



HARVARD EXTENSION SCHOOL



# CSCI E-117A SPRING 2024

SECURE APPLICATIONS: MANAGING THE DEPLOYMENT  
INFRASTRUCTURE

Lecture 12  
April 22, 2024

---

# LECTURE 12

## AGENDA

- 
- *Applying ZTMM with help from*
    - *Cyber Defense Matrix*
    - *Cybersecurity Framework (CSF)*
    - *Threat & Risk Assessments*
  - *Applied to Stuff In the News*
    - *MGM ALPHV Compromise*
    - *CapitalOne Compromise*
    - *Xzutils*
    - *Colonial Pipeline*
  - *Assignment IV, Capstone*
    - *Discussion, Q&A*

## QUICK ANNOUNCEMENTS

### April 22 Lecture

- Another Use Case and Capstone Q&A
- Discussion will essentially be bonus

### April 23 ...

- Verizon Data Breach & Incident Report published

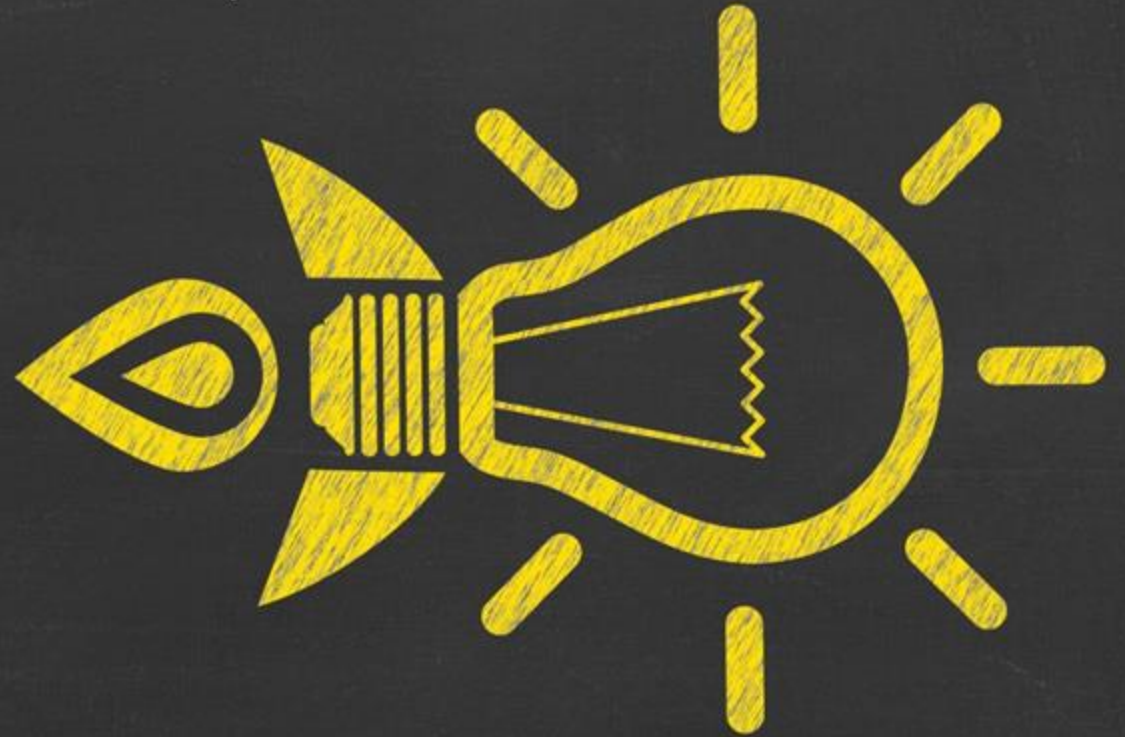
### April 29 Lecture

- Guest Lecturer, Gernette Wright, CISO-Americas, Schneider Electric
- Capstone Q&A with Carlos

May 4 (Saturday!) Capstone Due

May 6 – No Lecture (Exam Week)

# DISCUSSIONS LAST WEEK



## DISCUSSIONS

- The insurance company never asked for evidence! More recently I helped this same company with renewing PCI compliance, and it was the same thing: I gave answers to lots of questions that were never going to be validated (note: some PCI compliance levels do require an independent assessor and/or periodic third-party vulnerability scans, but not for this company since the number of transactions is very low). Thinking about PCI some more, I guess I don't really have a problem with their risk-based approach, but I still think there is a larger issue with validating security compliance of third parties. I guess the answer lies in the risk appetite of the organization.
- FOOD FOR THOUGHT: What if company doesn't properly evaluate their "attractiveness" as a target and so totally misreads the risk appetite they SHOULD have?

# DISCUSSIONS

- If I had liberty to twist the wordings in ZTMM functions and asset class than I will rephrase the e2e application development to "developer security"!! This will help me answer question - How can I secure my developer persona to securely develop an application? The answer will include considerations like,
  1. 1) developer login (short lived vs long lived)
  2. 2) session management per user
  3. 3) securing libraries - creation, updates, deletion, change propagation etc. (in content of xz utils CVE)
  4. 4) secrets management (rotation, expiration, discontinue use of weak secrets and tokens)
  5. 5) NHI's - rotating, secure generation
  6. 6) just in time, just enough access
  7. condition based policy enforcement for high risk actions
  8. testing - combination of security + quality (performance) + data science to see anomalies

## DISCUSSION

- My understanding of how third-party risk assessments are carried out draws more from my education in this cybersecurity degree program than any personal experiences - in my professional life, I haven't spent any time working on or near third-party security risk. What I've gathered is the following - risk assessments are performed by sending a questionnaire or checklist to a potential (or current) business partner. Questionnaire responses are not validated. There is no next step or follow-up audit or verification that the responses are accurate. No proof or evidence is offered. Boxes are checked and everyone moves on.
- PROFESSOR'S RESPONSE:
  - Some customers will require evidence but this is a VERY intrusive activity and one that most companies will seriously push back on. This is why published, "not flexible" approaches such as NIST 800-53 are so powerful – you can point to them as "absolute controls that we manage to" in lieu of evidence

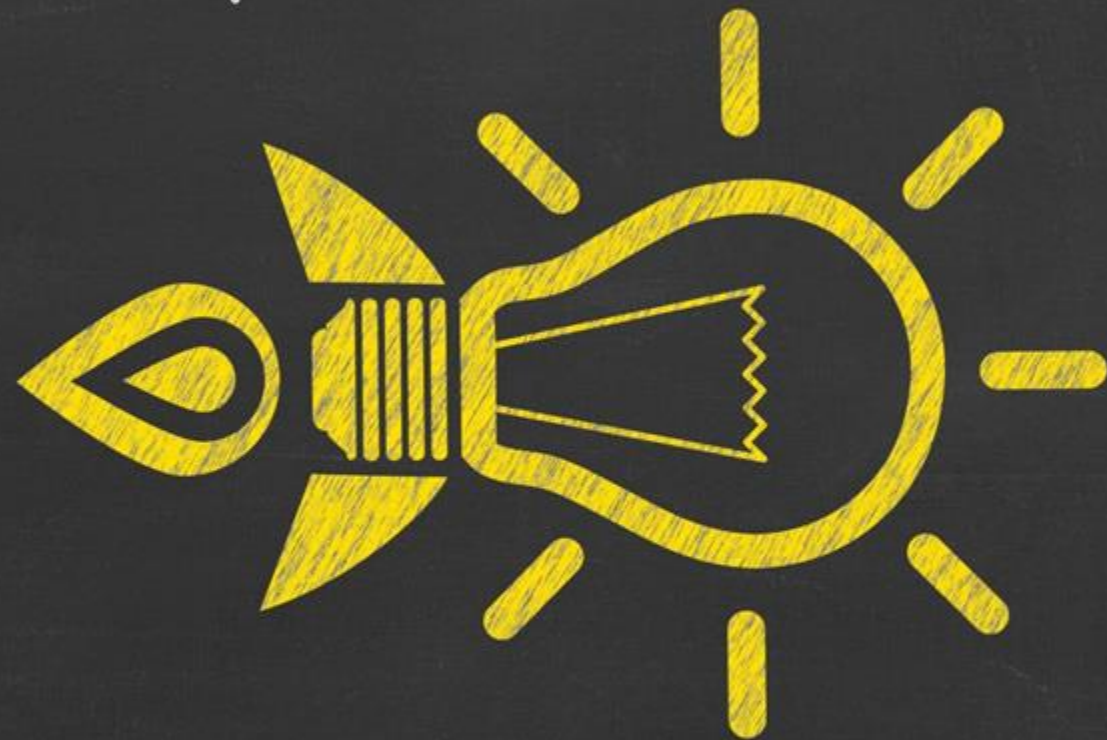


## DISCUSSION

- The DoD's TPRM program is built on continuous risk-based assessments, strict identity proofing (for both humans and non-human identities), and regular, documented evidence—not just trust or self-reporting. This is what the private sector should be aiming for. If a vendor can't demonstrate a strong identity discipline—proofing, credential rotation, and ongoing monitoring—they simply shouldn't get a free pass. Instead, we should be pushing for stronger contracts, more frequent and meaningful assessments, and a culture where security is everyone's job, not just a checkbox for compliance.
- In short, if we want to get serious about supply chain security, we need to look to what's worked for the DoD: comprehensive frameworks, continuous validation, organizational buy-in, and a relentless commitment to improvement. Otherwise, we'll keep spinning our wheels—and giving threat actors an open invitation.



YELLOWDIG LAST  
WEEK



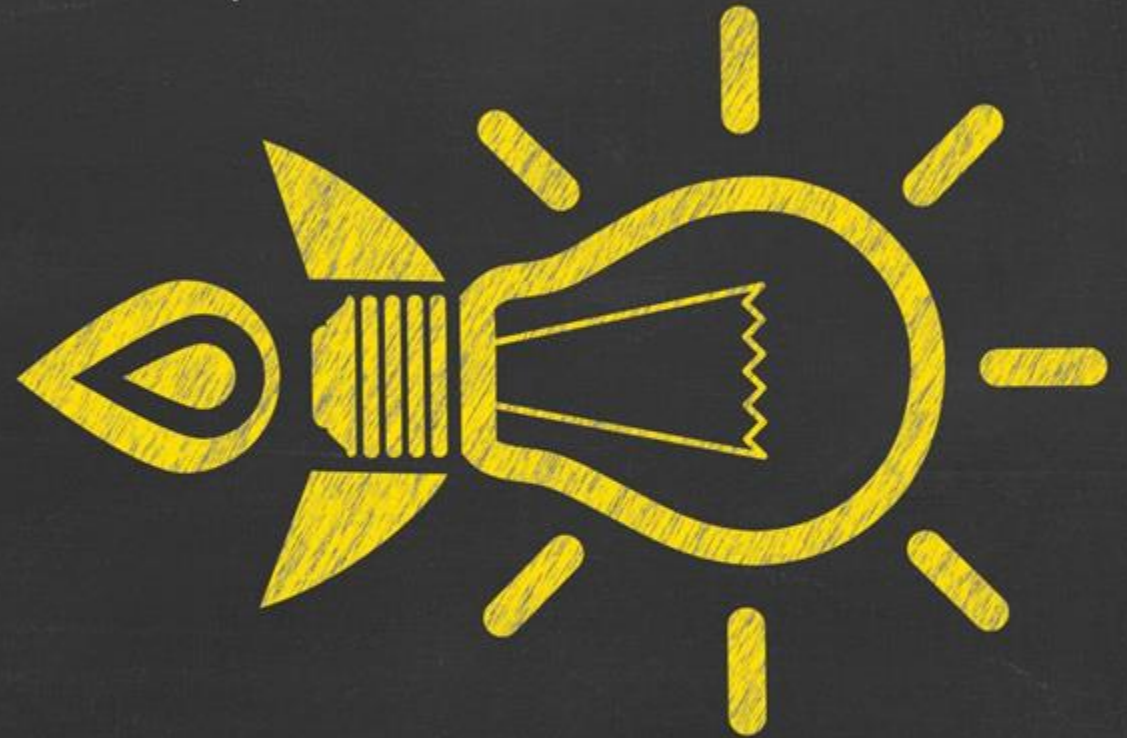
---

# LECTURE 12

## AGENDA

- 
- *Applying ZTMM with help from*
    - *Cyber Defense Matrix*
    - *Cybersecurity Framework (CSF)*
    - *Threat & Risk Assessments*
  - *Applied to Stuff In the News*
    - *MGM ALPHV Compromise*
    - *CapitalOne Compromise*
  - *Assignment IV, Capstone*
    - *Discussion, Q&A*

ZTMM  
CATEGORIES &  
FUNCTIONS



## CAPABILITIES

	Traditional	Initial	Advanced	Optimal
Visibility and Analytics Capability	Agency manually collects limited logs across their enterprise with low fidelity and minimal analysis.	Agency begins to automate the collection and analysis of logs and events for mission critical functions and regularly assesses processes for gaps in visibility.	Agency expands the automated collection of logs and events enterprise-wide (including virtual environments) for centralized analysis that correlates across multiple sources.	Agency maintains comprehensive visibility enterprise-wide via centralized dynamic monitoring and advanced analysis of logs and events.
Automation and Orchestration Capability	Agency relies on static and manual processes to orchestrate operations and response activities with limited automation.	Agency begins automating orchestration and response activities in support of critical mission functions.	Agency automates orchestration and response activities enterprise-wide, leveraging contextual information from multiple sources to inform decisions.	Agency orchestration and response activities dynamically respond to enterprise-wide changing requirements and environmental changes.
Governance Capability	Agency implements policies in an ad hoc manner across the enterprise, with policies enforced via manual processes or static technical mechanisms.	Agency defines and begins implementing policies for enterprise-wide enforcement with minimal automation and manual updates.	Agency implements tiered, tailored policies enterprise-wide and leverages automation where possible to support enforcement. Access policy decisions incorporate contextual information from multiple sources.	Agency implements and fully automates enterprise-wide policies that enable tailored local controls with continuous enforcement and dynamic updates.



## Category/Asset Class: Networks

	Network Segmentation	Network Traffic Management	Traffic Encryption	Network Resilience
Traditional	Agency defines their network architecture using large perimeter/macro- segmentation with minimal restrictions on reachability within network segments. Agency may also rely on multi-service interconnections (e.g., bulk traffic VPN tunnels).	Agency manually implements static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities (e.g. application performance monitoring or anomaly detection) and manual audits and reviews of profile changes for mission critical applications.	Agency encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency configures network capabilities on a case-by- case basis to only match individual application availability demands with limited resilience mechanisms for workloads not deemed mission critical.
Initial	Agency begins to deploy network architecture with the isolation of critical workloads, constraining connectivity to least function principles, and a transition toward service-specific interconnections.	Agency establishes application profiles with distinct traffic management features and begins to map all applications to these profiles. Agency expands application of static rules to all applications and performs periodic manual audits of application profile assessments.	Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications, to formalize key management policies, and to secure server/service encryption keys.	Agency begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms for workloads not deemed mission critical.
Advanced	Agency expands deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress micro- perimeters and service-specific interconnections.	Agency implements dynamic network rules and configurations for resource optimization that are periodically adapted based upon automated risk-aware and risk-responsive application profile assessments and monitoring	Agency ensures encryption for all applicable internal and external traffic protocols, manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.	Agency has configured network capabilities to dynamically manage the availability demands and resilience mechanisms for the majority of their applications.
Optimal	Agency network architecture consists of 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 interconnections.	Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications based on mission criticality, risk, etc.	Agency continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprise-wide and incorporates best practices for cryptographic agility as widely as possible.	Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.

## Category/Asset Class: Devices

	Policy Enforcement & Compliance Monitoring	Asset & Supply Chain Risk Management	Resource Access	Device Threat Protection
AKA	(Config & Patch) Compliance	Inventory (Physical, Virtual, Third Party)		
Traditional	Agency has limited, if any, visibility (i.e., ability to inspect device behavior) into device compliance with few methods of enforcing policies or managing software, configurations, or vulnerabilities.	Agency does not track physical or virtual assets in an enterprise-wide or cross-vendor manner and manages its own supply chain acquisition of devices and services in ad hoc fashion with a limited view of enterprise risks.	Agency does not require visibility into devices or virtual assets used to access resources.	Agency manually deploys threat protection capabilities to some devices.
Initial	Agency receives self-reported device characteristics (e.g., keys, tokens, users, etc., on the device) but has limited enforcement mechanisms. Agency has a preliminary, basic process in place to approve software use and push updates and configuration changes to devices.	Agency tracks all physical and some virtual assets and manages supply chain risks by establishing policies and control baselines according to federal recommendations using a robust framework, (e.g., NIST SCRM.)	Agency requires some devices or virtual assets to report characteristics then use this information to approve resource access.	Agency has some automated processes for deploying and updating threat protection capabilities to devices and to virtual assets with limited policy enforcement and compliance monitoring integration.
Advanced	Agency has verified insights (i.e., an administrator can inspect and verify the data on device) on initial access to device and enforces compliance for most devices and virtual assets. Agency uses automated methods to manage devices and virtual assets, approve software, and identify vulnerabilities and install patches.	Agency begins to develop a comprehensive enterprise view of physical and virtual assets via automated processes that can function across multiple vendors to verify acquisitions, track development cycles, and provide third-party assessments.	Agency's initial resource access considers verified device or virtual asset insights.	Agency begins to consolidate threat protection capabilities to centralized solutions for devices and virtual assets and integrates most of these capabilities with policy enforcement and compliance monitoring.
Optimal	Agency continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. Agency integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets.	Agency has a <u>comprehensive, at- or near-real-time view of all assets across vendors</u> and service providers, automates its supply chain risk management as applicable, builds operations that tolerate supply chain failures, and incorporates best practices.	Agency's resource access considers real-time risk analytics within devices and virtual assets.	Agency has a centralized threat protection security solution(s) deployed with advanced capabilities for all devices and virtual assets and a unified approach for device threat protection, policy enforcement, and compliance monitoring.

## Category/Asset Class: Applications & Workloads (CSCI I7 VERSION)

	Application Access (*)	Application Threat Protections (*)	Application Resilience (*)	Secure Application Lifecycle Oversight (*)
<b>Traditional</b>	Agency authorizes access to its SaaS applications primarily based on local authorization and static attributes.	Agency's SaaS applications have minimal integration with Agency's SIEM, relying on general purpose protections for known threats for SaaS applications.	Agency ensures some mission critical applications have backups maintained by SaaS provider with on-demand access to backups (ability to download) and on-demand ability to restore from backups to SaaS provider.	Agency has ad hoc development, testing, and production environments with non-robust code deployment mechanisms. Agency performs application security testing prior to deployment, primarily via manual testing methods
<b>Initial</b>	Agency begins to implement contextual information as part of authorizing access capabilities to its SaaS applications.	Agency integrates SaaS application logs into Agency's SIEM / threat intel for mission critical application workflows, applying protections against known threats and some application-specific threats.	Agency ensures mission critical and some business critical applications have backups maintained by SaaS provider with integrated access to backups (ability to download) and on-demand ability to restore from backups to SaaS provider.	Agency provides infrastructure for development, testing, and production environments (including automation) with formal code deployment mechanisms through CI/CD pipelines and requisite access controls in support of least privilege principles. Agency begins to use static and dynamic (i.e., application is executing) testing methods to perform security testing, including manual expert analysis, prior to application deployment.
<b>Advanced</b>	Agency automates application access decisions with expanded contextual information and enforced expiration conditions that adhere to least privilege principles.	Agency integrates SaaS application logs into Agency's SIEM / threat intel for all application workflows, protecting against some application-specific and targeted threats.	Agency ensures all applications have backups maintained by SaaS provider with integrated access to backups (ability to download) and automated ability to restore from backups to SaaS provider for mission critical applications.	Agency uses distinct and coordinated teams for development, security, and operations while removing developer access to production environment for code deployment. Agency integrates application security testing into the application development and deployment process, including the use of periodic dynamic testing methods.
<b>Optimal</b>	Agency continuously authorizes application access, incorporating real-time risk analytics and factors such as behavior or usage patterns.	Agency integrates SaaS application logs and real-time monitoring for advanced threat protections for all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks, misuse and abuse of applications.	Agency ensures all applications have backups maintained by SaaS provider with integrated access to backups (ability to download) and automated ability to restore from backups to SaaS provider for all applications as needed.	Agency leverages immutable workloads where feasible, only allowing changes to take effect through redeployment, and removes administrator access to deployment environments in favor of automated processes for code deployment. Agency integrates application security testing throughout the software development lifecycle across the enterprise with routine automated testing of deployed applications.



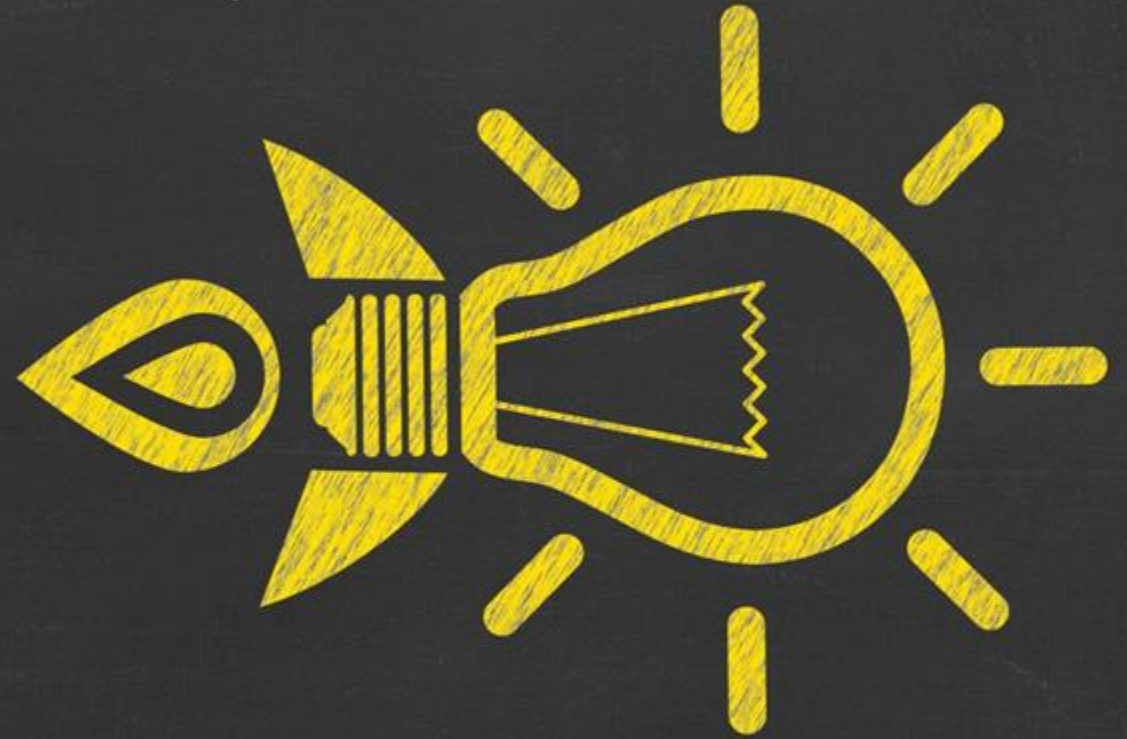
Accessible Applications	Agency makes some mission critical applications available only over private networks and <del>protected public network</del> connections (e.g., VPN) with monitoring.	Agency makes some of their applicable mission critical applications available over <u>open public networks</u> to authorized users with need via brokered connections.	Agency makes most of their applicable mission critical applications available over open public network connections to authorized users as needed.	Agency makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.
-------------------------	---	--	---	---

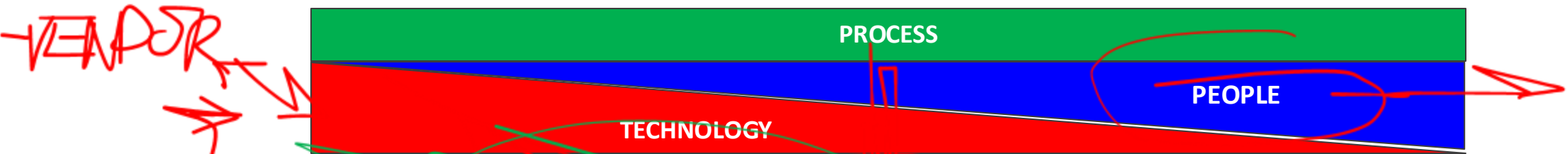


## Category/Asset Class: Identity

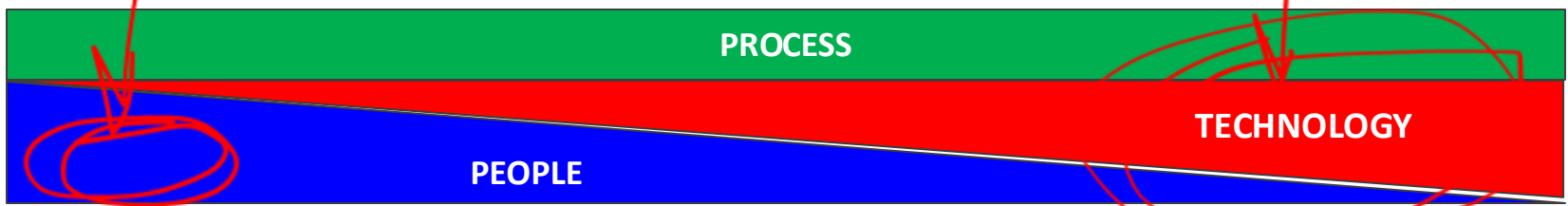
	Authentication	Identity Stores	Risk Assessments	Access Management
Traditional	Agency authenticates identity using either passwords or multi-factor authentication (MFA) with static access for entity identity.	Agency only uses self- managed, on-premises (i.e., planned, deployed, and maintained by agency) identity stores.	Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised).	Agency authorizes permanent access with periodic review for both privileged and unprivileged accounts.
Initial	Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).	Agency has a combination of self-managed identity stores and hosted identity store(s) (e.g., cloud or other agency) with minimal integration between the store(s) (e.g., Single Sign- on.).	Agency determines identity risk using manual methods and static rules to support visibility.	Agency authorizes access, including for privileged access requests, that expires with automated review.
Advanced	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of passwordless MFA via FIDO2 or PIV	Agency begins to securely consolidate and integrate some self-managed and hosted identity stores.	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.	Agency authorizes need- based and session-based access, including for privileged access request, that is tailored to actions and resources.
Optimal	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.	Agency securely integrates their identity stores across all partners and environments as appropriate.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.	Agency uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs.

# USE CASES & ZTMM COVERAGE





CYBERSECURITY FRAMEWORK	IDENTIFY	PROTECT	DETECT	RESPOND & RECOVER	
DEVICES					DEVICES
NETWORKS					NETWORKS
APPLICATIONS & DATA					APPLICATIONS & DATA
IDENTITIES					IDENTITIES
ZTMM	TRADITIONAL	INITIAL	ADVANCED	OPTIMIZED	



# CYBER DEFENSE MATRIX

## How to protect/detect/respond compromise



### PROTECT (ZTMM FOCUS)

- **Devices.** Inventory, secure configuration and vulnerability; remove unnecessary software, disable or [harden remote access](#) like RDP and VPNs; use [endpoint security software](#) that can detect exploits and malware; log and monitor activity
- **Networks.** Segment networks with strong authentication (incl 2FA/mutual auth) and authorization for least privilege access and monitor (encrypted) traffic
- **Applications.** Design for threats, secure development practices and environment, deploy into secure environments
- **[Data.** Maintain data inventory and data flow; encrypt data in transit and at rest; Create offsite, offline backups with regular tests to restore essential business functions.]
- **Users/Identities.** Provide ongoing security awareness training; strong identity proofing and validation, enforce 2FA/MFA; manage roles/permissions across user lifecycle



### DETECT

- **Devices:** Monitor / detect unusual activity including attempts to deploy ransomware (excessive/unexpected encryption).
- **Networks:** Monitor / detect unusual activity including C2 comms, data exfiltration
- **All:** Log all activity, aggregate and monitor logs to detect unusual activity

### RESPOND

- **Respond:** Established playbooks for addressing suspicious / abnormal behaviour with automation / manual actions



# BACKGROUND – CROWDSTRIKE GLOBAL THREAT REPORT

## Top 10 Industries Targeted by Interactive Intrusions

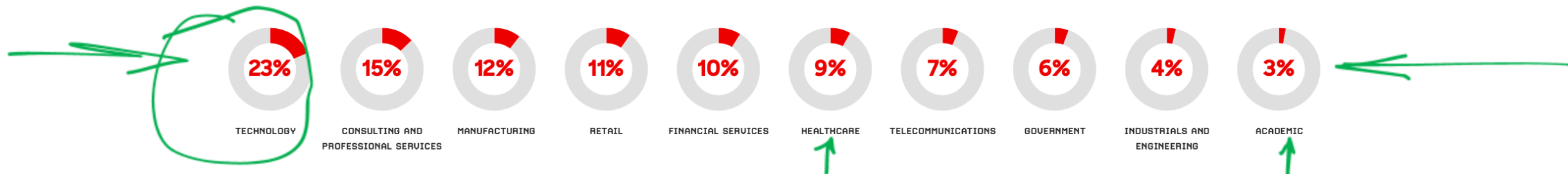


Figure 3. Top 10 industries targeted by interactive intrusions, January-December 2024

In 2024, new and unattributed cloud intrusions increased 26% compared to 2023, indicating more threat actors seek to exploit cloud services. CrowdStrike observed more intrusions in which attackers gained initial access via valid accounts, leverage cloud environment management tools for lateral movement, and abused cloud provider command line tools.

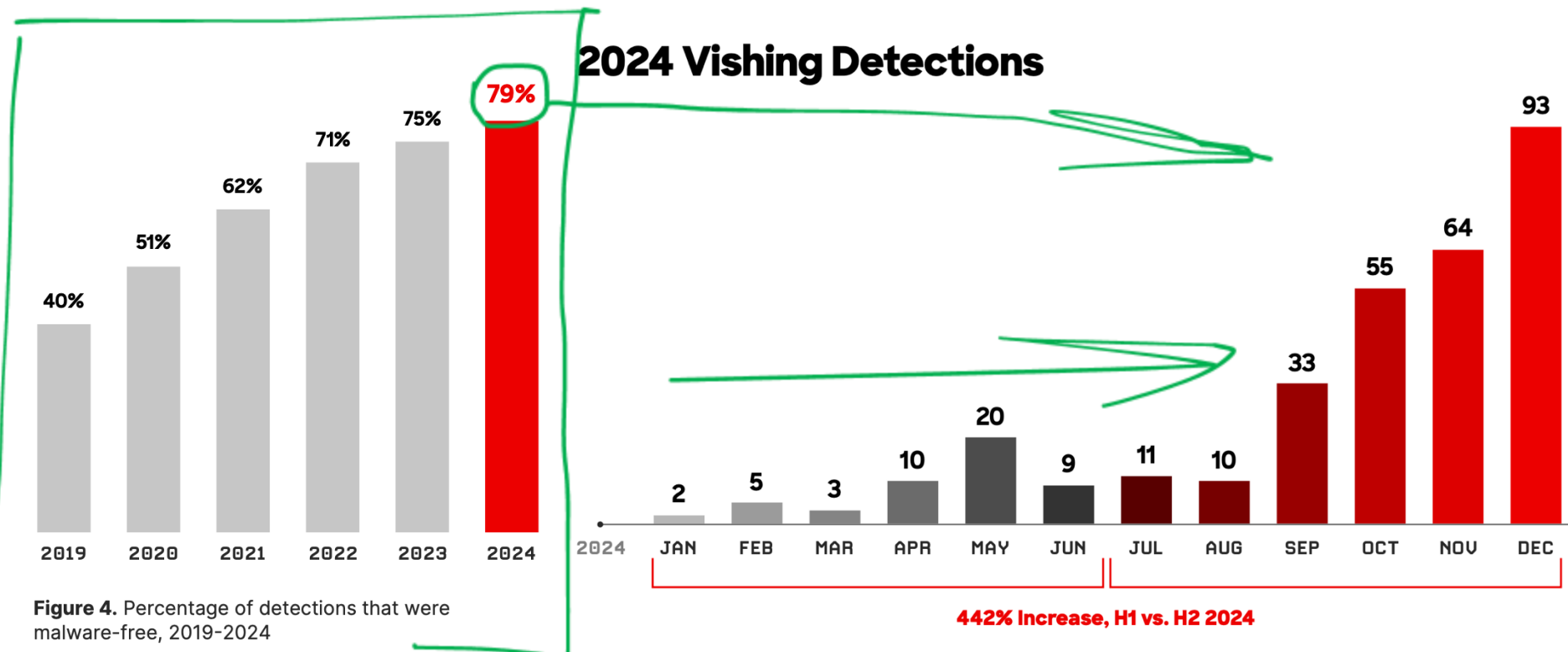


Figure 4. Percentage of detections that were malware-free, 2019-2024

# MITRE ATT&CK: ENTERPRISE TACTICS

<https://attack.mitre.org/tactics/enterprise/>





# STEP 1: INVENTORY & PREPARE

- Business type, focus (start to build a threat profile)
  - Publicly traded? Private? Regulated Industry? Defense / Public Sector / Critical Infrastructure?
- Understand why/how the Business is a target because compromising the business ...
  - Will (directly) hurt / negatively impact citizens and users
    - E.G. Colonial Pipeline, Texas Electrical Grid (not cyber but great example)
  - Will (can) provide access to the business, targeting the business's customers
    - E.G. Solarwinds, Progress
  - Will (can) provide access to the business, targeting the business's data
    - E.G. CaptialOne, Sony
  - Will (can) provide access to the business, targeting the business's data about it's customers/users
    - E.G. MGM, , SaltTyphoon/US Telcos
- Types of "risky behavior"
  - Employees do stuff on computers / online
  - Use "self-managed third-party code", Open Source Software, SaaS-based applications as part of supporting the business
  - Have Internet facing resources (devices, networks, applications)
  - Store / process data including PII, sensitive or confidential data
  - Provide services that are of value to consumers and/or citizens

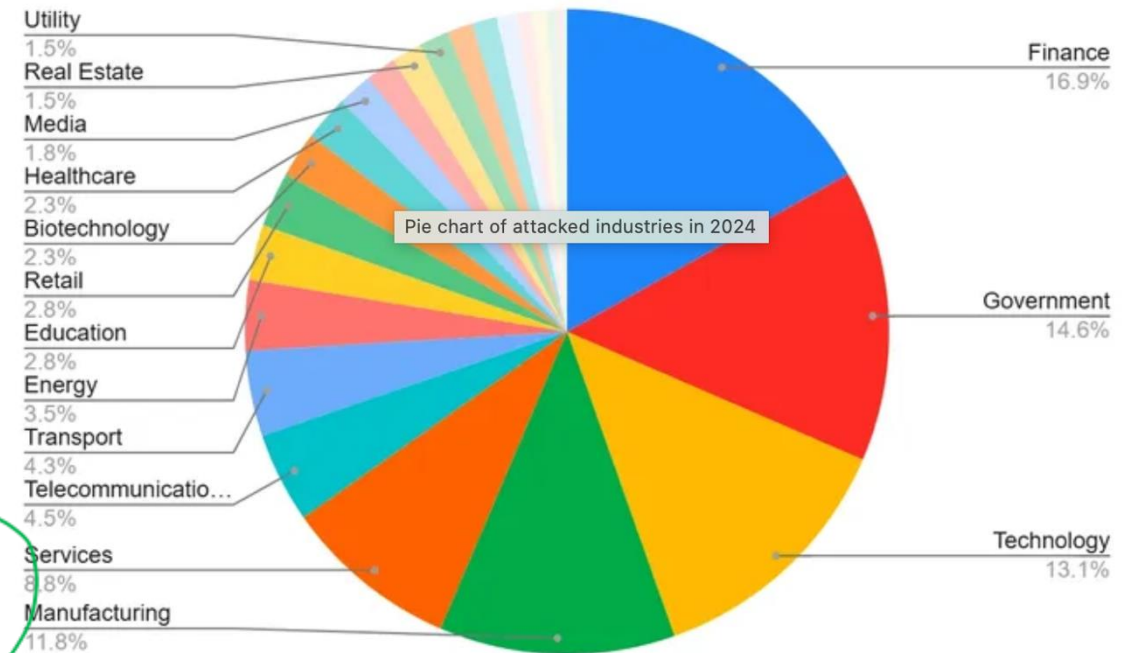
*Develop SW*

# Nation-State Threats Put SMBs in Their Sights

<https://www.darkreading.com/threat-intelligence/nation-state-threats-smb>

- Cyberthreat groups increasingly see small and medium-sized businesses, especially those with links to larger businesses, as the weak link in the supply chain for software and IT services.
- "The vast majority of organizations hit by nation-states are private sector and in the middle market."

#750 M ARR



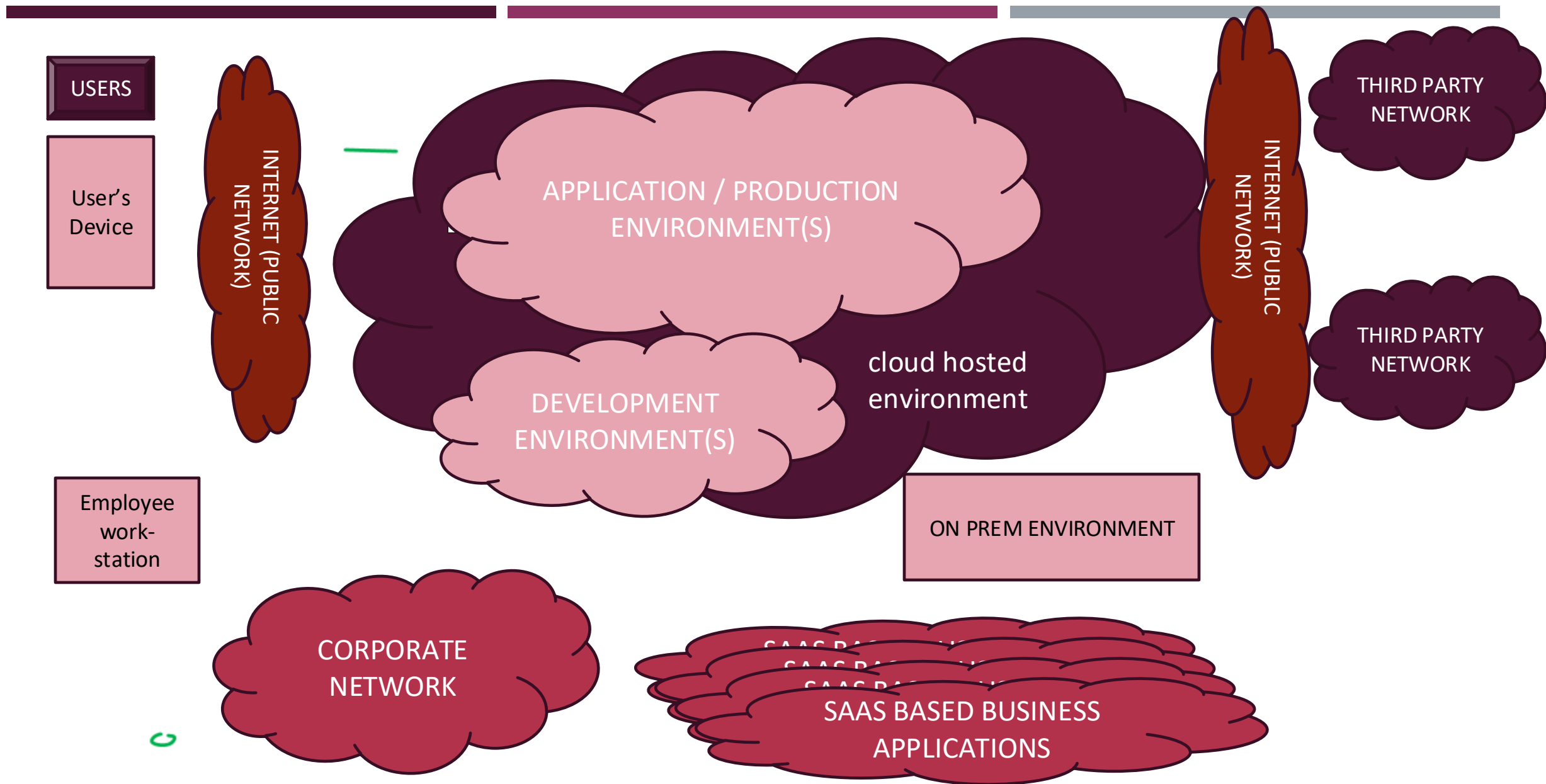
Attackers focused on financial firms, government agencies, and technology firms in 2024, with SMBs seeing a significant share of attacks. Source: Broadcom

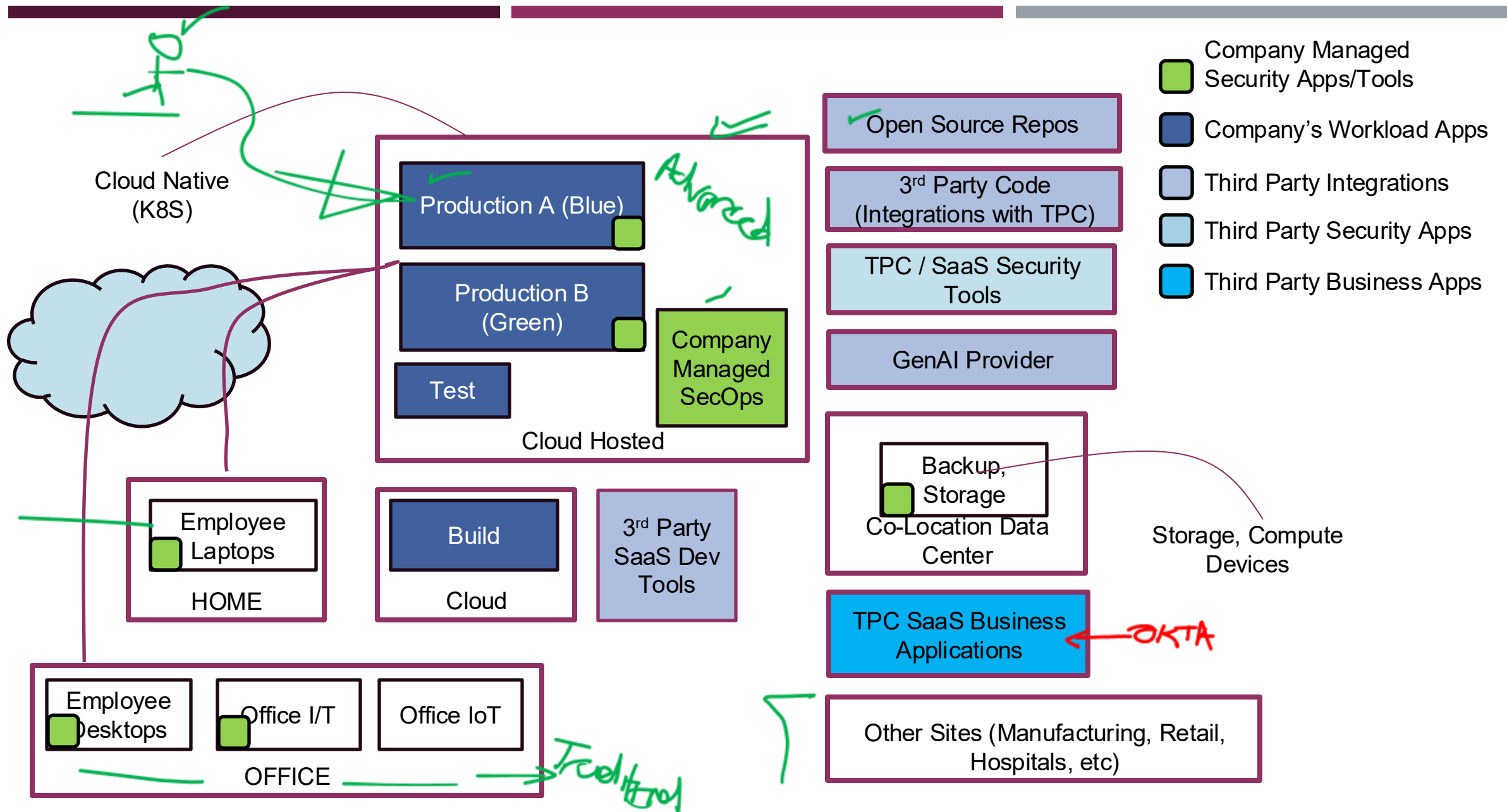
## STEP 2: INITIAL ACCESS

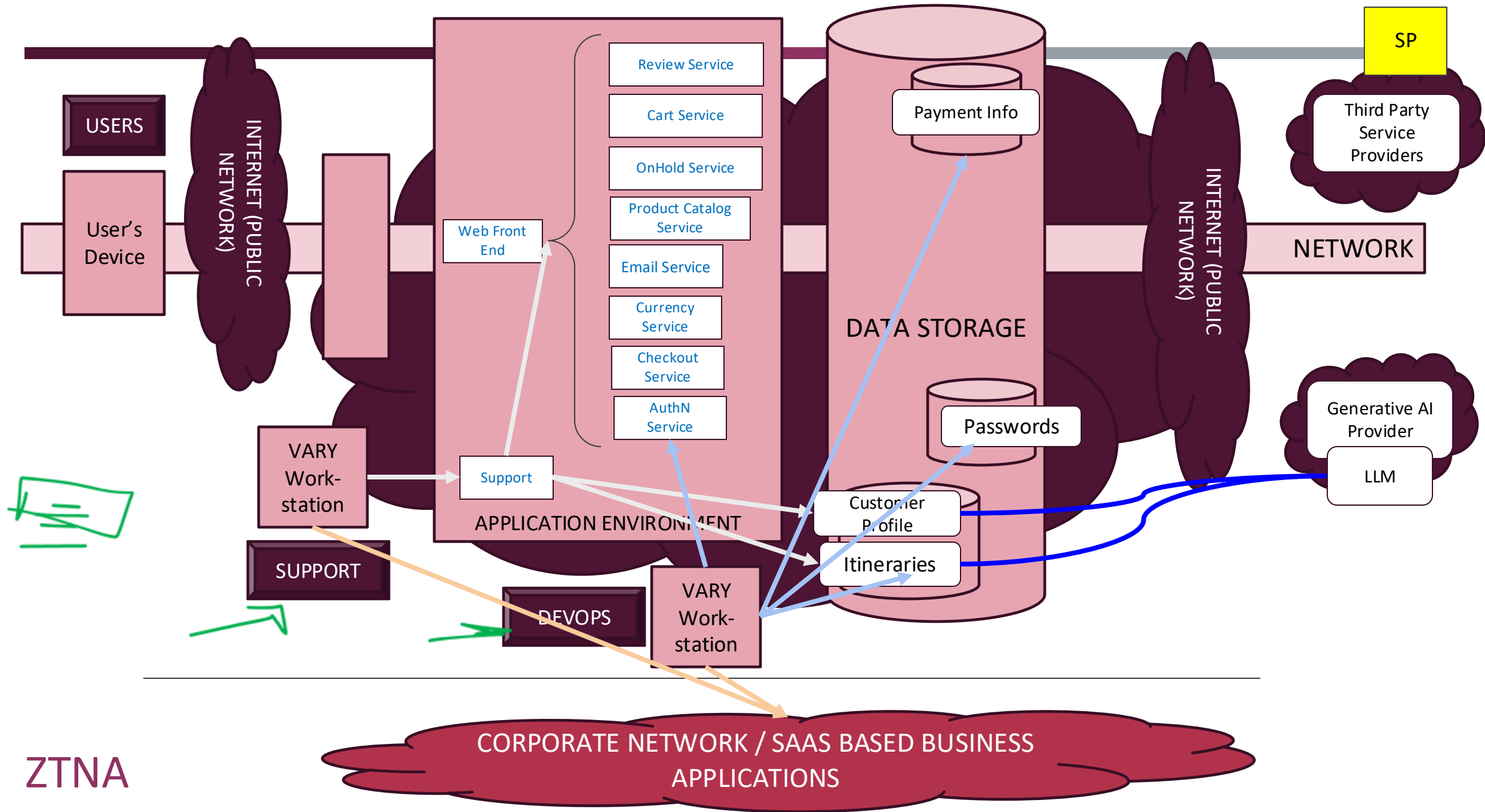
<https://attack.mitre.org/tactics/TA0001/>

- Ways that bad actors can implement initial access
  - Compromise employees (phishing++)
    - Identity: Identities, Credentials, Sessions
  - Compromise vulnerable, Internet facing components
    - Device: Firewalls, Servers, *Cloud based*
    - Devices: Workstations on public Internet
    - Applications & Workloads: Admin Consoles, *S3 buckets*
  - Compromise external remote services
    - Applications: VPN, Citrix Remote Desktop, File Transfer Services
  - Compromise third-party code       
    - Applications & Workloads: Trojan Horse as seen with SolarWinds, XZUtils
    - Applications & Workloads: Internet facing with exploitable vulnerabilities & weaknesses

*C*

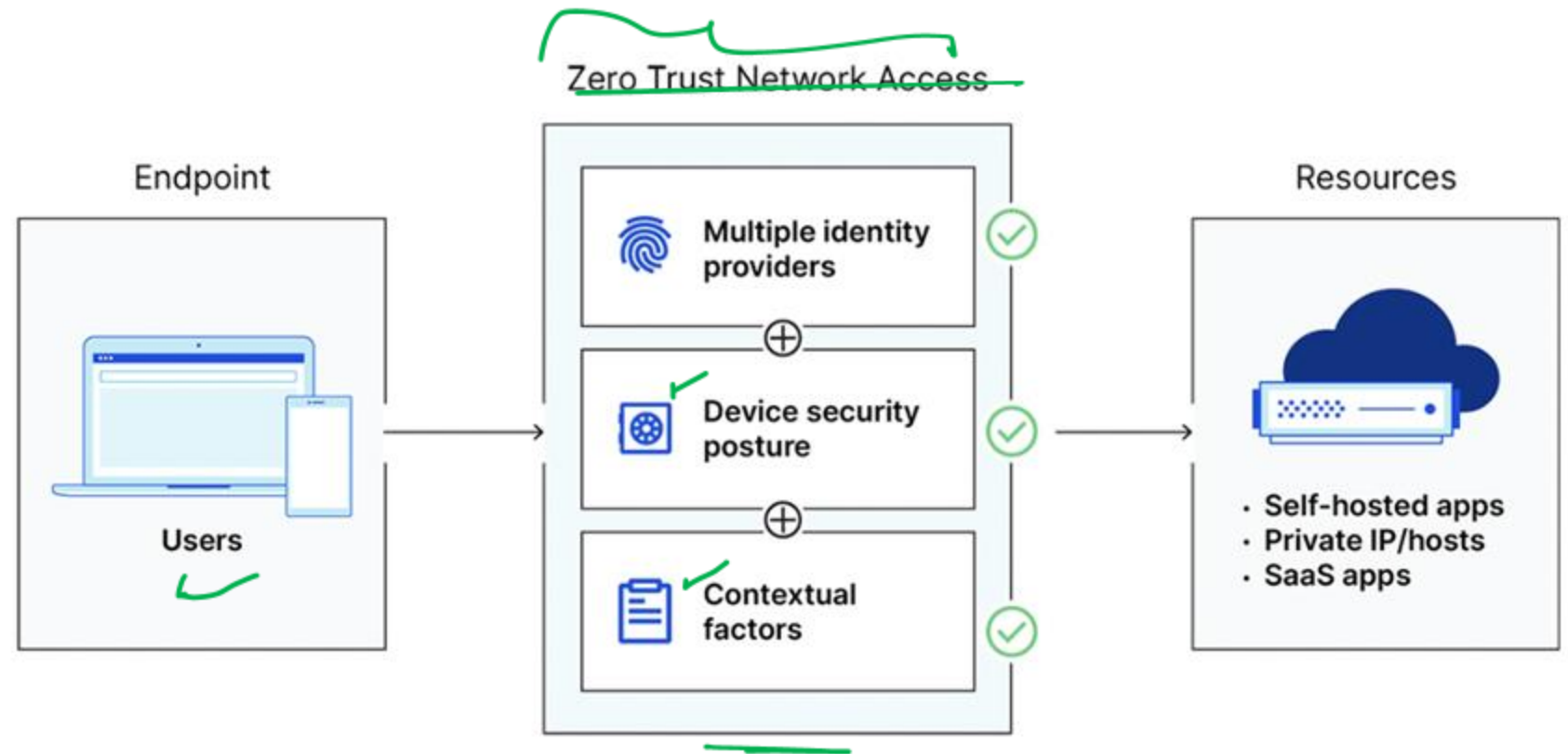






# ZERO TRUST NETWORK ACCESS: IN THEORY

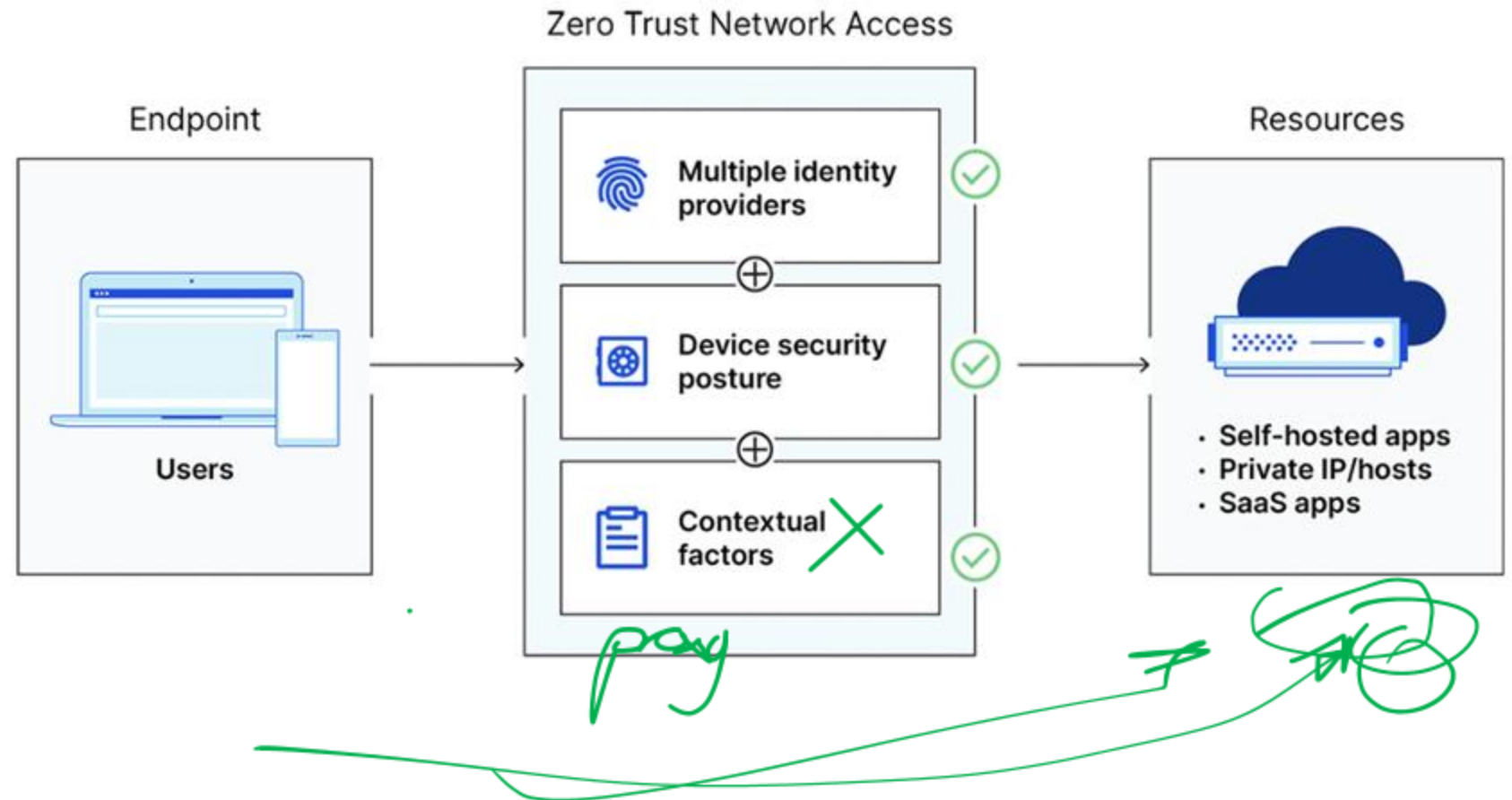
Zero Trust requires strict verification for every user and every device before authorizing them to access internal resources.





# ZERO TRUST NETWORK ACCESS: IN REALITY

Zero Trust requires strict verification for every user and every device before authorizing them to access internal resources.



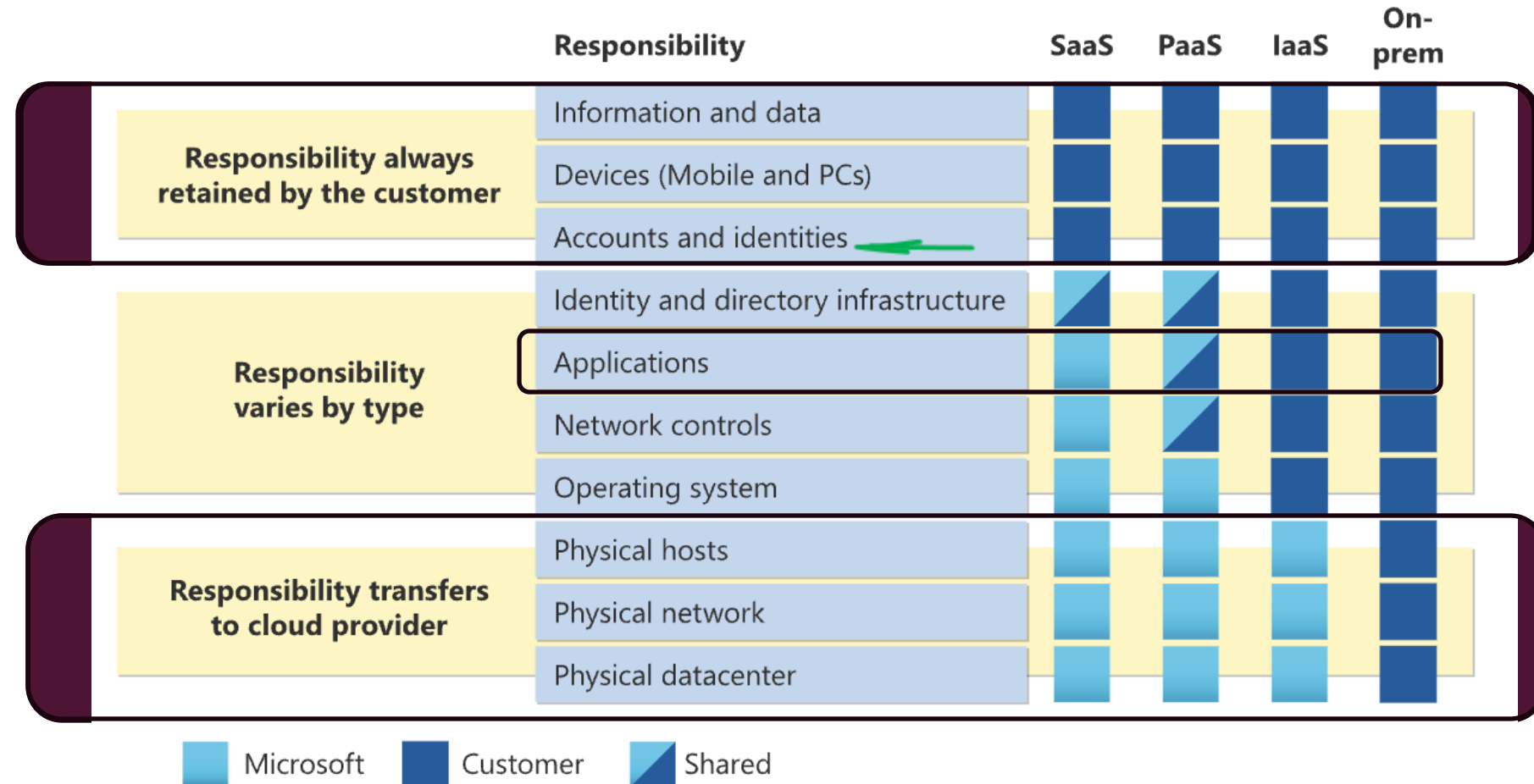
# SHARED RESPONSIBILITY AND APPLICATIONS/WORKLOADS

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

- IDENTITIES
- APPLICATIONS
- DEVICES
- NETWORK

- IDENTITIES
- APPLICATIONS
- DEVICES
- NETWORKS

- DEVICES
- NETWORKS



# ZERO TRUST MATURITY MODEL – CSC117 CATEGORIES & FUNCTIONS

<b>Identity</b>	<b>Devices</b>	<b>Networks</b>	<b>Applications and Workloads</b>
Authentication	Policy Enforcement & Compliance Monitoring	Network Segmentation	Application Access
Identity Stores	Asset & Supply Chain Risk Management	Network Traffic Management	Application Threat Protections
Risk Assessments	Resource Access	Traffic Encryption	Application Resilience (*)
Access Management	Device Threat Protection	Network Resilience	Secure Application Oversight & Lifecycle (*)

<https://www.thefinalhop.com/unmasking-the-alphv-mgm-saga-a-masterclass-in-cybersecurity-missteps-and-ethical-conundrums/> <-- no longer works

<https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/alphv-hackers-reveal-details-of-mgm-cyber-attack/>

- **ALPHV Initial compromise**

- (It appears that) the hackers found an employee's information [on LinkedIn](#) and impersonated them in a call to MGM's [IT help desk](#) to obtain credentials to access and infect the systems (including Okta Agents).
- They exploited vulnerabilities in MGM's Okta Agent servers to sniff passwords, gaining super administrator privileges to MGM's Okta and Global Administrator privileges to their Azure tenant.

- **MGM's Response**

- Upon discovering the breach, MGM shut down their Okta Sync servers, effectively locking themselves out. They also implemented conditional restrictions that barred all access to their Okta environment.
- **Technical Takeaway:** MGM's hasty actions demonstrate a lack of a well-thought-out incident response playbook. Their decision to 'take offline' crucial components of their infrastructure further exacerbated the situation.

- **ALPHV “Next Steps”**

- After failing to establish contact with MGM, ALPHV deployed ransomware attacks against more than 100 ESXi hypervisors in MGM's environment.
- ALPHV claims to have exfiltrated data, but they have not confirmed whether it includes personally identifiable information (PII).

# MGM & ALPHV

<https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/alphv-hackers-reveal-details-of-mgm-cyber-attack/>

- The cyber threat group Scattered Spider launched an impersonation and vishing scheme to enter MGM's systems.
- Scattered Spider used LinkedIn to identify a current MGM Resorts employee, assumed their identity, and called the MGM IT help desk requesting assistance logging into their accounts.
  - The phone call lasted ten minutes, and the attackers were able to gain administrator privileges to MGM's Okta and Azure tenant environments.
- The following day, MGM's security team discovered unusual activity and traffic
  - (ALPHV admitted to sniffing passwords on MGM's Okta servers).
- MGM deactivated their Okta Sync servers and essential infrastructure components to prevent an escalation of the attack
  - This in turn caused the interruption of reservation systems, digital room keys, slot machines, and more.
- ALPHV, still having access to the system, deployed ransomware to more than 100 ESXi hypervisors within MGM's network (Kagan, 2023).
  - The attackers claimed to have exfiltrated data from MGM systems but did not confirm whether it included personally identifiable information (PII) of MGM customers, employees, and vendors.
  - Furthermore, they threatened to notify Troy Hunt of HaveIBeenPwned.com if they could not come to an agreement with MGM. MGM's hotels and casinos have since resumed normal operations, although there may still be some "intermittent issues" (Morrison, 2023).

## MGM & ALPHV

<https://www.brown.com/us/insight/a-look-back-at-the-mgm-and-caesars-incident/>

### Timeline:

- **Early September 2023:** Both MGM and Caesars experience suspicious activity within their IT systems.
- **September 7th:** Caesars suffers a data breach, acknowledging a social engineering attack targeting a third-party IT vendor.
- **September 11th:** MGM faces a ransomware attack by the Scattered Spider (UNC3944) group, causing widespread disruption.
- **September 14th:** Scattered Spider claims to have exfiltrated 6 terabytes of data from both companies.
- **Mid-September:** Caesars reportedly pays a \$15 million ransom, while MGM opts for collaboration with law enforcement.
- **Late September:** Both companies restore normal operations.

Scattered Spider, a cybercrime group, initially gained a foothold through social engineering, phishing for employee credentials.

This breach provided access to the Okta platform, a crucial access management system.

The attackers then capitalized on weak multi-factor authentication (MFA) to escalate privileges and gain control of the Azure Active Directory domain controller.

This unfettered access allowed them to exfiltrate sensitive data and deploy BlackCat/ALPHV ransomware, crippling critical MGM's systems.

# MGM & ALPHV

<https://www.brown.com/us/insight/a-look-back-at-the-mgm-and-caesars-incident/>

- Several security shortcomings exacerbated the situation:
  - Inadequate MFA practices, exemplified by the compromised two-factor authentication, proved insufficient to prevent further intrusion.
  - ■ A lack of proper security awareness training left employees susceptible to social engineering tactics ←
  - *Vulnerable third-party SaaS business application exposed MGM to compromise*
  - The absence of network segmentation granted the attackers unrestricted movement within the system, facilitating lateral movement and data exfiltration.
  - *Lack of robust encryption of data meant that MGM was susceptible to threat of publication of data*
  - ■ Limited detection and response (D&R) capabilities delayed the identification and containment of the attack and allowed the situation to escalate.
  - *Lack of incident response testing / practice of responding and communicating during an incident*
  - *Lack of emergency access alternatives crippled MGM when Okta was disconnected BUT as not all apps were governed by Okta, bad actors still had access to those non-Okta governed apps*
  - ■ *Lack of penetration testing, vulnerability assessments to identify security gaps*



# ZERO TRUST MATURITY MODEL – CSC117 CATEGORIES & FUNCTIONS

Identity	Devices	Networks	Applications and Workloads
✓ Authentication	✓ Policy Enforcement & Compliance Monitoring	✓ Network Segmentation	Application Access
Identity Stores	Asset & Supply Chain Risk Management	Network Traffic Management	✓ Application Threat Protections
Risk Assessments	Resource Access	Traffic Encryption	Application Resilience (*)
✓ Access Management	Device Threat Protection	Network Resilience	Secure Application Oversight & Lifecycle (*)

TRAINING →  
INVENTORY

## DISCUSSION: MGM/OKTA



- *Looking at the description of MGM (previous slide), which ZTMM areas would have been the most impactful if they had been in place?*
- *Pick FIVE (5) areas of ZTMM that would be your focus / that you want to be as most mature as possible, to help prevent an MGM/Okta type compromise?*
- *If you could only implement THREE (3) of them, which would you pick and why?*



10 min

BREAK

BACK

6:45PM ET

# CAPSTONE DISCUSSION

- REMINDER: Rule is “At least one ADVANCED” (not Approved)

# ZERO TRUST MATURITY MODEL – CSC117 CATEGORIES & FUNCTIONS

<b>Identity</b>	<b>Devices</b>	<b>Networks</b>	<b>Applications and Workloads</b>
Authentication	Policy Enforcement & Compliance Monitoring	Network Segmentation	Application Access
Identity Stores	Asset & Supply Chain Risk Management	Network Traffic Management	Application Threat Protections
Risk Assessments	Resource Access	Traffic Encryption	Application Resilience (*)
Access Management	Device Threat Protection	Network Resilience	Secure Application Oversight & Lifecycle (*)

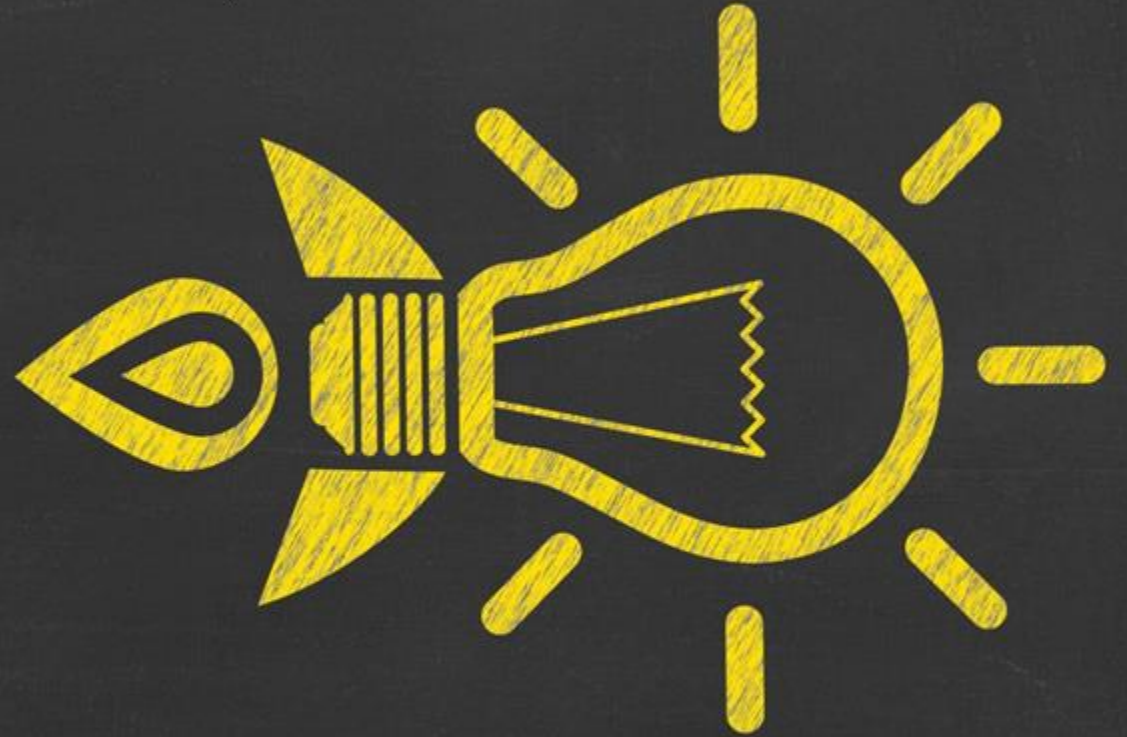
## IN THE NEWS: MOBILE DEVICES & PASSKEY VULNERABILITIES

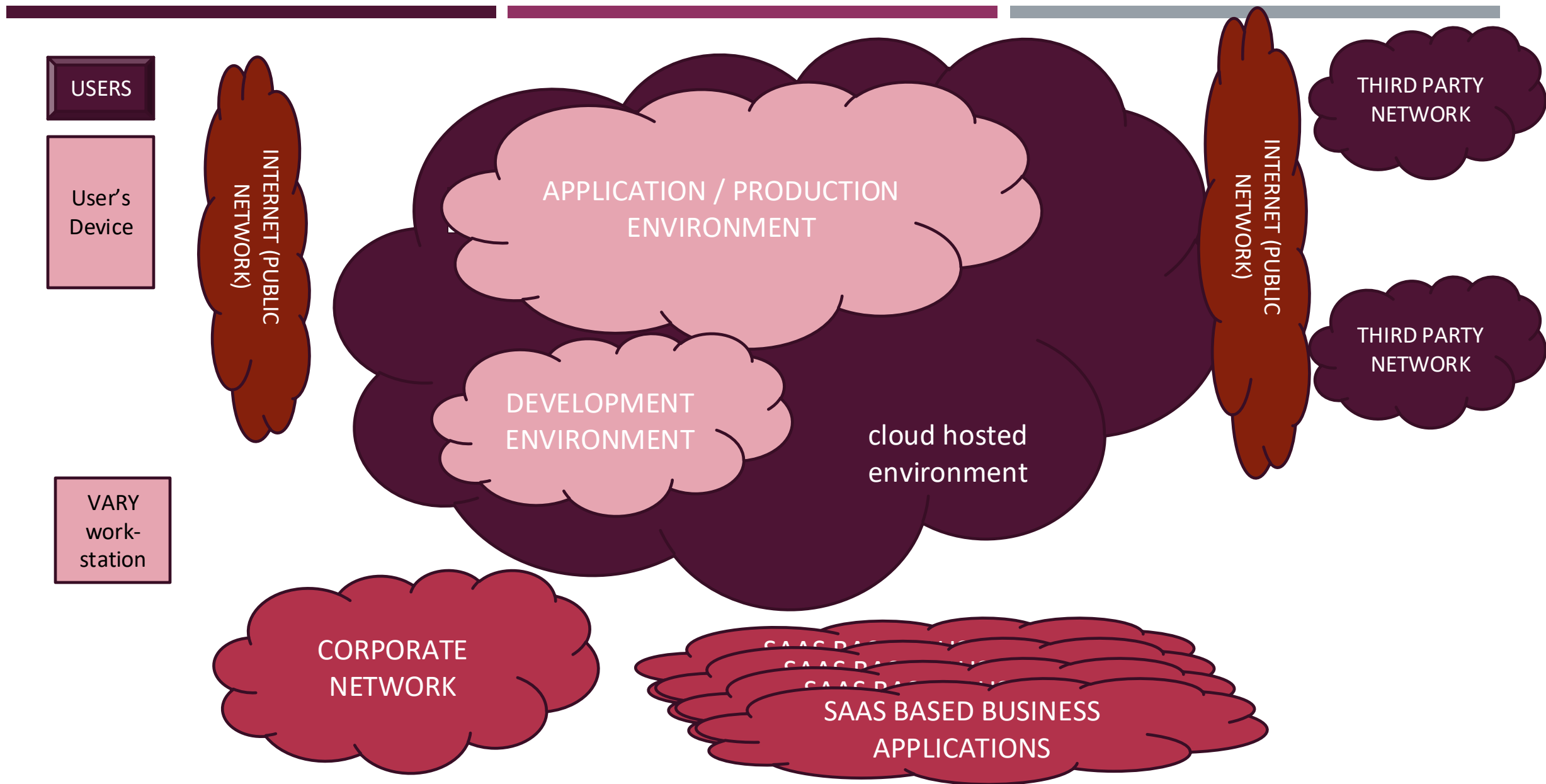
<https://mastersplinter.work/research/passkey/>

- **TLDR** An attacker within bluetooth range is able to trigger navigation to a FIDO:/ URI from an attacker controlled page on a mobile browser, allowing them to initiate a legitimate PassKeys authentication intent which will be received on the attacker's device. This results in the attacker being able to "phish" PassKeys credentials, completely breaking this assumption that PassKeys are impossible to phish.
- To put it simply, when a web application wants to make use of PassKeys to authenticate a user it must tell the browser which origins (or RP) are allowed to register and request credentials for that site.
- Otherwise any origin would be able to tell your browser "heeeeeey, fetch me credentials for yourbankthattotallydoesnotsupportpasskeys.com and authenticate this user pls"



# REFERENCES










# Zero Trust Maturity Matrix






Maturity Pillar	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Networks	<b>Manually configured</b> lifecycles (i.e., from establishment to decommissioning) and assignments of attributes (security and logging); <b>static</b> security policies and solutions that address one pillar at a time with discrete dependencies on external systems; least privilege established only at provisioning; siloed pillars of policy enforcement; <b>manual response and mitigation</b> deployment; and limited correlation of dependencies, logs, and telemetry.	<b>Starting automation</b> of attribute assignment and configuration of lifecycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external systems; <b>some responsive changes</b> to least privilege after provisioning; and <b>aggregated visibility</b> for internal systems.	Wherever applicable, <b>automated controls</b> for lifecycle and assignment of configurations and policies with <b>cross-pillar coordination</b> ; centralized visibility and identity control; <b>policy enforcement integrated</b> across pillars; response to pre-defined mitigations; changes to least privilege based on <b>risk and posture assessments</b> ; and building toward enterprise-wide awareness (including externally hosted resources).	<b>Fully automated, just-in-time lifecycles and assignments of</b> attributes to assets and resources that self-report with <b>dynamic policies based on automated/observed triggers</b> ; dynamic least privilege access (just-enough and within thresholds) for assets and their respective dependencies enterprise-wide; <b>cross-pillar interoperability with continuous monitoring</b> ; and <b>centralized visibility with comprehensive situational awareness</b>
Devices				
Applications				
Data				
Users / Identities				

# Zero Trust Maturity Matrix






	Identity	Devices	Networks	Applications and Workloads	Data
					
Traditional	Visibility and Analytics		Automation and Orchestration		Governance
	<ul style="list-style-type: none"> <li>• Passwords or MFA</li> <li>• On-premises identity stores</li> <li>• Limited identity risk assessments</li> <li>• Permanent access with periodic review</li> </ul>	<ul style="list-style-type: none"> <li>• Manually tracking device inventory</li> <li>• Limited compliance visibility</li> <li>• No device criteria for resource access</li> <li>• Manual deployment of threat protections to some devices</li> </ul>	<ul style="list-style-type: none"> <li>• Large perimeter/macro-segmentation</li> <li>• Limited resilience and manually managed rulesets and configurations</li> <li>• Minimal traffic encryption with ad hoc key management</li> </ul>	<ul style="list-style-type: none"> <li>• Mission critical applications accessible via private networks</li> <li>• Protections have minimal workflow integration</li> <li>• Ad hoc development, testing, and production environments</li> </ul>	<ul style="list-style-type: none"> <li>• Manually inventory and categorize data</li> <li>• On-prem data stores</li> <li>• Static access controls</li> <li>• Minimal encryption of data at rest and in transit with ad hoc key management</li> </ul>



# Zero Trust Maturity Matrix






	Identity	Devices	Networks	Applications and Workloads	Data
					
Initial	<ul style="list-style-type: none"><li>• MFA with passwords</li><li>• Self-managed and hosted identity stores</li><li>• Manual identity risk assessments</li><li>• Access expires with automated review</li></ul>	<ul style="list-style-type: none"><li>• All physical assets tracked</li><li>• Limited device-based access control and compliance enforcement</li><li>• Some protections delivered via automation</li></ul>	<ul style="list-style-type: none"><li>• Initial isolation of critical workloads</li><li>• Network capabilities manage availability demands for more applications</li><li>• Dynamic configurations for some portions of the network</li><li>• Encrypt more traffic and formalize key management policies</li></ul>	<ul style="list-style-type: none"><li>• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users</li><li>• Formal code deployment mechanisms through CI/CD pipelines</li><li>• Static and dynamic security testing prior to deployment</li></ul>	<ul style="list-style-type: none"><li>• Limited automation to inventory data and control access</li><li>• Begin to implement a strategy for data categorization</li><li>• Some highly available data stores</li><li>• Encrypts data in transit</li><li>• Initial centralized key management policies</li></ul>
	Visibility and Analytics		Automation and Orchestration		Governance

# Zero Trust Maturity Matrix

	Identity	Devices	Networks	Applications and Workloads	Data
					
Advanced	<ul style="list-style-type: none"> <li>Phishing-resistant MFA</li> <li>Consolidation and secure integration of identity stores</li> <li>Automated identity risk assessments</li> <li>Need/session-based access</li> </ul>	<ul style="list-style-type: none"> <li>Most physical and virtual assets are tracked</li> <li>Enforced compliance implemented with integrated threat protections</li> <li>Initial resource access depends on device posture</li> </ul>	<ul style="list-style-type: none"> <li>Expanded isolation and resilience mechanisms</li> <li>Configurations adapt based on automated risk-aware application profile assessments</li> <li>Encrypts applicable network traffic and manages issuance and rotation of keys</li> </ul>	<ul style="list-style-type: none"> <li>Most mission critical applications available over public networks to authorized users</li> <li>Protections integrated in all application workflows with context-based access controls</li> <li>Coordinated teams for development, security, and operations</li> </ul>	<ul style="list-style-type: none"> <li>Automated data inventory with tracking</li> <li>Consistent, tiered, targeted categorization and labeling</li> <li>Redundant, highly available data stores</li> <li>Static DLP</li> <li>Automated context-based access</li> <li>Encrypts data at rest</li> </ul>
	Visibility and Analytics		Automation and Orchestration		Governance



# Zero Trust Maturity Matrix

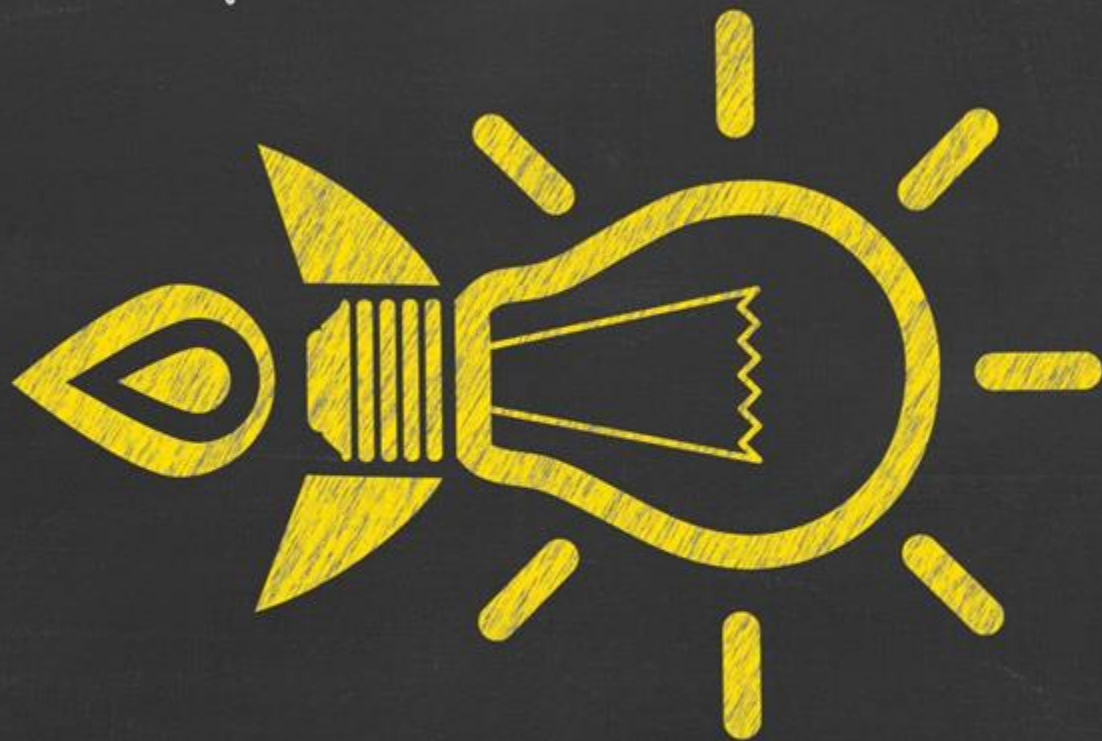
	Identity	Devices	Networks	Applications and Workloads	Data
					
Optimal	<ul style="list-style-type: none"> <li>Continuous validation and risk analysis</li> <li>Enterprise-wide identity integration</li> <li>Tailored, as-needed automated access</li> </ul>	<ul style="list-style-type: none"> <li>Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections</li> <li>Resource access depends on real-time device risk analytics</li> </ul>	<ul style="list-style-type: none"> <li>Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience</li> <li>Configurations evolve to meet application profile needs</li> <li>Integrates best practices for cryptographic agility</li> </ul>	<ul style="list-style-type: none"> <li>Applications available over public networks with continuously authorized access</li> <li>Protections against sophisticated attacks in all workflows</li> <li>Immutable workloads with security testing integrated throughout lifecycle</li> </ul>	<ul style="list-style-type: none"> <li>Continuous data inventorying</li> <li>Automated data categorization and labeling enterprise-wide</li> <li>Optimized data availability</li> <li>DLP exfil blocking</li> <li>Dynamic access controls</li> <li>Encrypts data in use</li> </ul>
	Visibility and Analytics		Automation and Orchestration		Governance



ANTICIPATED END OF LECTURE 11



CAPSTONE



# CAPSTONE

## Is now published

- Its LONG in terms of the numbers of pages. That means there is a lot of reading
- It builds on the assignments (so if you have done Assignments 1-4 it will help you a LOT)
- <https://canvas.harvard.edu/courses/150125/assignments/915129>

## 2. Question Format and Details

### 2.1 Budgeting

#### 2.1.1 Stay within budget

#### 2.1.2 The Optimal Kevin Bacon rule

#### 2.1.3 At least something at “Approved”

*Advanced*

### 2.2 ZTM Categories (Asset Classes): Questions and Marking Details

#### 2.2.1 Additional Complexity (1 mark)

#### 2.2.2 Proposed Functional Level Maturity (1 mark each)

#### 2.2.3 Justification of Function Level Maturity (5 marks each)

#### 2.2.4 Overall Asset Class (Category) Maturity (10 marks)

#### 2.2.5 Build the overall spend to protect your organization.

### 2.3 Essay Question Rubrics

### Additional Complexity (1 mark)

Will you include the additional complexity of employee / guest network segregation for the corporate network environment? Yes/No

Answer:

### Proposed Function Level Maturity (4 marks subtotal)

#### Function Title (1 mark) x 4 (Four functions per category)

What is the overall maturity level for **this function according to your budget** (chose from Traditional, Initial, Optimal, Advanced)

Answer:

### Justification of Function Level Maturity (20 marks subtotal)

For each **function**, provide a justification for this level of maturity. Include in your justification the threats and risks addressed, the **at-least-one-Advanced rule**, and the Optimal Kevin Bacon rule as well as any other notes that help make the case for the maturity of this **function** as well as any other notes that help make the case for this maturity level (remember that you will separately make the case for the overall category in the next question).

#### Function Title(5 marks) x 4 (Four functions per category)

Answer:

### Overall Category Spend Justification (10 marks)

Answer:

### [Bonus] Overall ACME Spend/Final Posture Justification (10 marks)

Answer:

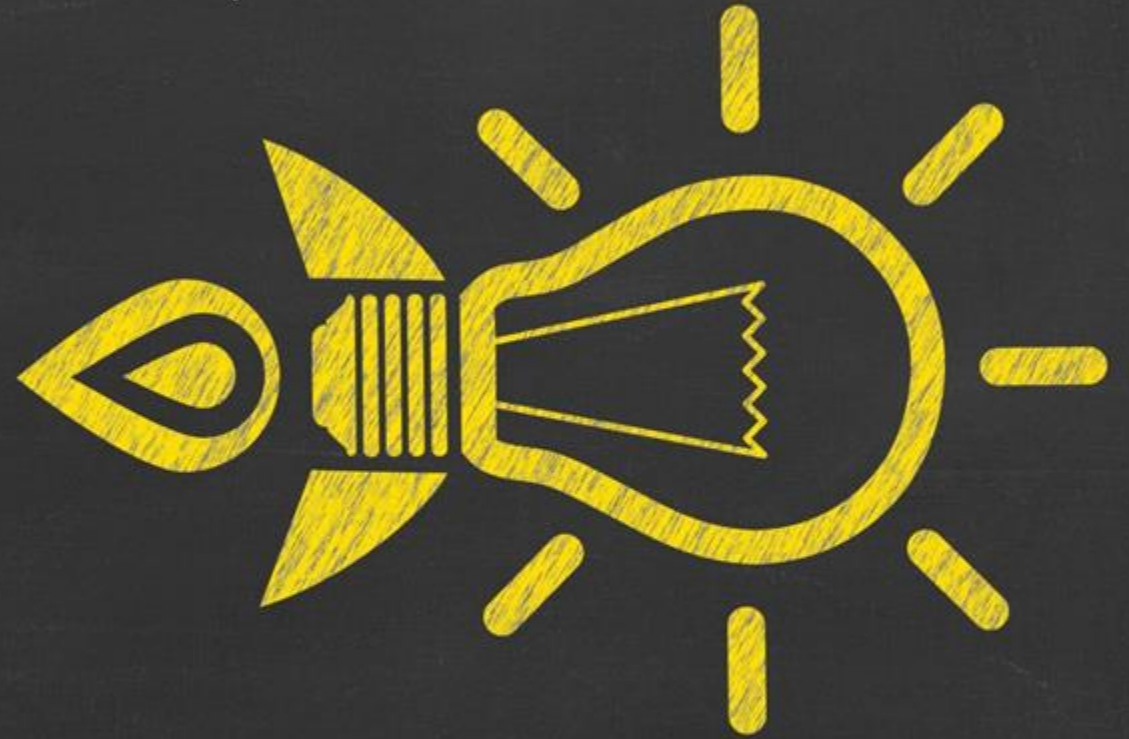
# QUESTIONS

- Are the complexity factors static, or we can change them?
  - **You CANNOT change the complexity factors**
- Do we have to have a left over small budget in the bank for later use?
  - **There is no question dealing with left over budget so use or leave, its up to you**
- What's the 3 year plan has to do with the scenario of the capstone? Do we have to do our plans chronologically?
  - **The specification of 3 years is to add realism to the timing – you don't get to add all this type of stuff in the real world in less than that. Your answers across the assignment are assumed to cover the 3-year timeline.**
  - **See also the Bonus question that was added – you can add more about the 3 year timeline implications if you like**



# ASSIGNMENT

4



## Mapping Mitre to ZTMM

	<b>Application Access</b>	<b>Application Threat Protection</b>	<b>Accessible Applications</b>
MI040 – Behavior Prevention on Endpoint	2	18	
MI038 – Execution Prevention	0	6	1
MI052 - User Account Control	5		1
MI032 – Multi-factor Authentication	29		2
MI035 - Limit Access to Resource Over Network	3	1	34
MI016 - Vulnerability Scanning	0	14	1

# Zero Trust Application Architecture prioritization

	<b>Priority 1</b>	<b>Priority 2</b>	<b>Priority 3</b>
Application Access (former Access Authorization)	30	8	1
Application Threat Protections (formerly Threat Protection)	7	27	5
Accessible Applications (formerly accessibility)	2	4	33

# Application controls and Generative AI

BENEFIT FROM GENAI DEFENSE	Selected
Application Access (former Access Authorization)	8
Application Threat Protections (formerly Threat Protection)	29
Accessible Applications (formerly accessibility)	1
BENEFIT (SUFFER) FROM GENAI ATTACK	
Application Access (former Access Authorization)	25
Application Threat Protections (formerly Threat Protection)	9
Accessible Applications (formerly accessibility)	4