CIO Association of Canada

Strategic Security

Our Approach to Zero Trust

- Zero trust is a way of thinking, not a specific technology
- Every Business is different & will have different security requirements
- Our goal
  - Align Security Requirements with your specific Business Requirements & Risks
  - Take Business environment view to ensure that it is not broken as security enforcement is activated
  - Use this process to build trust with the application owners and users
  - Ensure that security is not static but is proactively & reactively adaptive to new threats and risks as:
    - Others detect and mitigate them (threat intelligence)
    - As “we” internally detect and mitigate them (lessons learned)

I Need a Secure Environment to Enable my Business

Business Scenarios

Guiding North Star

- 1 - I want people to do their job securely from anywhere
- 2 - I want to minimize business damage from security incidents
- 3 - I want to identify and protect critical business assets
- 4 - I want to proactively meet regulatory requirements
- 5 - I want to have confidence in my security posture and programs

1. Strategic Framework

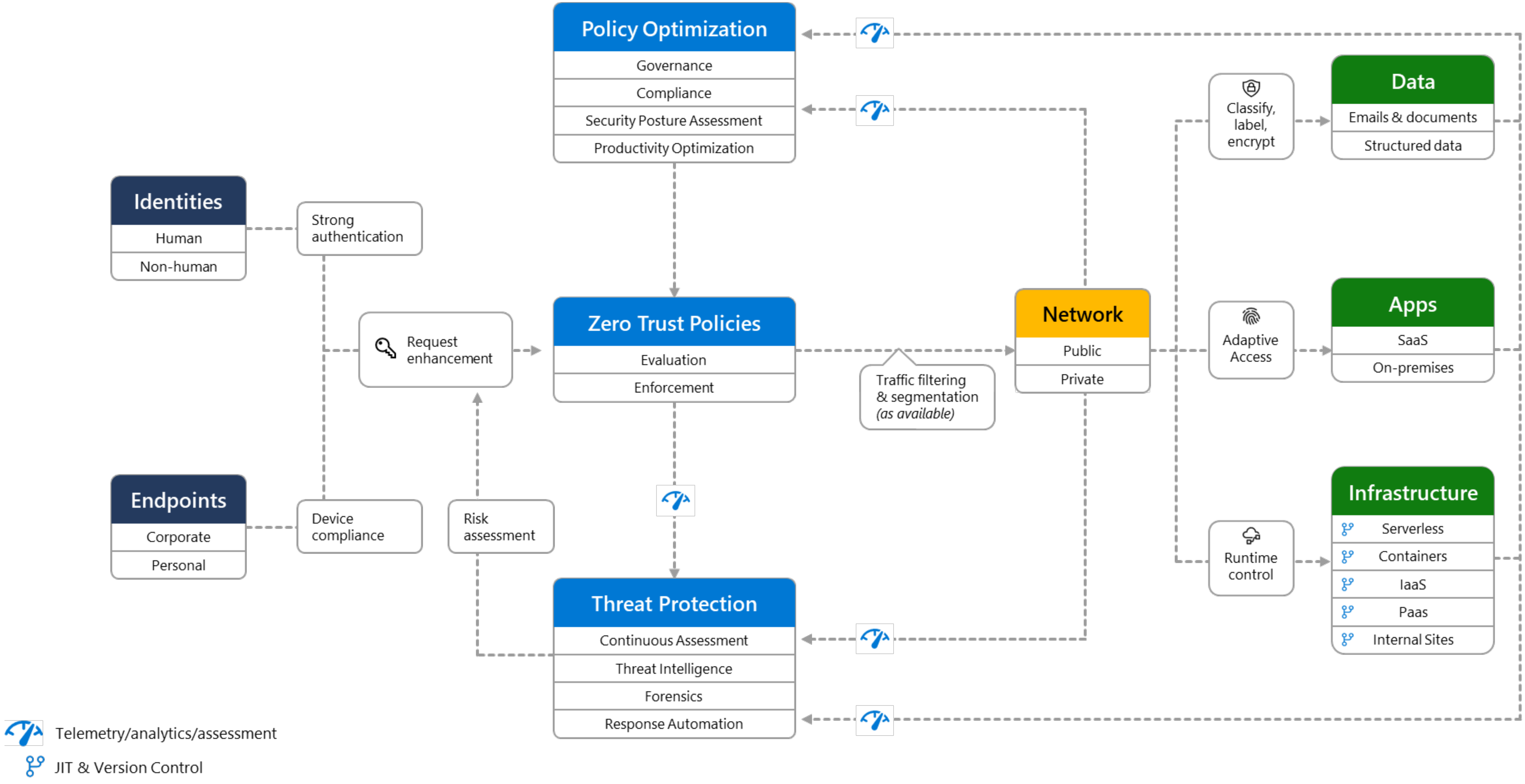
End to End Strategy, Architecture, and Operating Model

2. Strategic initiatives

Clearly defined architecture and implementation plans

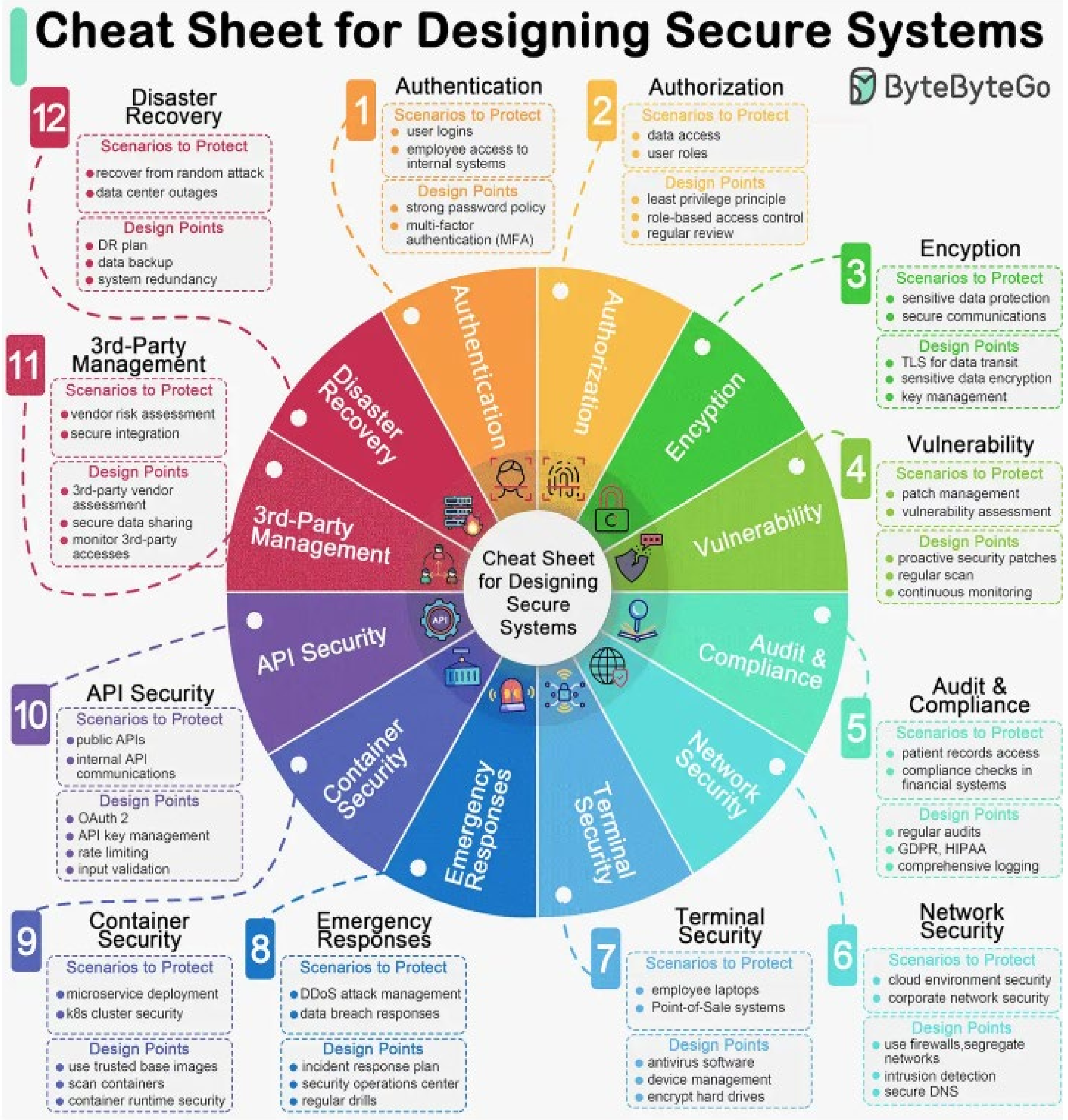
- Security Hygiene: Backup and Patching
- Secure Identities and Access
- Modern Security Operations
- Infrastructure and Development
- Data Security & Governance, Risk, Compliance (GRC)
- OT and IoT Security

Zero Trust Blueprint : What Could Go Wrong???



Source: Microsoft

Architecture Headaches



Cheat Sheet for Designing Secure Systems

ByteByteGo

Cheat Sheet for Designing Secure Systems

1 Authentication
Scenarios to Protect
- user logins
- employee access to internal systems

Design Points
- strong password policy
- multi-factor authentication (MFA)

2 Authorization
Scenarios to Protect
- data access
- user roles

Design Points
- least privilege principle
- role-based access control
- regular review

3 Encyption
Scenarios to Protect
- sensitive data protection
- secure communications

Design Points
- TLS for data transit
- sensitive data encryption
- key management

4 Vulnerability
Scenarios to Protect
- patch management
- vulnerability assessment

Design Points
- proactive security patches
- regular scan
- continuous monitoring

5 Audit & Compliance
Scenarios to Protect
- patient records access
- compliance checks in financial systems

Design Points
- regular audits
- GDPR, HIPAA
- comprehensive logging

6 Network Security
Scenarios to Protect
- cloud environment security
- corporate network security

Design Points
- use firewalls,segregate networks
- intrusion detection
- secure DNS

7 Terminal Security
Scenarios to Protect
- employee laptops
- Point-of-Sale systems

Design Points
- antivirus software
- device management
- encrypt hard drives

8 Emergency Responses
Scenarios to Protect
- DDoS attack management
- data breach responses

Design Points
- incident response plan
- security operations center
- regular drills

9 Container Security
Scenarios to Protect
- microservice deployment
- k8s cluster security

Design Points
- use trusted base images
- scan containers
- container runtime security

10 API Security
Scenarios to Protect
- public APIs
- internal API communications

Design Points
- OAuth 2
- API key management
- rate limiting
- input validation

11 3rd-Party Management
Scenarios to Protect
- vendor risk assessment
- secure integration

Design Points
- 3rd-party vendor assessment
- secure data sharing
- monitor 3rd-party accesses

12 Disaster Recovery
Scenarios to Protect
- recover from random attack
- data center outages

Design Points
- DR plan
- data backup
- system redundancy

The problem appears too big to address:

- Multi-year journey
- Choose tools based on a strategic architecture
- Rationalize all platform and app decisions based on the Strategic Security plan and roadmap

If you do not think about this holistically and strategically:

- Silos make individual decisions, policies and tool choices
- Policies are not cohesive
- Tools collide with each other
- Tools overlap with each other
- Telemetry and alerts are not shared between tools

Technical Faux Pas

Skipping basic maintenance

Skipping backups, disaster recovery exercises, and software updates/patching on assets

Securing cloud like on premises

Attempting to force on-prem controls and practices directly onto cloud resources

Wasting resources on legacy

Legacy system maintenance and costs draining ability to effectively secure business assets

Artisan Security

Focused on custom manual solutions instead of automation and off the shelf tooling

Disconnected security approach

Independent security teams, strategies, tech, and processes for network, identity, devices, etc.

Lack of commitment to lifecycle

Treating security controls and processes as points in time instead of an ongoing lifecycle

Best Practices

Develop and implement an **end to end technical security strategy** focused on durable capabilities and Zero Trust Principles

This workshop helps you define and rapidly improve on best practices across security including:

- ***Asset-centric security*** aligned to business priorities & technical estate (beyond network perimeter)
- ***Consistent principle-driven approach*** throughout security lifecycle
- ***Pragmatic prioritization*** based on attacker motivations, behavior, and return on investment
- ***Balance investments*** between innovation and rigorous application of security maintenance/hygiene
- ***'Configure before customize'*** approach that embraces automation, innovation, and continuous improvement
- ***Security is a team sport*** across security, technology, and business teams

Goal: Zero Assumed Trust

Reduce risk by finding and removing implicit assumptions of trust

With 30+ years of backlog at most organizations, it will take a while to burn down the backlog of assumed trust

False Assumptions

of implicit or explicit trust

- Security is the opposite of productivity
- All attacks can be prevented
- Network security perimeter will keep attackers out
- Passwords are strong enough
- IT Admins are safe
- IT Infrastructure is safe
- Developers always write secure code
- The software and components we use are secure

Zero Trust Mitigation

Systematically Build & Measure Trust

Business Enablement
Align security to the organization's mission, priorities, risks, and processes

Assume Compromise
Continuously reduce blast radius and attack surface through prevention and detection/response/recovery

Shift to Asset-Centric Security Strategy
Revisit how to do access control, security operations, infrastructure and development security, and more

Explicitly Validate Account Security
Require MFA and analyze all user sessions with behavior analytics, threat intelligence, and more

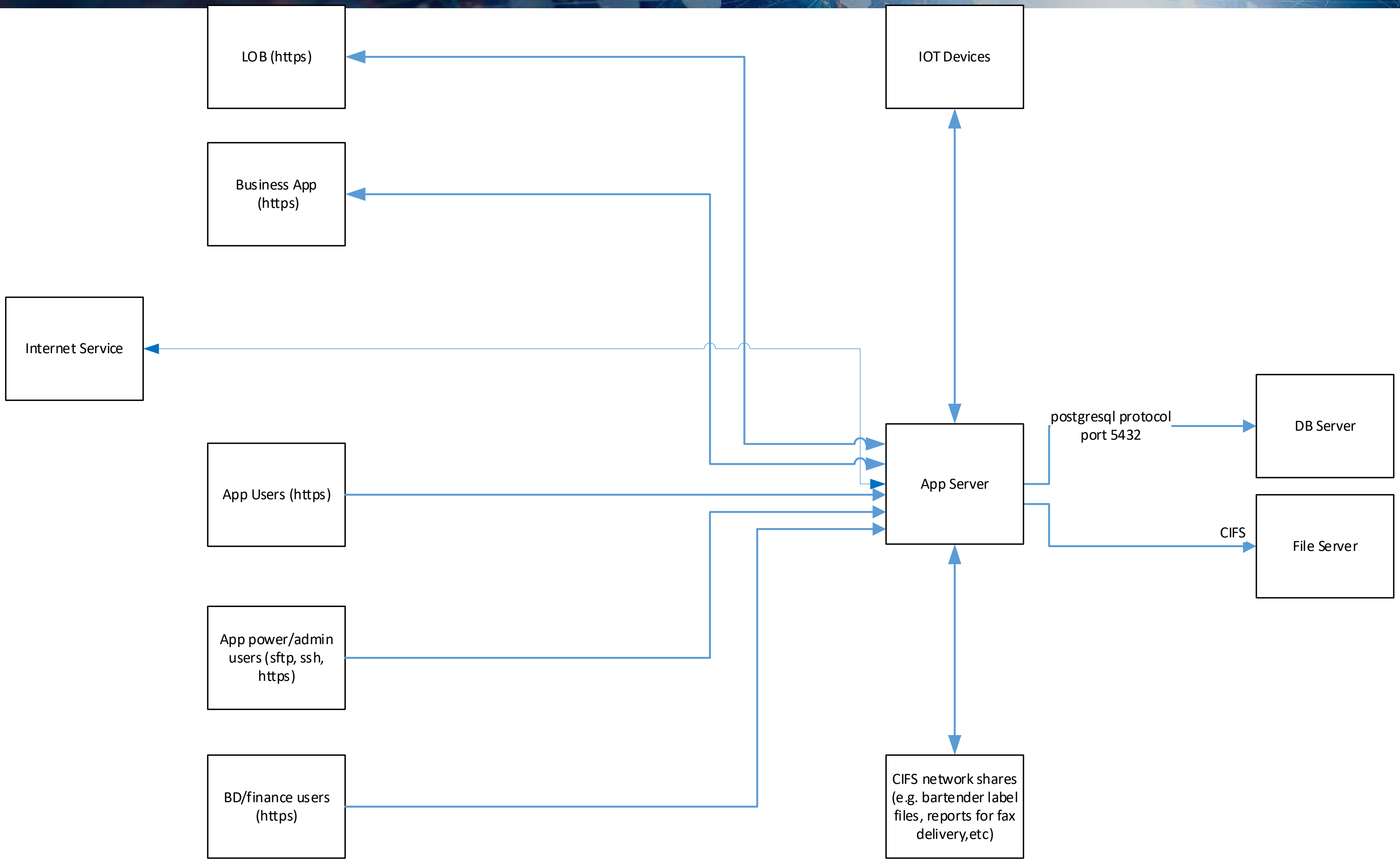
Plan and Execute Privileged Access Strategy
Establish security of accounts, workstations, and other privileged entities (aka.ms/spa)

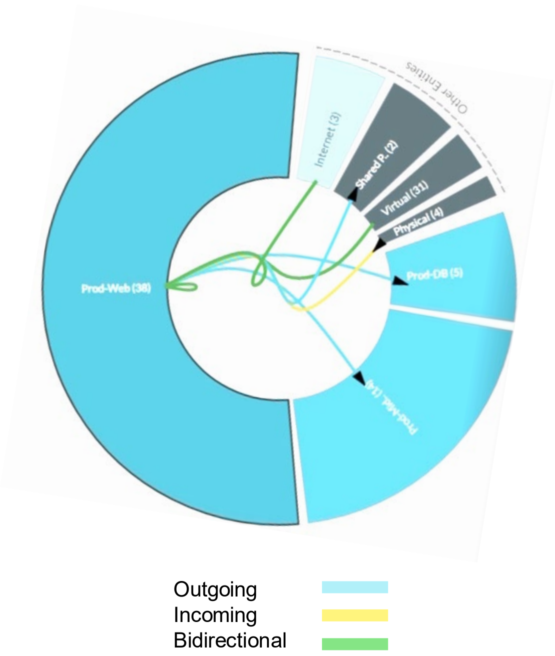
Validate Infrastructure Integrity
Explicitly validate trust of operating systems, applications, services accounts, and more

Integrate security into development process
Security education, issue detection and mitigation, response, and more

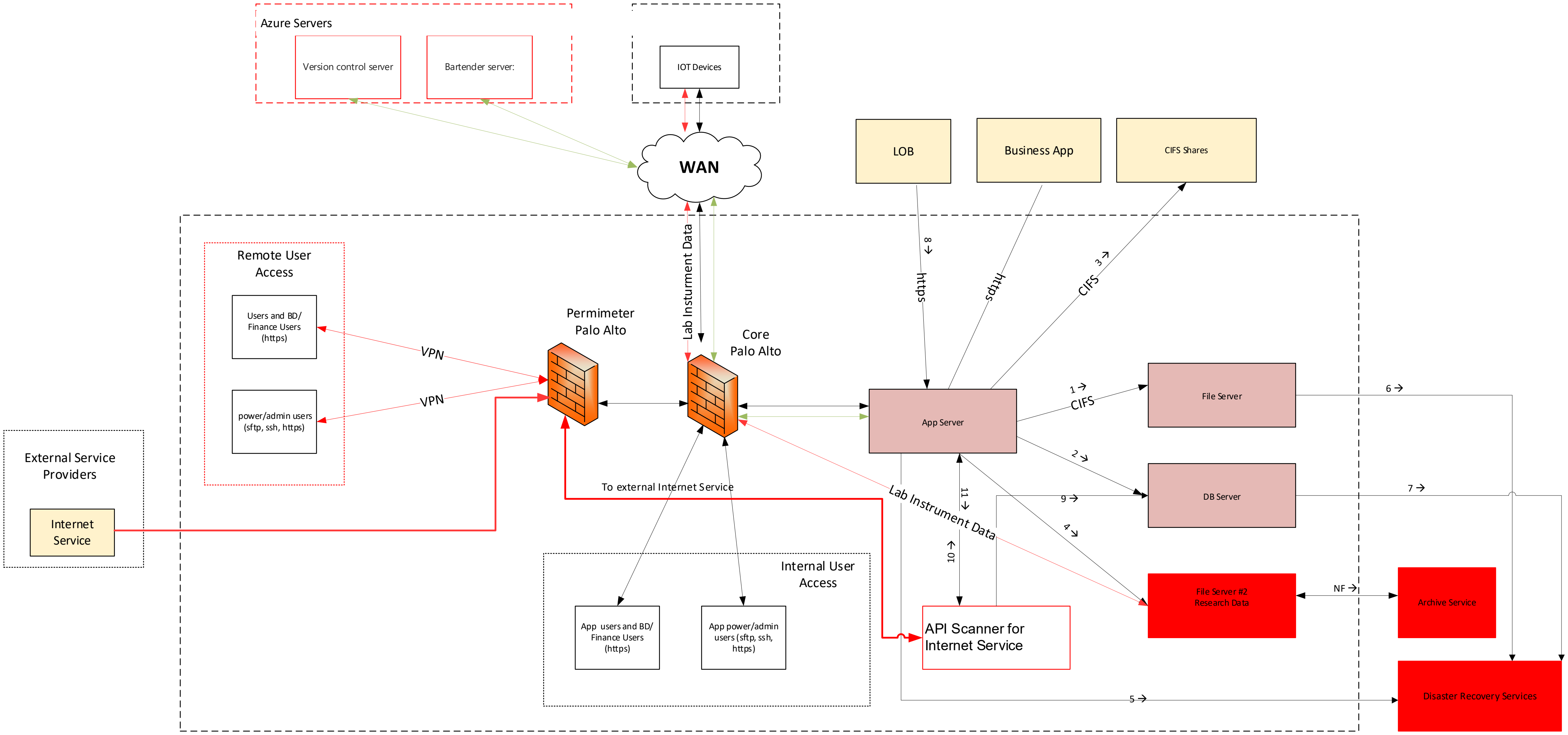
Supply chain security
Validate the integrity of software and hardware components from open source. vendors, and others

Perceived Application Maps

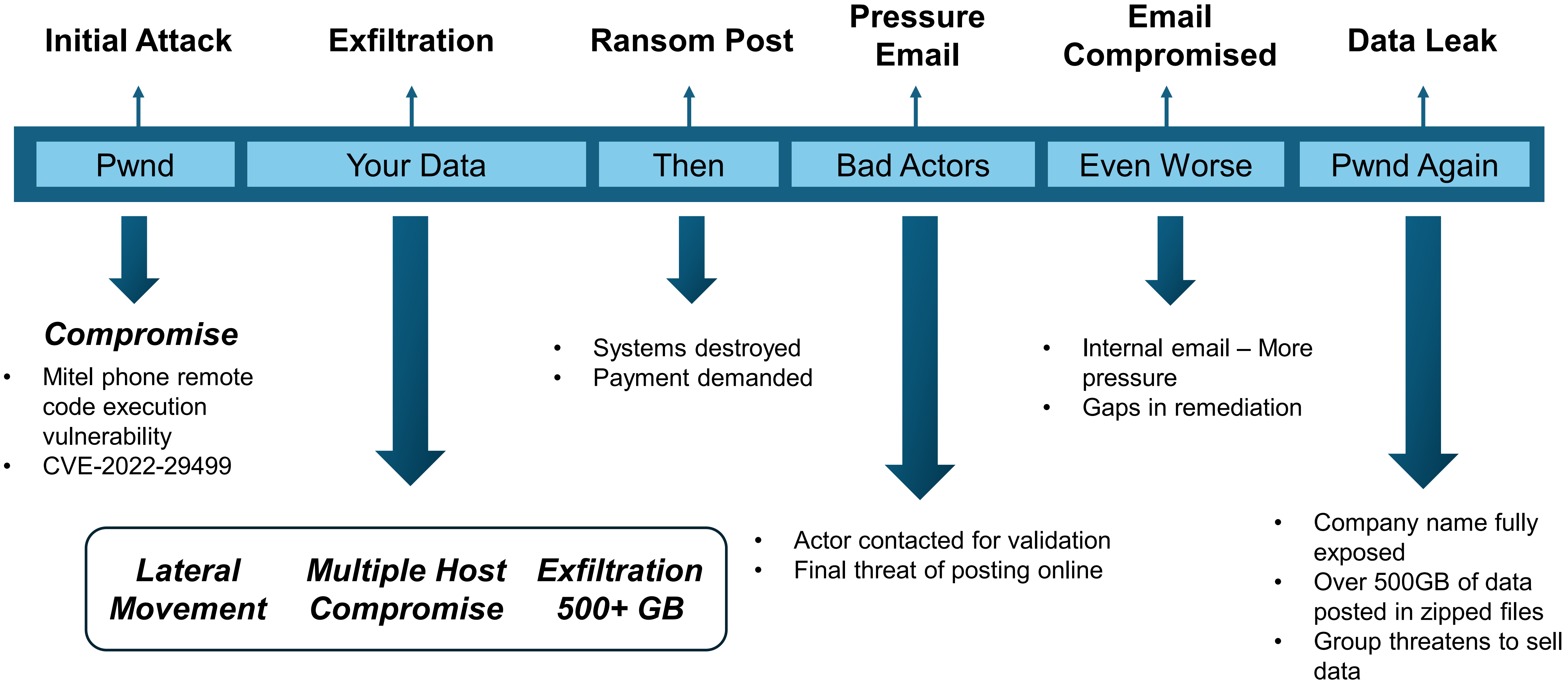

LOB (https)
IOT Devices
Business App (https)
Internet Service
postgresql protocol port 5432
DB Server
App Server
App Users (https)
CIFS
File Server
App power/admin users (sftp, ssh, https)
BD/finance users (https)
CIFS network shares (e.g. bartender label files, reports for fax delivery,etc)



Discovered Application Map



Not All Attacks are IT based



Initial Attack

Pwnd

Compromise

- Mitel phone remote code execution vulnerability
- CVE-2022-29499

Exfiltration

Your Data

Lateral Movement ***Multiple Host Compromise*** ***Exfiltration 500+ GB***

Ransom Post

Then

- Systems destroyed
- Payment demanded

Pressure Email

Bad Actors

- Actor contacted for validation
- Final threat of posting online

Email Compromised

Even Worse

- Internal email – More pressure
- Gaps in remediation

Data Leak

Pwnd Again

- Company name fully exposed
- Over 500GB of data posted in zipped files
- Group threatens to sell data

Prevention

Prevention

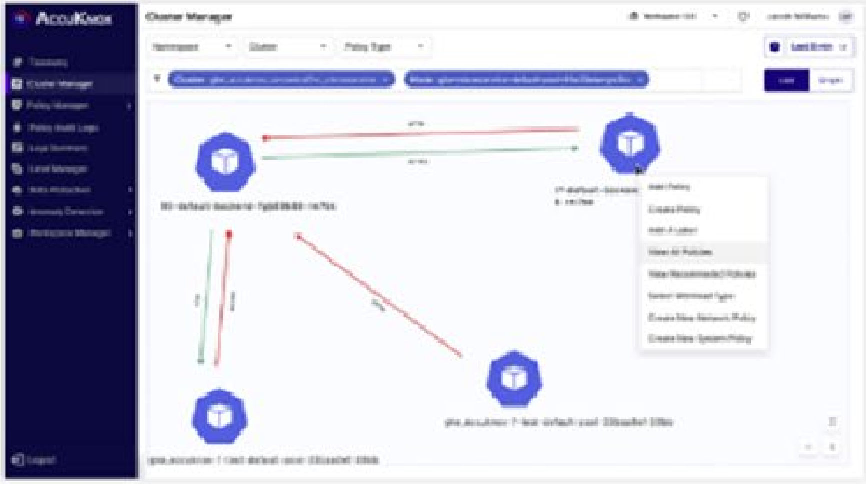
- Zero Trust Network Access
  - Contextual user auth – time of day, geography, device
  - Connect user to app not network
- Identity Management
  - Least Privileged Access
- Micro Segmentation
  - Prevent lateral discovery of network devices
  - API Security
- Configuration Management
  - Asset configuration discovery scanning & control
- Regular Security vulnerability scan

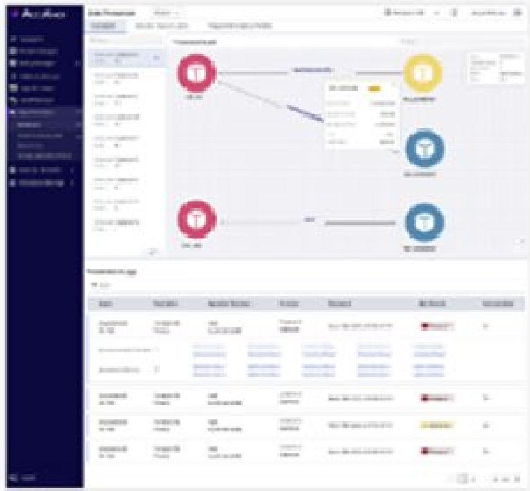
Defensive Response

- AI based Behavioural Monitoring
- Encryption monitor at O/S Kernel level
  - Immediate detection of encryption event
  - Decrypt few files with RPO of few minutes
- Security scan of recovered devices
- Adjust Threat Prevention System
- Adjust Policy Engine

Visibility

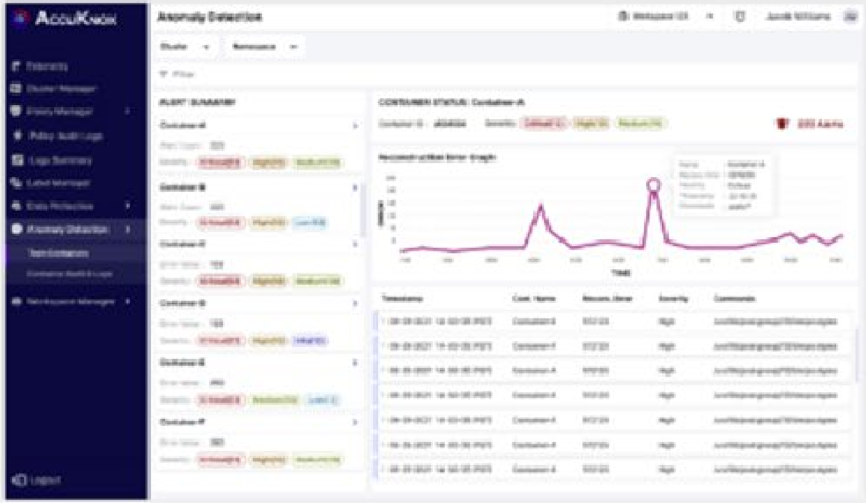
POLICY MANAGEMENT

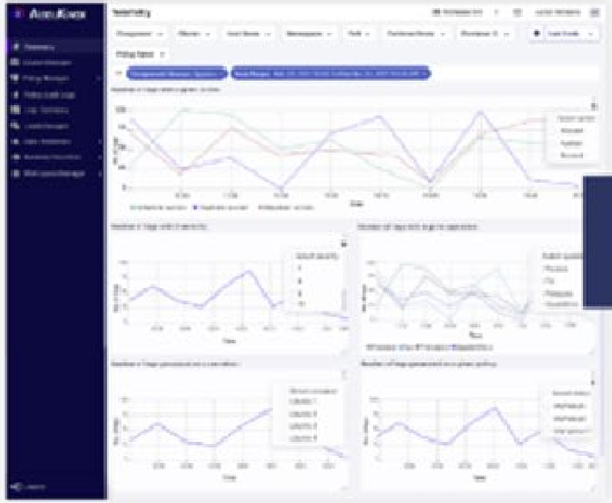




DATA SECURITY

ANOMALY DETECTION

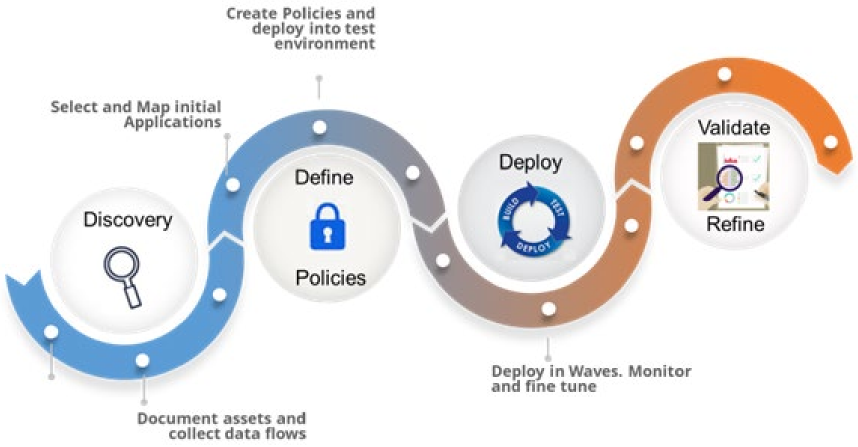




TELEMETRY

Key Take Aways

- Understand how applications enable your business
- Understand your risks
  1. External risks you are facing
  2. Internal risks resident in your Infrastructure
- Develop a strategy and policy to mitigate risks without breaking business revenue/service streams
- Use strategy and policy to
  1. Design Security Framework and select tools
  2. Rationalize all IT decisions for applications and infrastructure
  3. Prioritize risks
  4. Create a roadmap to addressing the prioritized risks


Create Policies and deploy into test environment
Select and Map initial Applications
Discovery
Define
Policies
Deploy
BUILD
TEST
DEPLOY
Validate
Refine
Deploy in Waves. Monitor and fine tune
Document assets and collect data flows

What’s in it for CIOCAN members

- Committed to deliver, close enough to care!

- Fred Zandberg fzandberg@esitechnologies.com
- Brian McColl bmccoll@esitechnologies.com

Questions