CSCI E-117A SPRING 2024

Lecture 10
April 8, 2024

SECURE APPLICATIONS: MANAGING THE DEPLOYMENT INFRASTRUCTURE

LECTURE 10 AGENDA

- *YellowDig Last Week*
- *Discussion Notes*
- *ZTMM: Identity*
  - *Human & Non Human Identities*
  - *Identity Verification & Deepfakes*
  - *Identity Risk : the new #1 focus area?*
- *Assignment IV*
  - *Feedback*
- *Capstone*
  - *Discussion, Q&A*

SOME HIGHLIGHTS FROM THE NEWS (2024 EDITION)

Read up on this: We will discuss next week in terms of ZTMM

- https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/
- **What is xz Utils?**
- xz Utils is nearly ubiquitous in Linux. It provides lossless data compression on virtually all Unix-like operating systems, including Linux. xz Utils provides critical functions for compressing and decompressing data during all kinds of operations.
- Infographic: https://infosec.exchange/@fr0gger/112189232773640259

NOTES FROM DISCUSSION

- Something that surprised me in this discussion was the perspective that it is hard to get stakeholders aligned on something like implementing an identity tool for ZTA. While I don't doubt that this can be the case but, in my experience, more often than not, the disagreements on security or IT tools or platforms happen below the decision maker level where it is the SOC or IT Team that has conflicting opinions on if something should/shouldn't be implemented and what specific tool (brand of tool) it is that is implemented. Executives that are signing off on implementing something (whether it be granting budget or simply granting approval for a 3rd party tool to be integrated into the environment and therefore accessing company data) are more focused on why the solution is necessary (i.e what are the risks of inaction) and how can we accomplish it/check the box in the most cost-effective way with minimal disruption to core business activities.

NOTES FROM YELLOWDIG

- https://www.cvedetails.com/cve/CVE-2024-10668/
- There exists an auth bypass in Google Quickshare where an attacker can upload an unknown file type to a victim.
- The flaw, tracked as CVE-2024-10668 (CVSS score: 5.9), is a bypass for two of the 10 shortcomings that were originally disclosed by SafeBreach Labs in August 2024 under the name QuickShell. … A consequence of these 10 vulnerabilities, collectively tracked as CVE-2024-38271 (CVSS score: 5.9) and CVE-2024-38272 (CVSS score: 7.1), was that they could have been fashioned into an exploit chain to obtain arbitrary code execution on Windows hosts.
  - A follow-up analysis by the cybersecurity company found that two of the vulnerabilities were not fixed correctly,
  - While this allows a file to be downloaded to a system, that file still needs to be run/executed to do something bad. But if a user can be tricked into executing it (including by going to a malicious site that then tries to look for it) then really bad things can happen

QUESTION IN YD: Why is EPSS score so low? I do wonder why the CVE is low given how serious it looks.

- ANSWER: Largely because the complexity is high

YELLOWDIG: “MALICIOUS VISUAL STUDIO CODE”

- https://www.bleepingcomputer.com/news/security/vscode-extensions-found-downloading-early-stage-ransomware/
- https://www.bleepingcomputer.com/news/security/vscode-extensions-with-9-million-installs-pulled-over-security-risks/
- Microsoft has removed two popular VSCode extensions, 'Material Theme – Free' and 'Material Theme Icons – Free,' from the Visual Studio Marketplace for allegedly containing malicious code.
- News of the extensions being malicious comes from cybersecurity researchers Amit Assaraf and Itay Kruk, who have expertise in scanning VSCode for malicious extensions.
  - In a report published today, the researchers say they discovered suspicious code in the extensions and reported their findings to Microsoft.
- "Microsoft removed both extensions from the VS Code marketplace and banned the developer," reads a post from a Microsoft employee to YCombinator's Hacker News.
- "A member of the community did a deep security analysis of the extension and found multiple red flags that indicate malicious intent and reported this to us. Our security researchers at Microsoft confirmed this claims and found additional suspicious code.

YELLOWDIG: “MALICIOUS VISUAL STUDIO CODE” TAKE 2

- https://www.bleepingcomputer.com/news/microsoft/microsoft-apologizes-for-removing-vscode-extensions-used-by-millions/
- ….
- "A member of the community did a deep security analysis of the extension and found multiple red flags that indicate malicious intent and reported this to us," stated a Microsoft employee at the time.
- Researchers Amit Assaraf and Itay Kruk, who were deploying AI-powered scanners seeking suspicious submissions on VSCode, first flagged them as potentially malicious.
- Astorino immediately objected to the allegations and the removal of his extensions from the VSCode Marketplace, alleging that the problem comes from an outdated sanity.io dependency used since 2016 to show release notes from sanity headless CMS.
- Microsoft's Scott Hanselman apologized to Astorino yesterday in a GitHub issue opened by the developer asking for his account and themes to be reinstated.
- "The publisher account for Material Theme and Material Theme Icons (Equinusocio) was mistakenly flagged and has now been restored," reads Hanselman's post.
- "In the interest of safety, we moved fast and we messed up. We removed these themes because they fired off multiple malware detection indicators inside Microsoft, and our investigation came to the wrong conclusion."

YELLOWDIG LAST WEEK: CYBER INSURANCE

- https://doi.org/10.1145/3676283
- Does Cyber Insurance Promote Cyber Security Best Practice? An Analysis Based on Insurance Application Forms.
- This article ties into Lecture 9 by questioning whether cyber insurance promotes real application security maturity. While insurance may push for basic compliance, it rarely incentivizes deeper adoption of Zero Trust Maturity Model (ZTMM) controls like Application Access or Threat Protections. As discussed, long-term security demands structured investment—not just meeting checkbox requirements for coverage.

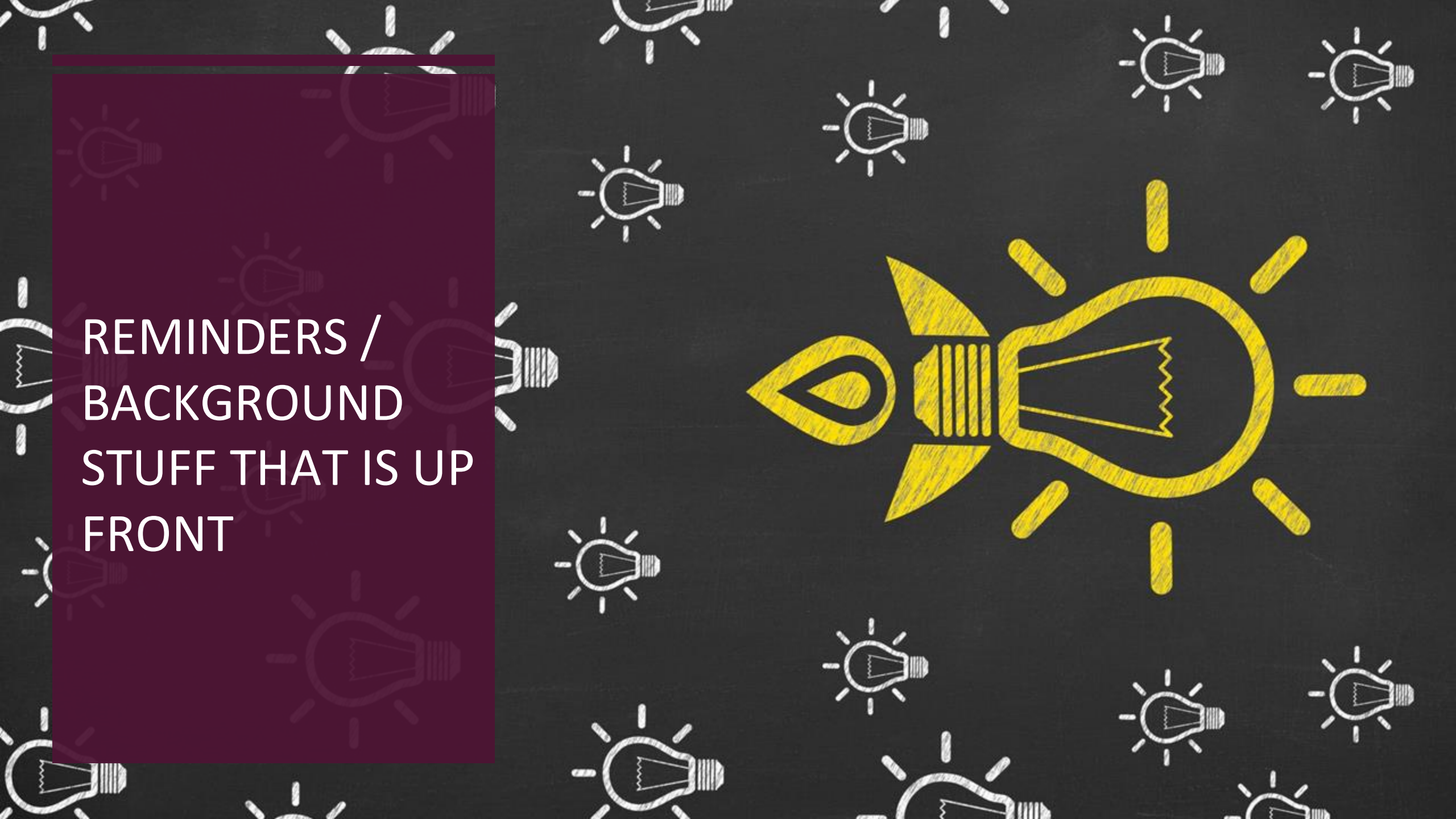
- INSTRUCTORS ANSWER: Never in my years filling out cyber insurance questionnaires / supporting responses to cyber insurance Q&A did insurance focus on our secure development practices. Cyberinsurance was all about the practices we had in place to protect ourselves from ransomware, NOT to make sure that our applications were built in a way to be resilient to / not contributing to a customer's ransomware posture

YELLOWDIG LAST WEEK: FAST FLUX

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-093a

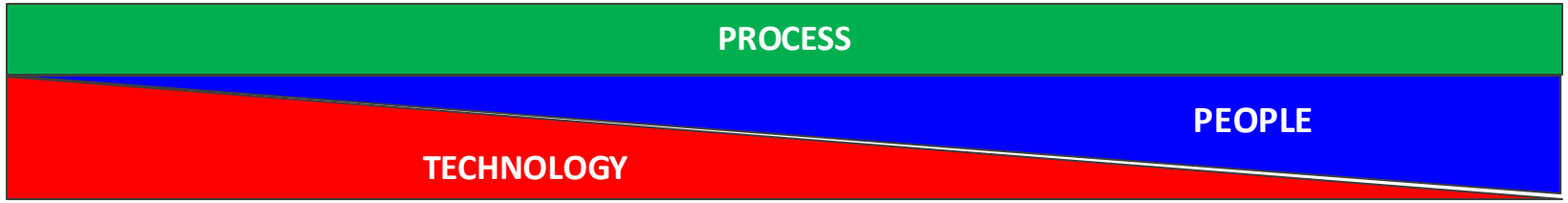
- If you are not familiar, JA+4 is definitely worth investigating
- https://medium.com/foxio/ja4-network-fingerprinting-9376fe9ca637

REMINDERS / BACKGROUND STUFF THAT IS UP FRONT

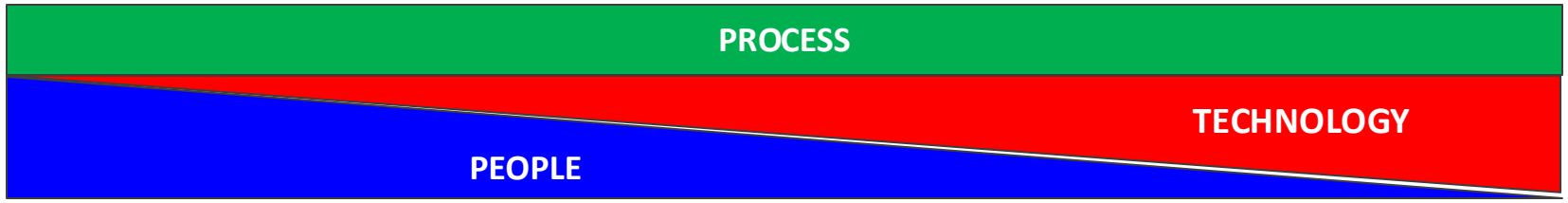


Asset Class	Examples
Network	Communication channels, connections and protocols that enable traffic to flow among devices and applications. Note that this does NOT refer to the actual infrastructure (routers, switches) but rather to the paths themselves and the protocols used in those paths. This class 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

Cyber Defense Matrix



	IDENTIFY	PROTECT	DETECT	RESPOND & RECOVER	
DEVICES					DEVICES
NETWORKS					NETWORKS
APPLICATIONS & DATA					APPLICATIONS & DATA
USERS					USERS
	TRADITIONAL	INITIAL	ADVANCED	OPTIMIZED	



Zero Trust Maturity

IDENTITY / USERS

IDENTITY: CISA ZTMM

- An identity refers to an attribute or set of attributes that uniquely describes an agency user or entity, including non-person entities.
  - Non human identities are “all the rage” – lots of focus by vendors …
- Guidance:
  - Agencies should ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access.
  - Agencies should integrate identity, credential, and access management solutions where possible throughout their enterprise to enforce strong authentication, grant tailored context-based authorization, and assess identity risk for agency users and entities.
  - Agencies should integrate their identity stores and management systems, where appropriate, to enhance awareness of enterprise identities and their associated responsibilities and authorities

	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.

USERS / ACCOUNTS / IDENTITIES / DIGITAL WORKERS

https://duo.com/assets/ebooks/cisco-duo-identity-security-blueprint.pdf

Users

Individuals who require access to an organization's systems and networks.

Accounts

Digital representations of users, third parties, contractors, ~~and machine accounts~~ that are created within an organization's identity and access management systems.

Identities

The information that identifies an individual or entity in an organization's systems and networks. It includes attributes such as usernames, roles, passwords, access privileges, and historical context.

Non Human Entities

Also known as service IDs, are associated with APIs and application as well as servers, services and endpoints.

NHI "Accounts"

Digital representation of NHE. Not all NHE have/need accounts. NHEs don't always have clear owners or lifecycle management.

NH Identities

NHIs are represented with IDs carried in tokens, certificates, tags and more and may well be over permissioned.

Digital Workers

A digital worker is an automated, software-based tool, application, or agent that performs a business task or process similar to a human user and uses Artificial Intelligence (AI) or other autonomous decision-making capabilities. https://www.idmanagement.gov/playbooks/dw/

(HUMAN) IDENTITY LIFECYCLE

- (People) Identity Proofing
  - Is this a real person? Is it the person that is claimed?
- Human Identity / Account Creation (Provisioning)
  - Create an account & bind to the (verified) identity with authenticators
  - Set up initial groups, roles for general / all-purpose permissions (stuff all employees have, like email)
- (Set up) Account Authentication (in support of Identity Verification)
  - Assign/set authenticators – passwords, passkeys, biometrics
  - Enhance authenticators – supplement with 2FA tokens, dongles
- Account Management
  - Assign permissions, roles to that account (and therefore that identity)
  - Continually review and manage account's permissions, including based on job role and context
- Identity Verification (Authentication)
  - (Continually) Validate Identifier and authenticators (passwords, passkeys, tokens, biometrics, etc)
- Account Decommissioning
  - Mark accounts inactive / remove privileges
  - DO NOT : Delete accounts

IDENTITY VERIFICATION

https://www.login.gov/help/verify-your-identity/overview/
https://www.transunion.com/blog/what-difference-between-identity-proofing-and-identity-verification?atvy=%7B%22264995%22%3A%22Experience+B%22%7D

- **Identity proofing** is the process of verifying an individual is who they claim to be *when they first interact with an organization.*
  - Collect and validate identity-related information to establish a person's identity before they can access services or complete transactions.
  - Focused on the authenticity of data provided during the onboarding or account creation processes.
  - Helps to combat synthetic identity fraud where fraudsters combine real and fake personally identifiable information (PII) to create convincing false identities.
- **Identity verification** helps ensure the person presenting the information is the rightful owner of that identity *and can be done at any time*
  - Uses various methods, such as device intelligence, knowledge-based authentication (KBA) questions, biometric verification and multi-factor authentication (MFA).

Verify your identity

Identity verification is the process where you prove you are you — and not someone pretending to be you. You will need to create your Login.gov account and verify your identity to access services at some government agencies.

What you'll need to verify your identity

You'll take a photo of your accepted driver's license or state ID card and enter your personal information to verify your identity online.

You may need to take a photo of yourself with a phone to verify your identity online. This is to check that you are the person on your ID. If you don't have a phone with a camera, you can verify your identity in person.

What you'll need to create a Login.gov account

- Email
- Password
- Authentication method

What you'll need to verify your identity

- Driver's license or state ID card
- Social Security Number
- Phone number or address

Some services need you to take a photo of yourself with a phone to verify your identity online.

DEEP FAKES AND IDENTITY PROOFING

- FROM LAST SLIDE: Collect and validate identity-related information to establish a person's identity before they can access services or complete transactions

- HOWEVER
  - Fraudsters are adept at passing off phony documentation to open accounts and complete credit applications, even to the point they can fool document verification technology. Documents, like Internal Revenue Service (IRS) forms, identification cards, business incorporation documents, can be faked using AI technologies. Backup document verification, like driver's license verification can be fooled using fake selfies and driver's licenses.
  - DeepFake AI can accurately mimic an individual's face and voice to bypass biometric identification.

REMOTE IDENTITY PROOFING & LIVENESS

https://www.fraud.com/post/identity-proofing

- Remote identity proofing works by verifying customer identities using a combination of techniques, such as biometric analysis, facial recognition, and documentation verification. This helps to ensure that customers are who they say they are and that the information they provide is accurate.

Liveness detection

- Liveness Detection is the process of verifying the identity of a person through a biometric scan. It is used to ensure that the person in front of a camera is a live person and not a photo, video, a deepfake or other recording.
- The process typically begins with a facial recognition scan, which can detect a person's face, even when they are wearing a mask. Then, it will look for changes in the person's eye movements, voice, and other facial features that can only be done by a living person.
- If the scan matches the person to a pre-existing biometric data set, their identity is verified. Liveness Detection is an important step in proofing a person's identity since it adds an extra layer of security that requires the person to be physically present at the time of authentication. This helps keep accounts and data secure from hackers and other malicious actors. As the world becomes increasingly digital, Liveness Detection will become an even more important tool for protecting identities.

CLASS DISCUSSION: POLL

- *Which scares you more, that:*
  - *AI Deepfakes are good enough to fake you online (verbal, visual)*
  - *AI Deepfakes are good enough to present a fake-but-`passable documents (eg Driver's Licenses) used as part of online/remote identity proofing*
  - *Biometric Verification (with or without Liveness Detection) relies on a comparison to a "pre-existing biometric data set" (your face is now literally your password and it is hashed and stored the same way your password is/was)*
  - *It is likely only a matter of time before "changes in the person's eye movements, voice, and other facial features that can only be done by a living person (Liveness Detection) will also be fake-able by AI Deepfakes?*

IDENTITY FRAUD – NORTH KOREAN BAD ACTORS

https://www.justice.gov/archives/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information

- **Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions**
- These included using stolen identities belonging to U.S. persons and others to apply for jobs; paying U.S. persons to attend job interviews and work meetings remotely under fake identities; and registering web domains and designing phony websites to convince prospective employers that the false identities were experienced, qualified, and previously employed by reputable contracting firms.
- The conspirators also sought to avoid detection by paying U.S. persons to receive, set up, and host laptops sent from employers to the U.S. persons' home addresses (often referred to as laptop farms). After these laptops were set up, the conspirators instructed the U.S. persons to install software that allowed them to access the laptops from overseas. By arranging to have laptops physically located in the United States, conspirators made it appear as if the fake U.S.-based employees were accessing laptops to do work, when in fact the IT workers were located outside the United States.

DEEP FAKE IDENTITY FRAUD

https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf

https://www.miteksystems.com/library/digital-fraud-defender-resources/Mitek-emerging-identity-fraud-playbook

- The DHS document is really good
  - I can't find a publication date but reading it, it is already out of date
- The Mitek Systems document is also good and explicitly addresses "Onboarding fraud"
  - Document Fraud
  - Biometric Spoofing
  - Passing Identity Checks with
    - Deepfakes
    - Injection Attacks
  - Synthetic Identities

	Onboarding fraud	Account fraud	Transactional fraud
Motives	Fraudsters often target the initial stages of the customer journey, using stolen or fabricated personal information to create fraudulent accounts in someone else's name.	Throughout the customer journey, businesses and their customers face threats from fraudsters attempting to gain unauthorized access to accounts.	Fraudsters use a range of scams to exploit accounts and conduct unauthorized transactions such as transferring money, making payments, or purchasing goods and services.

KNOWBE4 DEEPFAKE INCIDENT

Feb 2024

- KnowBe4 article on Deepfake CEO
- https://blog.knowbe4.com/social-engineering-masterstroke-how-deepfake-cfo-duped-a-firm-out-of-25-million

July 2024

- KnowBe4 admits to having (North Korean) Deepfake employees
- https://www.securityweek.com/knowbe4-hires-fake-north-korean-it-worker-catches-new-employee-planting-malware/
- https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

Synthentic Identities

- Cybercriminals use synthetic identities – usually the combination of deepfakes and stolen personally identifiable information (PII) – to apply for remote work positions.

CFO & TEAM DEEPFAKE

https://blog.knowbe4.com/social-engineering-masterstroke-how-deepfake-cfo-duped-a-firm-out-of-25-million

- In a worrying display of social engineering sophistication, a multinational company was defrauded of $25 million through an intricately planned deepfake scam. This scam brilliantly utilized deepfake technology to impersonate the company's Chief Financial Officer (CFO) during a video conference call, as reported by the Hong Kong police.

▪The scam unfolded when a finance worker at the company was lured into a video call, believing he was joining several colleagues for a meeting. In a revelation by the Hong Kong police, it was disclosed that the supposed colleagues were nothing more than deepfake fabrications.

▪The finance worker initially harbored suspicions after receiving a message, allegedly from the CFO based in the UK, suggesting a secretive transaction. The message, which initially raised red flags as a potential phishing attempt, was soon overshadowed by the convincing deepfake video call. The presence of familiar faces, recreated with staggering accuracy, led the worker to dismiss his doubts.

▪Convinced of the authenticity of the meeting, the finance worker was manipulated into transferring 200 million Hong Kong dollars (approximately $25.6 million), as per the instructions given during the call.

KNOWBE4 TL:DR
https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

- **TLDR:** KnowBe4 needed a software engineer for our internal IT AI team. We posted the job, received resumes, conducted interviews, performed background checks, verified references, and hired the person. We sent them their Mac workstation, and the moment it was received, it immediately started to load malware.
- Our HR team conducted four video conference based interviews on separate occasions, confirming the individual matched the photo provided on their application. Additionally, a background check and all other standard pre-hiring checks were performed and came back clear due to the stolen identity being used. This was a real person using a valid but stolen US-based identity. The picture was AI "enhanced".
- The EDR software detected it and alerted our InfoSec Security Operations Center. The SOC called the new hire and asked if they could help. That's when it got dodgy fast. We shared the collected data with our friends at Mandiant, a leading global cybersecurity expert, and the FBI, to corroborate our initial findings. It turns out this was a fake IT worker from North Korea. The picture you see is an AI fake that started out with stock photography (below). The detail in the following summary is limited because this is an active FBI investigation.
- CRITICAL CONTROL: New employees are in a highly restricted area when they start and have no access to production systems.

KNOWBE4 - MORE DEETS

- KnowBe4 hired and onboarded a North Korean operative posing as a software engineer
  - Individual slipped past its hiring background checks and spent the first 25 minutes on the job attempting to plant malware on a company workstation.
- "We sent them their Mac workstation, and the moment it was received, it immediately started to load malware"
  - It was the MALWARE that triggered alerts (not the location, as it was shipped to a laptop farm)
- KnowBe4 said it first flagged the incident on July 15, 2024 at 9:55pm EST when an anti-malware software sent alerts about anomalous activity. Upon investigation, the new employee said he was following steps on his router guide to troubleshoot a speed issue and that it may have caused a compromise.
  - However, [KnowBe4 stated] the attacker performed various actions to manipulate session history files, transfer potentially harmful files, and execute unauthorized software.
- "He used a Raspberry Pi to download the malware. We attempted to get more details from [the employee] including getting him on a call [but] he said he was unavailable for a call and later became unresponsive."
- At around 10:20pm EST, [KnowBe4] said the company contained the infected workstation and stressed that "no access was gained or compromised on KnowBe4 systems."

IDENTITY ZTMM: AUTHENTICATION, RISK ASSESSMENTS

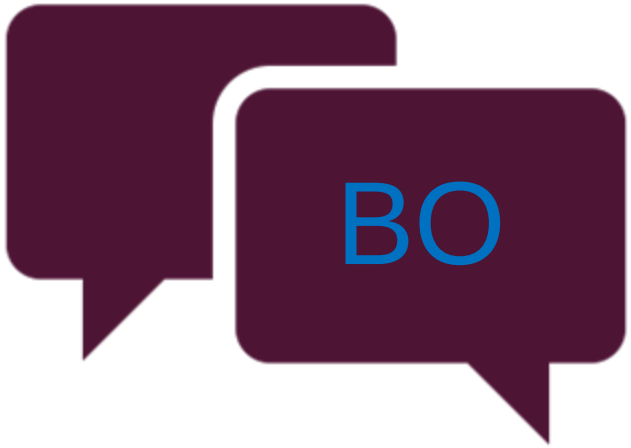
	Authentication	Risk Assessments
	Agency authenticates identity using either passwords or multi-factor authentication (MFA) with static access for entity identity.	Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised).
	Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).	Agency determines identity risk using manual methods and static rules to support visibility.
	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of passwordless MFA via FIDO2 or PIV	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.
	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.

CLASS DISCUSSION: POLL

- *Do we need a new ZTMM function within Identity to address Identity Proofing and Verification (Onboarding)*
- *Or is the coverage (that we haven't discussed in detail) in the Identity Risk category good enough?*

Identity / Risk Assessments			
Traditional	**Initial**	**Advanced**	**Optimal**
Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised).	Agency determines identity risk using manual methods and static rules to support visibility.	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.

CLASS DISCUSSION: SHORT DISCUSSION



- *Affirmative: Yes, "we need a new ZTMM function for Identity Proofing and Verification"*
  - *Is the problem that identities are too easily spoofed*
    - *OR*
  - *That when onboarding a new employee, we (almost always) send their corporate email to the user's identified personal email address?*
  - *What are some things that we (companies) can do to ensure irrefutable, correct identification during the initial identity onboarding process?*
- *Negative: No, Identity Risk is good enough*
  - *How do we ensure that "determination that an identity is compromised" is robust enough DURING ONBOARDING that the risk assessment is based on an effective/accurate baseline (as opposed to a baseline that is true but has been compromised since day 0)*
  - *Do we need to bring in the other ZTMM Categories and Asset Classes to be successful?*

Identity Onboarding	Authentication	Risk Assessments
Agency confirms user's identity with through (online) interview, and establishes their agency identifier by sending to the user's (user identified) personal email for bootstrapping	Agency authenticates identity using either passwords or multi-factor authentication (MFA) with static access for entity identity.	Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised).
Agency confirms user's identity ….. Establishes their agency identifier …..	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 determines identity risk using manual methods and static rules to support visibility.
Agency confirms user's identity ….. Establishes their agency identifier …..	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of passwordless MFA via FIDO2 or PIV	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.
Agency confirms user's identity ….. Establishes their agency identifier …..	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.

10 min
BREAK
BACK
9:05PM ET

(IDENTITY) RISK ASSESSMENTS ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency makes **limited determinations for identity risk** (i.e., likelihood that an identity is compromised).	Agency determines **identity risk using manual methods and static rules to support visibility**.	Agency determines identity risk with some **automated analysis and dynamic rules to inform access decisions** and response activities.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.

IDENTITY RISK

- Identity risk: risk that identity has been compromised or is otherwise being abused / engaging in suspicious or abnormal behaviour
  - Can be handled with analytics (user behaviour analytics)
  - With good MFA/Passkeys, can be mitigated by continual authentication
- In the news: XZ Utils and open source software committers

SUSPICIOUS IDENTITY ACTIVITY ….

https://www.centerforcybersecuritypolicy.org/insights-and-research/ai-brings-challenges-and-opportunities-for-digital-identity-in-financial-services

- FinCEN's June 2024 announcement that "2023 identity-related suspicious activity reports (SARs) filed by banks accounted for around half of value and almost three quarters of volume" underscores the impact that inadequate digital identity infrastructure is having on the financial services market.
- A core point that we made: while technologies like AI-powered liveness detection for biometrics and risk analytics engines offer promising defenses, we do not believe that their use alone will be sufficient to thwart the increasing use of generative AI by adversaries.
- AI may be able to spoof voices, photos and videos, but it cannot spoof – or defeat (yet at least) – systems that rely on the correct individual demonstrating possession of a private key. At a time when many identity proofing tools are focused on predicting whether someone is who they claim to be, public key cryptography provides a deterministic factor that can help to counter new AI-powered attacks.

(IDENTITY) AUTHENTICATION ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency authenticates identity using **either passwords or multi-factor authentication (MFA) with static access** for entity identity.	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 begins to authenticate all identity using **phishing-resistant MFA and attributes,** including initial implementation of **password-less MFA via FIDO2 or PIV**	Agency **continuously validates identity with phishing-resistant MFA**, not just when access is initially granted.

IDENTIFICATION - AUTHENTICATION

- Authentication is the process of proving that a user (holder of an identifier) is who they say they are
- Authentication is (traditionally) based on
  - Something the user knows (passwords)
  - Something the user has (one-time passwords issued by a dongle/PIV/CAC card etc)
  - Something the user is (biometrics)
- Two Factor Authentication (2FA) is usually password + one of the other two factors
- Multi-factor is usually a rebranding of 2FA to sound more complex (MFA is usually not 3+ factors)
- BUT
  - How do we know that the user who has these factors is in fact who they say they are? Missing from the ZTMM is the (not easy) area of Identity Verification

EXAMPLES OF PHISHING / MFA BOMBING

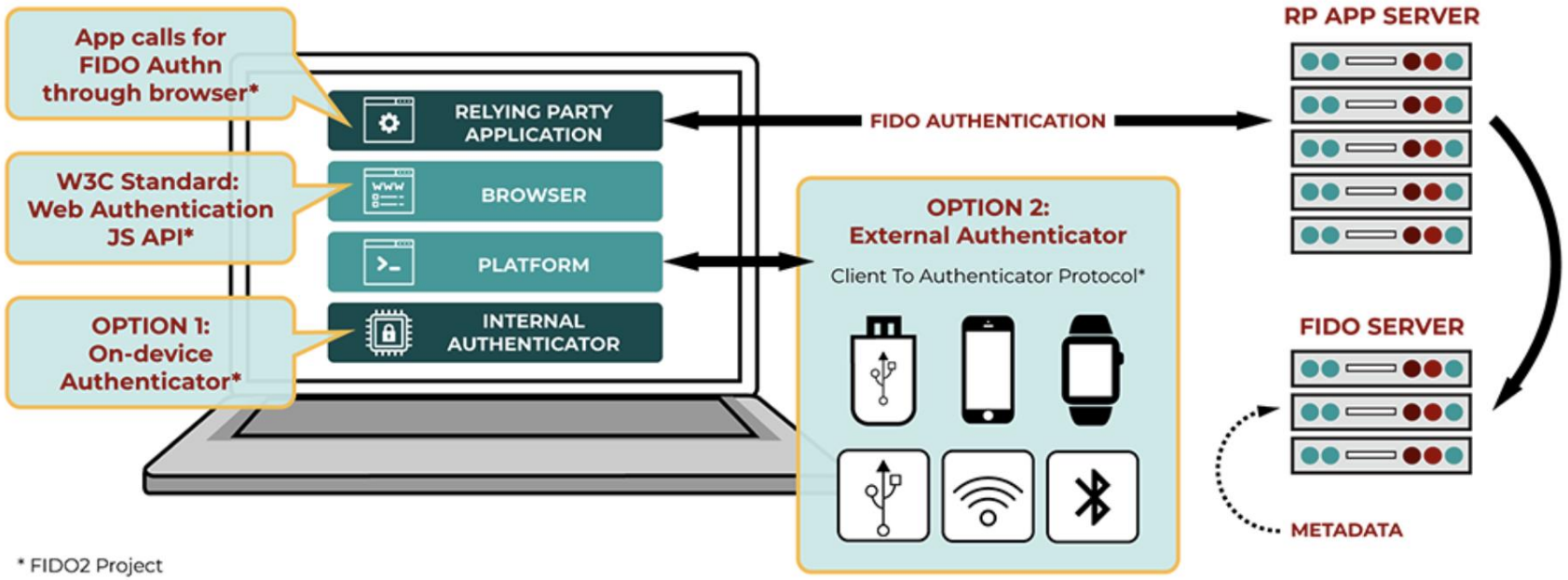
- MFA Bombing relies on a particular type of MFA - mobile phone based “Push”
- *Aside from MFA bombing, what else makes mobile push based MFA “not great”?*
- MFA Bombing in the news : https://krebsonsecurity.com/2024/03/recent-mfa-bombing-attacks-targeting-apple-users/

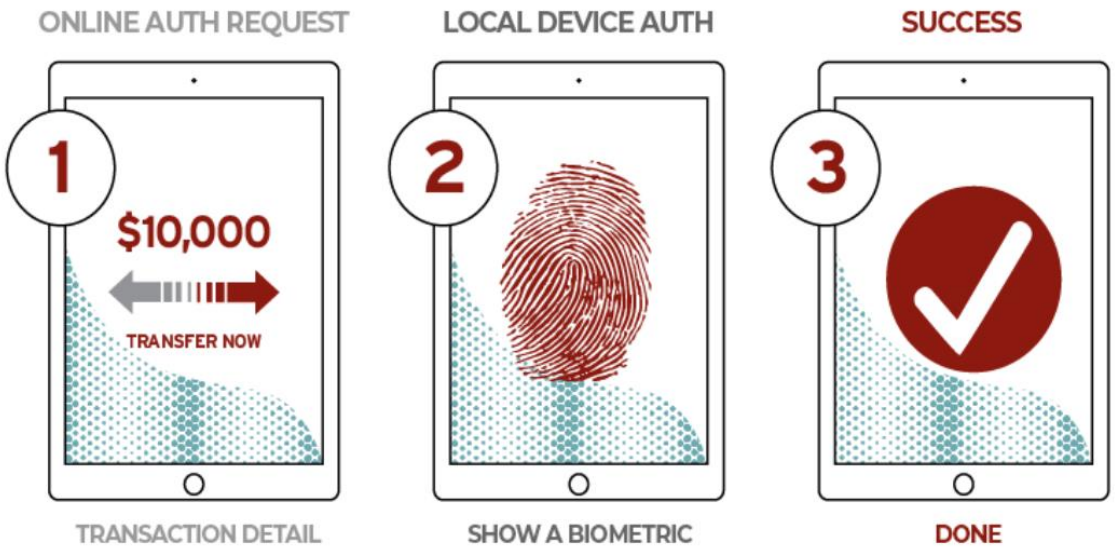
FIDO, PASSKEYS, PIV

- FIDO sets up a crypto key-pair for cryptographic signing-based authentication for each target authentication
- Using a (FIDO) Passkey for Sign-in
  - User is prompted by a service to sign in with a passkey
  - User signs in locally to their “Passkey utility”
    - Using local authentication method such as biometrics, local PIN or touching their FIDO security key
  - Passkey Utility uses the user’s account identifier provided by the service to
    - select the correct key and
    - sign the service’s challenge.
  - Passkey Utility sends the signed challenge back to the service,
  - Service verifies it with the stored public key and signs-in the user
- PIV stands for a "Personal Identity Verification" Credential.
  - PIV cards are used government-wide to control access to Federally Controlled Facilities and information systems at the appropriate security level
  - PIV cards require specialized card readers

PASSKEYS : THE EMPORER'S CLOTHING

- Passkeys are generated codes—created using public key cryptography—that are stored on your device or in your password manager and let you log in to websites and apps using your fingerprint, face recognition, or a PIN.
- Put very simply, when you create a passkey, the website or app you're using generates two pieces of code. One is stored by the website or app; the other is saved on your device. When you log in, you prove it is you via a face scan, fingerprint, PIN, or however you'd usually unlock your device, and the two pieces of saved code communicate with each other.
- QUOTE: "They are a true password replacement that eliminate the threat of phishing, eliminate the hassle of password resets, and eliminate the liability that service providers have when they're managing thousands, tens of thousands, or tens of millions, or billions of passwords," (from an article in WIRED)


App calls for FIDO Authn through browser*
W3C Standard: Web Authentication JS API*
OPTION 1: On-device Authenticator*
RELYING PARTY APPLICATION
BROWSER
PLATFORM
INTERNAL AUTHENTICATOR
FIDO AUTHENTICATION
OPTION 2: External Authenticator
Client To Authenticator Protocol*
RP APP SERVER
FIDO SERVER
METADATA
* FIDO2 Project


ONLINE AUTH REQUEST
LOCAL DEVICE AUTH
SUCCESS
1
$10,000
TRANSFER NOW
2
3
TRANSACTION DETAIL
SHOW A BIOMETRIC
DONE

CLASS DISCUSSION: POLL

- *How confident are you that your mobile device (or whichever device you are using as part of MFA) is secure?*
  - *If someone steals it, can they break in?*
- *How confident are you that your biometric info (face, finger) are yours and yours alone and can't be used by EvilCore to compromise your ID?*

(IDENTITY) IDENTITY STORES ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency only uses **self- managed, on-premises** (i.e., planned, deployed, and maintained by agency) **identity stores.**	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 begins to **securely consolidate and integrate some self-managed and hosted identity stores.**	Agency securely **integrates their identity stores across all partners and environment**s as appropriate.

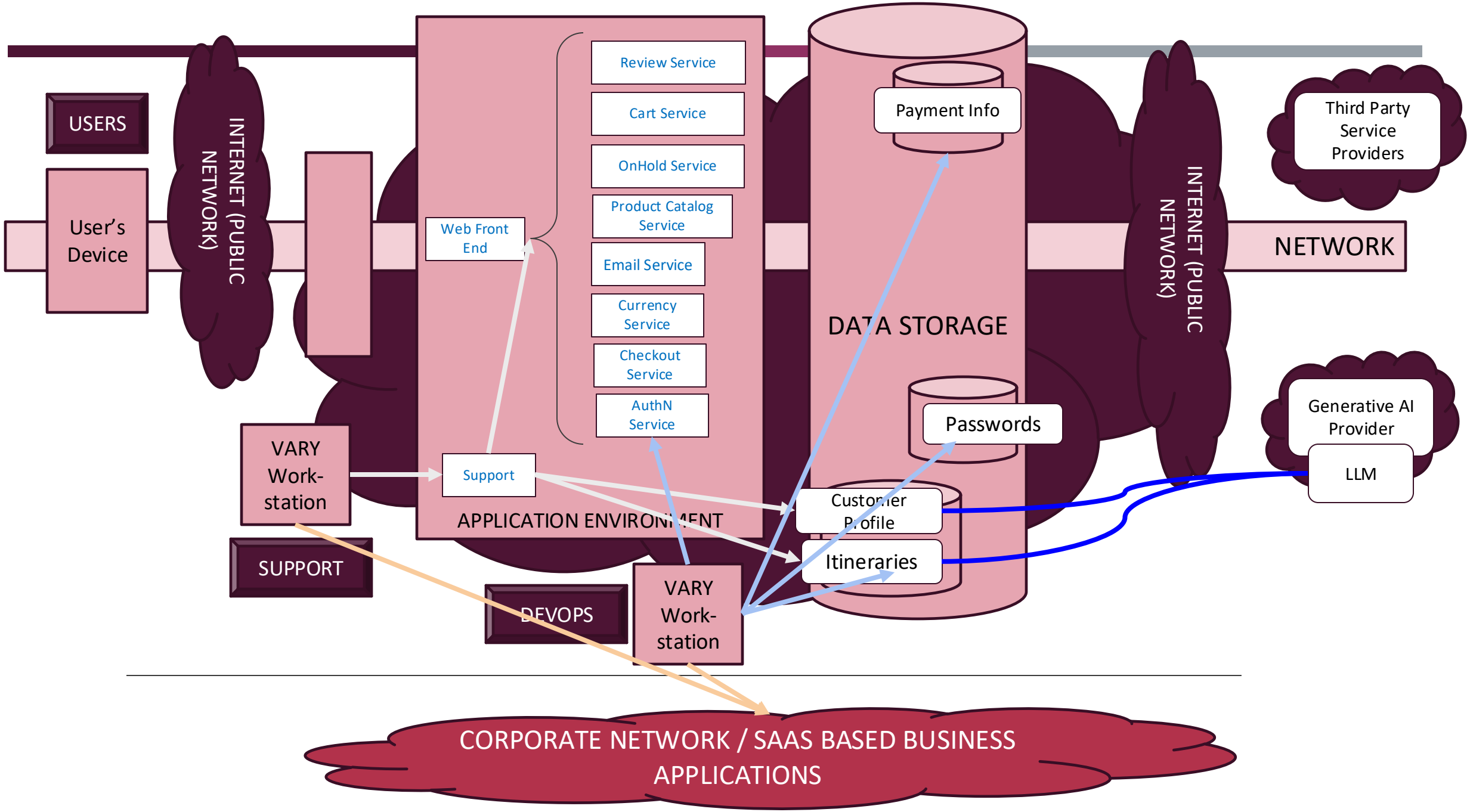
ACCESS MANAGEMENT ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency authorizes **permanent access with periodic review** for both privileged and unprivileged accounts.	Agency **authorizes access,** including for privileged access requests**, that expires with automated review**.	Agency **authorizes need-based and session-based access**, including for privileged access request, that is tailored to actions and resources.	Agency uses **automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs**

ANTICIPATED END OF LECTURE 9

IDENTITY	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Visibility and Analytics Capability	Agency collects user and entity activity logs, especially for privileged credentials, and performs some routine manual analysis.	Agency collects user and entity activity logs and performs routine manual analysis and some automated analysis, with limited correlation between log types.	Agency performs automated analysis across some user and entity activity log types and augments collection to address gaps in visibility.	Agency maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behavior-based analytics.
Automation and Orchestration Capability	Agency manually orchestrates (onboards, offboards, and disables) self-managed identities (users and entities), with little integration, and performs regular review.	Agency manually orchestrates privileged and external identities and automates orchestration of non-privileged users and of self-managed entities.	Agency manually orchestrates privileged user identities and automates orchestration of all identities with integration across all environments.	Agency automates orchestration of all identities with full integration across all environments based on behaviors, enrollments, and deployment needs.
Governance Capability	Agency implements identity policies (authentication, credentials, access, lifecycle, etc.) with enforcement via static technical mechanisms and manual review.	Agency defines and begins implementing identity policies for enterprise-wide enforcement with minimal automation and manual updates.	Agency implements identity policies for enterprise-wide enforcement with automation and updates policies periodically.	Agency implements and fully automates enterprise- wide identity policies for all users and entities across all systems with continuous enforcement and dynamic updates.

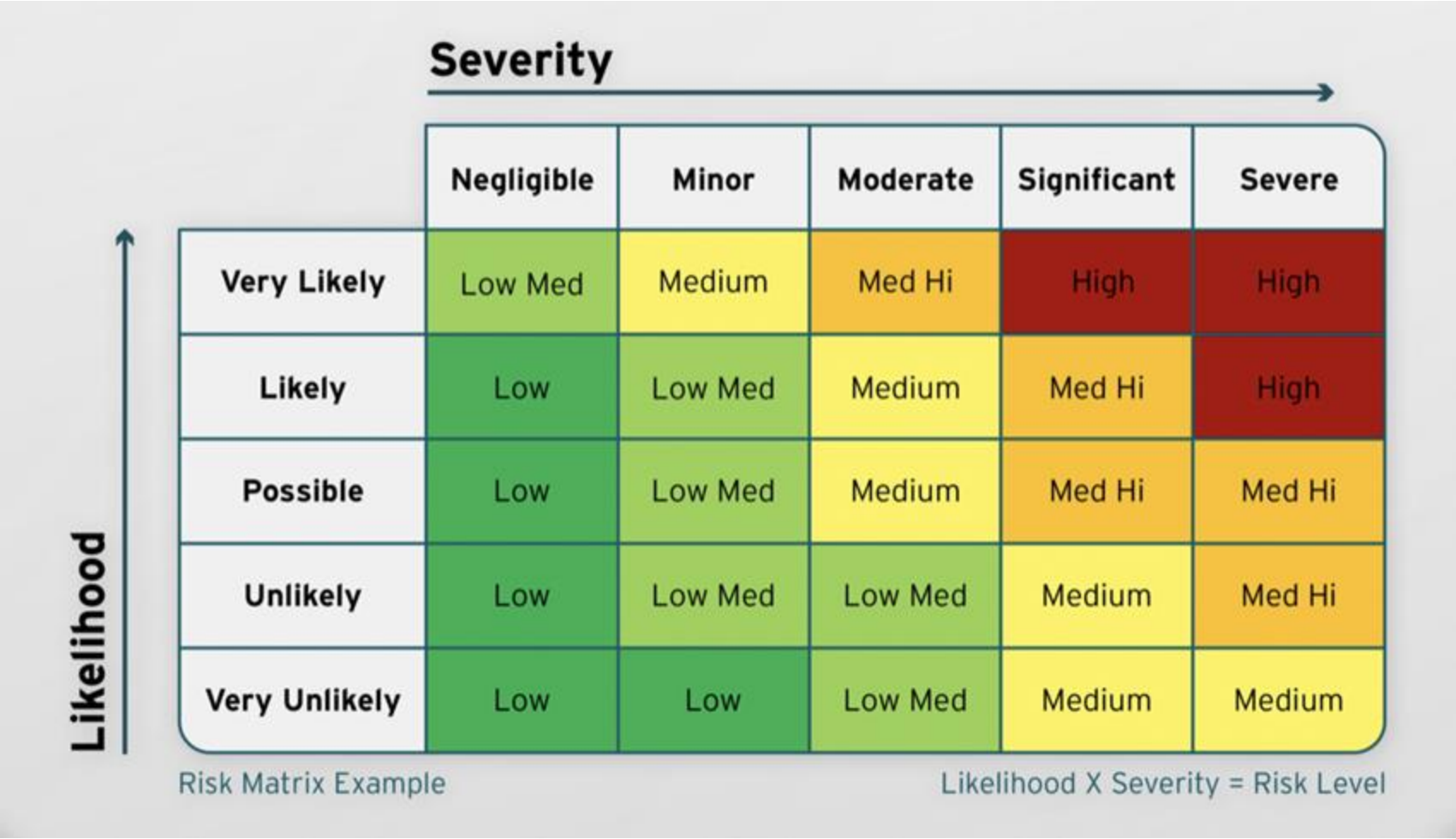
REFERENCE STUFF


USERS
User's Device
INTERNET (PUBLIC NETWORK)
Review Service
Cart Service
OnHold Service
Product Catalog Service
Email Service
Currency Service
Checkout Service
AuthN Service
Web Front End
Support
APPLICATION ENVIRONMENT
VARY Work-station
SUPPORT
DEVOPS
VARY Work-station
Payment Info
DATA STORAGE
Passwords
Customer Profile
Itineraries
INTERNET (PUBLIC NETWORK)
NETWORK
Third Party Service Providers
Generative AI Provider
LLM
CORPORATE NETWORK / SAAS BASED BUSINESS APPLICATIONS

RISK ASSESSMENT MATRIX

A risk assessment matrix identified IMPACT or CONSEQUENCES based on

- the *likelihood* the risk event will occur, and,
- the potential *severity* of the risk event



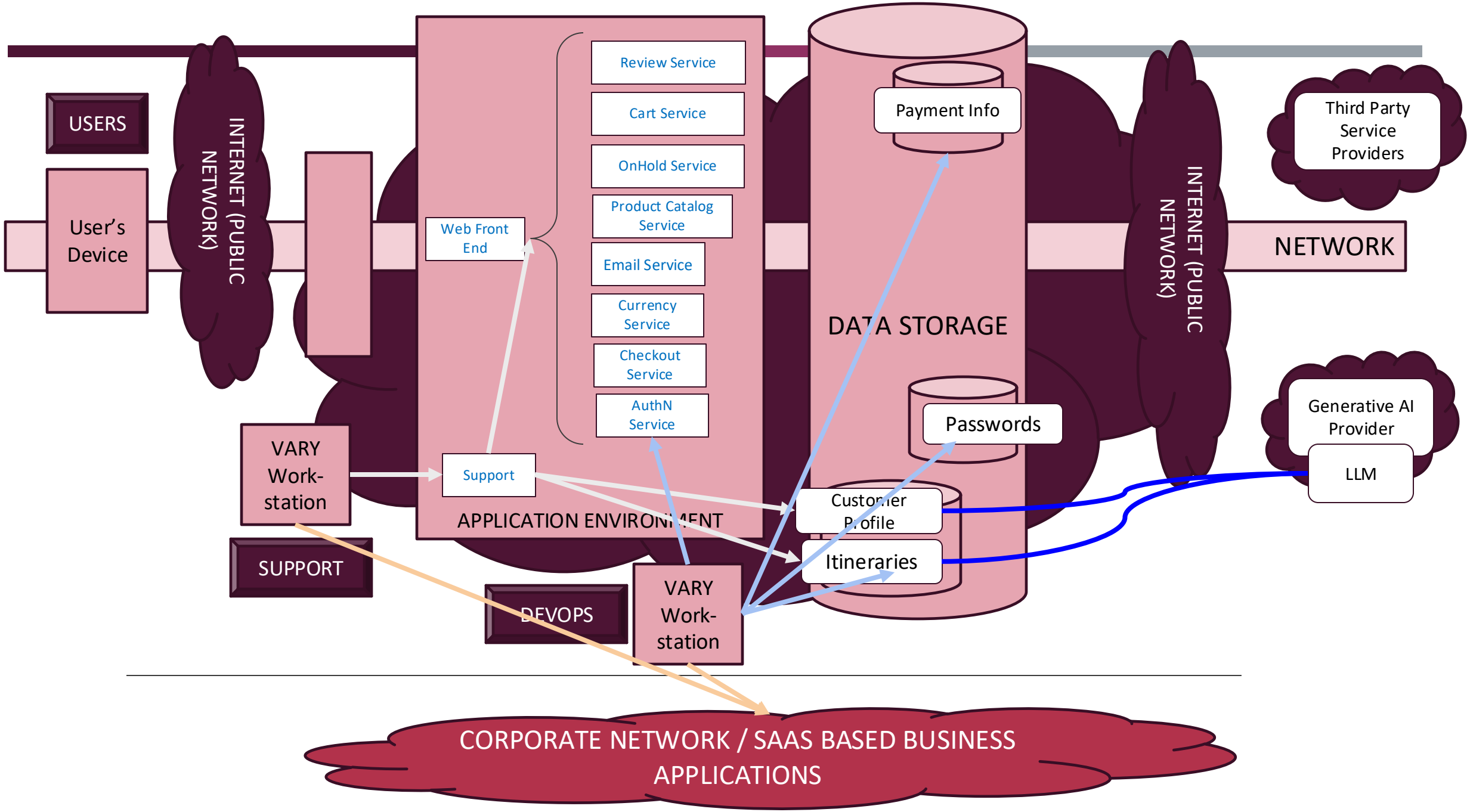
COURSE “USE CASE / CASE STUDY”

- We are going to use a fictional company with a web-facing application throughout the course, to illustrate concepts and decision points IF AND WHEN NEEDED

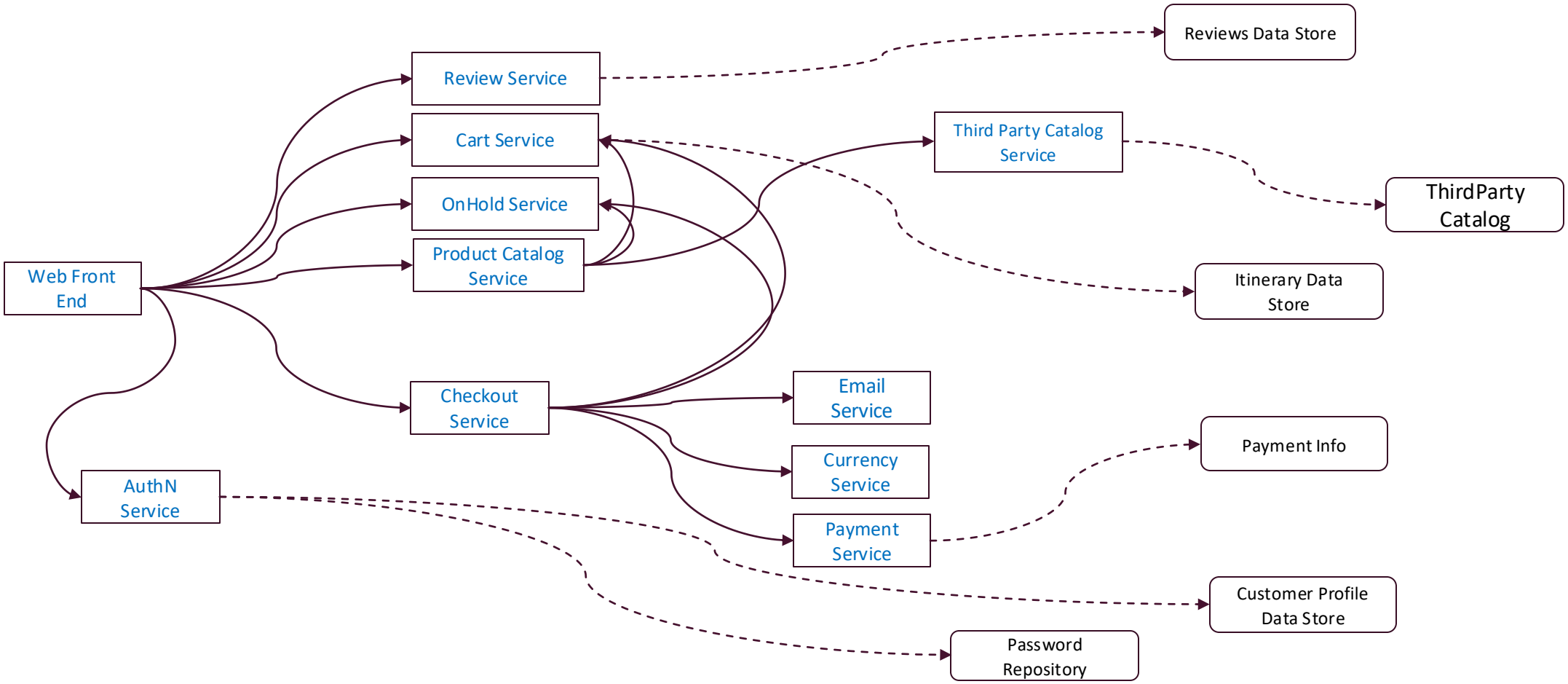
- OUR course use case : “Vacations and Rest for You” (VARY)

OUR COURSE USE CASE : “VACATIONS AND REST FOR YOU” (VARY)

- We provide
  - Online travel resource for all things vacation: hotels,/B&B, flights, car service, local site-seeing, etc
  - Concierge services for high end vacation including car service, fully arranged itinerary, personal tours, etc
- Users access us through our (mobile and browser formatted) Web page
  - Booked clients interact with us through a mobile application for viewing/managing their itinerary, chatting with agents
- We have phone, web chat, app chat, email support, including ability to turn a chat into a phone call
- We allow clients to view and download their itinerary
  - We are thinking about allowing them to upload files (esp photos) of good/bad things as part of reviews
- We want to improve our recommendations by adding GenAI functionality
    - Provide more targeted recommendations for things to do for customers


USERS
User's Device
INTERNET (PUBLIC NETWORK)
Review Service
Cart Service
OnHold Service
Product Catalog Service
Email Service
Currency Service
Checkout Service
AuthN Service
Web Front End
Support
APPLICATION ENVIRONMENT
VARY Work-station
SUPPORT
DEVOPS
VARY Work-station
Payment Info
DATA STORAGE
Passwords
Customer Profile
Itineraries
INTERNET (PUBLIC NETWORK)
NETWORK
Third Party Service Providers
Generative AI Provider
LLM
CORPORATE NETWORK / SAAS BASED BUSINESS APPLICATIONS

VARY SERVICE ARCHITECTURE



VARY APPLICATION: RESERVATION/CHECKOUT