



HARVARD EXTENSION SCHOOL

CSCI E-117A SPRING 2025

SECURE APPLICATIONS: MANAGING THE DEPLOYMENT
INFRASTRUCTURE

Lecture 9,
April 1, 2025

LECTURE 9

AGENDA

-
- *Case Study – Comments on Discussion*
 - *Rippling v Deel*
 - *How Zero Trust Maturity concepts played a role*
 - *Applications & Workloads*
 - *Zero Trust Maturity*
 - *Data*
 - *ZTM*
 - *Data as Target*
 - *Assignment III*
 - *Q&A , “Class Office Hours”*

SOME HIGHLIGHTS FROM LAST WEEK'S YELLOW DIG

- In late September 2024, the Internet Archive, a nonprofit digital library, experienced a significant data breach that compromised the personal information of 31 million users. The breach originated from an unpatched vulnerability in its GitLab instance, a widely used web-based application for source code management and DevOps collaboration
- ...
- time and time again we're reminded that even in the face of scary new AI technology and emerging threats, the bread and butter of cybersecurity hygiene boils down to the basics of regularly rotating secret tokens and keeping up to date with patching. a great reminder, thanks for sharing!

DISCUSSIONS

- Something that surprised me during the discussion was the mention of email often qualifying as mission critical vs business critical. This was an interesting perspective and prior to this discussion, I would not have thought of email as being mission critical for an organization. The more I've thought about it, email really is the main way that organizations communicate. Of course there are other platforms as well, but email is the main outlet used for both internal users within an organization communicate with each other AND how internal users communicate with their organization's customers. If email is down for even 4 hours, that lack of communication could cause chaos for the business.
- Some feedback from Instructors:
 - You should ALWAYS have a backup form of communication, if nothing else to support comms during an incident
 - Many companies view Slack as a backup – if you are a Google Enterprise customer, this is probably okay. If you are an all-in-on-Microsoft company, using Teams as your backup to Outlook may not make so much sense
 - IBM survived a 6-week outage of Lotus Notes (its email platform) during the pandemic – because they had started to build a Slack discipline and were able to pivot very quickly to Slack *but it was still very painful*

DISCUSSIONS

- In the discussion, I was surprised by the comments around if you do have a buggy application, you can combat a lot of it with security controls. This does make sense to me, but I found it surprising because typically we try to build things to be secure and get in front of any security issues vs relying on tools to counteract poor app dev security.
- ...
- However, Option 1 is more favorable for me (Especially when I learned what happened with the Deel/Rippling case) where those 2 organizations already have a mature development pipeline. Even with excellent secure development processes, applications in production can be exposed through social engineering and insider threats. The main vulnerability is that far too many employees have wide-ranging permissions into sensitive apps, or the trouble in tracking intrusions once an attacker is inside, Option 1's access and threat protections could deliver immediate value.
- ...
- What surprised me the most was how little control we have over SaaS applications. In my company, we extensively use them, and we often think they are inherently secure. However, in reality, they may pose significant security risks.

DISCUSSIONS

- I viewed the choices initially based on the majority of my career being as a software developer yet I failed to consider all the many third party services we used. Additionally now that I am in a cyber role its was a good reminder to thing about the business as a whole and how best to protect it with the many third party apps used
- I was surprised by the fact that so many of the folks in class work for companies that don't do a significant amount of custom development.
- AND....
- At IBM we once counted there were 18,000 business applications required to run the business. The likelihood of one of those systems being breached is far higher and the damage potential is outside a few corner case scenarios, far higher.

DISCUSSIONS

- But one thing that I didn't necessarily think about when I made my choice of #2 is that some of the applications that I rely on for my secure development (like GIT Lab, or Snyk, or any other security tool) is also a third party application, and I must have some baseline to define how those applications are vetted, tested, and ensured that they are secure. So this brings up an important aspect of technology - no one can be self sufficient! You cannot realistically build everything yourself. You have to rely on third parties for your business to run - and so there needs to be a high bar for the quality of applications the business should use and deploy.
- ...
- I picked option 2. To me, it sounds like the obvious choice to implement increased maturity in the development stage of an application rather than after its deployment. Retroactively implementing increased maturity in places like application access and threat protections is easier when the application has a strong foundation.
- ...
- . This week reminded me to evaluate risk in terms of likelihood, business impact, and visibility, not just where I have the most control.

SIGNALGATE – AFTER CLASS SAFE DISCUSSION SPACE

- Using *Signal* for national security or defense, or any official US government business is both absurdly stupid and reckless.
- However, it is a very valuable tool for many others. It is commonly portrayed as associated with subversive behavior, but *Signal* is an end-to-end encryption service that doesn't require a huge investment by an organizations. Let me give you a practical example.
- If you have a legal department, they have to abide by rules of professional conduct to ensure attorney-client communications are secure. Allowing a third party not in the scope of the legal privilege to access to the communications destroys the privilege and allows those communications to be handed over in discovery or any investigation.
- *Signal* allows for forward secrecy, deniability, and post-compromise security, and it is considered cryptographically sound.
- However, *Signal* was never meant to replace secure classified systems like:
 - SIPRNet (Secret Internet Protocol Router Network), for up to SECRET
 - JWICS (Joint Worldwide Intelligence Communications System), for TOP SECRET/SCI
 - NSANet – NSA's internal classified system
 - DISS and NIPRNet – for DoD administrative communication

SIGNALGATE – AFTER CLASS SAFE DISCUSSION SPACE

The Policy and Security implications include:

1. Violation of Executive Orders & DoD Cyber Hygiene Guidelines

Per EO 13526 and DoD Manual 5200.01, classified or sensitive information must never be transmitted over unclassified networks unless explicitly approved, encrypted, and monitored.

Signal is encrypted, but it is unclassified and not auditable by government standards.

2. Loss of Non-Repudiation

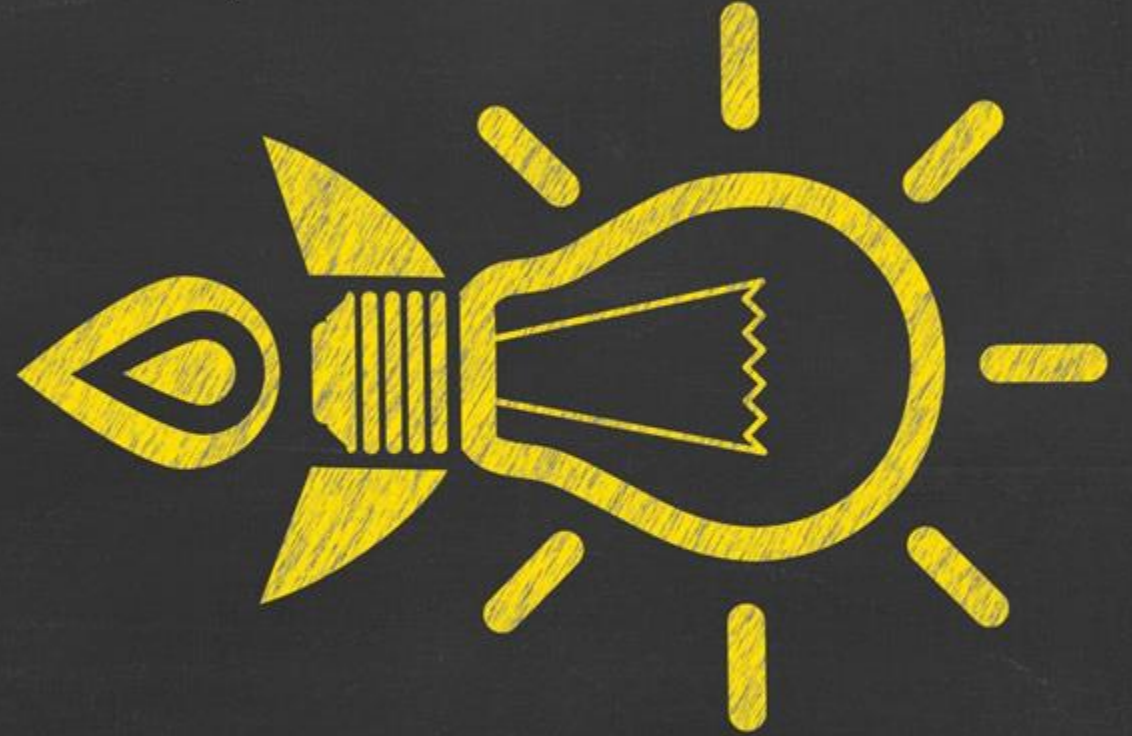
Because *Signal* uses “deniable authentication,” there’s no cryptographic proof of message authorship, useful for activists, but a disaster for command responsibility in military ops.

3. Strategic Exposure

An adversary (say, a foreign SIGINT agency) who socially engineers or exploits contact syncing in *Signal* could observe operational tempo, response posture, and leadership intent, even without decrypting content.

- Encryption does not equal secure comms
- Zero Trust must extend to identity, not just infrastructure
- Consumer platforms lack the administrative controls, forensic visibility, and access governance required for national security use
- Humans are the unpatchable vulnerability

ASSIGNMENT 3



ASSIGNMENT 3: Devices



Due Date: March 16

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

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

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

FEEDBACK

- Option Question (3 months, 6 months, Delaying 9 months for all 3)
- It felt like a non zero number of you fed this question into an AI somewhere and came back with “Delaying 9 months” – the arguments for why were all similar and not (honestly) well reasoned
- Long term benefits of delaying by 9 months from a maturity standpoint but this comes with its own risks which were not well reasoned on the whole.
- What are the downsides of delaying all programs?
 - Company has already accepted the risk of not doing #3 – that is why it didn’t make the cut the first time. What we don’t know (you weren’t given info, and very few people highlighted) is how significant is the risk and how “easy” would it be for threat actors to compromise based on lack of options #1 and #2. This should have been highlighted in the responses when making a decision the stay with option 3 (keep all programs but delay by 9 months)

RUBRICS: QUESTION 2B/C/D (JUSTIFICATIONS)

Criteria	Exceeds Expectations (4 pts)	Meets Expectations (3 pts)	Approaching Expectations (2 pts)	Below Expectations (1 pt)
Threat Identification	Clearly identifies a specific and relevant threat with precise articulation.	Identifies a relevant threat.	Mentions a vague or generic threat.	No threat identified or irrelevant.
Likelihood & Severity of Compromise	Accurately assesses both likelihood and severity with clear reasoning.	Addresses both likelihood and severity, but reasoning may lack clarity.	Mentions only one (likelihood or severity), or reasoning is weak.	No clear mention of either likelihood or severity.
Cost & Intrusiveness	Provides a thoughtful analysis of cost and intrusiveness across dollars, people, and time.	Addresses cost and intrusiveness, but with limited detail or scope.	Mentions cost or intrusiveness, but not both; lacks specifics.	Omits consideration of cost and intrusiveness.
Clarity & Conciseness	Justification is highly clear, concise, and well-structured.	Justification is mostly clear and within the length requirement.	Somewhat unclear or goes slightly over/under the length.	Unclear and significantly off in length or focus.

“GOOD” ANSWER FROM CHAT GPT

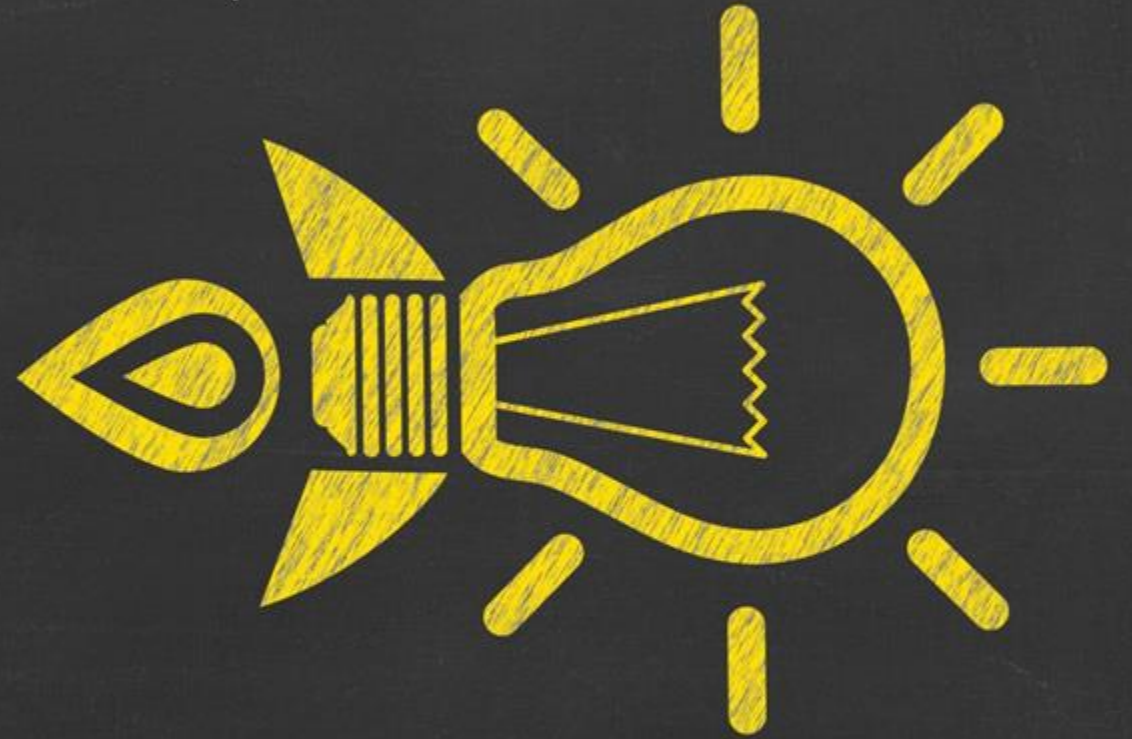
Harvard's ChatGPT

- I would choose to **keep all three programs but slip the delivery of all three by nine months**. While the delay is unfortunate, the risks associated with dropping Priority 3 are too severe—this application class is exposed to high likelihood of compromise due to outdated segmentation and lacks adequate monitoring.
- The impact of a compromise in this area could result in credential theft or lateral movement into sensitive systems. Though the program is resource-intensive, spreading the delay evenly across all programs preserves long-term security. The extended timeline allows for realistic reallocation of staff without overloading teams or increasing costs dramatically.

Instructor's answer (note depends on selection of 1, 2, 3; this answer is provided to make the case that it is NOT a slam dunk to keep all 3 programs and slip by 9 months, despite what ChatGPT tells you to do)

- I would choose to drop program 3, keeping programs 1 and 2 but with a 3-month slip in delivery. While it is tempting to keep all 3 programs and live with a 9-month delay, the business has already accepted the risk with not implementing program 3. We know that there are active threats to the environment that we must address through programs 1 and 2; we do not believe that it is appropriate to accept those risks for an additional 6 months as would be required by option 3. By limiting the extension of the timeline, staff can continue to work on the initial project goals (programs 1 and 2) with a realistic timeline, and then move on to projects that were delayed/moved aside for the initial option (all 3 priorities). It is unfortunate that we will sideline program 3; however, we believe that at a minimum the groundwork done as part of the initial work (before this reset) will allow us to pick up program 3 in a timely manner in the future.

ASSIGNMENT 4



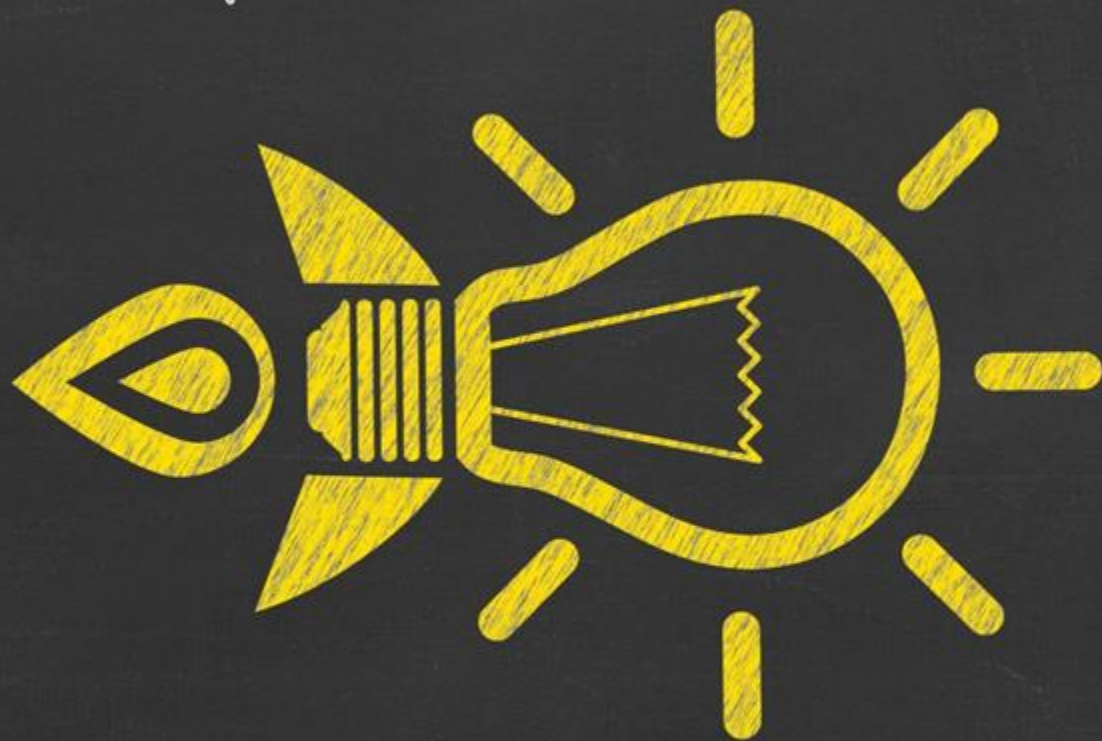
ASSIGNMENT 4



Due Date: April 6

Purpose: Understand Application category of Zero Trust Maturity

CAPSTONE

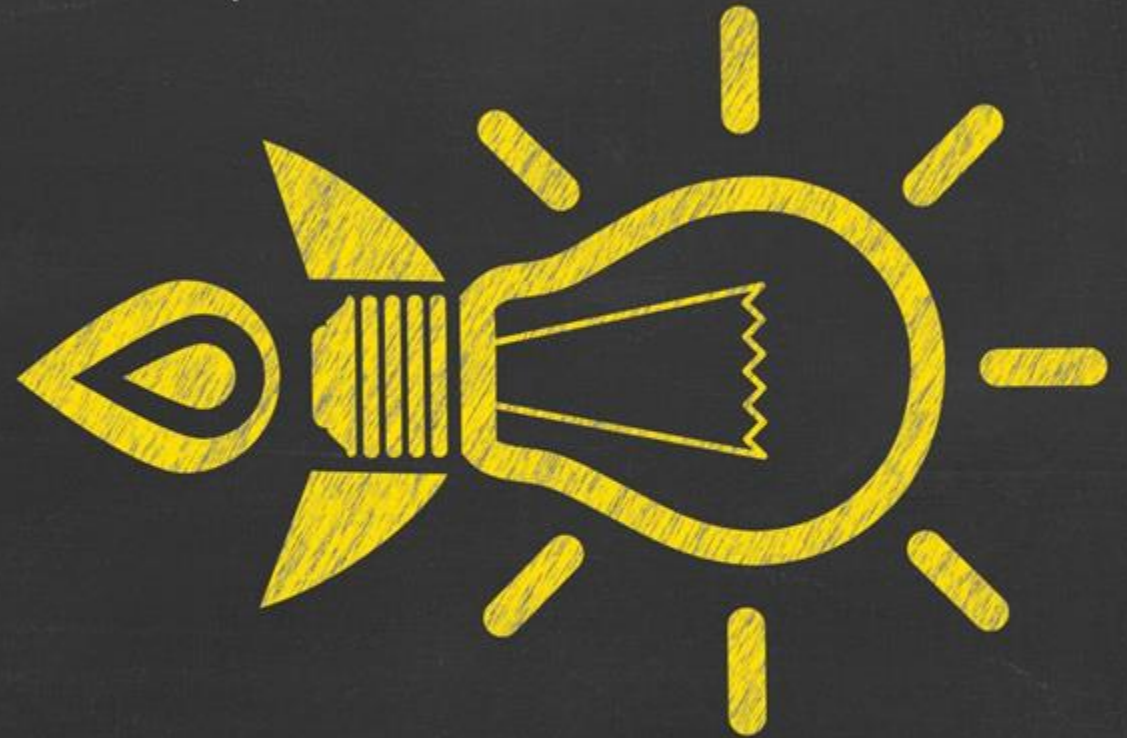


CAPSTONE

Published

Discussion at end of class

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

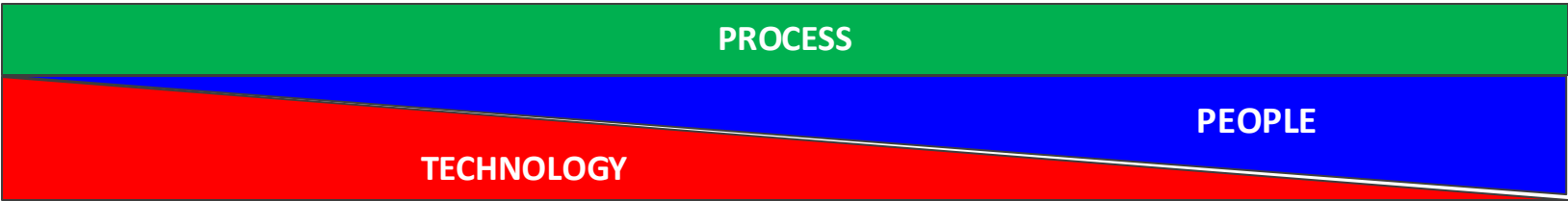
CYBER DEFENSE MATRIX

	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DEVICES					
NETWORKS					
APPS					
DATA					
USERS					
DEGREE OF DEPENDENCY	TECHNOLOGY		PEOPLE		
	PROCESS				

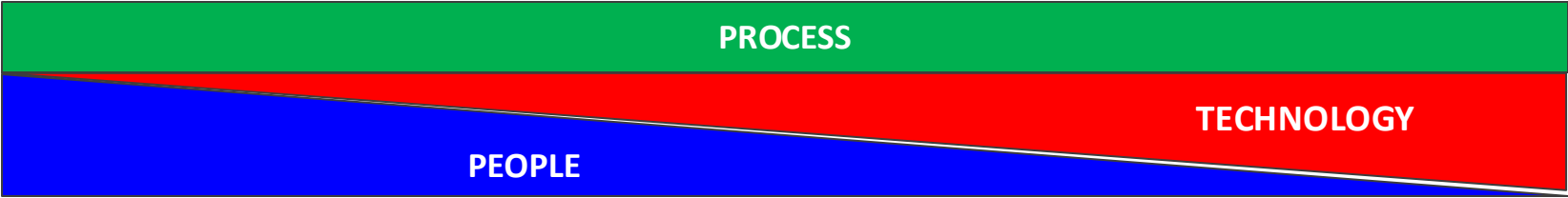
Figure 1: Cyber Defense Matrix



Cyber Defense Matrix

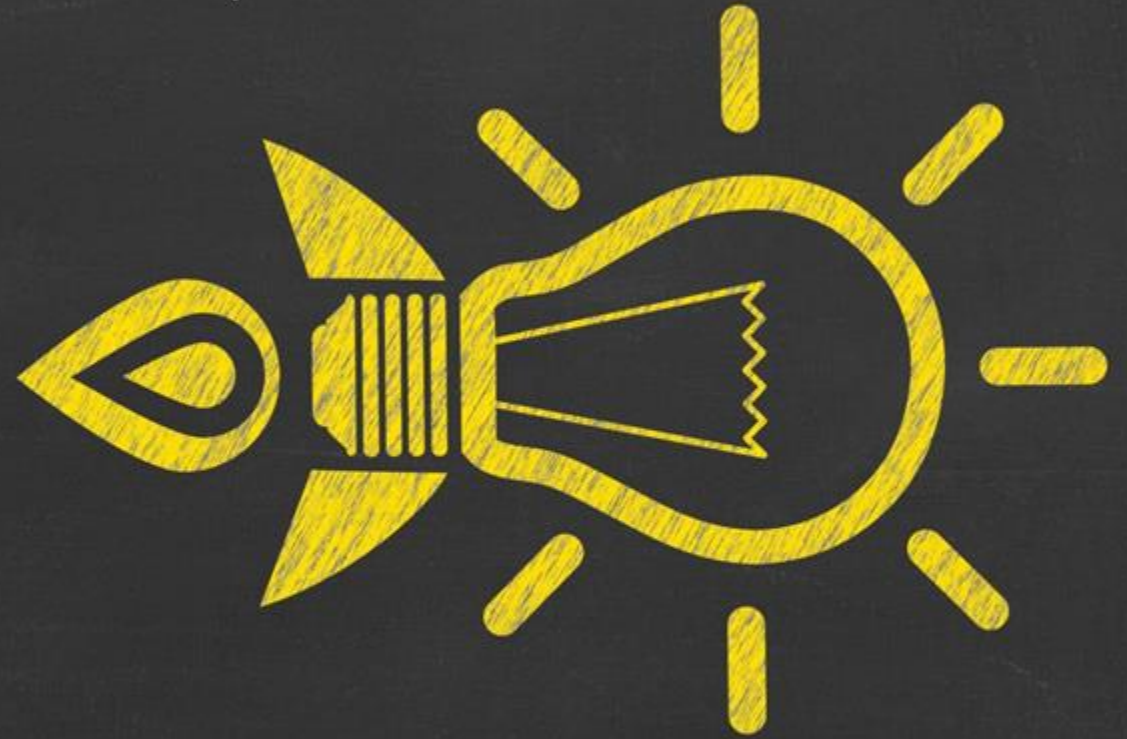


	IDENTIFY	PROTECT	DETECT	RESPOND & RECOVER	
DEVICES					DEVICES
NETWORKS					NETWORKS
APPLICATIONS & DATA					APPLICATIONS & DATA
USERS					USERS
	TRADITIONAL	INITIAL	ADVANCED	OPTIMIZED	



Zero Trust Maturity

APPLICATION, IDENTITY BASICS



APPLICATIONS & WORKLOADS

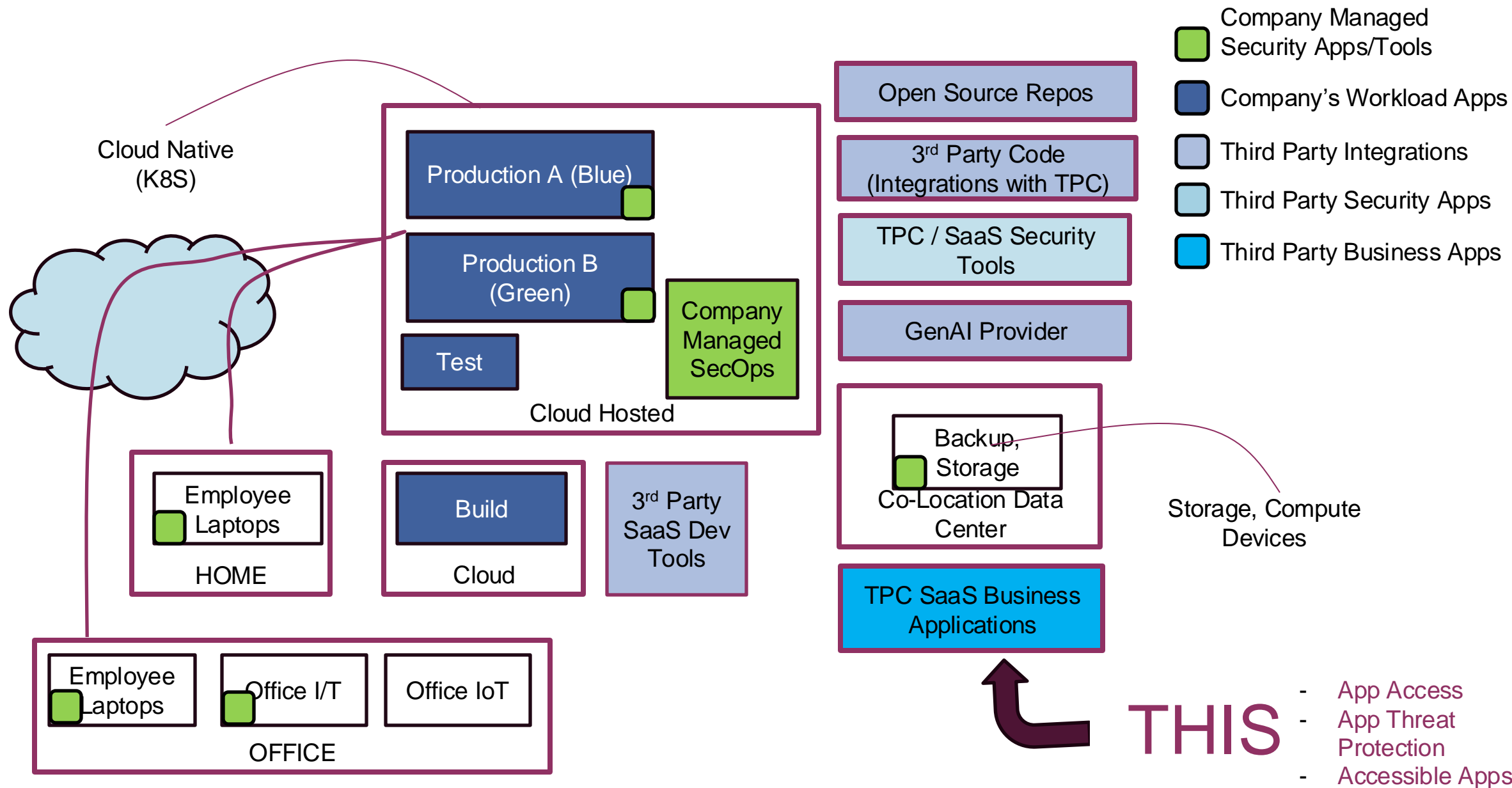
Software code and applications on the devices, separate from the operating system/firmware. This class includes serverless functions, APIs and microservices.

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)

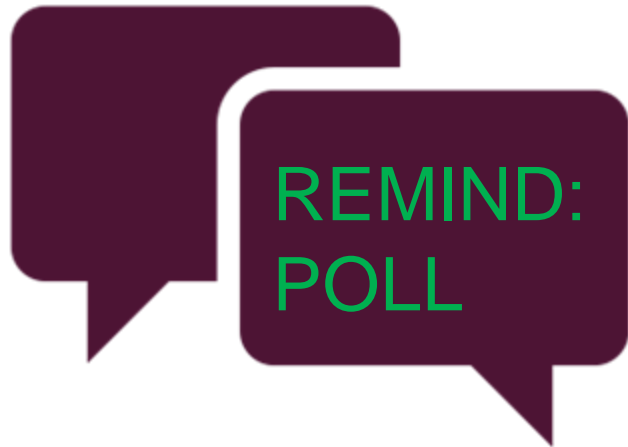
- Application Access
 - Formerly Access Authorization
- Application Threat Protections
 - Formerly Threat Protection
- Accessible Applications
 - Formerly accessibility
- Secure Application Development and Deployment workflow
 - New function
- Application Security Testing
 - Formerly Application Security

APPLICATION & WORKLOAD ZERO TRUST FUNCTIONS

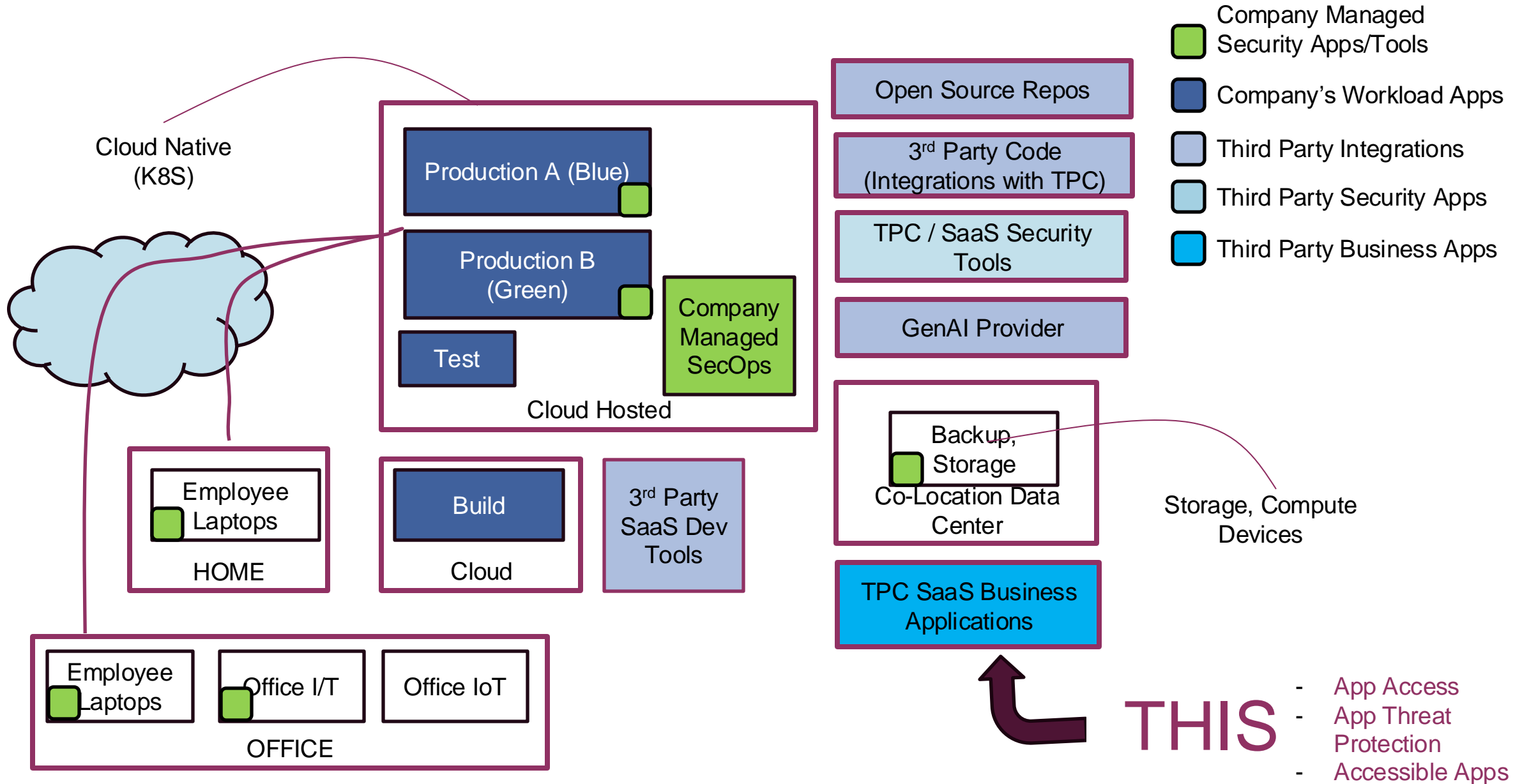
- Application Access (former Access Authorization)
 - Covers authorization for access to applications moving from local authorization and static attributes to real-time risk analytics and factors such as behavior or usage patterns
- Application Threat Protections (formerly Threat Protection)
 - Covers threat protections including general purpose protections for known threats moving to continuous dynamic monitoring across all applications for comprehensive visibility.
- Accessible Applications (formerly accessibility)
 - Moves from some mission critical applications available only over private networks and protected public network connections (e.g., VPN) with monitoring.
 - Moves towards all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed
- Secure Application Development and Deployment workflow (new function)
 - Covers development, testing, and production environments and code deployment mechanisms.
- Application Security Testing (formerly Application Security)
 - Covers application security testing prior and post deployment moving from manual testing to automated continuous testing.



REMINDER CLASS DISCUSSION: LAST WEEK'S POLL & DISCUSSION



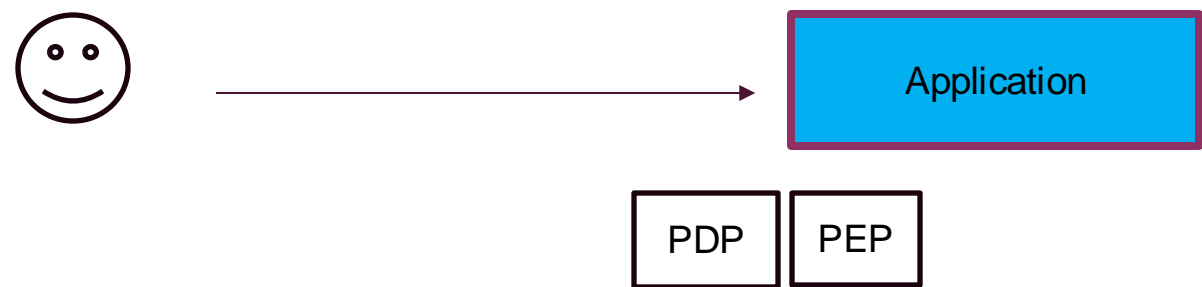
- *Regardless of the Case Study (which you should have already read), which would you rather make the case for increased maturity within YOUR organization*
- **Option 1:**
 - *Application Access*
 - *Application Threat Protections*
 - *Accessible Applications*
- **Option 2:**
 - *Secure Application Development and Deployment workflow*
 - *Application Security Testing*



APPLICATION ACCESS ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency authorizes access to applications primarily based on local authorization and static attributes.	Agency begins to implement authorizing access capabilities to applications that incorporate contextual information (e.g., identity, device compliance, and/or other attributes) per request with expiration.	Agency automates application access decisions with expanded contextual information and enforced expiration conditions that adhere to least privilege principles.	Agency continuously authorizes application access, incorporating real-time risk analytics and factors such as behavior or usage patterns.

Secure use of an application that you do not control: Access



TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Access control decision (authorizes access) based successful authentication (AuthZ done elsewhere)	AuthZ based on role / permissions set for user and may include context (device, location)	Time-bounded AuthZ based on user's least privileged based with additional context (device, location)	AuthZ continually re-checked, including behavior and usage factors in each decisions
Coarse grained permissions	Move to fine-grained permissions for user's privileges, context Start to introduced Policy Decision / Enforcement Split	More control to PDP & PEP model	

CLASS (RHETORICAL FOR NOW) QUESTION:



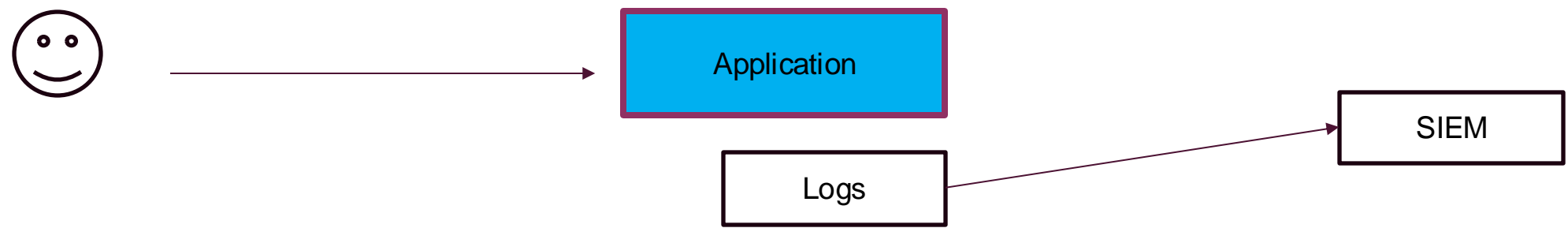
QQ?

- *How do we practically ensure zero-trust driven application access maturity for an environment with more than (eg) 5 applications?*
- *Is the complexity of this type of approach one that actually pushes us away from a zero trust model (individual access to 100s of apps with least privilege, device complexity, etc etc is not simple)*

APPLICATION THREAT PROTECTION ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency threat protections have minimal integration with application workflows, applying general purpose protection for known threats	Agency integrates threat protections into <u>mission critical application</u> workflows, applying protections against known threats and some application- specific threats.	Agency integrates threat protections into <u>all application workflows</u> , protecting against some application-specific and targeted threats	Agency integrates advanced threat protections into <u>all application workflows</u> , offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.

Secure use of an application that you do not control: Threat Protection

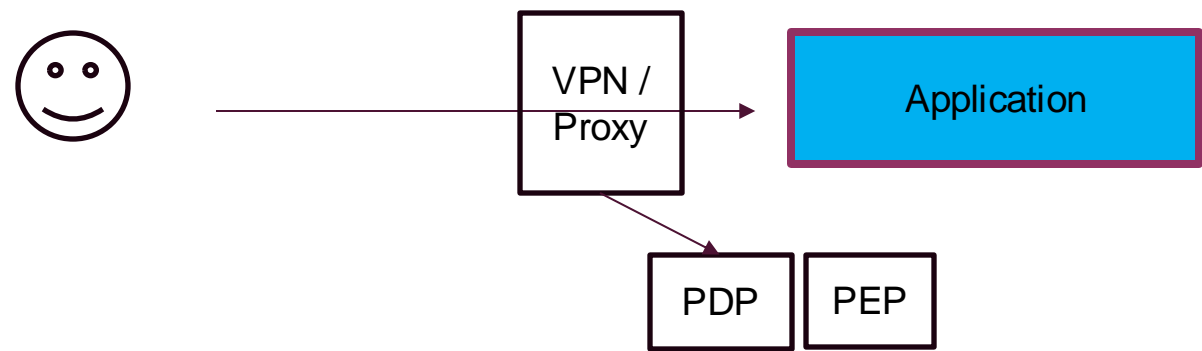


TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
General purpose protection for known threats	Threat protections for mission critical apps, against known threats & app-specific threats	Extend threat protection to all apps	Add real-time visibility and content-aware protections against sophisticated attacks tailored to applications
Access control (unauthZ access) (address insider threat/malicious use by trusted user)	Add controls for privilege escalation, data exfiltration Monitor logs for anomalous behavior	Monitor logs for “system wide” anomalous behavior Monitor for “known suspicious” behavior	Increasingly sophisticated monitoring that includes / depends on increasingly mature controls across the board

ACCESSIBLE APPLICATION ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency makes some mission critical applications available only over private networks and protected public network connections (e.g., VPN) with monitoring.	Agency makes some of their applicable mission critical applications available over open public networks 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.

Secure use of an application that you do not control: (Network) Access



TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Mission critical applications available only over private networks and protected public network connections (VPN)	Some mission critical available over open public networks to authorized users with need via brokered connections	Most of their applicable mission critical applications available over open public network connections to authorized users as needed	All applicable applications available over open public networks to authorized users and devices
Network access is part of the protection (crunchy exterior)	Brokered connections with authorized/VPN client	Move to application-driven authZ (move crunchy exterior to the app / remove app squishiness)	Depends on robust authentication, authorization of users/identities AND devices

CISA SECURE BY DESIGN PLEDGE

▪ PLEDGE GOALS

- MFA
- Passwords
- Removing "classes" of vulnerability
- Security patching
- Vulnerability disclosure
- CVE transparency
- Evidence of intrusion

▪ IMPLICATIONS

- Available at no extra cost
- Default Passwords removed
- (EG) No more SQLi
- Easier for customer to install patches (OnPrem s/w)
- Support responsible disclosure by public
- Accurate CWE, CVE for applications
- Customer's have access to logs for intrusion evidence

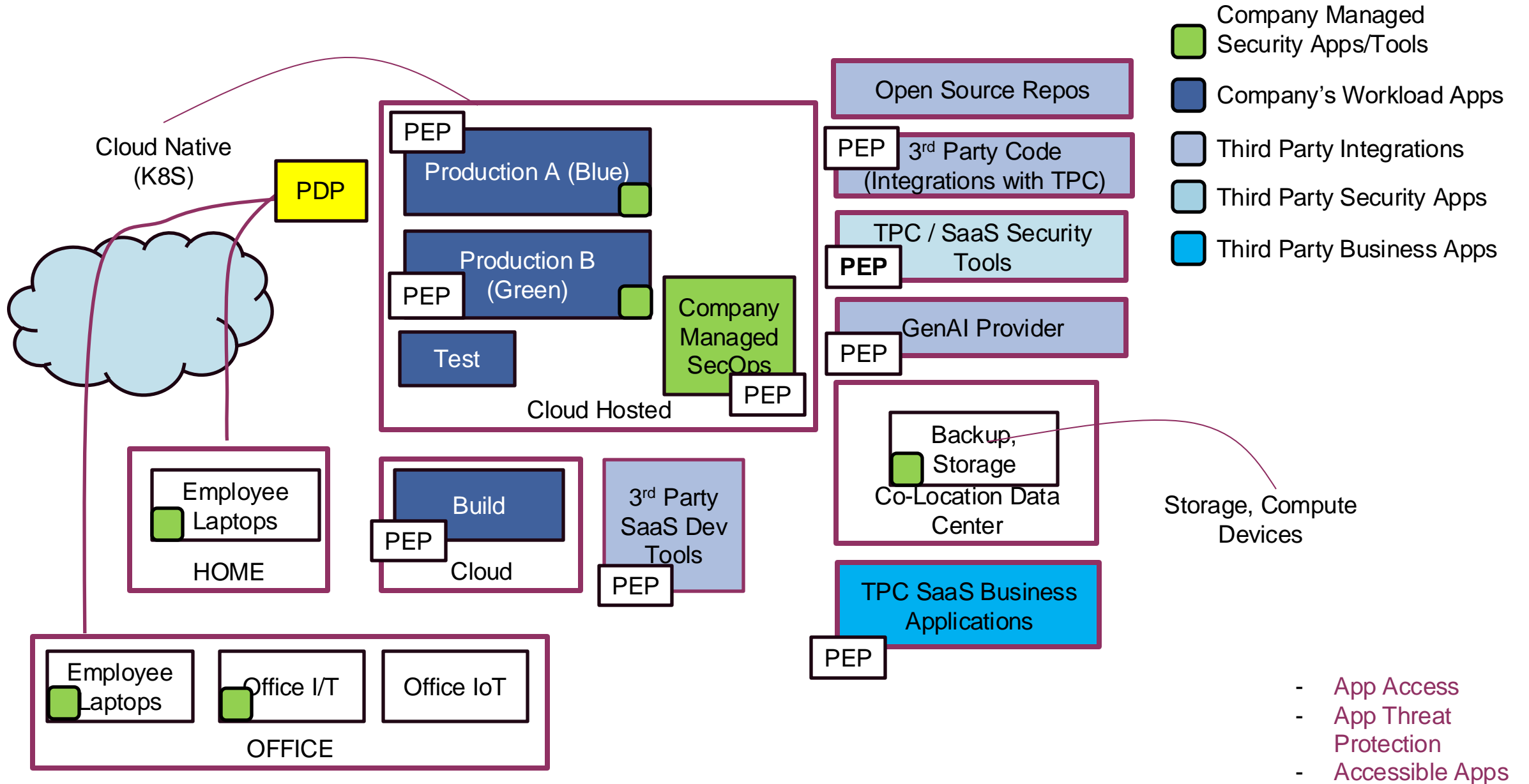
SECURE APPLICATION DEVELOPMENT ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency has ad hoc development, testing, and production environments with non-robust code deployment mechanisms.	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 uses distinct and coordinated teams for development, security, and operations while removing developer access to production environment for code deployment.	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.

APPLICATION SECURITY TESTING ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency performs application security testing prior to deployment, primarily via manual testing methods.	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.	Agency integrates application security testing into the application development and deployment process, including the use of periodic dynamic testing methods.	Agency integrates application security testing throughout the software development lifecycle across the enterprise with routine automated testing of deployed applications.

APPLICATION				
	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Visibility and Analytics Capability	Agency performs some performance and security monitoring of mission critical applications with limited aggregation and analytics.	Agency begins to automate application profile (e.g., state, health, and performance) and security monitoring for improved log collection, aggregation, and analytics.	Agency automates profile and security monitoring for most applications with heuristics to identify application-specific and enterprise-wide trends and refines processes over time to address gaps in visibility.	Agency performs continuous and dynamic monitoring across all applications to maintain enterprise-wide comprehensive visibility.
Automation and Orchestration Capability	Agency manually establishes static application hosting location and access at provisioning with limited maintenance and review.	Agency periodically modifies application configurations (including location and access) to meet relevant security and performance goals.	Agency automates application configurations to respond to operational and environmental changes.	Agency automates application configurations to continuously optimize for security and performance.
Governance Capability	Agency relies primarily on manual enforcement policies for application access, development, deployment, software asset management, security testing and evaluation (ST&E) at technology insertion, patching, and tracking software dependencies.	Agency begins to automate policy enforcement for application development (including access to development infrastructure), deployment, software asset management, ST&E at technology insertion, patching, and tracking software dependencies based upon mission needs (for example, with Software Bill of Materials).	Agency implements tiered, tailored policies enterprise- wide for applications and all aspects of the application development and deployment lifecycles and leverages automation, where possible, to support enforcement.	Agency fully automates policies governing applications development and deployment, including incorporating dynamic updates for applications through the CI/CD pipeline.



CLASS DISCUSSION: POLL



- *The Application Asset Class/Category is the one that most depends on maturity of other categories (network, devices, identity) AND the types of applications you are using (self-developed&hosted/on-prem/SaaS)*
- **Question 1:**
 - *If you are developing your own applications, which approach to improvement do you want to focus on (Application ZTMM or Secure by Design Pledge & Principles)*
- **Question 2:**
 - *If you are using primarily “other-developed” applications, including SaaS and on-prem (you manage), which do you want to focus on?*
- **Question 3:**
 - *Next page*

CLASS DISCUSSION: POLL



- **Question 3:**

- *How would you prioritize Application ZTM for your environment (assume you are primarily SaaS/Cloud Native) with respect to Networks, Devices*
 1. *Networks, Devices, Applications*
 2. *Networks, Applications, Devices*
 3. *Devices, Applications, Networks*
 4. *Devices, Networks, Applications*
 5. *Applications, Networks, Devices*
 6. *Applications, Devices, Network*

CLASS QUESTION / SET UP FOR BREAKOUTS:



- *How do we practically ensure zero-trust driven application access maturity for an environment with lots of applications?*
 - *What is the cross over point of applications that must be included in ZTM that makes the Application ZTM category “too difficult” to progress beyond initial maturity?*
- *Is the complexity of this type of approach one that actually pushes us away from a zero trust model (individual access to 100s of apps with least privilege, device complexity, etc etc is not simple)*

CLASS DISCUSSION: BREAKOUTS



DISCUSS



Auth0 Platform

Built to tackle both Consumer and SaaS Apps across every industry. Authenticate, authorize, and secure access for applications, devices, and users.

- *Tools such as Okta Moving to ZTM is associated with adoption of zero trust*
- *Does moving to an Okta-enabled zero trust environment break the cycle of crunchy exterior / squishy interior we associate with OnPrem networks?*
- *Or does it just change what you have to do to get unauthorized access to the interior?*
 - *With “legacy data center” worlds, access to the network (or access to a device authorized to get access to the network) gave you access to everything on the network (hence the squishiness)*
 - *Is the zero trust proxy just the new (also single point of failure), such that access to the ZTP (zero trust proxy) OR an identity managed by the zero-trust proxy the new equivalent of granting access to everything?*
 - *Have we really reduced the risks or just transferred the focus of our threats?*



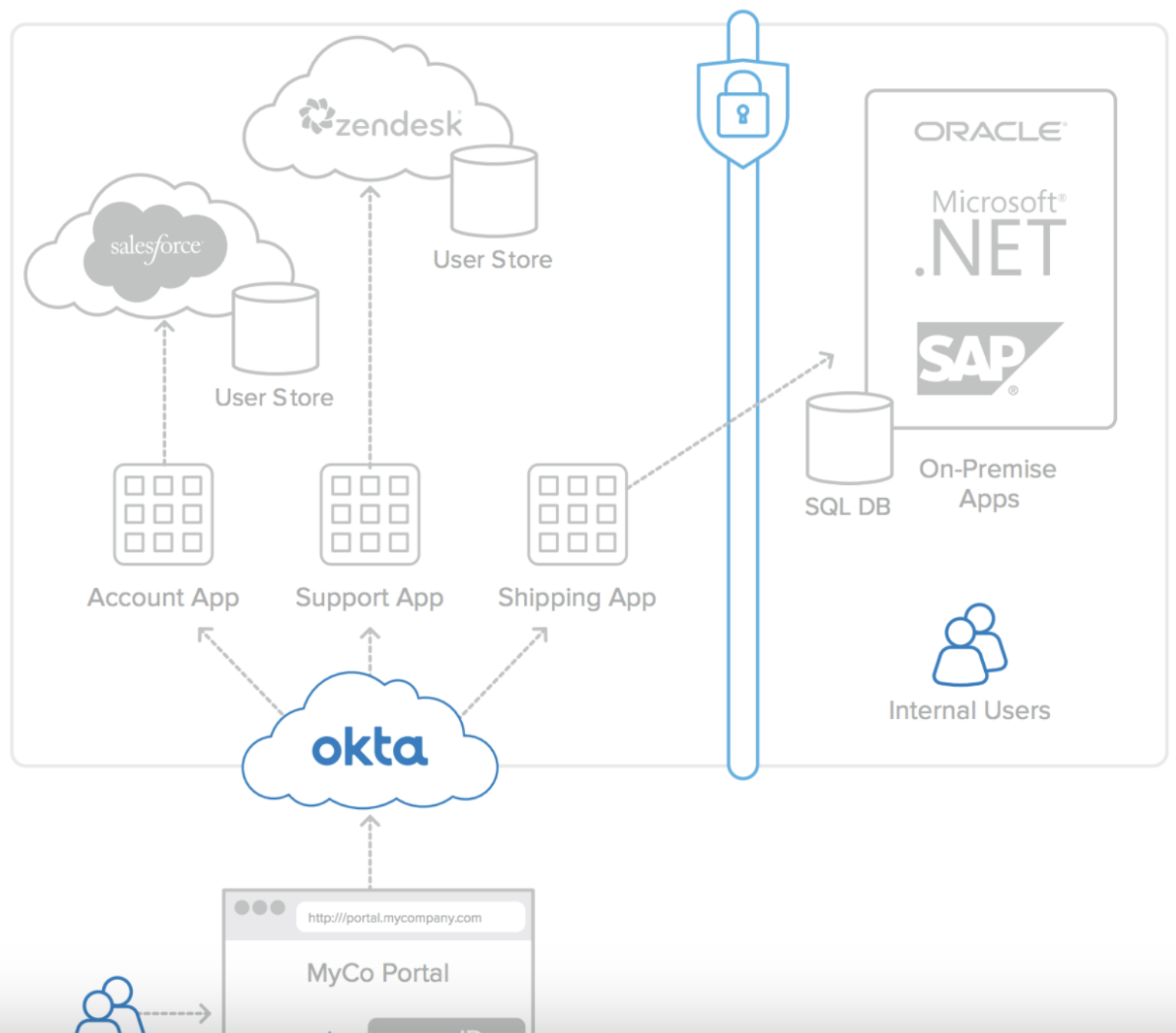
Auth0 Platform

Built to tackle both Consumer and SaaS Apps across every industry. Authenticate, authorize, and secure access for applications, devices, and users.

Internet

Firewall

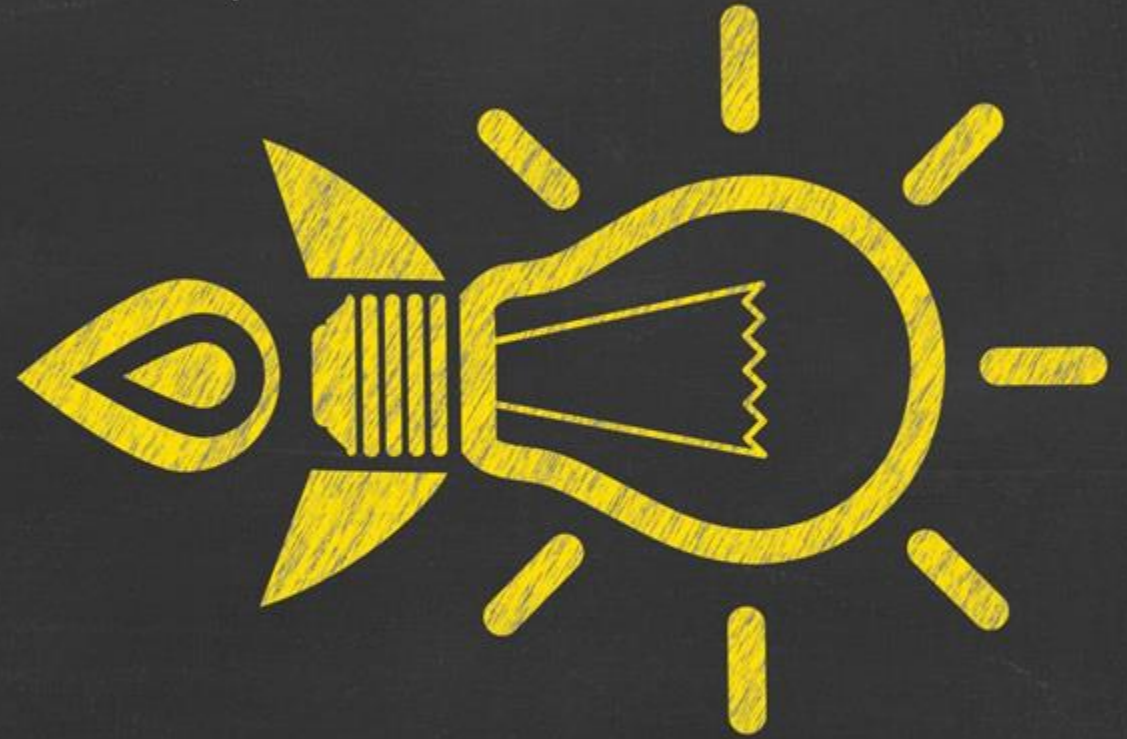
Your Network





10 min
BREAK
BACK
6:05PM ET

DATA ZERO TRUST



DATA

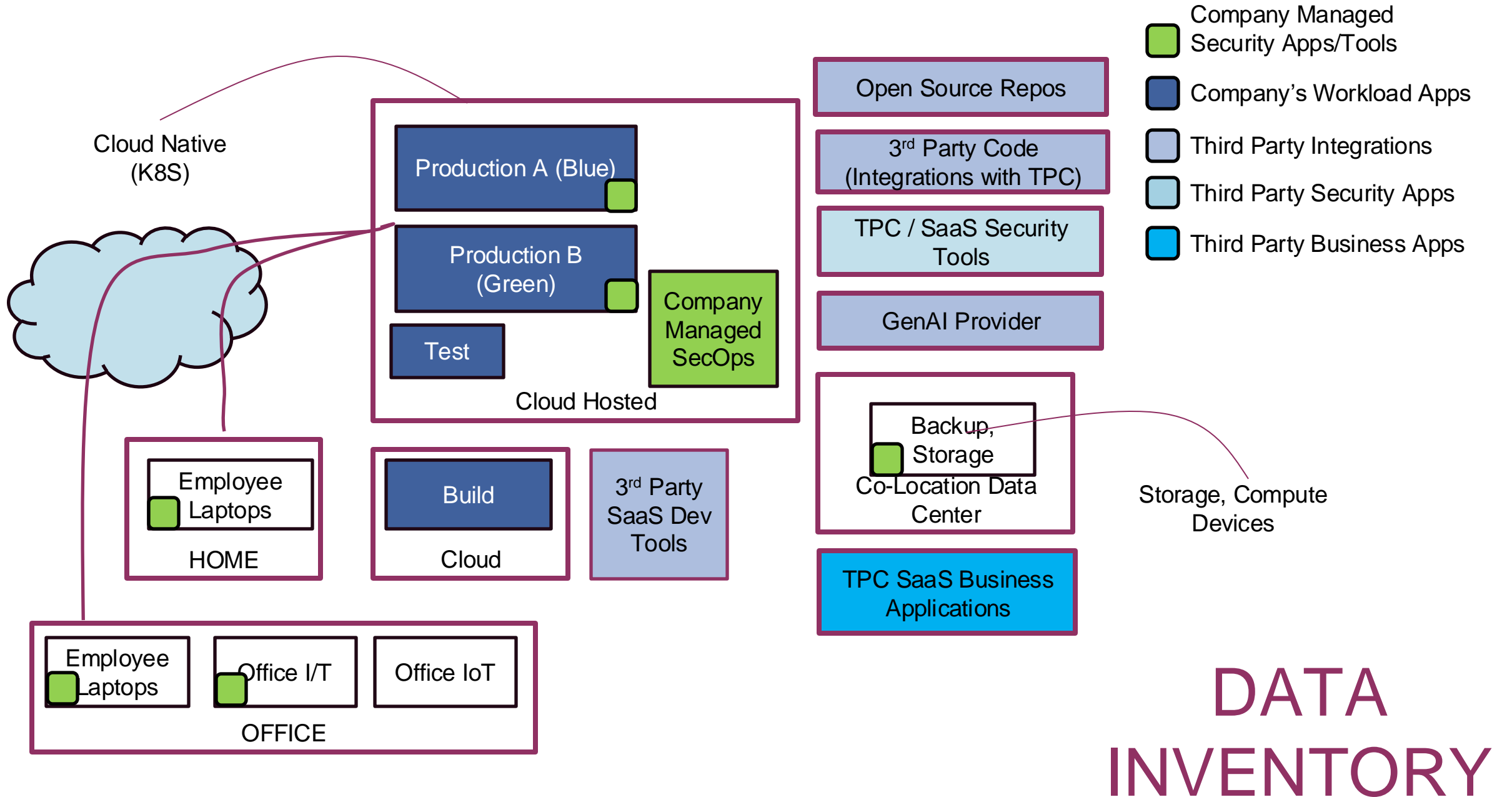
- Data protection is all about securing data that we manage (process) with the assumption that we have the right and requirement to process that data
- We often over-rotate to Privacy as the defining consideration for handling data
 - At the expense of our other data which may be neglected from a protection point of view
- BUT...

DATA PRIVACY: (GDPR) PRINCIPLES

- Section 1: Transparency and modalities
 - Data subject has right to have processing of their data described in a concise, transparent, intelligible form, using clear and plain language
- Section 2: Information and access to personal data
 - Data subject must be provided with clear information about collection of their personal data
 - Data subject shall have the right to be told if and which personal data concerning them is being processed
- Section 3: Rectification and erasure
 - Data subject has right to correct their personal data (eg update address)
 - Data subject has right to have all of their personal data be “erased” (Deleted) so that the subject is “forgotten”
 - Data subject has right to limit how their personal data can be used
 - Data subject has right to be TOLD they can have their personal data be rectified/erased
 - Data subject has right to download/move their data from one controller to another (eg porting cell phone numbers)
- Section 4: Right to object and automated individual decision-making
 - Data subject can object to processing of their data (causing controller to stop processing, such as stop marketing to data subject)
 - Data subject has right to not have decisions based through automated processing (eg programs – including AI – cannot make decisions such as eligibility for a loan)

DATA INVENTORY MANAGEMENT ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency manually identifies and inventories some agency data (e.g., mission critical data).	Agency begins to automate data inventory processes for both on-premises and in cloud environments , covering most agency data, and begins to incorporate protections against data loss.	Agency automates data inventory and tracking enterprise-wide , covering all applicable agency data, with data loss prevention strategies based upon static attributes and/or labels.	Agency continuously inventories all applicable agency data and employs robust data loss prevention strategies that dynamically block suspected data exfiltration.



CLASS (RHETORICAL FOR NOW) QUESTION:

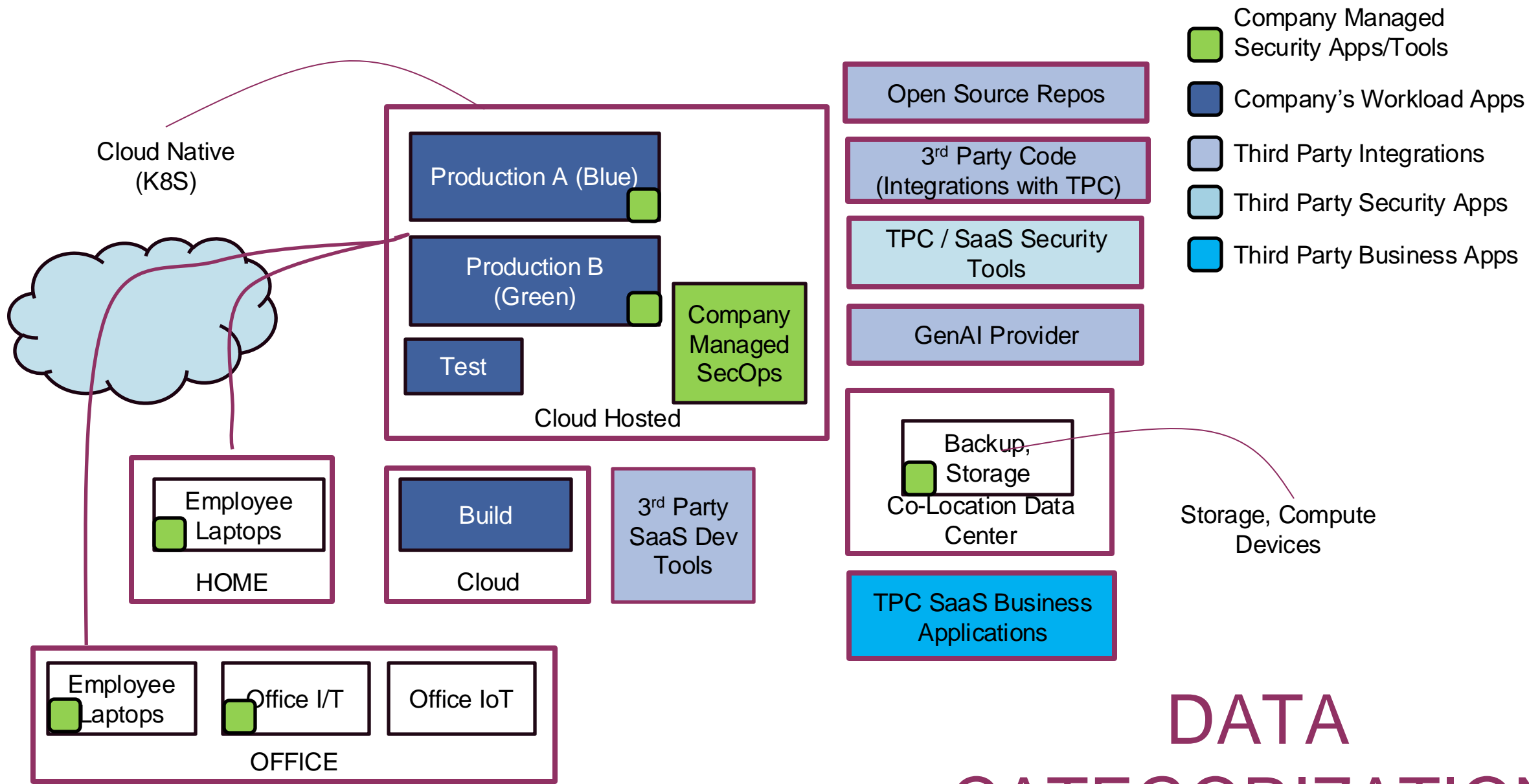


QQ?

- *(Starting here as Data Inventory ZTM introduces DLP)*
- *How do we consider “our” data that may be stored / processed by third parties?*
 - *How do we know what they are doing with our data?*
- *Is using your data to train a neural net/GenAI environment a form of data loss?*
 - *If your data is used to train, it helps set the model weights that govern future analysis and output from that model*

DATA CATEGORIZATION ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency employs limited and ad hoc data categorization capabilities.	Agency begins to implement a data categorization strategy with defined labels and manual enforcement mechanisms.	Agency automates some data categorization and labeling processes in a consistent, tiered, targeted manner with simple, structured formats and regular review.	Agency automates data categorization and labeling enterprise-wide with robust techniques; granular, structured formats; and mechanisms to address all data types.



DATA CATEGORIZATION

CLASS (RHETORICAL FOR NOW) QUESTION:

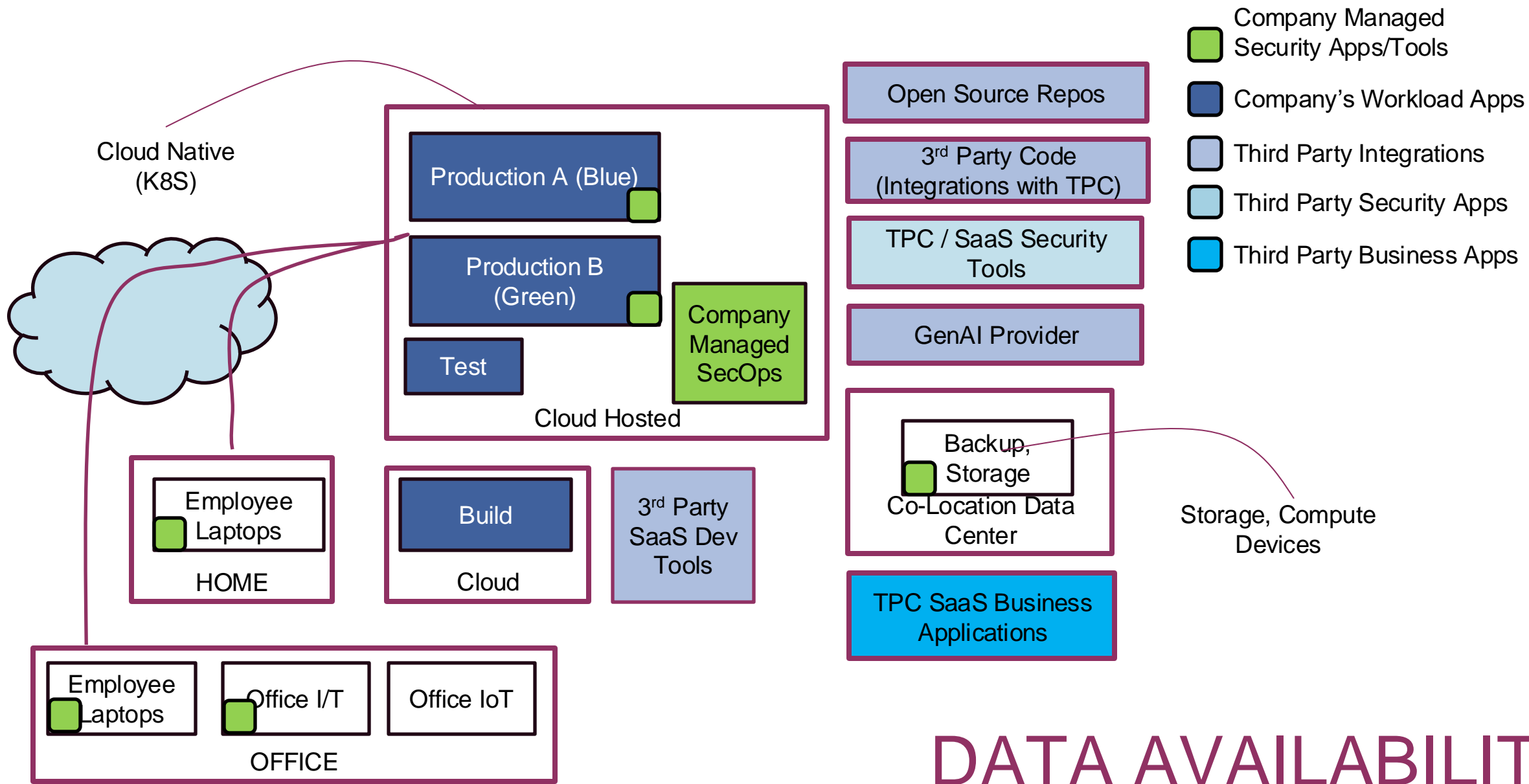


QQ?

- *(Continuing given Data Categorization ZTM)*
- *Should we keep an “inventory” of all data that has been provided to third parties and mark it as such?*
- *Is using your data was used to train a neural net/GenAI environment, should it be categorized as such?*
 - *If your data is used to train, it helps set the model weights that govern future analysis and output from that model*

DATA AVAILABILITY ZERO TRUST MATURITY

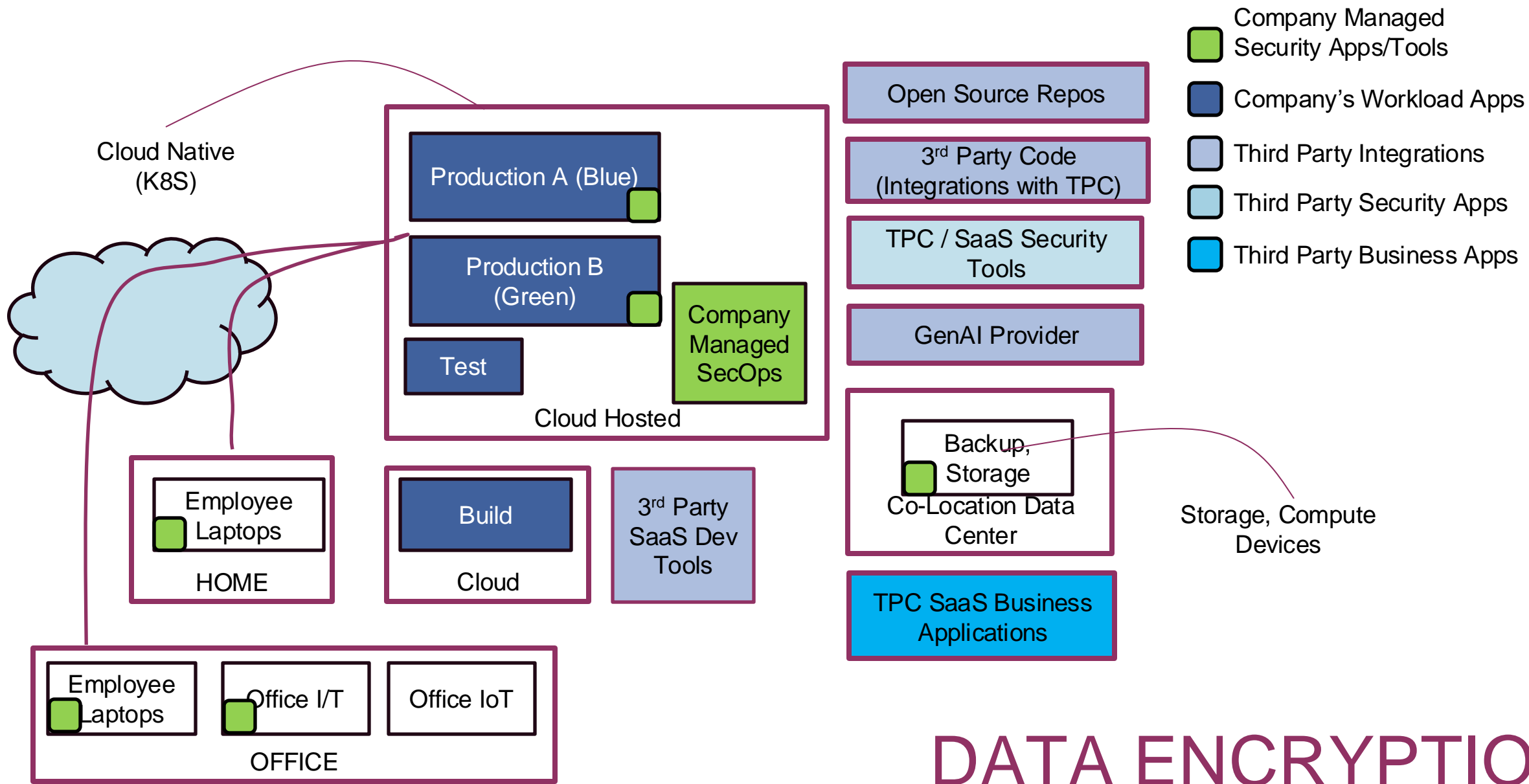
TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency primarily makes data available from on-premises data stores with some off-site backups.	Agency makes some data available from redundant, highly available data stores (e.g., cloud) and maintains off-site backups for on- premises data.	.Agency primarily makes data available from redundant, highly available data stores and ensures access to historical data.	Agency uses dynamic methods to optimize data availability , including historical data, according to user and entity need.



DATA AVAILABILITY

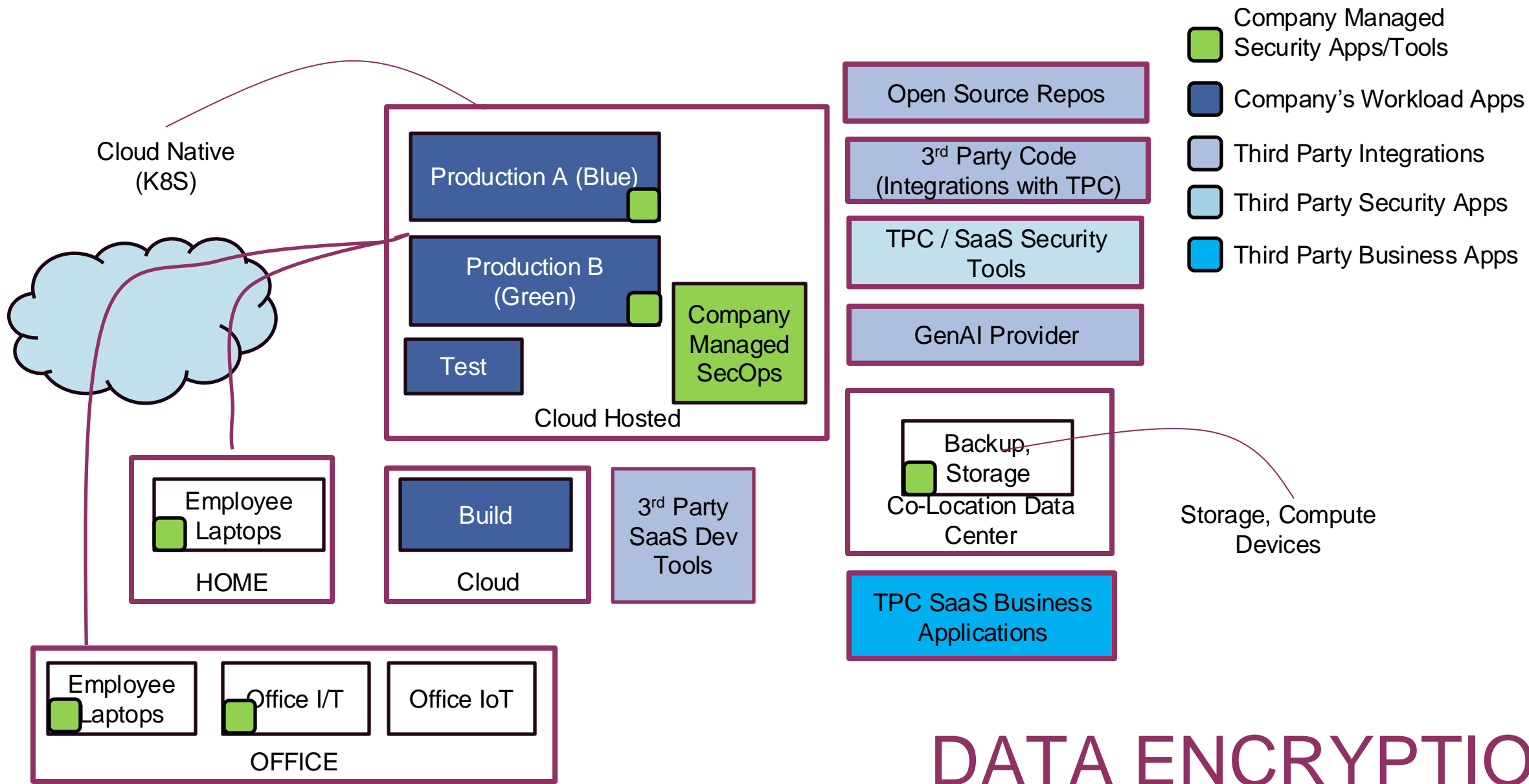
DATA ENCRYPTION ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency encrypts minimal agency data at rest and in transit and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency encrypts all data in transit and, where feasible, data at rest (e.g., mission critical data and data stored in external environments) and begins to formalize key management policies and secure encryption keys	Agency encrypts all data at rest and in transit across the enterprise to the maximum extent possible, begins to incorporate cryptographic agility , and protects encryption keys (i.e., secrets are not hard coded and are rotated	Agency encrypts data in use where appropriate, enforces least privilege principles for secure key management enterprise-wide, and applies encryption using up-to-date standards and cryptographic agility to the extent possible



DATA ACCESS ZERO TRUST MATURITY

TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
Agency governs user and entity access (e.g., permissions to read, write, copy, grant others access, etc.) to data through static access controls .	Agency begins to deploy automated data access controls that incorporate elements of least privilege across the enterprise.	Agency automates data access controls that consider various attributes such as identity, device risk, application, data category, etc., and are time limited where applicable.	Agency automates dynamic just-in-time and just-enough data access controls enterprise-wide with continuous review of permissions.



	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
DATA Visibility and Analytics Capability	Agency has limited visibility into data including location, access, and usage, with analysis consisting primarily of manual processes.	Agency obtains visibility based on data inventory management, categorization, encryption, and access attempts, with some automated analysis and correlation.	Agency maintains data visibility in a more comprehensive, enterprise-wide manner with automated analysis and correlation and begins to employ predictive analytics.	Agency has visibility across the full data lifecycle with robust analytics, including predictive analytics, that support comprehensive views of agency data and continuous security posture assessment.
Automation and Orchestration Capability	Agency implements data lifecycle and security policies (e.g., access, usage, storage, encryption, configurations, protections, backups, categorization, sanitization) through manual, and potentially ad hoc, processes.	Agency uses some automated processes to implement data lifecycle and security policies.	Agency implements data lifecycle and security policies primarily through automated methods for most agency data in a consistent, tiered, targeted manner across the enterprise.	Agency automates, to the maximum extent possible, data lifecycles and security policies for all agency data across the enterprise.
Governance Capability	Agency relies on ad hoc data governance policies (e.g., for protection, categorization, access, inventorying, storage, recovery, removal, etc.) with manual implementation.	Agency defines high-level data governance policies and relies primarily on manual, segmented implementation.	Agency begins integration of data lifecycle policy enforcement across the enterprise, enabling more unified definitions for data governance policies.	Agency data lifecycle policies are unified to the maximum extent possible and dynamically enforced across the enterprise.



ANTICIPATED END OF LECTURE 9



DATA INVENTORY & CATEGORIZATION

- Used to build understanding of what we have, what we need to protect, how to protect, etc
- Data inventory (neither ZTM or other) considers information that results from the aggregation of data
 - Is this a problem?
- Data categorization and tagging are a critical aspect of a privacy-informed data protection discipline
 - Categorization / sensitivity of data informs how we store it, who can read/write to it, when we delete it
 - For PII/SPI, we also need to report on how we used it, including if any "automated decisions" have been made on the basis of my data
- With data being used as part of generative AI solutions,
 - Should we explicitly tag/categorize data that has been used as part of genAI investigations?

SOME BENEFITS OF GENAI WITH DATA (from genAI)

1. **Data Quality Improvement:** Generative AI can assist in identifying data quality issues by generating reports or alerts about anomalies, inconsistencies, or missing entries, enabling proactive data cleansing and validation.
2. **Pattern Recognition and Anomaly Detection:** By analyzing large datasets, generative AI can identify patterns and detect anomalies that may not be immediately obvious, helping organizations understand data relationships and trends.
3. **Natural Language Queries:** Generative AI can empower users to interact with the data inventory using natural language queries, allowing non-technical stakeholders to easily access and understand the data without requiring complex query languages.
4. **Data Summarization:** Generative AI can summarize large datasets, producing insights and key findings, which helps stakeholders quickly grasp essential information without sifting through extensive data.
5. **Dynamic Updates:** With AI, your data inventory can be dynamically updated based on usage patterns and changes in data sources, ensuring that the inventory remains accurate and reflective of current data assets.

DYNAMIC UPDATES : MORE....

1. **Automated Monitoring:** AI can continuously monitor data sources, such as databases or data lakes, for changes or updates. By tracking these alterations in real-time, the data inventory can be maintained without manual intervention.
2. **Change Detection:** AI algorithms can detect changes in data patterns, structure, or volume. When significant alterations occur, the system can trigger updates in the data inventory to ensure that the information remains accurate and relevant.
3. **Classification and Tagging:** As new data is generated, AI can automatically categorize and tag this data based on its content and context. This helps in maintaining an organized inventory and adjusting it according to new entries or datasets.
4. **Integration with Other Systems:** AI can facilitate the integration of disparate data sources, ensuring that when data is updated in one system, it gets reflected across others. This helps maintain consistency and accuracy in the data inventory.

CASE STUDY (SIMILAR TO CAPSTONE ENVIRONMENT)

- For the purposes of “case study” for this course, we are going to consider third-party SaaS business apps including
 - Slack (discuss sales, customers, churn, success stories, etc)
 - (Salesforce) Databases (CRM typically used to manage sales leads, pipeline, client sentiment/churn)
 - Internal Web - eg Confluence (Battlecards, Customer Success Stories)
 - ”Gong” (Record and pull intelligence from customer meetings/recordings)
 - Workday (HR system)

CASE STUDY : INITIAL ZERO TRUST CHARACTERISTICS

NETWORK

- Network Segmentation (through SaaS based applications)
- Network Encryption (presumed based on SaaS best practices)

DEVICES

- Resource Access (limited for BYOD Mobile Device, no info on Laptop)

APPLICATIONS

- Application Access (local authorization, static attributes)
- Application Threat Protections (logging good enough to support investigation)
- Accessible Application (SaaS apps open public networks to authorized users and devices,)

DATA

- Data Access (data access controls that incorporate elements of least privilege across the enterprise)
- Data Encryption (presumed in place based on SaaS characteristics)

IDENTITY

- Risk Assessments (has identity been compromised)
- Access Management (“permanent access” with period review of access)

IDENTITY

- REFERENCE SO THAT WE CAN CONSIDER DURING CASE STUDY
- Identity Authentication
 - Covers username, passwords, moving to continually validated identity phishing resistant MFA
- Identity Stores
 - Covers identity stores, moving from self-managed and on-prem to identity stores integrated across all partners and environments as appropriate
- Identity Risk Assessment
 - Move from “trust” that identity not compromised identity to automated analysis and dynamic rules to inform access decisions to continuous analysis and dynamic rules to identity/prevent identity compromise
- Access Management
 - Permanent access with periodic review for both privileged and unprivileged accounts to automation to just-in-time authorization and just-enough access tailored to individual actions and individual resource needs.

APPLICATIONS.& WORKLOADS V IDENTITIES

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)

An identity refers to an attribute or set of attributes that uniquely describes an agency user or entity, including non-person entities.

This includes people using resources and assets and their associated identities, including customers (using the applications/services your company provides) and the employees of your company.

This also includes all of the “tokens” or “Non-Human Identities” that are used to authenticate between servers (eg mutually authenticated TLS) and to authenticate on behalf of a human (eg OAuth for SSO)

