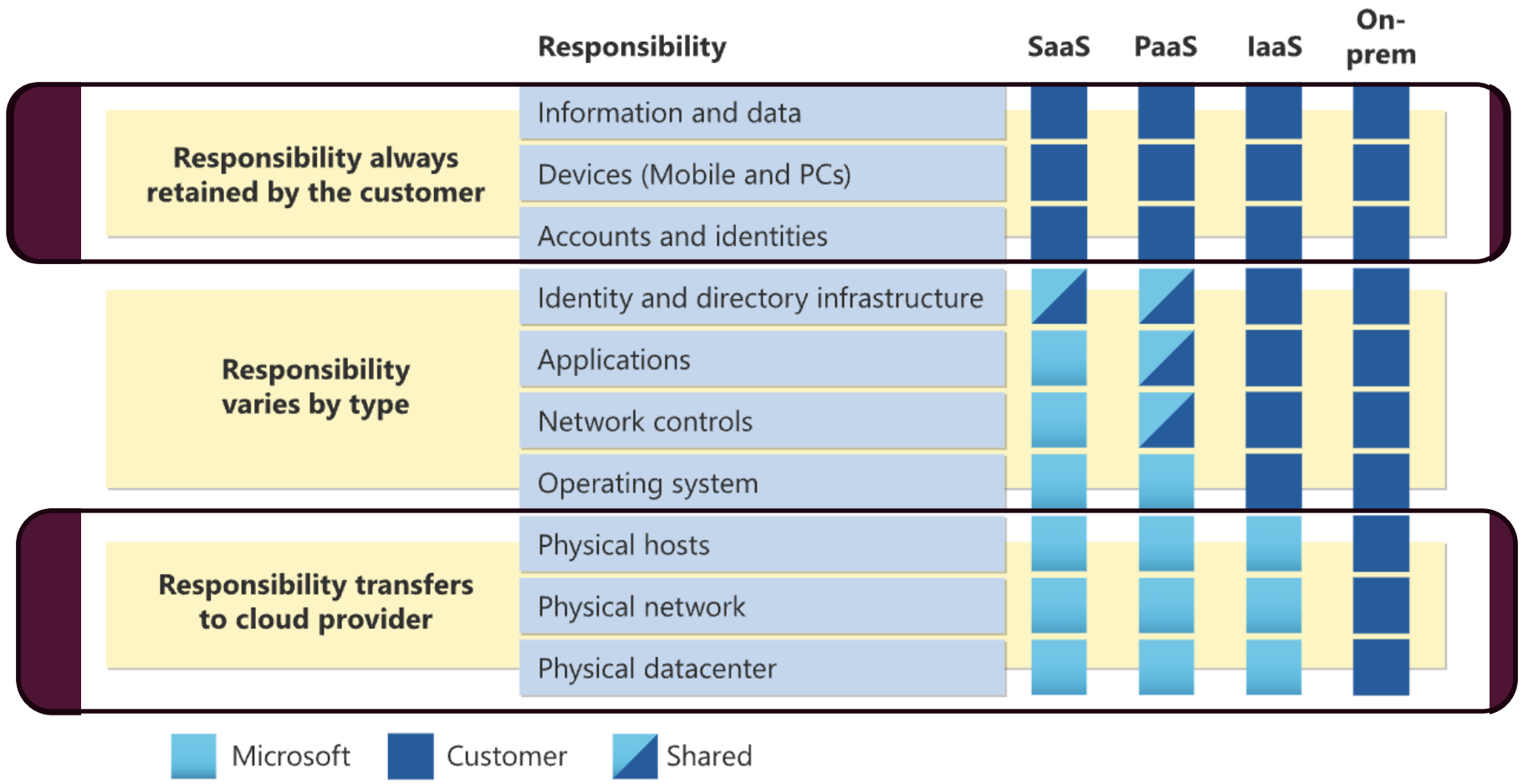
SHARED RESPONSIBILITY AND APPLICATIONS/WORKLOADS

https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

- DATA
- IDENTITIES
- APPLICATIONS
- DEVICES

- DATA
- IDENTITIES
- APPLICATIONS
- DEVICES
- NETWORKS

- DEVICES
- NETWORKS



10 min
BREAK
BACK
9:05PM ET

REFERENCE / REMINDER: CONTROLS FOR DEVICES

RESOURCE/REMINDER: SERVER PROTECTION

https://www.malwarebytes.com/cybersecurity/business/what-is-server-security

1. Inventory: Maintain accurate inventory of all servers / devices (technically includes compute)
2. Security software: Endpoint security / next gen anti-virus is in place to prevent/detect malware (where possible)
3. Secure Configuration: Maintain secure configuration baseline
4. Software updates: Regularly install security patches to plug vulnerabilities and improve security features.
5. Firmware updates: Regularly check your hardware for vulnerabilities and ensure access is restricted
6. Login security: Reset default passwords, Enforce strong passwords and multi-factor authentication
7. Network Segmentation: Block unauthorized access; control incoming and outgoing network traffic
8. Restrict access: Leverage permissions and access control to restrict actions.
9. Event logging: Monitor server logs and security events to detect and respond to security incidents.
10. Backups: Regularly backup server data to minimize disruptions from a cyber attack or disaster.
11. Encryption (In Transit, At Rest): Protect sensitive data, stored on or moving across a network between servers.
12. Secure remote access: VPN / Bastion Host .
13. Risk assessments: Identify and address vulnerabilities and check the strength of your security measures.
14. Insider threat:. Complete background checks and monitor activity to stop inadvertent or deliberate insider threats.

RESOURCE/REMINDER: NETWORK DEVICE PROTECTION
adapted from https://www.malwarebytes.com/cybersecurity/business/what-is-server-security

1. Inventory: Maintain accurate inventory of all network devices
2. Security software: Usually not possible, but where possible, add NGAV
3. Secure Configuration: Maintain secure configuration baseline; Do not allow EOL/EOS devices;
    1. Do not rely on extended support agreements
4. Software updates: Regularly install security patches to plug vulnerabilities and improve security features.
5. Firmware updates: Regularly check your hardware for vulnerabilities and ensure access is restricted
6. Login security: Reset default passwords, enforce strong passwords and where possible multi-factor authentication
7. Network Segmentation: Limit admin access to local network only; Block unauthorized access
8. Restrict access: Leverage permissions and access control to restrict actions.
9. Event logging: Monitor network access, event logs for anomalous activities.
10. Backups: Regularly backup configuration data to minimize disruptions from a cyber attack or disaster.
11. Encryption (In Transit): See secure remote access
12. Secure remote access: Limit access VPN / Bastion Host .
13. Risk assessments: Identify and address vulnerabilities and check the strength of your security measures.
14. Insider threat:. Complete background checks and monitor activity to stop inadvertent or deliberate insider threats.

RESOURCE/REMINDER: WORKSTATION/ENDPOINT PROTECTION

https://www.strongdm.com/blog/workstation-security-policy

At a high level, a workstation is a device - be it personal or company-owned - that contains company data. This includes desktops and laptops, as well as mobile devices.

1. Inventory: Maintain accurate inventory of all endpoints (including mobile devices!)
2. In Support / Software updates: Do not allow EOL/EOS devices; Regularly install security patches.
3. Require centralized management for inventory and standard (remote) configuration..
4. Require an operating system baseline (secure configuration baseline)
5. Require workstation (hard drive) encryption
6. Require that workstations are locked when not in use / deploy session timeout restrictions
7. Define that workstations must be used for authorized business purposes only
8. Require loss or theft of devices should be reported immediately
9. Require laptops and desktop devices to have the latest version of antivirus software (part of device configuration)
10. Require endpoints to have their operating system patched monthly and on-demand as required
11. Require endpoints to have 3rd party applications (Adobe, Java, browsers, etc.) to be patched monthly and on-demand as required
12. Deploy physical safeguards (secure when travelling, physical locks when in office)

	Server / Compute	Work-station	Network Device
Inventory: Maintain accurate inventory of all devices			
Security software: Endpoint security / anti-virus is in place to prevent/detect malware			
Secure Configuration: Maintain secure configuration baseline (CIS, STIG, etc)			
Software updates: Regularly install security patches to plug vulnerabilities and improve security features.			
Login security: Enforce strong passwords and multi-factor authentication (reset default passwords)			
Firewalls: Block unauthorized access and control incoming and outgoing network traffic (remove Internet facing admin)			
Restrict access: Leverage permissions and access control to restrict actions.			
Event logging: Monitor server logs and security events to detect and respond to security incidents.			
Backups: Regularly backup server data to minimize disruptions from a cyber attack or disaster.			
Encryption (In Transit, At Rest): Protects sensitive data, whether stored on a server or moving across a network.			
Risk assessments: Identify and address vulnerabilities and check the strength of your security measures.			
Encryption in Transit: Include certificate based TLS mutual authentication .			
Secure remote access: VPN / Bastion Host .			
Physical security: Regularly check your hardware for vulnerabilities and ensure access is restricted. Complete background checks and monitor activity to stop inadvertent or deliberate insider threats.			

APPLICATIONS

Asset Class	Examples
Network	Communication channels, connections and protocols that enable traffic to flow among devices and applications. Note that this does NOT refer to the actual infrastructure (routers, switches) but rather to the paths themselves and the protocols used in those paths. This class includes VPC, VPN, CDN as well as DNS, BGP, email and web filtering
Devices	Workstations, servers, phones, tablets, IoT, containers, hosts, compute, peripherals storage devices, network devices, web cameras, infrastructure, etc. This asset class includes the operating systems and firms of these devices as well as other software that is native to or inherent to the device. Networking devices like switches and routers are included here because the devices themselves need to be considered separately from the communication path they create.
Applications	Software code and applications on the devices, separate from the operating system/firmware. This class includes serverless functions, APIs and microservices. This also includes the business applications that support a company - from HR Systems (eg Workday), to Customer Relationship Management (eg Salesforce), to payroll, billing, and the applications that are “used” to do work (email,G Suite/Box, web conferencing, telephone systems)
Data	The information residing on (data-at-rest), traveling through (data-in-motion), or processed (data-in-use) the resources listed above. This class includes databases, S3 buckets, storage blobs, and files
Users	The people using the resources listed above and their associated identities. This includes customers (using the applications/services your company provides) and the employees of your company

APPLICATIONS, WORKLOAD: DEFINITION

Apps	Applications and workloads include agency systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments. Software code and applications on the devices, separate from the operating system/firmware. This class includes serverless functions, APIs and microservices. This also includes the business applications that support a company - from HR Systems (eg Workday), to Customer Relationship Management (eg Salesforce), to payroll, billing, and the applications that are "used" to do work (email, GSuite/Box, web conferencing, telephone systems, etc)

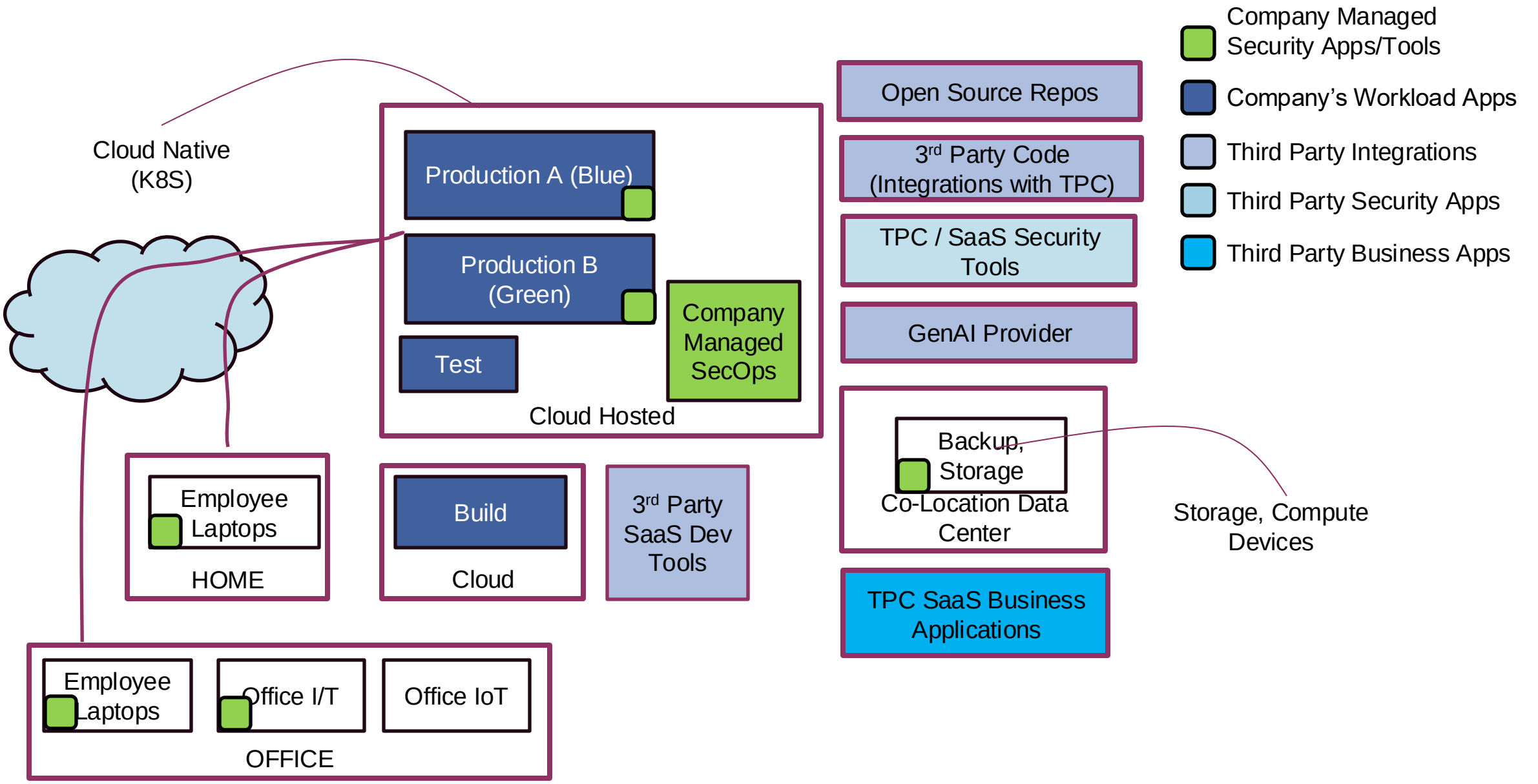
APPLICATIONS AND WORKLOADS

https://www.ibm.com/think/topics/workload

- An "application" refers to the software itself, like a web app or mobile app, designed to perform specific tasks for users
  - Application is static: The application itself is a fixed entity with defined features and functions.
- A "workload" represents the processing demands that application places on the system, including CPU usage, memory, and disk space needed to run that application, essentially the "amount of work" it generates based on user activity and features used
  - Workload is dynamic: A workload can fluctuate depending on user activity, number of concurrent users, and the tasks being performed within the application.
- In simpler terms, an application is the program, and a workload is the "load" that program puts on the system when it's running

APPLICATIONS AND WORKLOADS: ZTA FUNCTIONS

- Application Access (formerly Access Authorization)
  - Increasingly automated, real-time just-in-time/just-enough/behaviorusage pattern-based access
- Application Threat Protections (Formerly Threat Protections)
  - Increasingly advanced (continuous) monitoring for including anomalous behavior, endpoint verification, and threat detection and response.
- Accessible Applications (Formerly Accessibility)
  - Moving from private network/VPN access to public network access
- Secure Application Development and Deployment Workflow (NEW FUNCTION)
  - Covered in CSCI 149
  - Lower-level maturity focused on development; optimal/advanced focused on workload in production
- Application Security Testing (Formerly Application Security)
  - Covered in CSCI 149; Focused on security testing throughout application develop/deploy lifecycle


Company Managed Security Apps/Tools
Company's Workload Apps
Third Party Integrations
Third Party Security Apps
Third Party Business Apps
Cloud Native (K8S)
Production A (Blue)
Production B (Green)
Test
Company Managed SecOps
Cloud Hosted
Open Source Repos
3rd Party Code (Integrations with TPC)
TPC / SaaS Security Tools
GenAI Provider
Backup, Storage
Co-Location Data Center
Storage, Compute Devices
TPC SaaS Business Applications
Employee Laptops
HOME
Build
Cloud
3rd Party SaaS Dev Tools
Employee Laptops
Office I/T
Office IoT
OFFICE

APPS/WORKLOADS

Company's Product/Services

1. [OnPrem] Company Developed/Deployed/Managed Workload - the products/services provided by the Company
2. [SaaS, PaaS] Company Managed TPC "Workload" Apps – developed/deployed/BC-DR by TP, integrated into company's developed Workload Apps
3. [OnPrem] Company Deployed/Managed TPC "Security" Apps - developed by TP, deployed/managed by Company in support of Company's Workload apps
4. [SaaS] TPC Developed/Deployed SaaS Development Tools – develop/deploy/BC-DR by TP, configured by Company

Company's Business and IT Operations

1. [OnPrem] Company Deployed/Managed TPC "IT Security" Apps / Tools – security apps developed by TP, deployed/managed by Company on workstations, mobile devices
2. [OnPrem, MSP] TPC Developed/Deployed, Shared Management "IT Security" Apps Tools – deployed on workstations, mobile devices, managed by third party (MSP)
3. [SaaS] TPC Developed/Deployed, Shared Management Business Apps – used to run company's business

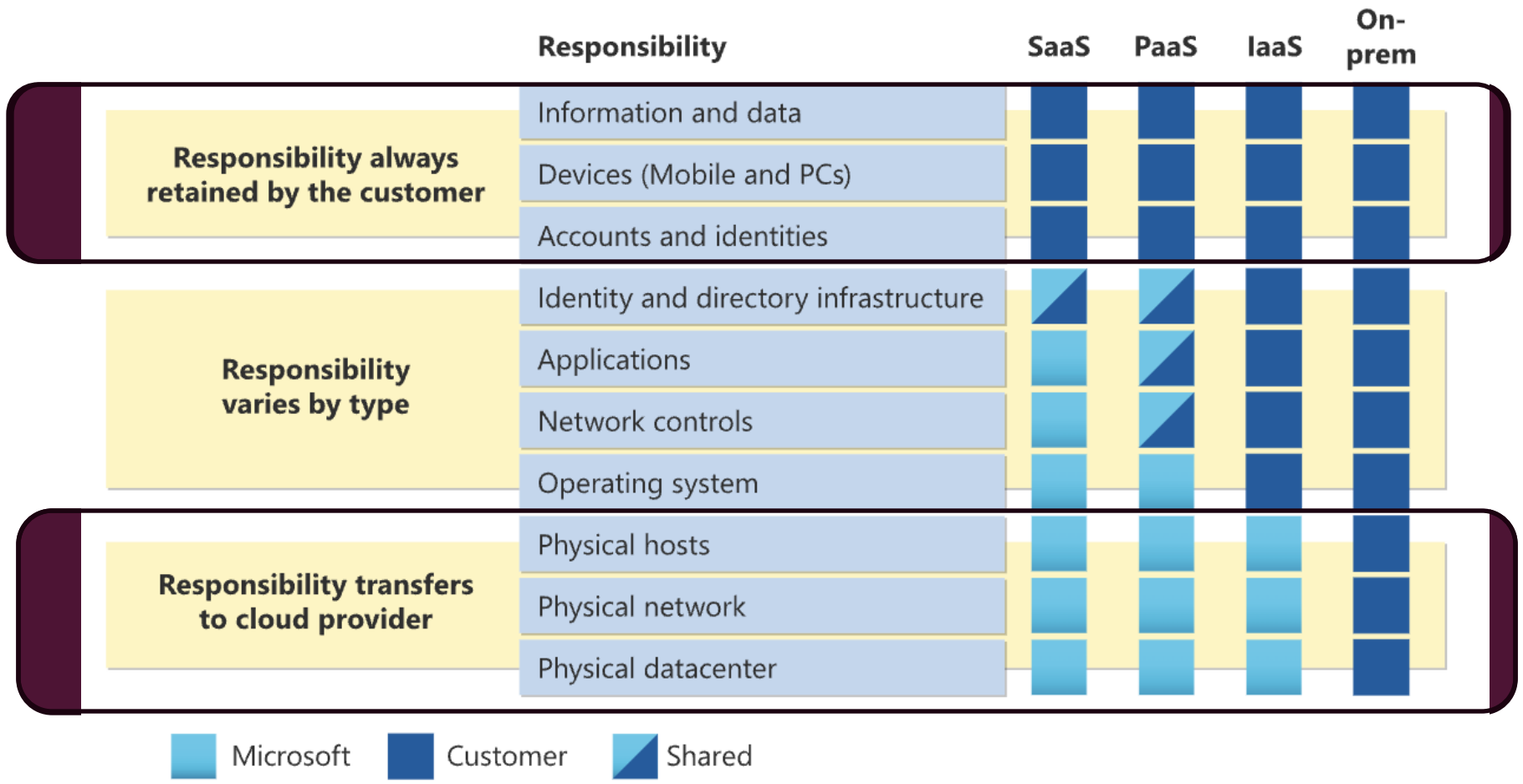
SHARED RESPONSIBILITY AND APPLICATIONS/WORKLOADS

https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

- DATA
- IDENTITIES
- APPLICATIONS
- DEVICES

- DATA
- IDENTITIES
- APPLICATIONS
- DEVICES
- NETWORKS

- DEVICES
- NETWORKS



A NOTE ON SHARED RESPONSIBILITY

- Shared Responsibility is the downside of Cloud-based environments
  - Sometimes the lack of control (control is what you give up) is not worth the risk that the control is not done well / to the level you expect
  - Sometimes the handoff of control is not that clear or clearly-handled
- Sometimes the information sharing is not always as clean as it should be
  - Reference the requirements in Secure by Design Pledge for access to logs….

APPLICATIONS: Zero Trust Maturity Levels

Applications and workloads include agency systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments.			
Traditional	**Initial**	**Advanced**	**Optimized**
• Mission critical applications accessible via private networks • Protections have minimal workflow integration • *Ad hoc development, testing, and production environments*	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • *Formal code deployment mechanisms through CI/CD pipelines* • *Static and dynamic security testing prior to deployment*	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • *Coordinated teams for development, security and operations*	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout the lifecycle

Figure 4: High Level Zero Trust Maturity Model Overview

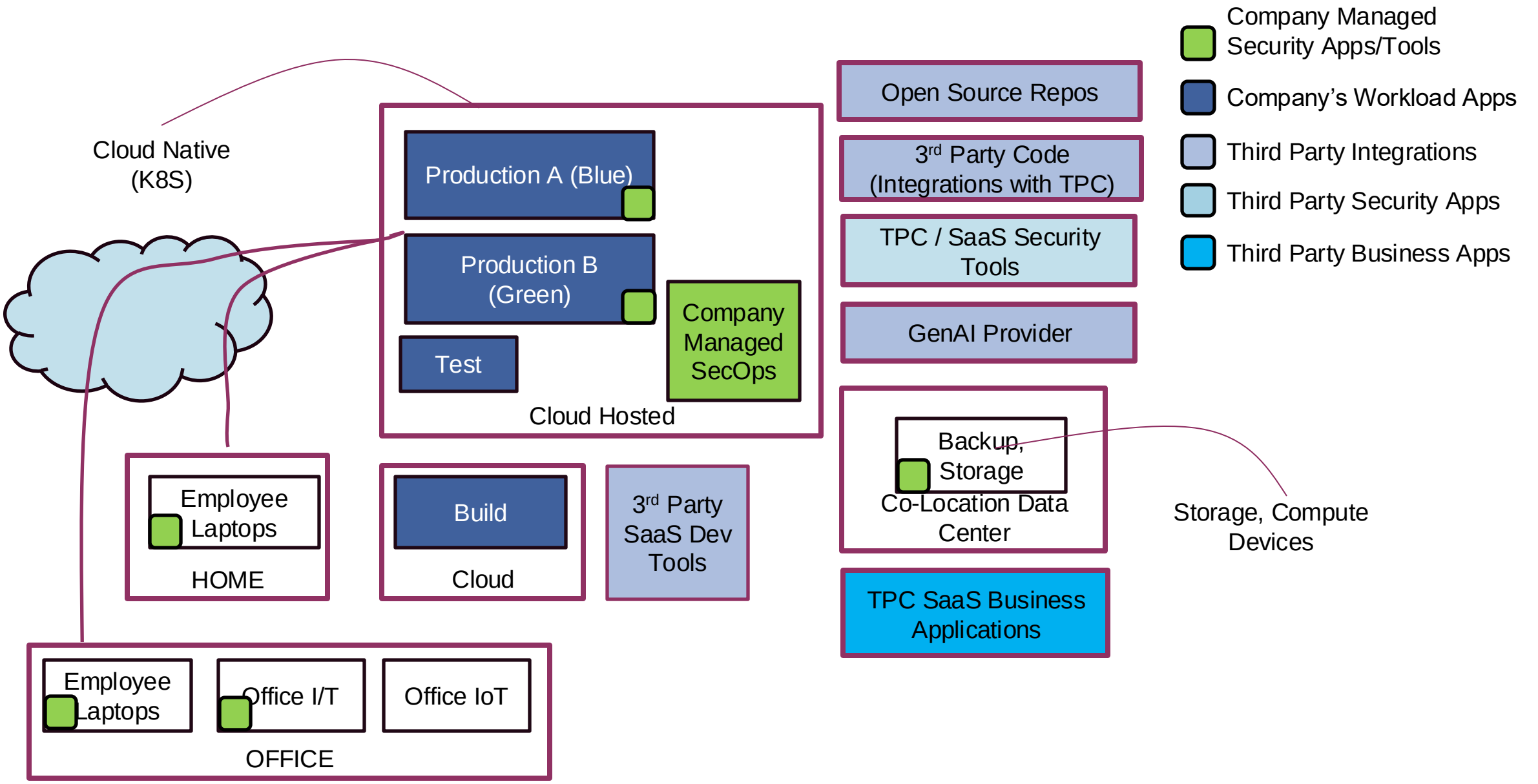
A NOTE ON APPLICATION INVENTORY

- Implicit in the Application category is that you have
  - An INVENTORY of applications
  - A CATEGORIZATION of applications

APPLICATION CRITICALITY

https://www.ibm.com/think/topics/mission-critical-applications

- Mission critical applications and workloads are those on which a business depends: if they fail or experience downtime, a business' core operations, reputation and sources of revenue are at risk
  - Mission-critical applications are often important to business continuity (an organization's ability to perform during and after a crisis) and disaster recovery (a set of technologies and processes designed to restore essential functions after an unexpected event).
- Business critical applications (and workloads) are important for normal business function, but their failure might not be as catastrophic; their failure may cause disruptions to productivity but may not necessarily halt operations completely
  - Business critical applications are included business continuity plans (BCPs) or disaster recovery plans (DRPs)
- Business important applications
  - Business important workloads can perform below peak levels or sustain long periods of outage without damaging business operations or causing financial losses.


Company Managed Security Apps/Tools
Company's Workload Apps
Third Party Integrations
Third Party Security Apps
Third Party Business Apps
Cloud Native (K8S)
Production A (Blue)
Production B (Green)
Test
Company Managed SecOps
Cloud Hosted
Open Source Repos
3rd Party Code (Integrations with TPC)
TPC / SaaS Security Tools
GenAI Provider
Backup, Storage
Co-Location Data Center
Storage, Compute Devices
TPC SaaS Business Applications
Employee Laptops
HOME
Build
Cloud
3rd Party SaaS Dev Tools
Employee Laptops
Office I/T
Office IoT
OFFICE

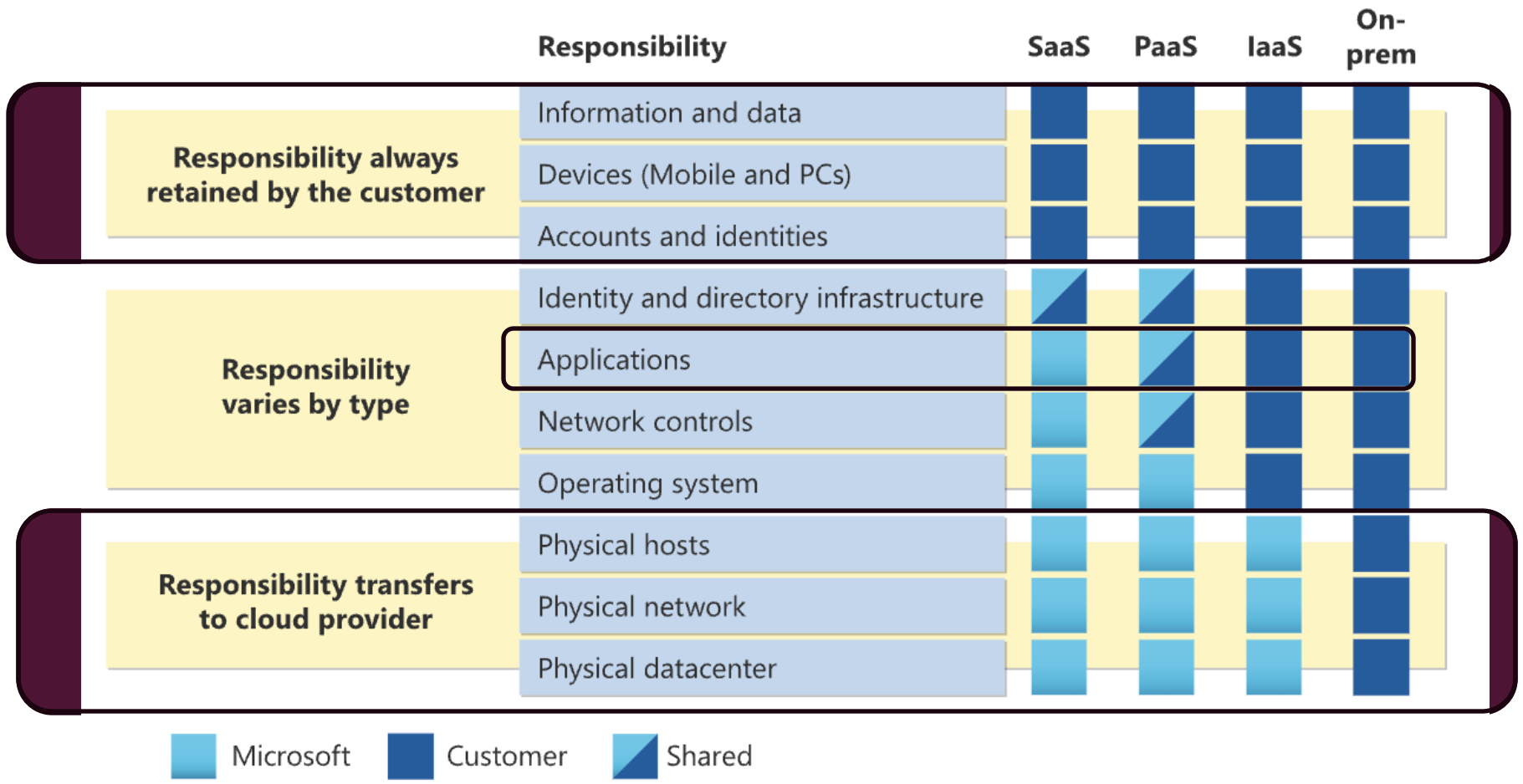
SHARED RESPONSIBILITY AND APPLICATIONS/WORKLOADS

https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

- DATA
- IDENTITIES
- APPLICATIONS
- DEVICES

- DATA
- IDENTITIES
- APPLICATIONS
- DEVICES
- NETWORKS

- DEVICES
- NETWORKS



CLASS POLL PROMPT: MISSION & BUSINESS CRITICAL

Which of the following is your #1 priority for designation as a Mission Critical application (Business fails if workload is not available)? *(Single choice)*

1. *[OnPrem] Company Developed/Deployed/Managed Workload - the products/services provided by the Company*
2. *[SaaS, PaaS] Company Managed TPC "Workload" Apps – developed, deployed by TP, integrated into company's developed Workload Apps*
3. *[OnPrem] Company Deployed/Managed TPC "Security" Apps - security tools developed by TP, deployed/managed by Company in support of Company's Workload apps*
4. *[OnPrem] Company Deployed/Managed TPC "IT Security" Apps / Tools – security apps developed by TP, deployed/managed by Company on workstations, mobile devices*
5. *[SaaS] TPC Developed/Deployed SaaS Development Tools – develop, deploy BC/DR by TP, configured by Company*
6. *[OnPrem, MSP] TPC Developed/Deployed, Shared Management "IT Security" Apps Tools – deployed on workstations, mobile devices, managed by third party (MSP)*
7. *[SaaS] TPC Developed/Deployed, Shared Management Business Apps – used to run company's business*

CLASS DISCUSSION PROMPT: PROTECTING DEVICES & NETWORKS

- *How does your assessment of Mission Criticality and Business Criticality – when considering unavailability of workloads – align with how you think about the most important security considerations?*
- *Assuming (hoping) that class' number on priority was "Business Apps", how does this impact how you think about the prioritization of securing your organization?*
  - *How does all of the time, effort, money that vendors pour into marketing security tools to you align with (does it align with) your business's mission and business criticality protection priorities?*

ANTICIPATED END OF LECTURE 7

ANTICIPATED END OF LECTURE 7