VIRGINIA
IT AGENCY

WELCOME TO THE

DEC. 1, 2021

ISOAG MEETING

VIRGINIA IT AGENCY

AGENDA

- WELCOME/INTRODUCTION: MIKE WATSON
- DOUGLAS STREIT, ODU
- STEVE AIELLO & TIM GAWNE, AHEAD
- PATRICK ROBINSON & BINDU SUNDARESAN, ATT
- STEVE COLLE, ARI FRIEDMAN & ALYSSA CONTEREAS, NTTDATA
- UPCOMING EVENTS
- ADJOURN

OLD DOMINION UNIVERSITY

The Four Legs of the Enterprise Security Table

Doug Streit

CISO, Old Dominion University

VITA ISOAG Meeting

December 1, 2021

The Four Legs of the Enterprise Security Table

I've come to the conclusion that if you give a data point to a company, they will eventually sell it, leak it, lose it or get hacked and relieved of it. There really don't seem to be any exceptions, and it gets depressing.

- Brian Krebs

Understand what data you hold, how you are using it, and make sure that you are practicing good data hygiene.

- David Mount

The Four Legs of the Enterprise Security Table

There's no silver bullet solution with cybersecurity, a layered defense is the only viable defense.

- James Scott

The Four Legs of the Enterprise Security Table

- **Incident Management (IM) vs. Incident Response (IR)**
  - Data & System Breach Management Framework
  - IT Security Incident Handling Standard
  - Incident Handling Procedure

- CISO fills a key role in IM and IR

- We have levels of severity for incidents
  - Incident Response (IR) handled by our security team
  - IR handled by Sec Team, & raise the awareness of our CIO
  - The formation of an Incident Management (IM) Team

The Four Legs of the Enterprise Security Table

- **The IM team**
  - System Owner
  - Regulated Data Owner(s)
  - Risk Management
  - University Counsel
  - Others as warranted – CIO, VP Admin & Finance, Strategic Communication, Emergency Management Office

The Four Legs of the Enterprise Security Table

- **Security Team Support**
  - Support the department
  - Assess and make decisions
- **Department IR –**
  - Discovery, eradication, recovery
- **ITS provided Network, Server, IDM, and Security SME support**
  - CISO led IM
    - Coordinator, facilitator, and reporter
    - Interface – IM Team, IR Team, in-house and 3rd party stakeholders and support teams

The Four Legs of the Enterprise Security Table

- **Forensics & Recovery**
  - **Recovery:**
    - In-House
    - DR Plan that is tested
    - HA design, backups, documentation
    - Structure in place to mobilize and recover
  - **Forensics:**
    - Some in-house, small scope capability
    - In-house initial assessment and determination of scope
    - Large-scale, domain compromise, requires external support

The Four Legs of the Enterprise Security Table

- **The four tools that proved to be instrumental:**
  - Firewalls
  - SIEM
  - Endpoint and EDR
  - 2FA

The Four Legs of the Enterprise Security Table

1. Firewall (segmentation & visibility)

- **Segmentation based on risk**
  - Lower risk academic / research environments
  - Higher risk administrative / regulated data environments

- **If we cannot validate the security practices, isolate:**
  - Academic, research environments
  - Affiliates that maintain their own IT
  - 3rd party businesses
  - Isolate based on the risks to the institution

The Four Legs of the Enterprise Security Table

- **Firewall Lessons Learned**
  - Segmentation protected us
  - The forensic investigation was limited due to limited logging
  - Desktops on the same segments today can communicate to each other
    - In most cases there is no need to do so
    - **Note to self:** Restrict East-West communication on desktop networks wherever possible
    - Contain lateral movement when a desktop is compromised

The Four Legs of the Enterprise Security Table

2. SIEM (Security Incident & Event Monitoring)

- Goal is logging that can be managed
  - Such as check-summed
  - zipped
  - rotated
  - preserved for at least a year
- Provides data that becomes of great interest!

The Four Legs of the Enterprise Security Table

- **What to log?**
  - Application logs, key apps
  - Firewall network traffic
  - Authentication
  - Key workstations
- **Think possible attack scenarios**
  - What logs would we want after a compromise?
  - Develop a plan to collect those logs
  - Maintain them for an extended period of time

The Four Legs of the Enterprise Security Table

- **The SIEM could have detected**
  - Compromised accounts
  - A large file extraction
  - A series of less significant events
- Helped paint a picture of what happened
- **With indicators of compromise in our possession,**
  - SecOps searched attempts from IP addresses, accounts
  - The University SIEM provided a valuable threat hunting resource
  - Assurance was needed
    - No lateral movement to the campus
    - No expansion of the attack

The Four Legs of the Enterprise Security Table

- **SIEM Lessons Learned**
  - The first, most valuable tool after an incident is the SIEM
  - The University SIEM provided assurances that the attackers had not used the same addresses or accounts to attempt an attack on the main campus
  - The compromise could have been prevented by certain SIEM rules that could have detected suspicious account or network activity
  - **Note to self:** Review logging strategy and gaps, considering what we would want to know after an attack

The Four Legs of the Enterprise Security Table

3. Endpoint with EDR

- **The primary functions of an EDR:**
  - Monitor and collect activity data from endpoints that could indicate a threat
    - Analyze endpoint data to identify threat patterns
    - Automatic response for containment and notifications
    - Forensics and analysis tools to research threats and search for suspicious activities

The Four Legs of the Enterprise Security Table

- **3rd Party Forensic/Recovery Team**
  - Protocol for assurance during recovery:
    - The first question they asked, Do you have an EDR installed?
    - Their first action, Offer 30-days of EDR with 24x7 managed monitoring services
  - Gave us time to develop a plan

The Four Legs of the Enterprise Security Table

- **Endpoint / EDR Lessons Learned**
  - EDR provides visibility across the endpoints
    - Mixed with an advanced firewall and SIEM provide layers of defensive monitoring and visibility and logging
  - Alerts should be enabled
  - Active blocking should be enabled

  - **Note to self:** The cost of EDR in terms of management and assurance of the endpoints is worth the investment

The Four Legs of the Enterprise Security Table

4. MFA (multi-factor authentication)

- The use of MFA with a VPN that restricts internet access to only what is essential to face the internet.

- Departmental Accounts
  - Independent of the University IAM infrastructure
  - Agility in support of instruction and research

The Four Legs of the Enterprise Security Table

- **As part of recovery,**
  - The department worked with the central identity team
    - Provided tools to create new accounts for their users
  - New accounts tied to University identities
  - All Faculty, staff and student accounts enabled for 2FA
  - VPN configured for 2FA
  - All staff accounts were required to use VPN

The Four Legs of the Enterprise Security Table

- **2FA Lessons Learned**
- The University:
  - 2FA and VPN
  - Restricting internet SSH and RDP
  - Privileged account access: VPN with 2FA / profiling
  - Account event logging and monitoring

The Four Legs of the Enterprise Security Table

- **Final Thoughts…**
  - DLP program
  - Records Management program
  - Risk Management Program
  - Vulnerability Management Program
  - Cloud Security (AWS, Office365, AzureAD)
  - Cyber Insurance

The Four Legs of the Enterprise Security Table

- **The four tools that proved to be instrumental:**
  - Firewalls
  - SIEM
  - Endpoint and EDR
  - 2FA

OLD DOMINION UNIVERSITY

The Four Legs of the Enterprise Security Table

Doug Streit

CISO, Old Dominion University

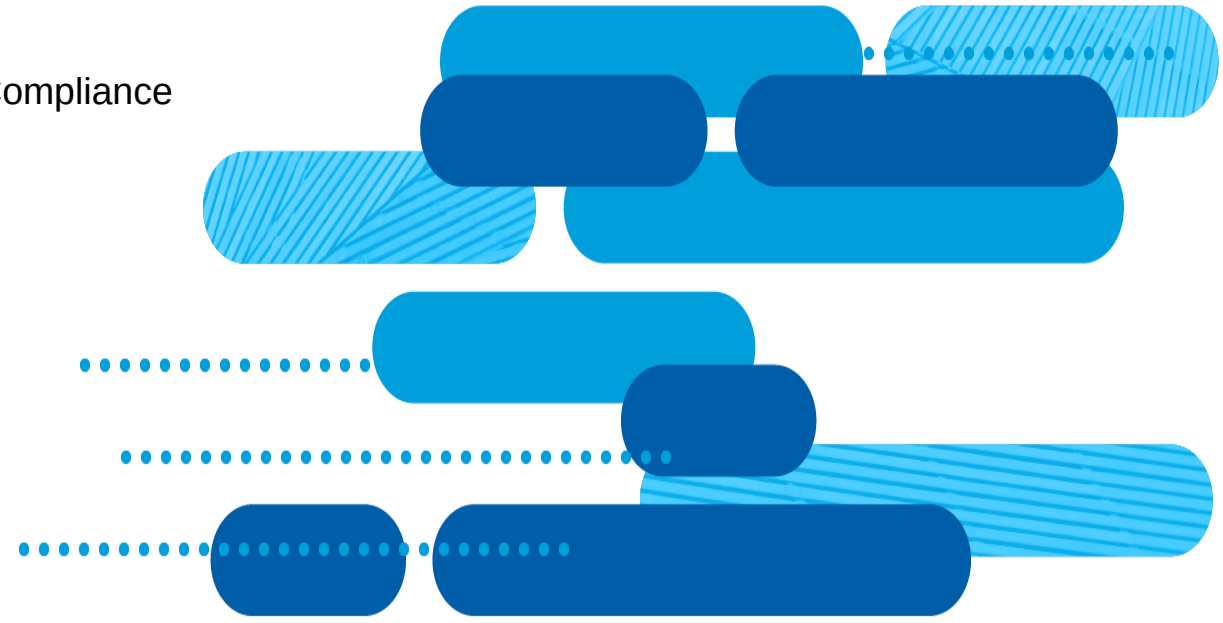
VITA ISOAG Meeting

December 1, 2021

AHEAD

Ransomware, Highlighting Security Imperfections

Steven Aiello
Delivery Director Security & Compliance



AHEAD's Security Philosophy

"Security is a process, not a product"…

- The security industry has been overly focused on products.

Align security controls to proven threat actions

- Data clearly articulates the top TTPs that occur in over 99% of data breaches.

Build a program consisting of quality security processes

- There has been little focus on quality of outcomes in the security industry. Why do companies constantly pass audits, and constantly fail penetration tests?

Ransomware

“Ransomware is a type of malware from crypto-virology that threatens to publish the victim's personal data or **perpetually block** access to it unless a ransom
is paid.”

This is not “new” but is a new focus of attackers, it is not “novel”… All previous controls are applicable to protecting against ransomware.

AHEAD

CYBER RECOVERY & NIST CSF FUNCTIONS

The traditional NIST CSF functions help build a defense in depth model against ransomware. What ransomware has done is expose the flaws in security programs that weren't previously visible.

AHEAD

AHEAD

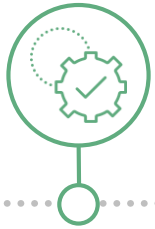
Ransomware Attack Lifecycle

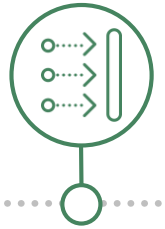
Understanding Ransomware Tactics Techniques & Procedures

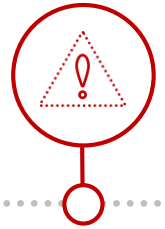
Negative Outcomes Still Preventable

Attack Successful

Impact Determined







Initial Access

1. Email Phishing
2. Exposed Vulnerable Application

Attack Propagation

1. Installation of Command and Control and Persistence
2. Capture Credentials (Steal Passwords)
3. Lateral Movement
4. Authenticate to Systems & Data

Attacker Objectives

1. Ransomware Execution

Recovery

1. I.R. Processes
2. Data Recovery Protections
3. Data Recovery Processes
4. Data Recovery Technology

AHEAD

OBJECTIVE

DEFENSE IN DEPTH

1. Using the right set of preventative, detective, and recovery controls.

2. Mature the process around those controls so they are executed the same way every time.

3. Ensure those controls are applied to the right attacker tactics techniques and procedures.

TECHNICAL

ACCURACY

1. Attackers are targeting backups
2. Organizations are overly governance focused
3. Leverage something like the MITRE ATT&CK framework

PROCESS

MATURITY

1. Security controls must be mature and executed the same way every time
2. Attackers exploit weak processes to circumvent protective and detective controls.
3. Use the ISO 33004 process maturity standard to assess the maturity

AHEAD

How Mature are Your Security Processes?

Level Zero	Control not implemented*
Level One	Control implemented and produces: an artifact, a change in state, or meets a constraint
Level Two	Control has been documented, and reporting measures are in place to validate the process has been run and produces a measurable result
Level Three	Control and been documented, and results are tracked and improvements to the process has been run and produces a measurable result
Level Four	Optimized or Automation is used to execute the process and report upon result trends*

ISO 33004 is an international process maturity framework that AHEAD uses to assist customer in improving their security program processes.

AHEAD

Common Ransomware Attack Actions

Email Phishing

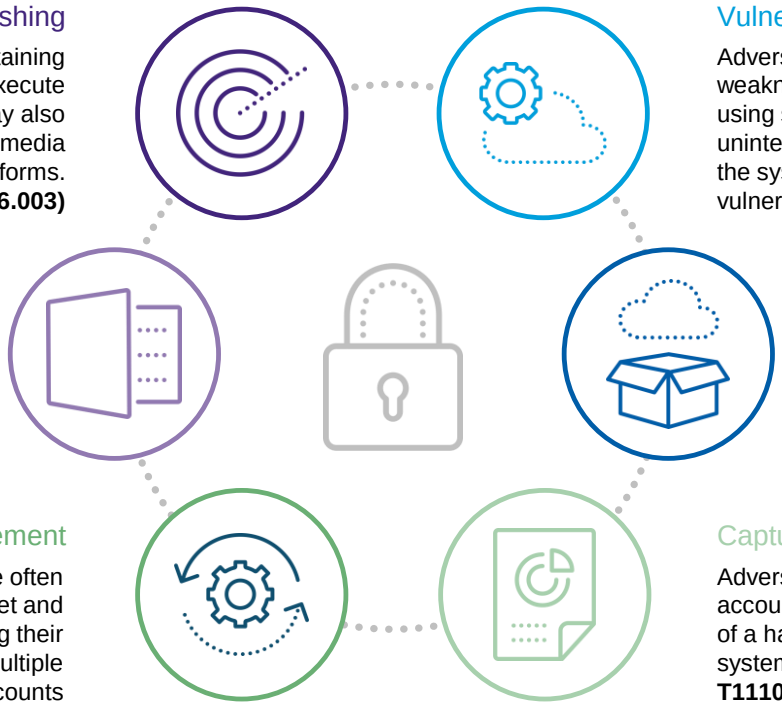
Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms.
(MITRE IDs: T1566.001, T1566.002, T1566.003)

Credentialed Access

Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.
(MITRE IDs: T1187, T1528, T1552)

Lateral Movement

Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts
(MITRE IDs: T1021.001, T1021.002, T1021.004, T1570)



Vulnerable Applications

Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. **(MITRE IDs: T1190, T1133, T1195)**

C2 & Persistence

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
(MITRE IDs: T1136.001, T1136.002, T1098.003)

Capture Credentials

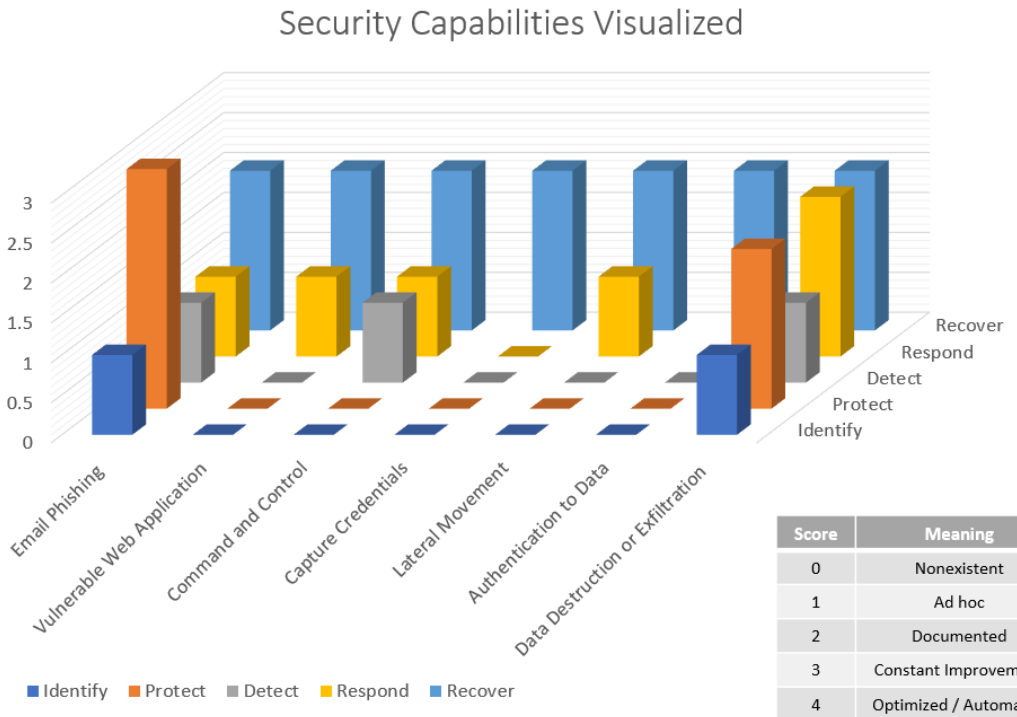
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. **(MITRE IDs: T1110.001, T1110.002, T1110.003, T1003)**

AHEAD

Defense in Depth Assessment

AHEAD cross references common TTPs with the NIST CSF functions to provide recommendations for process, tooling, and architecture. AHEAD will work with the organization to establish a current state risk posture.

AHEAD leverages in scope TTPs, NIST CSF functions, and evaluates process maturity via the ISO 33004 methodology scoring process maturity on a scale of 1 - 4



Score	Meaning
0	Nonexistent
1	Ad hoc
2	Documented
3	Constant Improvement
4	Optimized / Automated

AHEAD

Designing for Ransomware Recovery

RECOVERY

IS THE TARGET

Attackers are targeting backup environments specifically before launching their attacks. In a recent attack AHEAD helped an organization recover from, the attackers gained access to the backup admins calendar, waited for them to go on vacation, reformatted backup storage devices, and then launched their ransomware. The recovery effort took months…

RECOVERY

DESIGN CONSIDERATIONS

Distance

Unlike a natural disaster scenario, distance to the recover environment is no longer a critical factor when building a plan for recovery from ransomware.

Bottlenecks

Bottlenecks for cyber recovery change when compared to nature disaster planning. Usually, organizations were limited by network bandwidth. This is no longer the case, now disk throughput on recovery targets, backup appliance limitations have replaced WAN links as the bottleneck

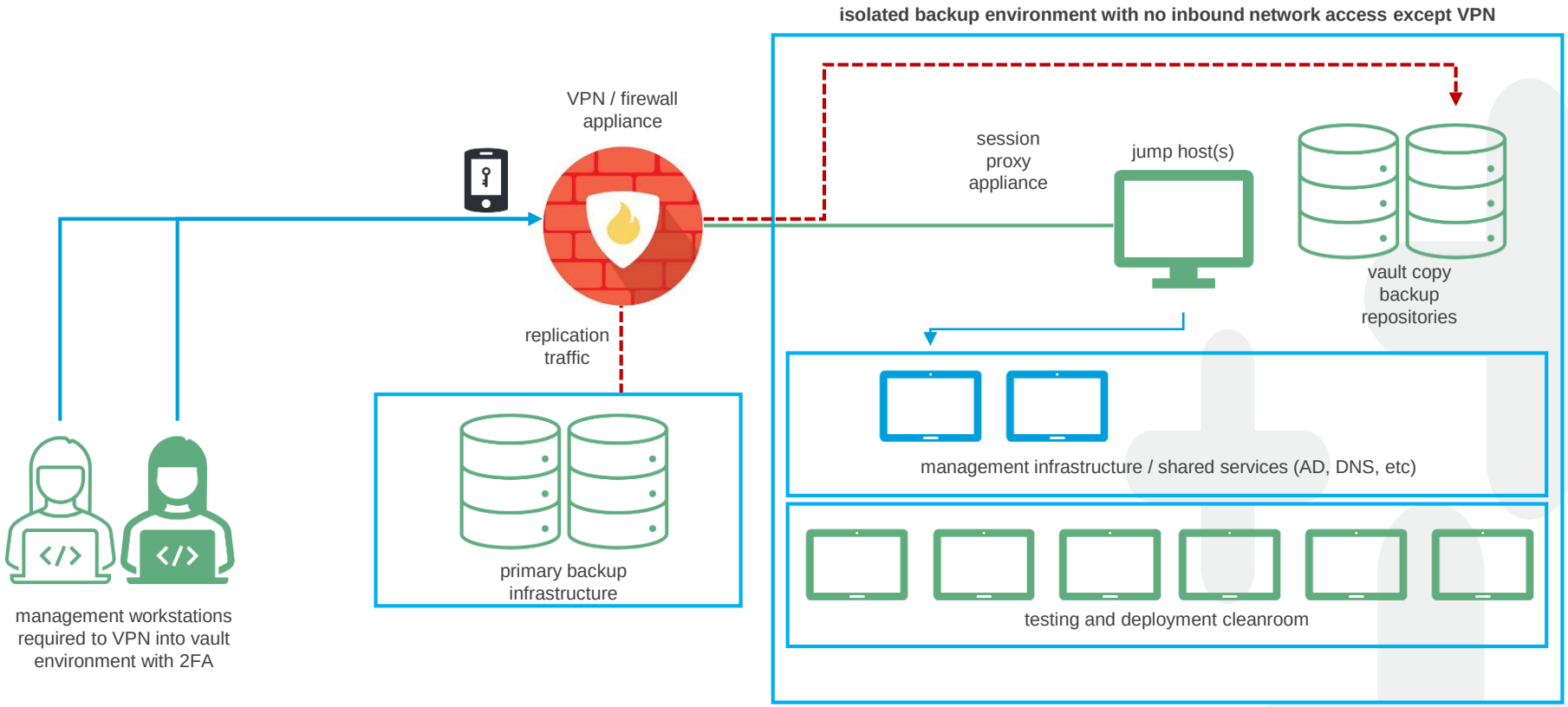
Access

Access and protecting the recovery infrastructure has become the single most important element of cyber recovery.

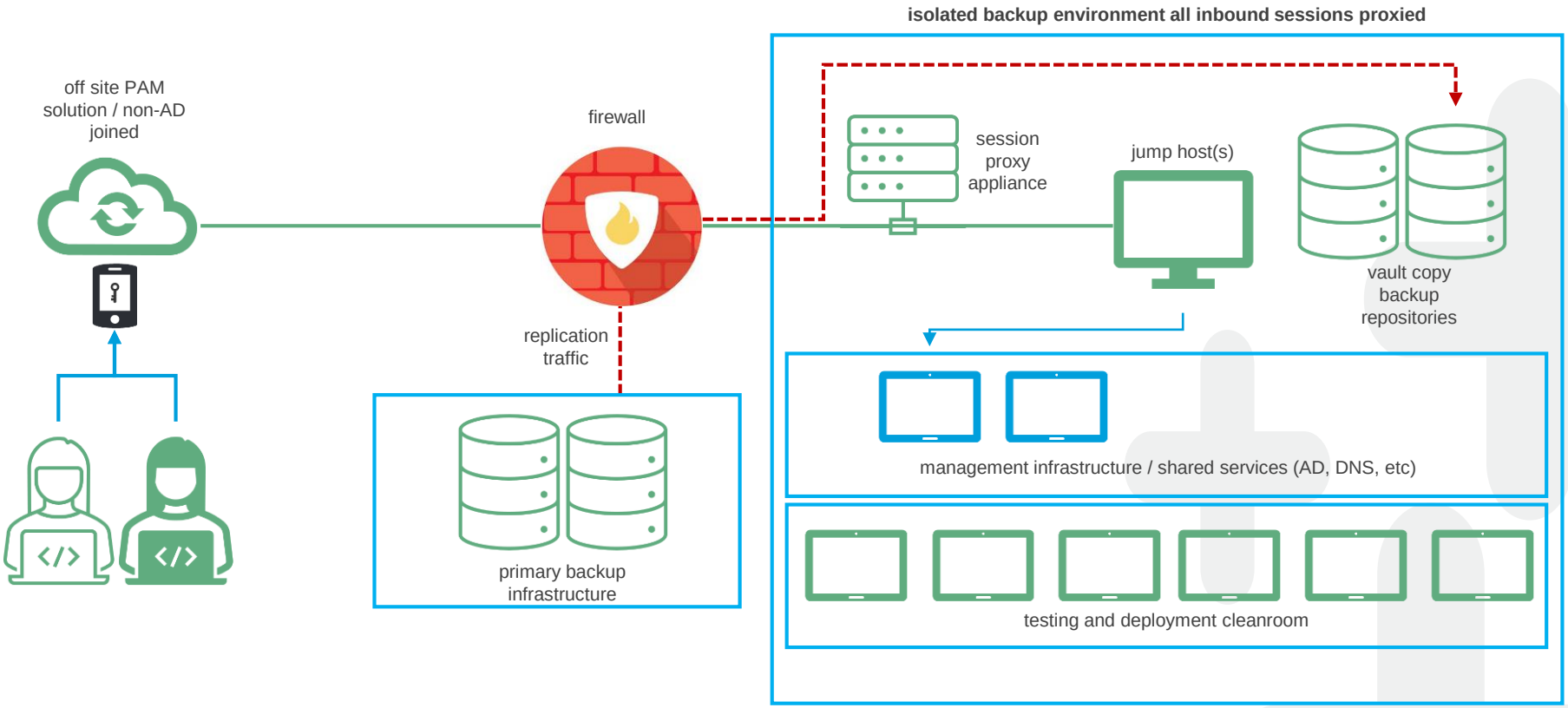
Monitoring and Management

A properly designed cyber recovery solution will likely need a scaled down but fully functioning infrastructure such as identity stores, DNS, monitoring, etc.

Prevention Cyber Recovery Architecture



Detect & Respond Cyber Recovery Architecture

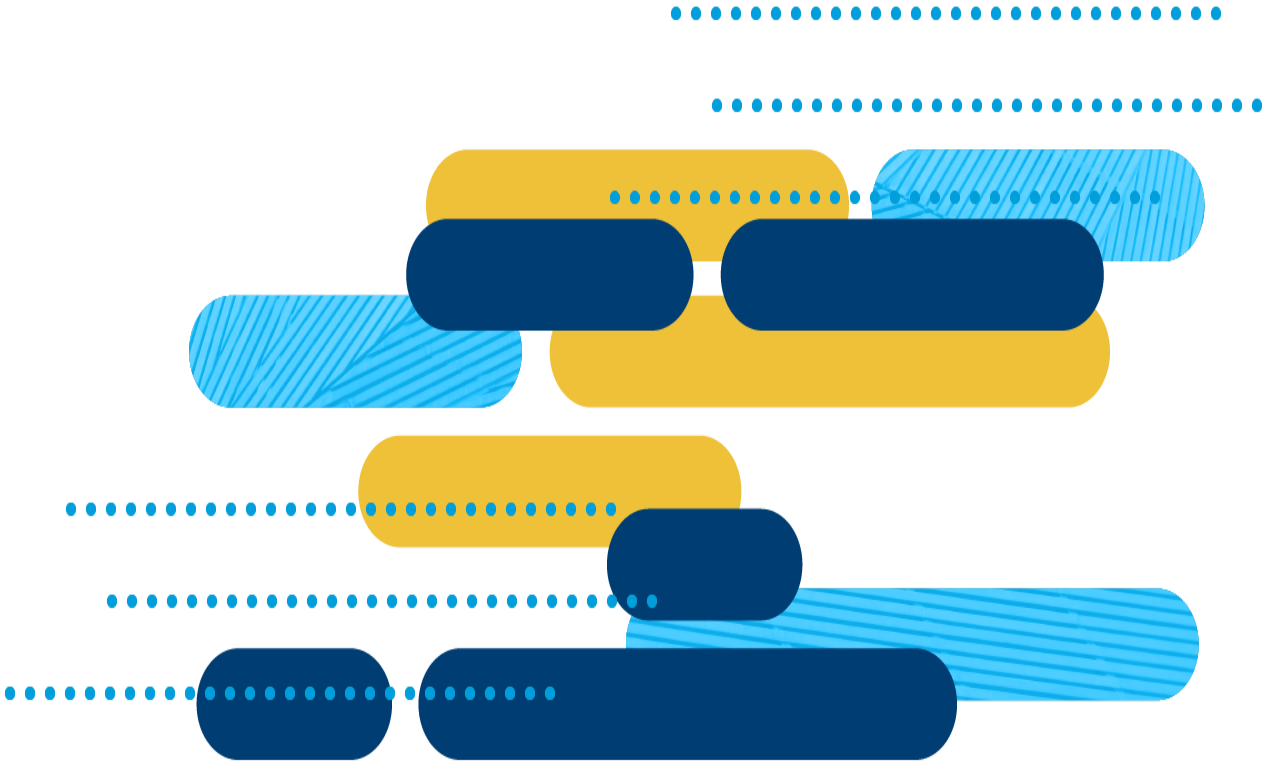


Questions?

AHEAD

Learn. Grow. Achieve.

thinkahead.com

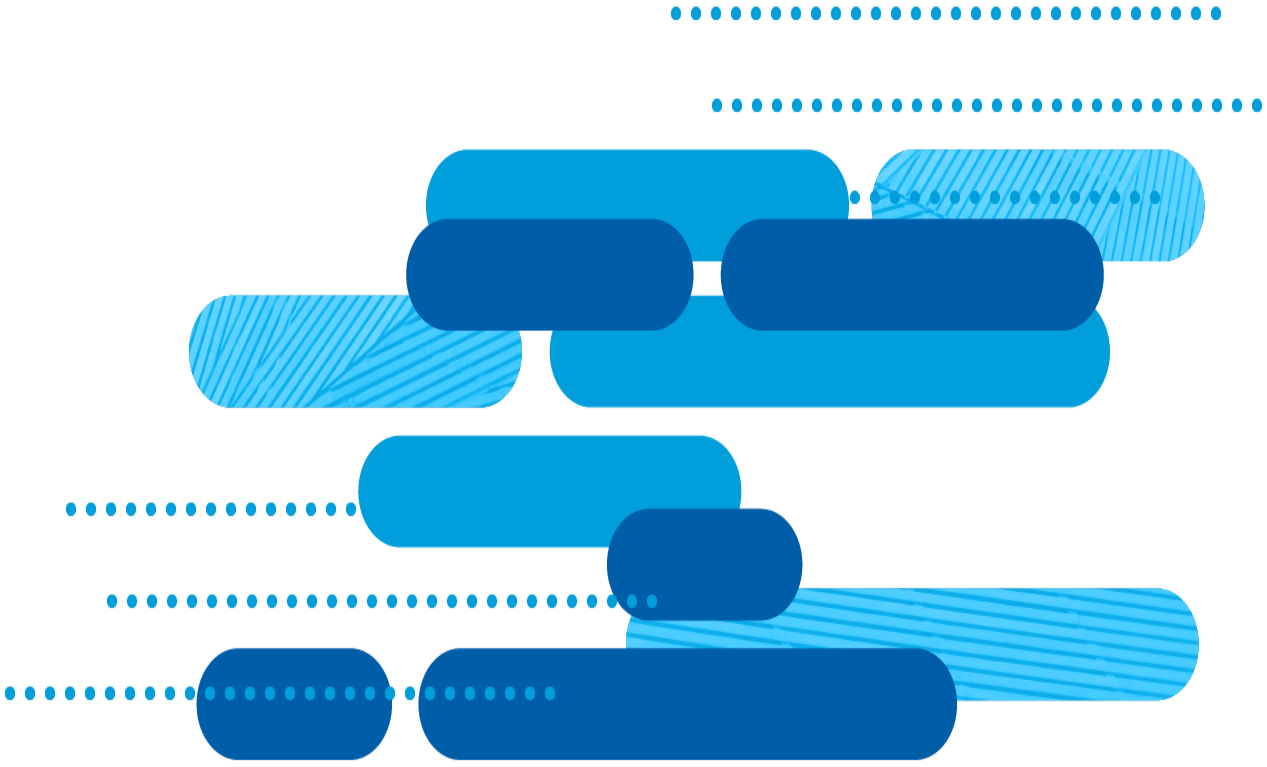


Thank You

AHEAD

Learn. Grow. Achieve.

thinkahead.com



To Zero Trust

A strategy to embrace Zero Trust as a Cybersecurity Concept

Bindu Sundaresan
Patrick Robinson

AT&T Business

Agenda

Introductions

- Director
- AT&T Cybersecurity Consulting

Bindu Sundaresan

- Associate Director
- Cybersecurity – Public Sector

Patrick Robinson

Zero Trust Start to Finish

1. **The "What"**

   Elaborate on the concept of Zero Trust

2. **The "Why"**

   What does Zero Trust Get You?

3. **The "How"**

   A working plan on how to move to Zero Trust

Zero Trust

Term coined by John Kindervag while working at Forrester Research in 2010

Zero Trust is centered on the belief that trust should be removed from packets – nothing outside or inside the perimeter is trusted.

Zero Trust Model

Enterprises that adopt Zero Trust leverage micro-segmentation and granular perimeter enforcement based on users, their locations and other data to determine whether to grant access to a particular part of the enterprise.

Once users, machines or applications are approved, pre-defined entitlements allow them to access what they need - and only what they need - for the task at hand.

Basic Principles of Zero Trust

- Network is always hostile
- Internal and external threats are always present
- Internal network is not sufficient to equal trusted
- Every device, user, and network flow must be proven
- Log and inspect all traffic

Zero Trust is Changing How Agencies Operate

- Ensure all data and resources are accessed securely, based on user and location.
- Adopt a least-privileged access strategy and strictly enforce access control.
- "Always verify," meaning inspect and log all traffic. Add more authentication methods to counter credential-based attacks.
- Never trust, always keep adding context and keep your roles up-to-date.
- Inspect everything

Organizations will need to incrementally implement Zero Trust principles, process changes and technology solutions to protect their data.

1: Source: Clarifying What Zero Trust Is – and Is Not – Palo Alto Networks Blog - https://blog.paloaltonetworks.com/2018/08/clarifying-zero-trust-not/
2: The Jericho Forum (2007) *Jericho Forum Commandments*, version 1.2. Available at https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf
3: Department of Defense Global Information Grid Architecture Vision Version 1.0 June 2007. http://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,%20June%2007.pdf

Clarifying what Zero Trust *is not*

Zero Trust is not standardized.

No single deployment plan was issued in NIST SP800-207 and no standard exists for policy enforcement or agent data.

Zero Trust is not quick and dirty.

Replacing a decades-old strategy and framework is not fast or easy.

Zero Trust is not solutioned.

Not achieved through any single technology, tool, or tech refresh.

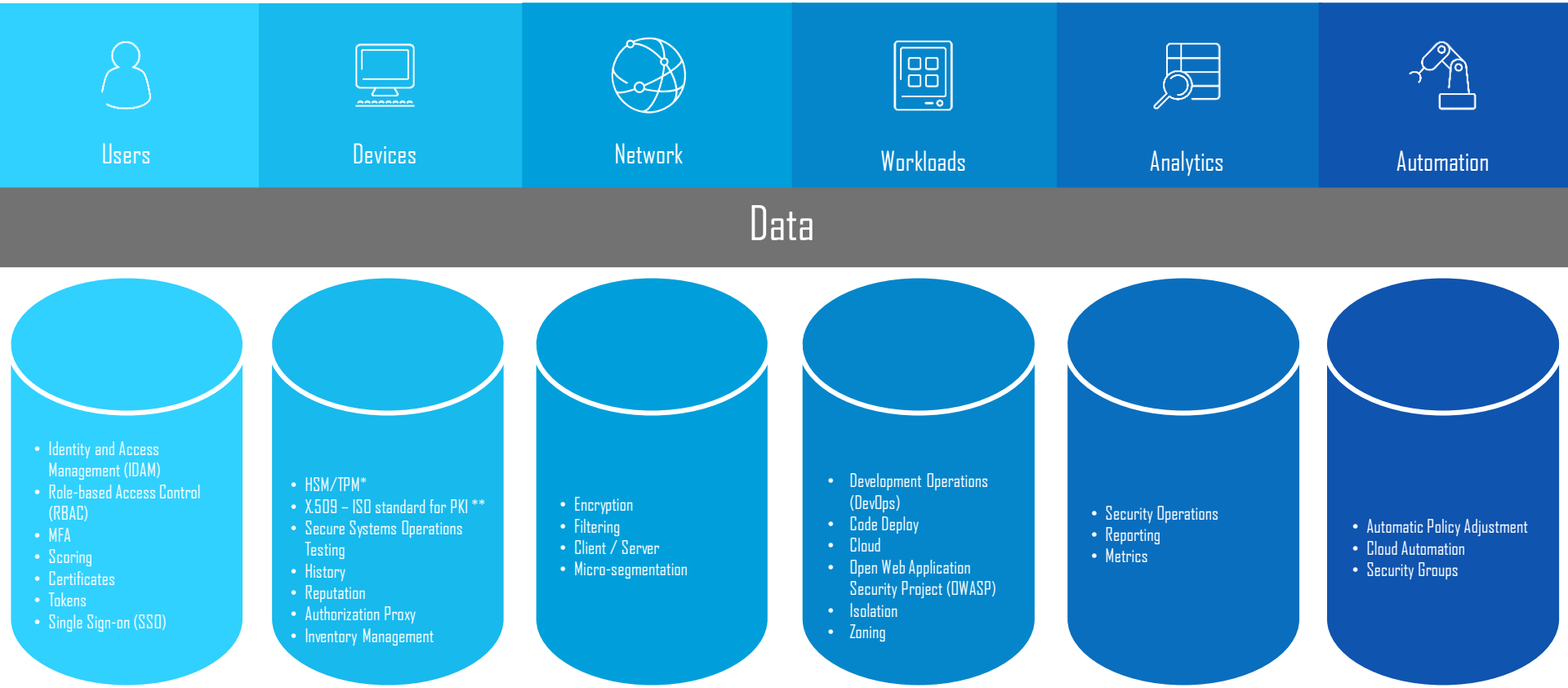
Zero Trust is not limited to IT and cybersecurity teams.

Multiple cross-functional stakeholders throughout the enterprise (internal and external) are affected.

Zero Trust is not cheap.

Implementation is a journey that can take years, considering each business process at a time.

Zero Trust Pillars

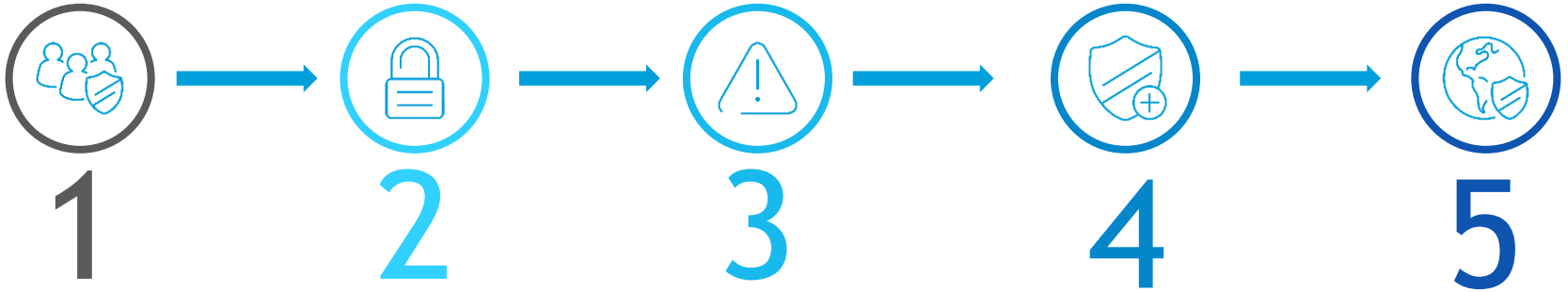


*HSM/TPM – Hardware Security Module/Trusted Platform Module
**X.509 – International Standards Organization (ISO) standard for Public Key Infrastructure (PKI)

Zero Trust Readiness Implementation

- Organizations will need to incrementally implement Zero Trust principles, process changes and technology solutions to protect their data.
- Many organizations already have elements of a Zero Trust architecture in place.

How to Achieve a Zero Trust Network



1 Define the protection surface

Cluster/classify sites, users, and assets by type, role, or location.

2 Follow the transaction flows

Who talks to whom, what, when, where, why, and how?

3 Establish policies to support the flows

Network, content, and authentication policies.

- Establish countermeasures.
- Define change processes.

4 Define the security architecture

Where will the countermeasures lie? Premises, network, edge, cloud, or hybrid?

5 Deploy, monitor, update

Deploy countermeasures. Continuously monitor and update.

Transitioning to Zero Trust is a journey, not accomplished with a complete replacement of technology.

Zero Trust Readiness Implementation

Zero Trust Readiness Implementation

- Designed for customers who need to evaluate their current state cybersecurity program and its maturity in moving to a Zero Trust Architecture
- Multiple stages of analysis, interviews, design and documented recommendations leading to a comprehensive strategy with priorities and milestones to get to Zero Trust

Discovery

Intensive workshop designed to minimize impact on client staff schedules by bringing all major parties to the table (IT, Development, Security, Operations, etc.) at the onset to discover and understand the environment.

Capabilities Assessment

Analysis of the present inventory gathered during the discovery workshop:

- Documentation, including data classification and handling
- Cybersecurity policies in effect: management abd governance, asset management, security organization, 3rd party management, change management, etc.
- Current network architecture and technologies
- Current state of technical security practices spanning access control, application security, Vuln/Patch Mgt, logging/monitoring, SOC, encryption/key management, DLP, etc.

Maturity Assessment

- Authentication/Authorization of Users and Devices
- Network Design, Authorization and Function
- Workload Security
- Intelligence and Analytics
- Automation and Orchestration

Strategy and Roadmap

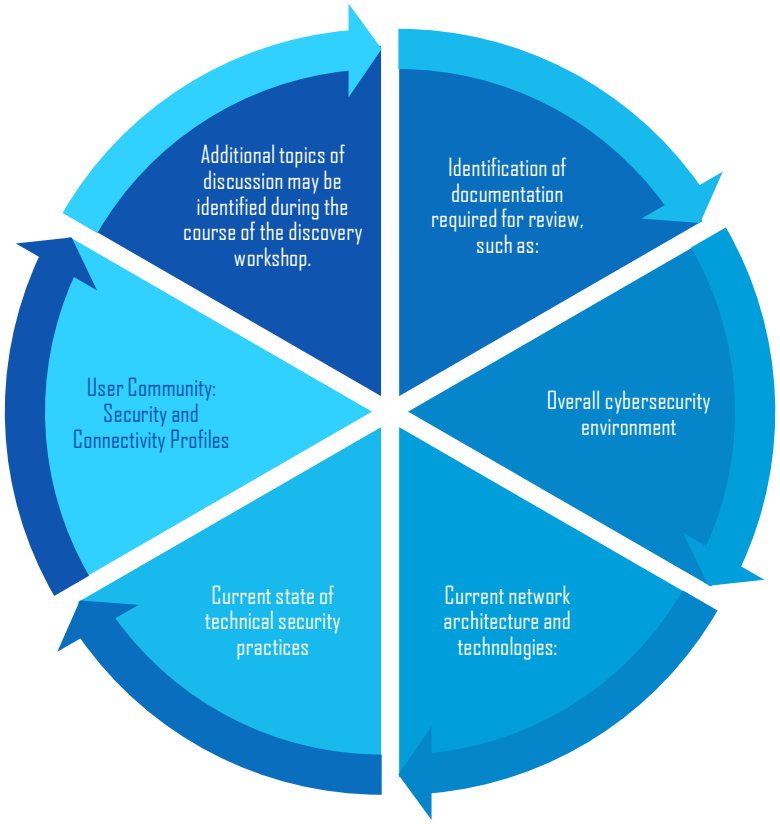
The determination of which of the five Maturity Rating categories applies will help to define the path forward.

To Zero Trust

A strategy to embrace Zero Trust as a Cybersecurity Concept from a financial standpoint

In this section we will look at the financial aspects of moving from a legacy type network to a Zero Trust Network.

Zero Trust Readiness



Overview of Zero Trust

Zero Trust Readiness ($500k)

Zero Trust Readiness

Users

Authentication and Authorization of Users ($675k)

Identity	Access	Data store	Policies/ Procedures	Integration
$200k	$100k	$100k	$75k	$200k
Identity and Access Management (IDAM) implementation and technologies	Role-based Access Control (RBAC)	Trust/reputation scoring		
Physical bootstrapping				
Digital Identity provisioning	Single Sign-On (SSO)	User inventory store		
User authoritative System-of-Record				
Onboarding/offboarding procedures	Multifactor Authentication (Biometrics, X.509, Time-based OTP, Tokens, etc.)	User accounting		
Certificate assignment and handling				

Zero Trust Readiness

Devices

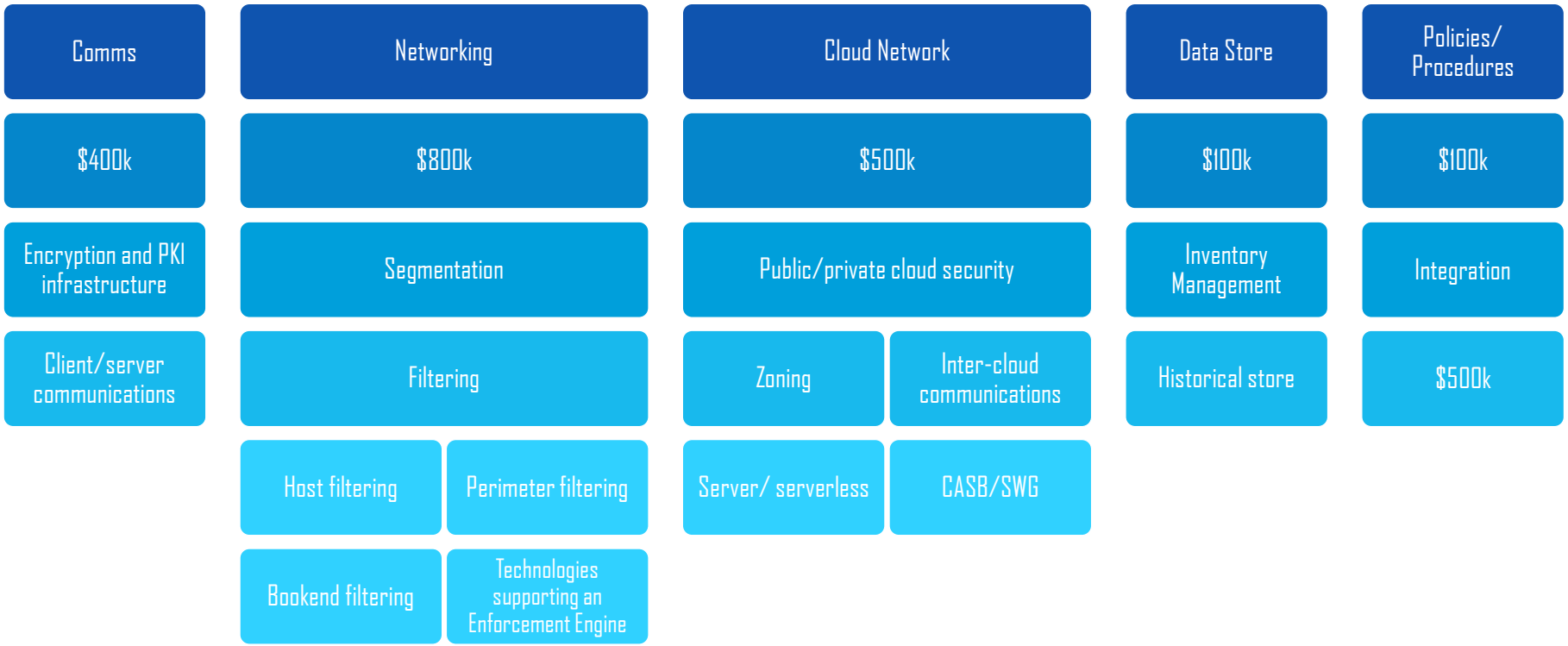
Authentication & Authorization of Devices ($575k)

Device Identity	Authentication	Data Store	Policies/ Procedures	Integration
$50k	$100k	$200k	$75k	$150k
Hardware Security Module / Trusted Platform Model	X.509	Device historical data store		
Secure Source of Truth for device configurations	Authentication Proxy	Device inventory store	Inventory Management	
		Device reputation	Device accounting	

Zero Trust Readiness

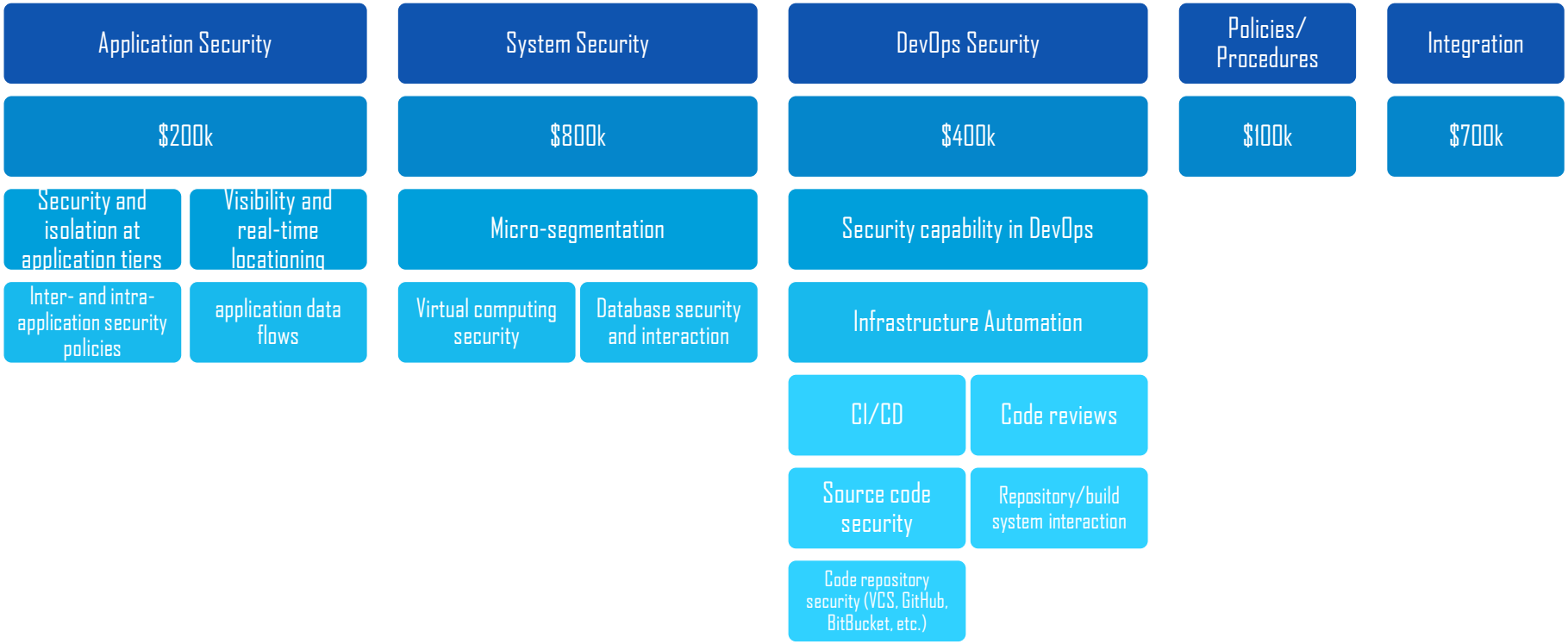
Workloads

Workload Security ($2.2M)



Zero Trust Readiness

Network Design, Authorization and Function ($2.4M)



Zero Trust Readiness

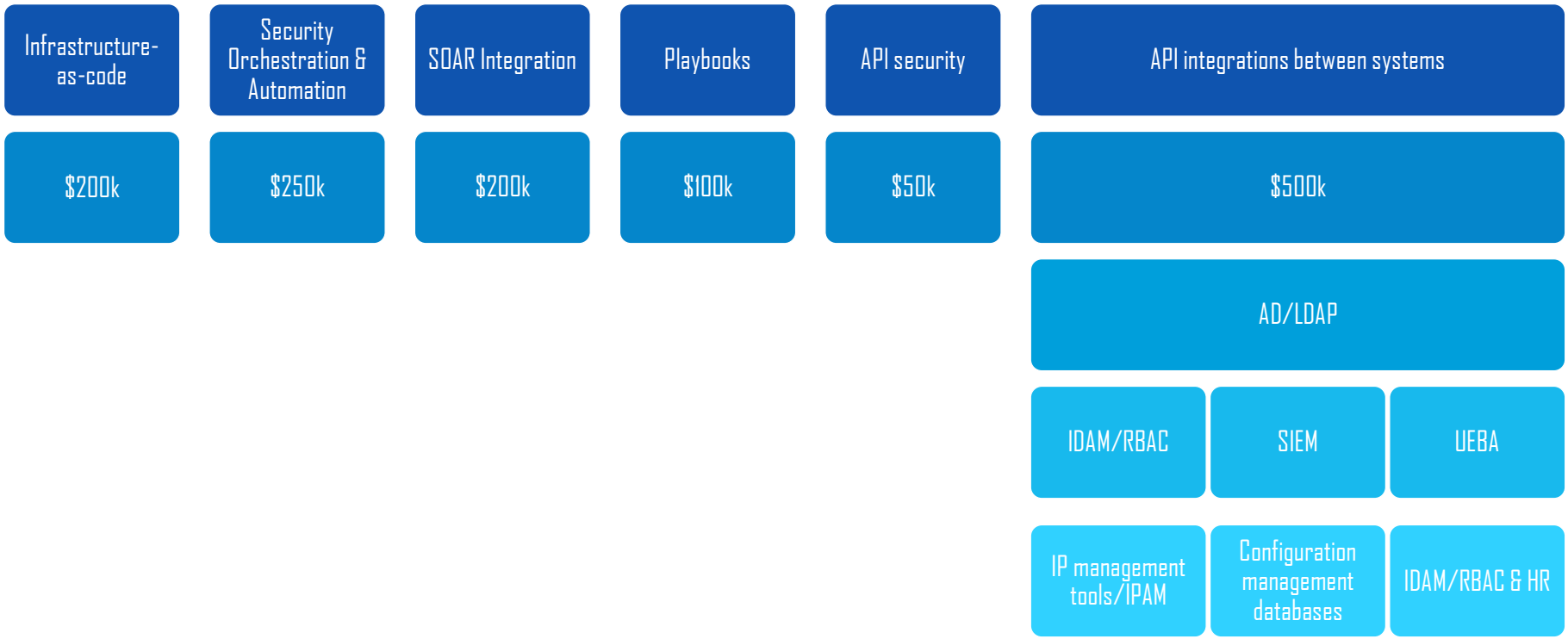
Analytics

Intelligence and Analytics ($1.85M)

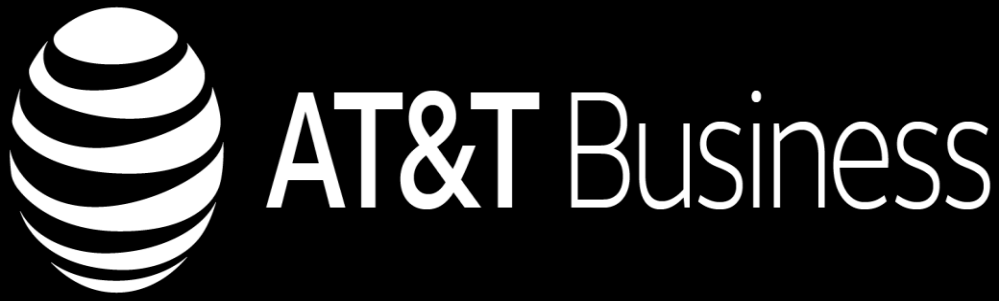
Monitoring capability (On-Prem and cloud)	Cyberthreat intelligence program	UEBA and geography-based reporting	Security Operations	Incident handling and reporting	Policies/ Procedures
$200k	$250k	$150k	$300k	$200k	$250k
	Cyberthreat intel collection, analysis, distribution, fusion		EDR/XDR		Integration
	Trending		Vulnerability Management		$500k
	Assessment				

Zero Trust Readiness

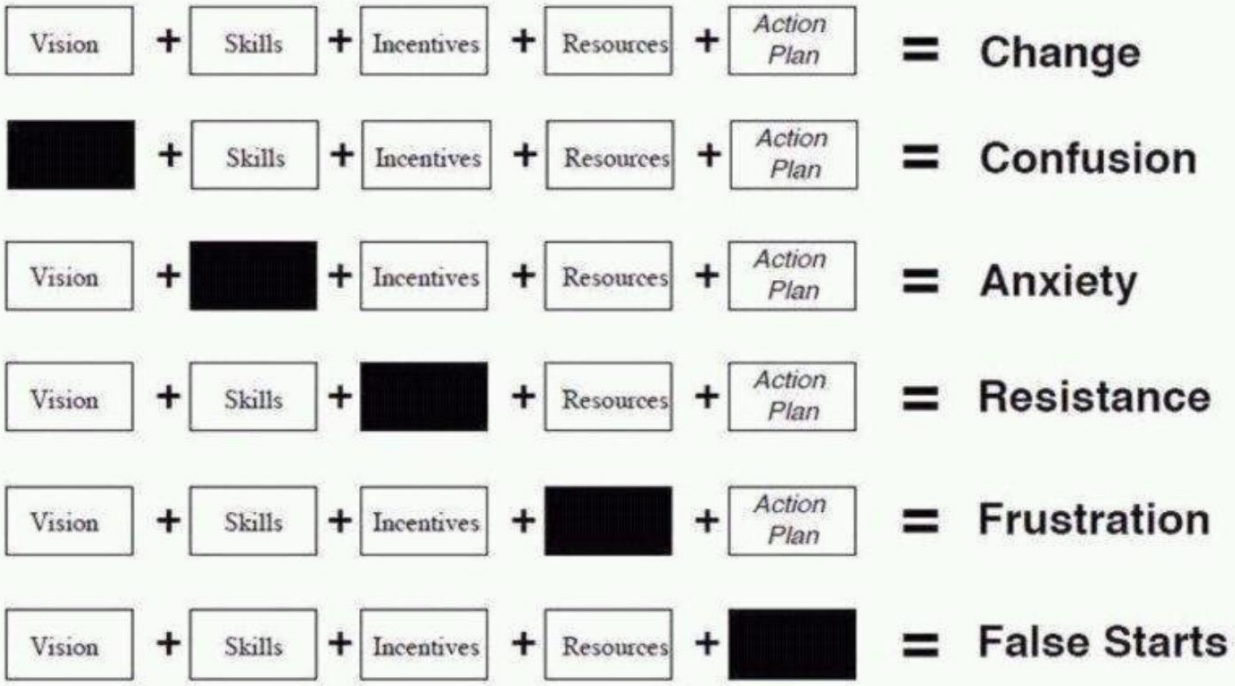
Automation and Orchestration ($1.3 m)



Further questions?



Managing Complex Change



Adapted from Knoster, T., Villa R., & Thousand, J. (2000). A framework for thinking about systems change. In R. villa & J. Thousand (Eds.), Restructuring for caring and effective education: Piecing the puzzle together (pp. 93-128). Baltimore: Paul H. Brookes Publishing Co.

https://intenseminimalism.com/2015/a-framework-for-thinking-about-systems-change/

VIRGINIA
IT AGENCY

NTT DATA MESSAGING SERVICES

STEVE COLLE

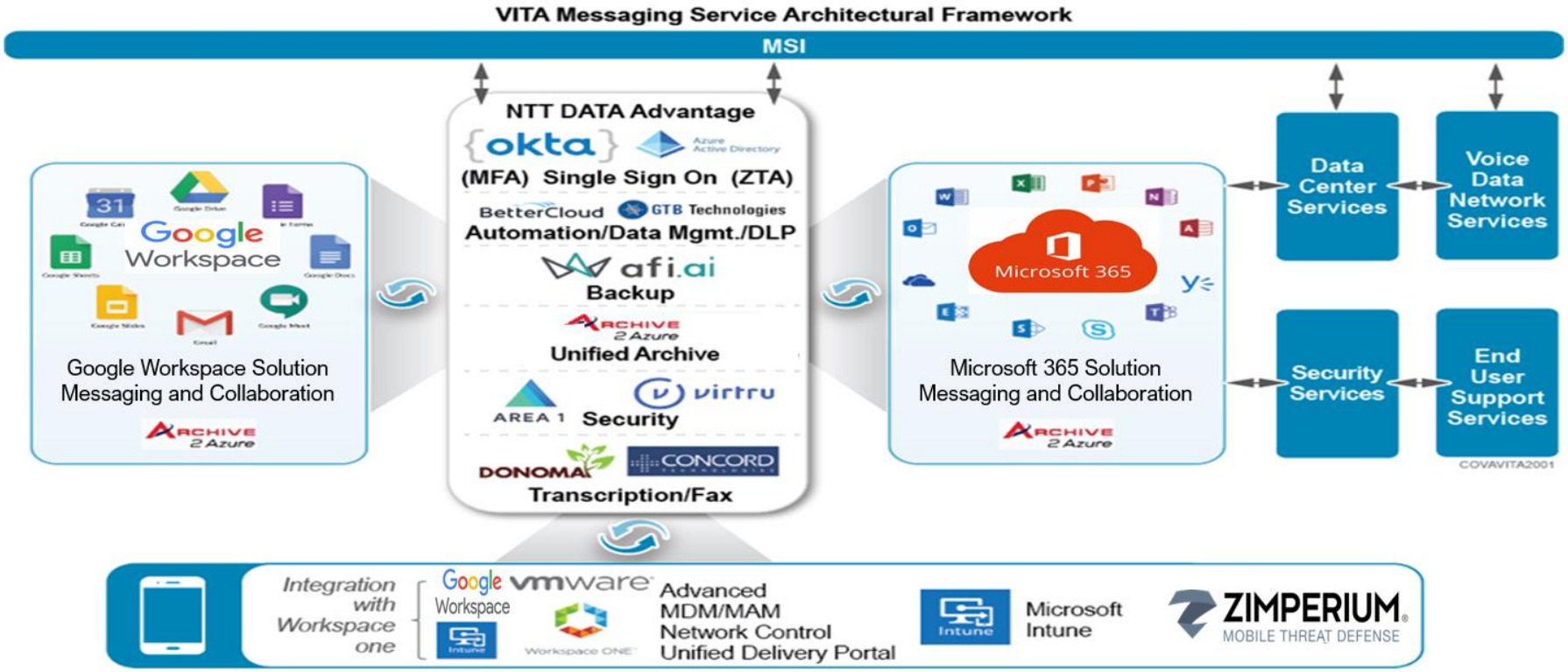
ARI FRIEDMAN

NTT DATA

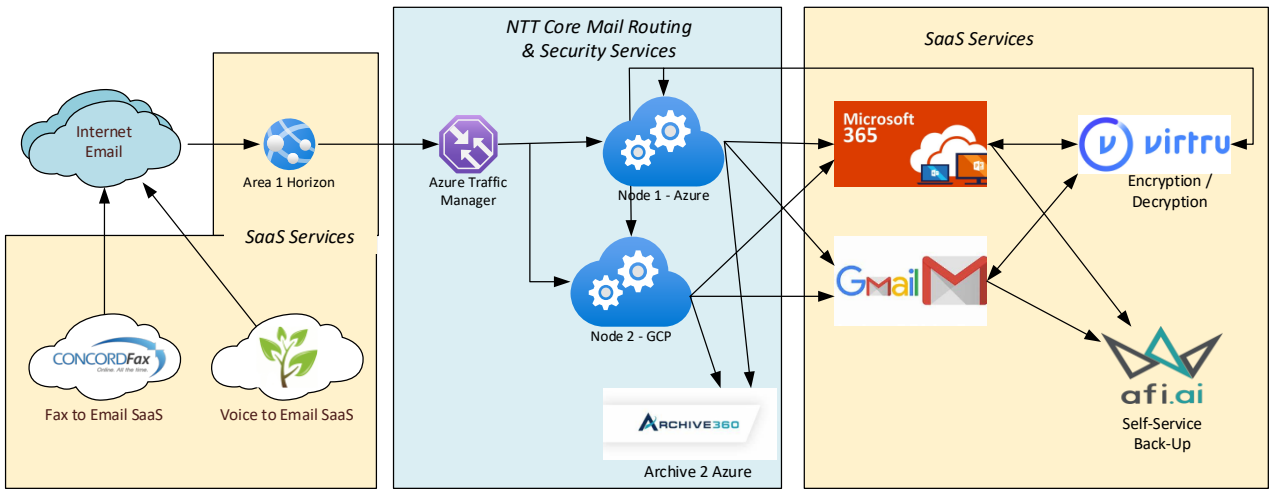
ISOAG MEETING

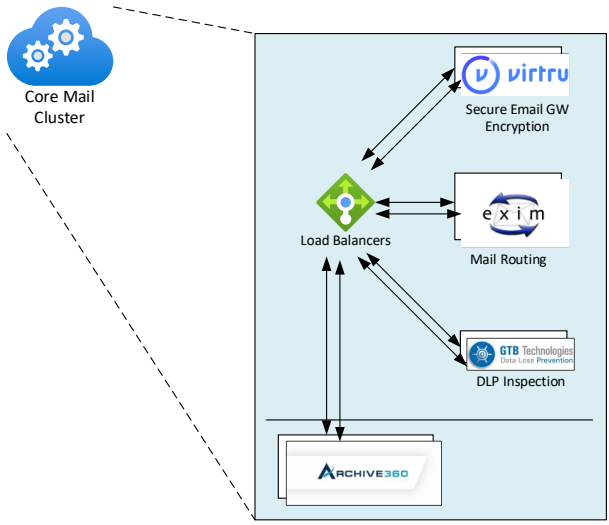
DEC. 1, 2021

1. Messaging Solution Overview
2. Core Messaging Routing
3. Data Management and Data Loss Prevention
4. Security
5. Unified Archiving
6. Transcription and Fax
7. Questions

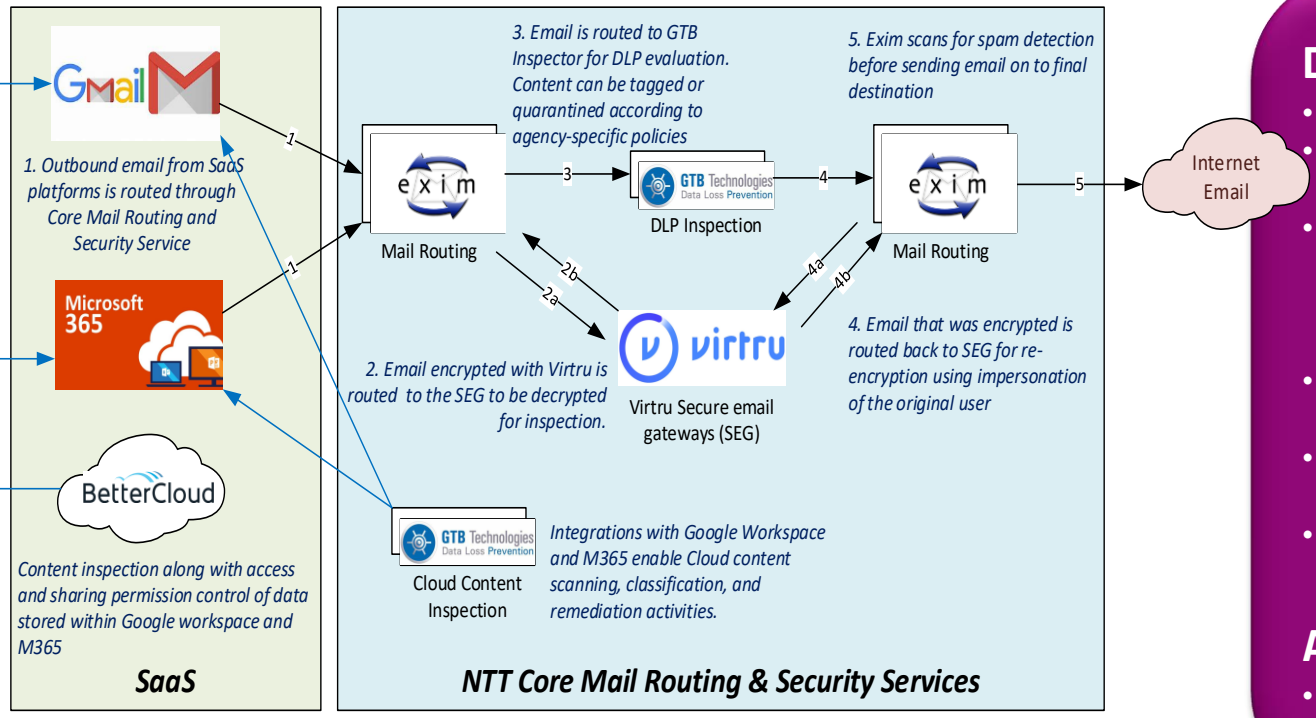

VITA Messaging Service Architectural Framework
MSI
NTT DATA Advantage
okta
Azure Active Directory
(MFA) Single Sign On (ZTA)
BetterCloud
GTB Technologies
Automation/Data Mgmt./DLP
afi.ai
Backup
Archive 2 Azure
Unified Archive
AREA 1 Security
virtru
DONOMA
CONCORD
Transcription/Fax
Google Workspace
Google Workspace Solution
Messaging and Collaboration
Archive 2 Azure
Microsoft 365
Microsoft 365 Solution
Messaging and Collaboration
Archive 2 Azure
Data Center Services
Voice Data Network Services
Security Services
End User Support Services
COVAVITA2001
Integration with Workspace one
Google Workspace
vmware
Workspace ONE
Advanced
MDM/MAM
Network Control
Unified Delivery Portal
Intune
Microsoft Intune
ZIMPERIUM
MOBILE THREAT DEFENSE

MESSAGING PLATFORMS MAIL ROUTING





DATA MANAGEMENT AND DATA LOSS PREVENTION



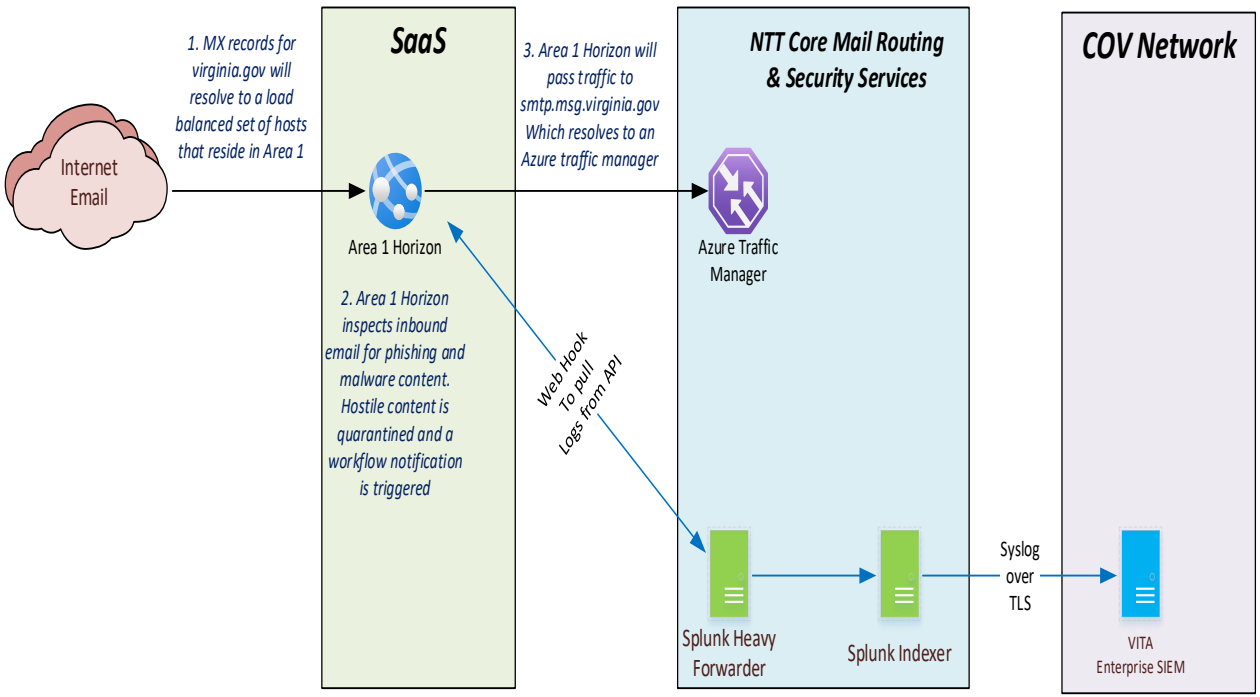
DLP includes:

- Content scanning of data in cloud.
- Access and permission inspection and remediation.
- Inspection classification of content in-transit with and remediation – warning, quarantining and encrypting.
- Inspection and journaling of encrypted email.
- Enhanced anti-malware, anti-phish and anti-spam services.
- All components integrated w/ VITA enterprise SIEM

Agency requirements:

- GTB and BetterCloud can be configured to provide agency specific requirements.

SECURITY - AREA 1



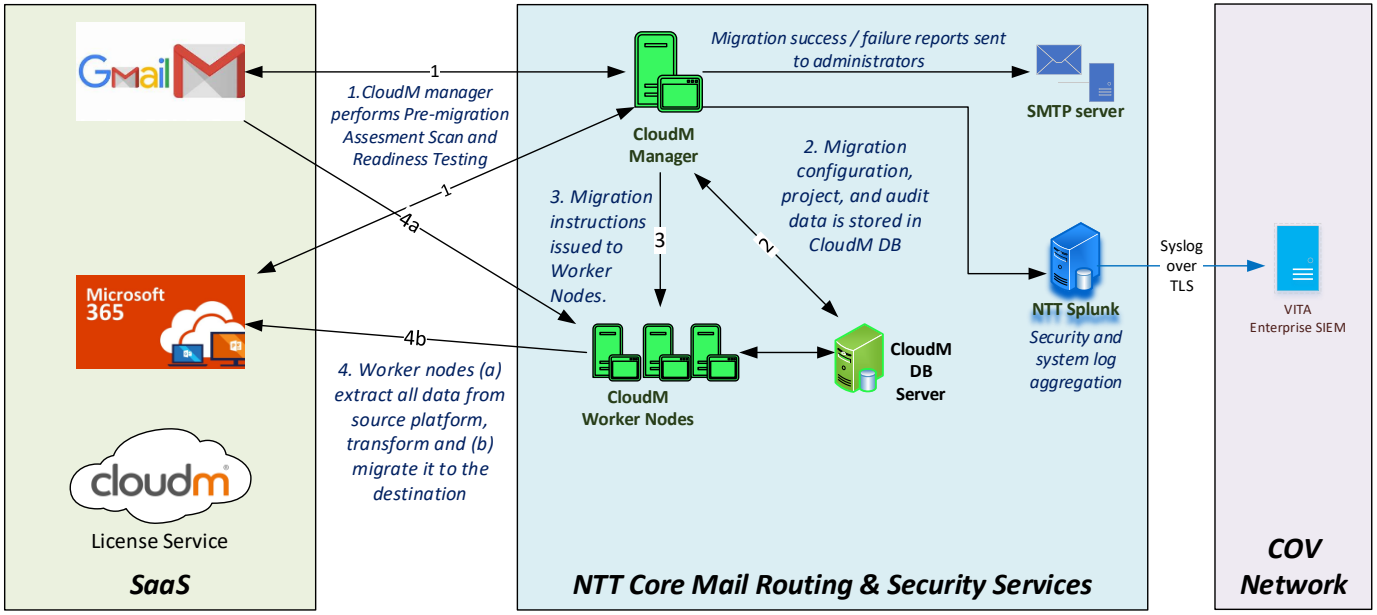
Area 1 includes:

- Provides anti-malware and anti-phishing and spam interdiction
- Integration with the messaging platform APIs to provide an avenue for users to report a message as SPAM or phishing

Agency requirements:

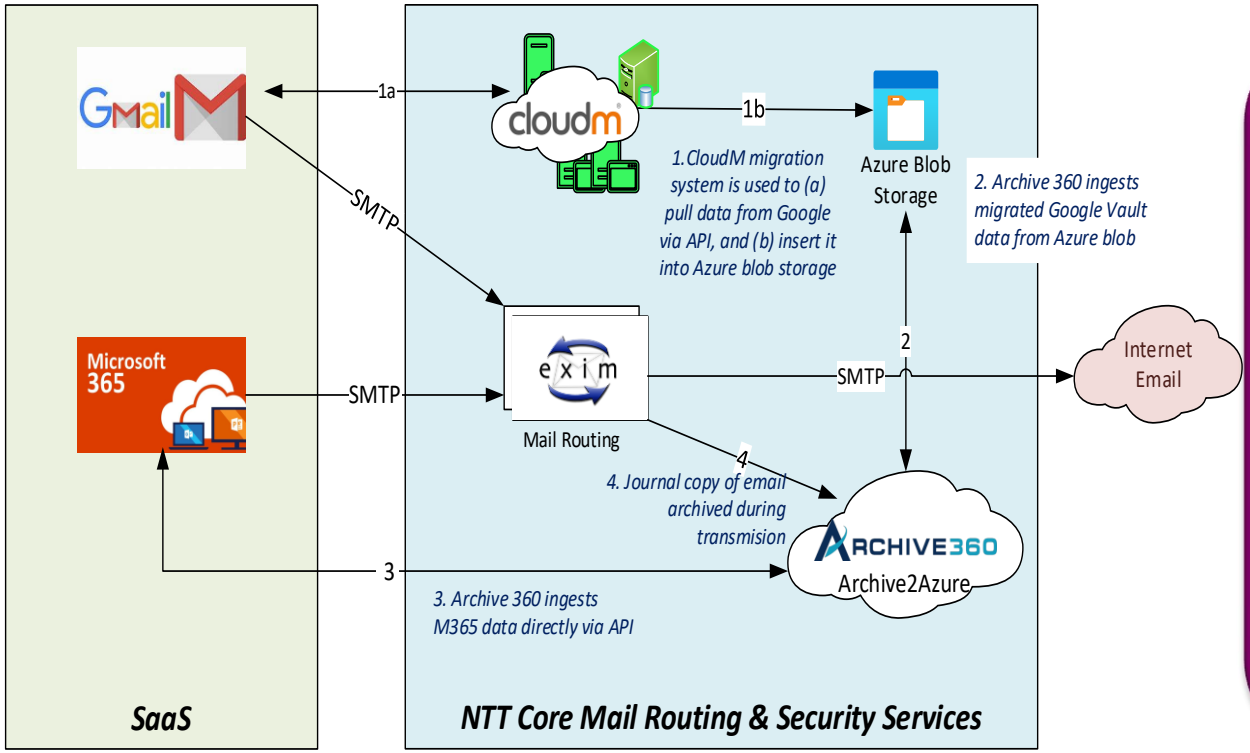
- Can be configured for agency specific requirements.

CLOUD M SKYLINE



Cloud M includes:

- Cloud M migrator for M365 and Google Workspace with Virtru integration
- Provides an enterprise class migration experience with full and in-depth reports, logging, auditing, and security at each phase of the entire migration.



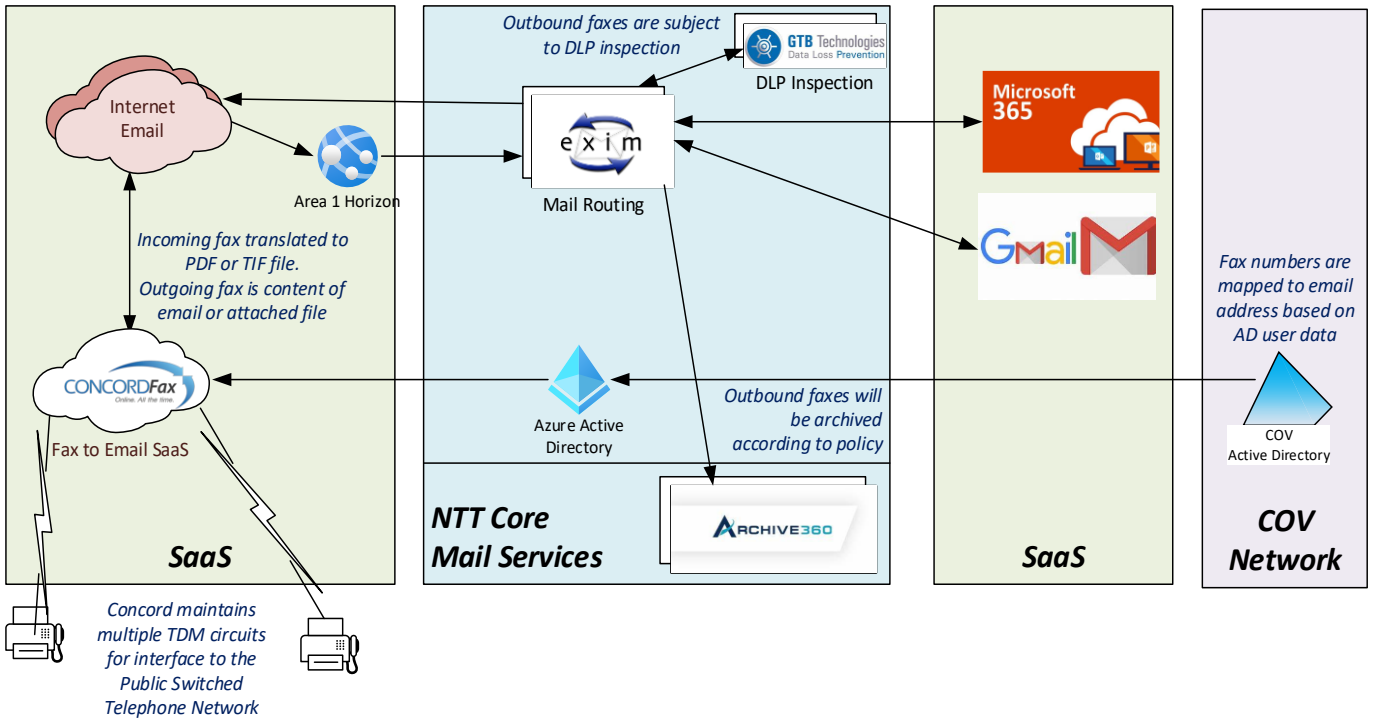
Archive 2 Azure includes:

- Perform all eDiscovery tasks including FOIA requests, legal discovery, legal hold, content search document preservation, redaction, classification, workload division with status tracking, and export of data in multiple industry standard formats.

Agency requirements:

- Can be configured for agency specific requirements.

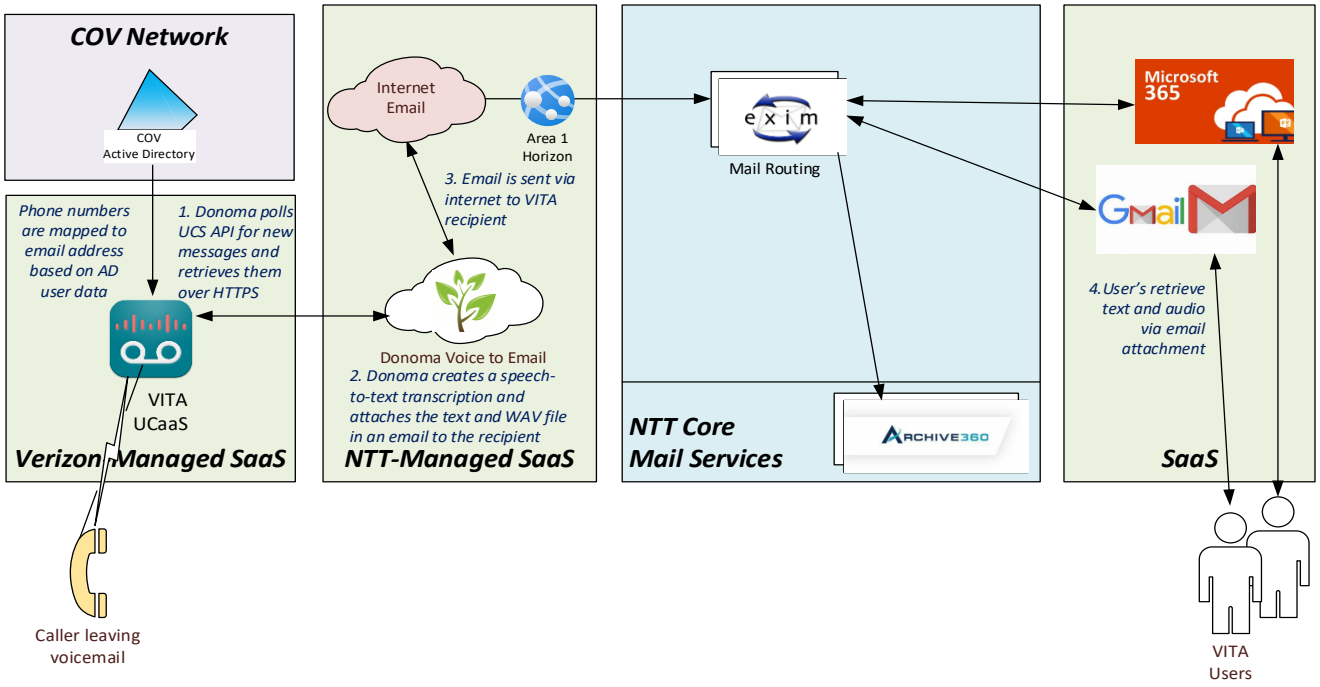
TRANSCRIPTION AND FAX - CONCORD



Concord includes:

- Cloud-based solution – no telco infrastructure to maintain.
- Highly reliable service
- Fax content subject to DLP inspection and control
- All data is encrypted in transit and at rest.
- Faxes delivered directly to recipients' mailbox

TRANSCRIPTION AND FAX - DONOMA



Donoma includes:

- Speech-to-Text transcription of voicemail provided in email along with audio file
- Click-to-call for return phone calls
- Reply by email for internal callers
- All data is encrypted in transit and at rest.
- Only ephemeral data stored in provider platform

THANK YOU!

VIRGINIA
IT AGENCY

VIRGINIA
IT AGENCY

Upcoming events

SECURITY AWARENESS TRAINING ANNUAL CERTIFICATION FOR REPORTING AND COMPLIANCE

Each organization shall:

Annually, by January 31, submit to VITA their proposed annual IT security awareness training plans with appropriate artifacts to VITA for approval (using the form in Appendix I or using a VITA supplied web portal if available).

Use the approved security awareness training for its employees/contractors

Provide employees and contractors agency cybersecurity training *within 30 days of initial employment or contract engagement* and by January 31 of each year thereafter.

Annually submit the following compliance information to VITA (using the table in Appendix II or by web portal when available):

A certification statement that all employees and contractors have completed required training,

An evaluation of the efficacy of the cybersecurity training program that the agency provided,

Any requests for improvement to the curriculum or other aspects of the training program.

ISO CERTIFICATION END OF YEAR REQUIREMENTS

You have until Dec. 31, 2021 to complete any outstanding requirements for your 2021 ISO Certification.

Contact Tina Gaines if you have any questions.

LITMOS END OF YEAR TRAINING CLOSE OUT

If you are part of VITA ISO Services or have an agreement with VITA to link to our security awareness training solution, please join us for our LITMOS End of Year security awareness training review.

Presenter: Debra Hurst (SANS)

Date: Dec. 2, 2021 at 11 a.m.

https://www.google.com/url?q=https://www.gotomeet.me/DebraHurst&sa=D&source=calendar&ust=1638654657771600&usg=AOvVaw0cw62D6Kvj6XiJNxrmP4aG

IS ORIENTATION

Final IS Orientation 2021

Dec. 8, 2021, 1 – 3 p.m.

Presenter: Marlon Cole

Registration Link :
https://covaconf.webex.com/covaconf/onstage/g.php?MTID=e6299241bfefde9a4e45b6e1b8a81e7cb

JANUARY 2022 ISOAG

Jan. 12, 2022, from 1 to 4 p.m.

Presenters:

Rick Shaw – Awareity

Barry Condrey – CIO Chesterfield County

Beth Waller – Woods Rogers

VIRGINIA
IT AGENCY

THANK YOU FOR ATTENDING!