The Commonwealth of Pennsylvania

Harrisburg University Cyber Security Summit
9/29/2022

Microsoft

A Holistic Approach to Cybersecurity

Habib Nawabi
Senior Security Technical Specialist
US State & Local Government

9/20/2022

Headlines

Chinese Hackers Stole Boeing, Lockheed Military Plane Secrets: Feds

July 11, 2014, 3:42 PM PDT / Updated July 11, 2014, 2:31 PM PDT

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise M... Victims With SUNBURST Backd...

December 13, 2020 | by FireEye

New Report Finds DOD "Could Be Pretty Easily Hacked"

One test was able to penetrate a system within nine seconds.

BY DAVID GROSSMAN OCT 9, 2018

CISA: Hackers breached ... more than SolarWinds b...

China compromised F-35 subcontractor and forced expensive software system rewrite, academic tells MPs

Gareth Corfield Thu 12 Nov 2020 // 16:27 UTC

Officials: Hack exposed U.S. military and intel data

Russians hacked DOD's unclassified networks

BY ELISE VIEBECK - 04/23/15 03:03 PM EDT

China hacked a Navy contractor a... secured a trove of highly sensitive... on submarine warfare

US DoD Department Hacked And Data Compromised

Tom Jowitt, February 21, 2020, 12:56 pm

Cloud security challenges

Visibility into security and compliance

- **52%** of organizations cite secure configuration of cloud resources as a top priority.[1]

Increase in number and sophistication of attacks

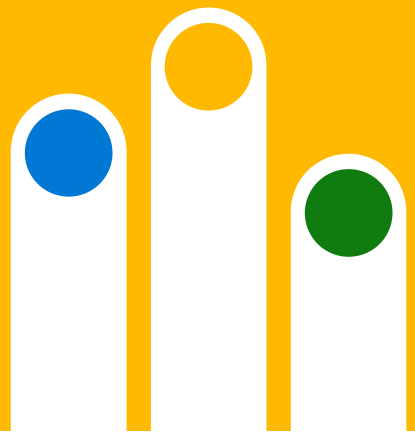
- In 2021, the average cost of a breach was **$4.24M**.[2]

Complexity managing multi-cloud environments

- **92%** of organizations are embracing a multi-cloud strategy

[1]Source: 451 Research
[2]Source: Ponemon Institute, Cost of a Breach Report

Security has never been more critical



Cyber-attacks are becoming more **frequent and sophisticated**

Pressures to address **multi-cloud IT environment**

Increasingly **complex regulatory landscape**

The Challenge of Securing Your Environment

Reactive Security

When centralizing data into one source, actions are performed after the fact.

Signals that provides status of current risk cannot be used across services/environments

Operational complexity

Responding to a threat often requires acting or validating enforced policies across multiple security solutions or managed systems.

Likewise common security tasks, such as generating evidence for compliance audits, or applying security policies span multiple solutions.

Asset/Vulnerability/Risk Management and Reporting

Visibility and control over on-premises, cloud, mobile, and IoT resources

Assess, remediate, and report risk from vulnerabilities

Regulatory Compliance Management

Assess and Manage compliance risk across cloud assets

Meet new regulatory needs

Outcomes of information security and privacy controls (vs. control adherence)

Too Many Alerts

Shortage of skilled Workforce

The number of Alerts tend to exceed the capacity of security teams so not all issues can be investigated.

Even if ways are defined to filter and prioritize alerts based on your unique environment, these static definitions tend not to address the needs of an ever-changing ecosystem.

Decentralized data

Much of the business context needed for comprehensive investigation lives in systems not being monitored

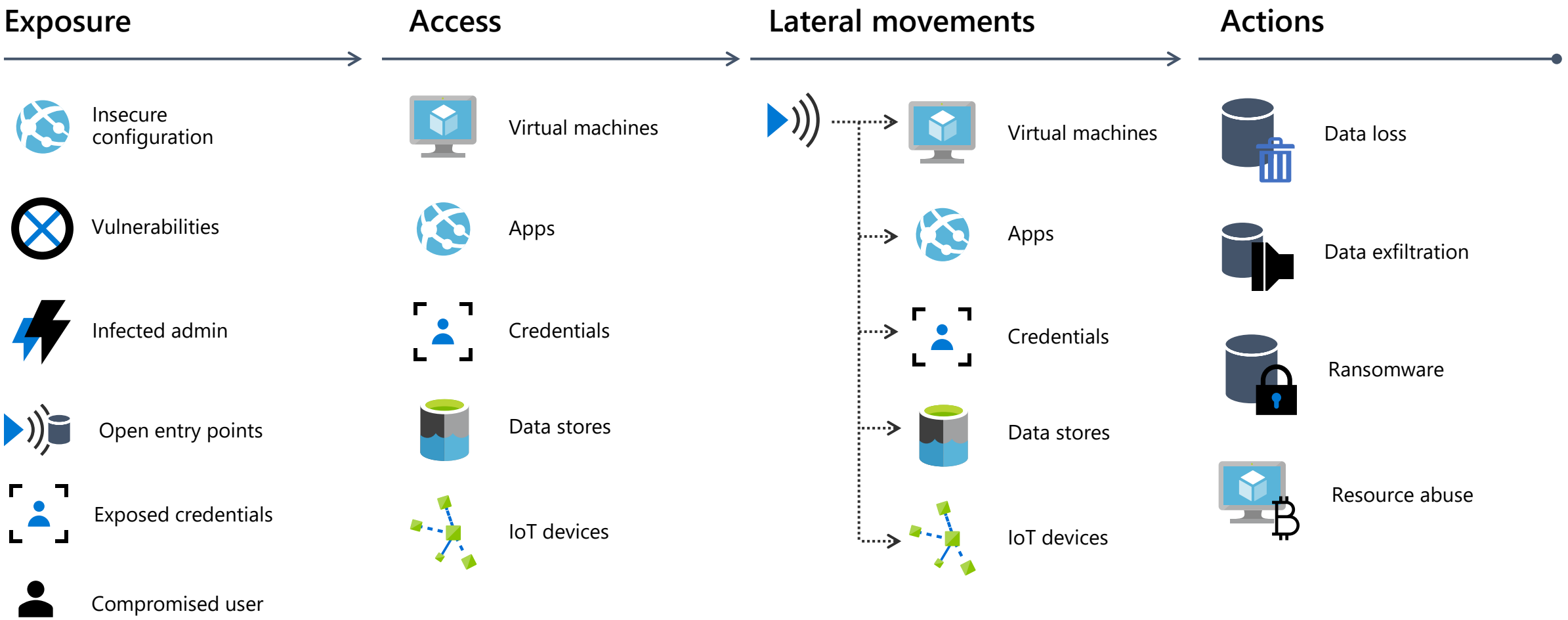
When investigating a threat, valuable time is wasted collecting and synthesizing data from multiple sources

Top concern for organizations

A constantly evolving threat

Ransomware (Mid-2010's)	Human-operated Ransomware (Present)
Targets individual systems	Targets **entire company**
Broad targeting, narrow impact	Customized attacks driven by **determined human intelligence**
Opportunistic data encryption	**Calculated** data encryption or data exfiltration
Unlikely to cause catastrophic business disruption	Guaranteed to cause **catastrophic** and **visible** business disruption
Defense via malware prevention is possible	Successful defense requires **holistic security**

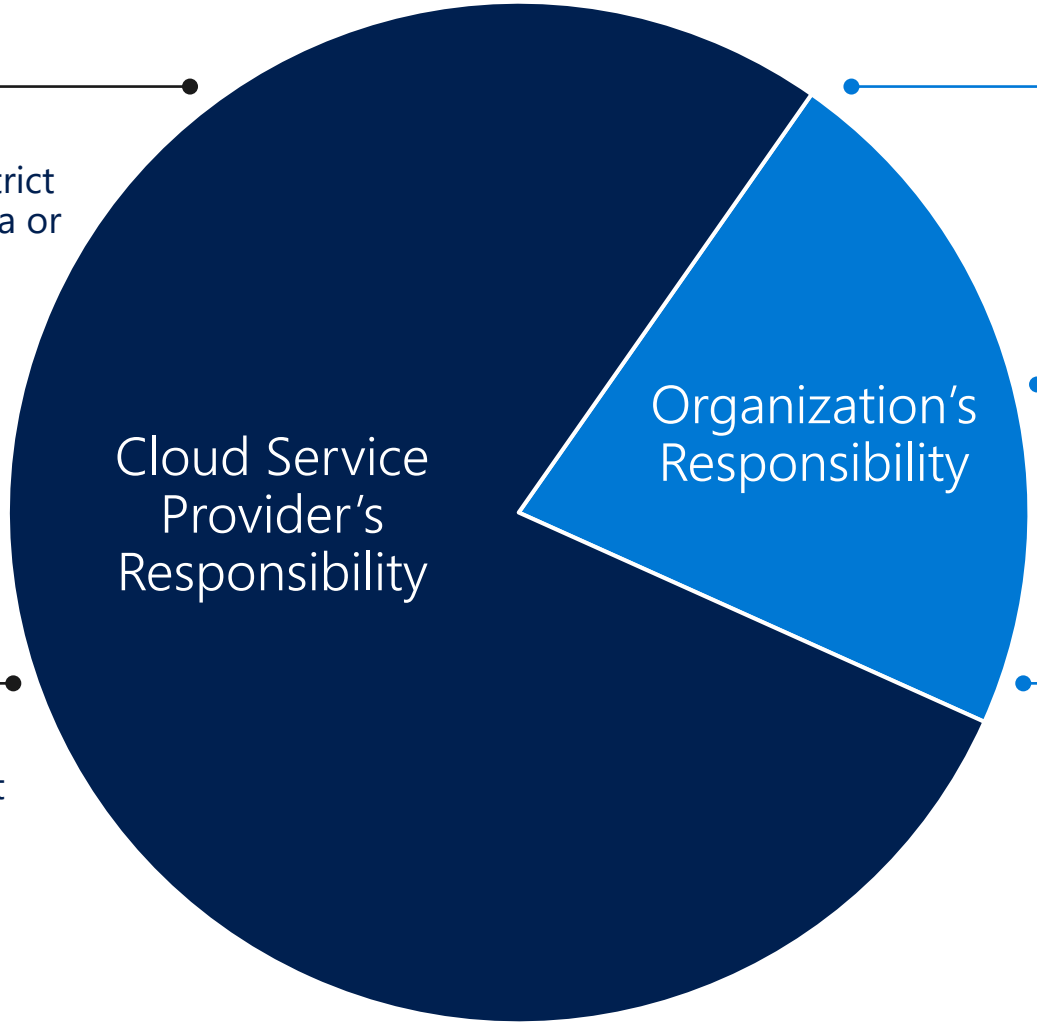
The Cloud Kill Chain Model



Trusted Cloud Principles

Security	Privacy & Control	Transparency	Compliance
			
Protect confidentiality, integrity, and availability	Control access and use of your data	Visibility into how your data is handled and used	Managed in compliance with applicable laws, regulations, and standards

Compliance & Security is a Shared Responsibility



ACCESS TO PRODUCTION ENVIRONMENT

Set up access controls that strictly restrict standing access to any customer's data or production environment

PROTECT DATA

Encrypt data at rest and in transit based on industry standards

PERSONNEL CONTROL

Strict screening for employees, vendors, and contractors, and conduct trainings through onboarding process

ACCESS TO PRODUCTION ENVIRONMENT

Set up access control policy and SOP, leveraging identity management solutions

PROTECT DATA

Encrypt FTI in transit

PERSONNEL CONTROL

Provide staff and sufficient resources to implement and operate an organization-wide privacy program, including awareness-raising and training

Standards Shifting Over Time

- Cybersecurity and Compliance Intersection
  - StateRAMP
  - NERC
  - HIPAA
- Convergence toward NIST 800-53
  - CJIS Security Policy
  - IRS 1075
  - MARS-E
- Commercial cloud impact
  - Technical vs personnel controls
  - Critical role of customer-managed key encryption
  - Data residency

A modernization strategy drives innovation + growth

80%
Administration

Remove patching, network setup, firewall configuration

Enable application innovation

—Forrester TEI of Azure[1]

Websites running in
minutes

Remove the need to wait for servers[2]

Improve app delivery time by 50%[1]

Data
analysis

With cloud, we collect data we couldn't before

Make personal connections that standout in sea of information

—Anheuser-Busch InBev

Organizations that harness data, the cloud, and AI outperform their peers[3]

~2x operating margin

$100M additional operating income

[1]The Total Economic Impact™ Of Microsoft Azure Platform-As-A Service, Forrester Consulting, June 2016
[3]Source: Keystone Strategy interviews Oct 2015 - Mar 2016

…but change is difficult. We understand this impacts people, culture, and can feel risky.

It requires new and disruptive thinking

It requires leaders to adapt, take risks, and learn quickly

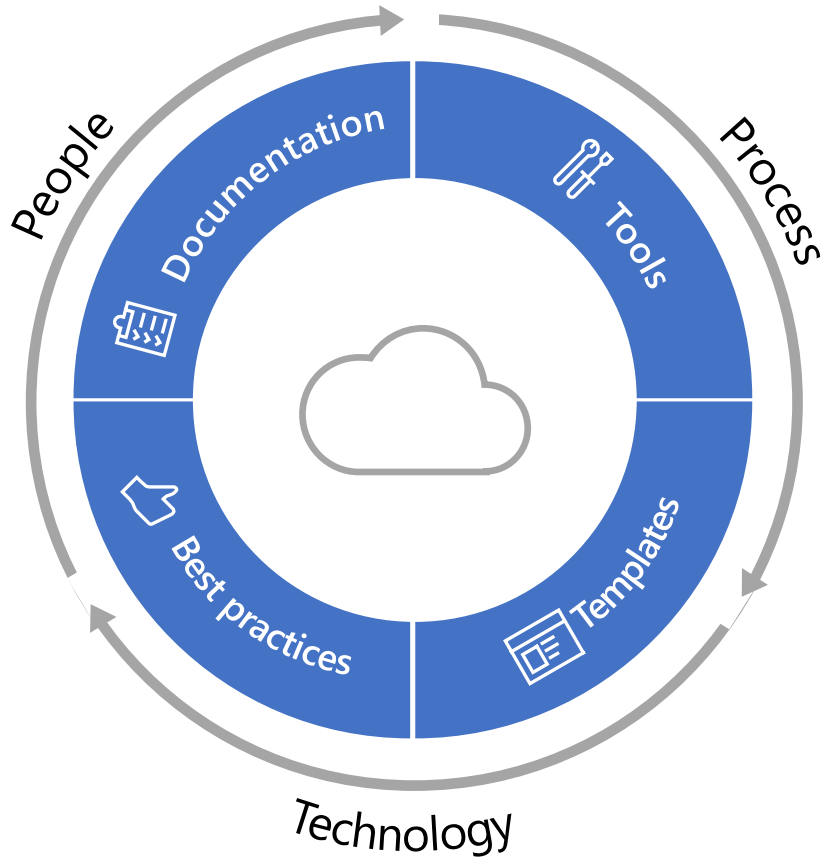
It requires a culture shift from within the organization

Modern business in the cloud is the new normal

Today's world reflects a new reality:
Technology is ever-present through the cloud, offering easy access to digital services…

Capitalizing on this shift is key for the organization's innovation and growth

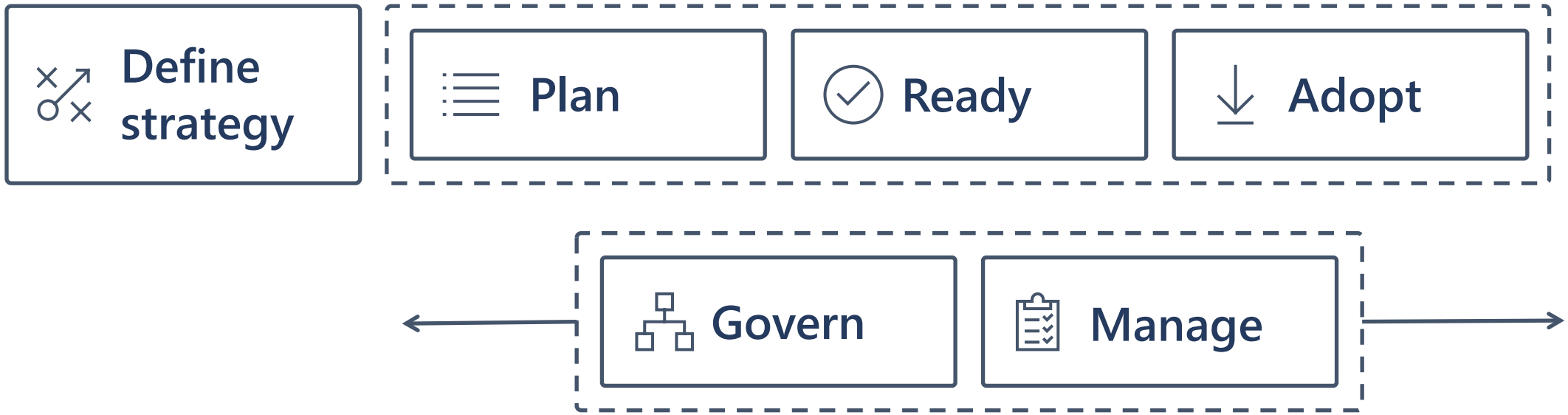
A Holistic Framework

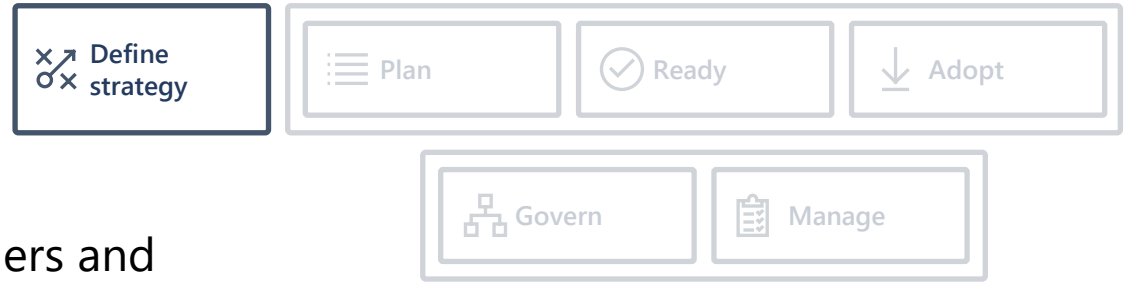


Align **business, people and technology strategy** to achieve business goals with **actionable, efficient, and comprehensive** guidance to deliver fast results with control and stability.

Building the framework

Modular approach, meeting the customer in their journey





Define strategy

Documenting the cloud strategy will help business stakeholders and technicians understand the benefits the organization is pursuing by adopting the cloud.

Motivations

- Executive mandate
- DC Exit
- Merger and acquisitions
- Cost savings
- Optimization
- Agility
- Tech capabilities
- Market demands
- Geo expansion
- Migration
- Innovation

Business outcomes

- **Fiscal:** revenue, cost, profit
- **Agility:** timer to market, provisioning,
- **Reach:** global access, sovereignty
- **Customer engagement:** cycle time, from request to release
- **Performance:** SLAs, Downtime, operations, reliability

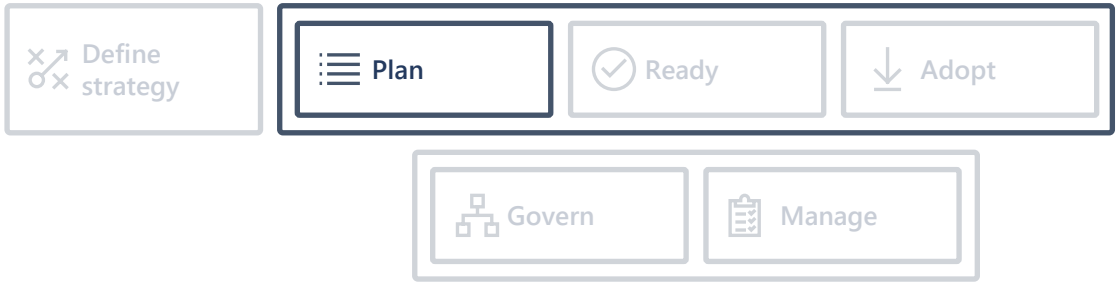
Business justification

- **Business case:** the cloud is not always cheaper, mirroring is not cloud, servers drive cost analysis
- **Financial model:** Capex/ Opex, ROI, gain, cost avoidance/reduction
- **Cloud accounting:** cost center, procurement, profit center, revenue generating, chargeback

First project

- **Business criteria:** workload supported by a BDM
- **Technical criteria:** minimum dependencies and test path, no governance
- **Qualitative analysis:** Current Team analysis

Plan



Cloud adoption plans convert the aspirational goals of the cloud adoption strategy into actions. It will help guide technical efforts, in alignment with the business strategy.

Digital estate

- **Rationalization:** inventory
- **Quantitative analysis:** asset optimized and sized properly
- **Qualitative analysis:** operational process

Initial organization alignment

- **Cloud Strategy Team**
  - Business IT: requirements and needs
  - IT management operations: traditional IT
  - Governance: executive sponsor, finance, business leadership, legal, security, HR
  - Cloud platform vendor: account success team
- **Cost management**
- **IT-business alignment**
- **Governance MVP**

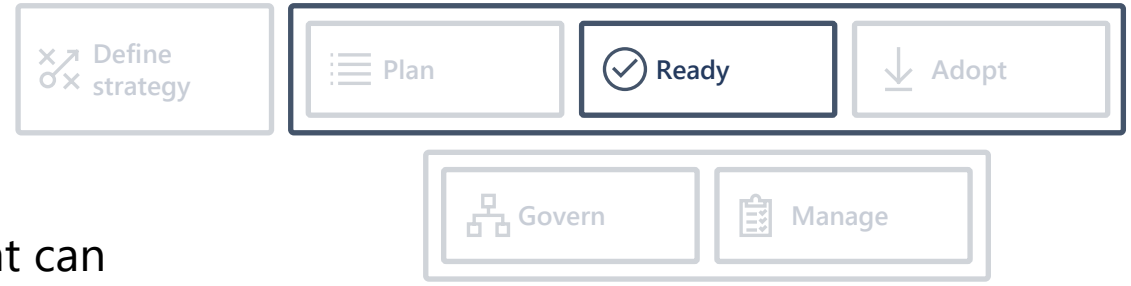
Skill readiness plan

- **Organizational readiness**
- **Governance and security alignment**
- **Initial organization alignment**
- **Building technical skills:** business/technical, and certifications
- **Change management guidance**

Cloud adoption plan

- **5R strategy:** rehost, refactor, rearchitect, rebuild, replace
- **Infrastructure migration:** VM, server, database focus
- **Application innovation:** born in the cloud applications, APIs
- **Data-driven innovation:** Focus on data consolidation and analysis

Ready



Ready establishes a cloud foundation or Adoption Target that can provide hosting for any adoption efforts. This should consist of common denominators across 80–90% of cloud adoption.

Azure readiness guide

- **Resource management:** management groups, subscriptions, resource groups, resources tree hierarchy
- **Naming Standards**
- **Resource tags**

Landing zone infrastructure

- **Network design:** Vnet, hybrid, firewall, hub, front door, endpoints
- **Storage design:** disk, file, blobs, CDN
- **Compute design:** VMs, containers, apps, serverless
- **Data design:** Structured/ unstructured

Landing zone ID

- **Identity and access**
- Role-based access control **RBAC**
- Manage to **least privilege**

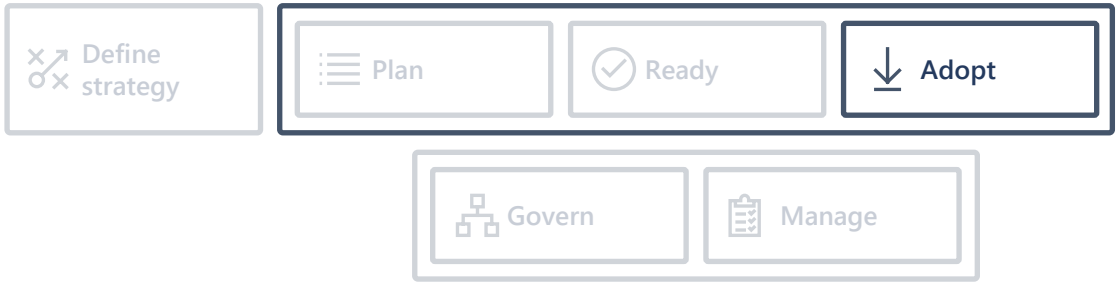
Landing zone cost

- **Costs and billing**
- Analyze **Cloud Costs**
- Monitor with **budgets**
- **Optimize** with recommendations
- **Manage** invoices and payments

Blueprints

- **AI**
- BigData
- Hybrid networks
- **Identity management**
- **IoT**
- **Serverless**
- **SAP**
- VMs
- WebApps
- DevOps

Adopt: Migrate



Cloud adoption will include workloads which do not warrant significant investments in the creation of new business logic. Those workloads could be moved to the migrated to the cloud.

Assess

- **Evaluate** assets and establish a plan
- **Validate pre-requisites:** landing zone, skilling
- **Drivers:** reducing capex, freeing up DC
- **Quantitative factors:** VMs, networking, compatibility
- **Qualitative factors:** process dependencies, critical business events

Migrate: rehost

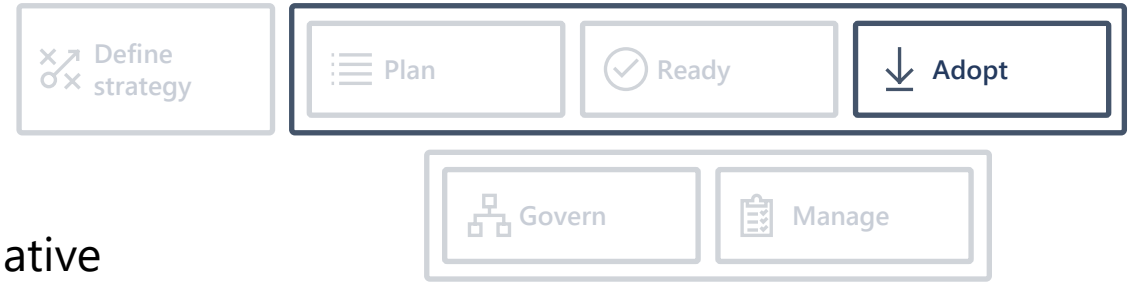
- **Replicate** (lift and shift) on-prem functionality using cloud native technology
- Leverage **Azure Migration Guide**

Optimize

- **Balance performance and price**
- Deliver the right experience **within budget**
- **Resize VM size, resize storage, resize database**

Secure and manage

- Prepare the migrated asset for ongoing operations: **security, monitoring, configuration**



Adopt: Innovate

Older apps can take advantage of many of the same cloud-native benefits by modernizing the solution or components of the solution. Modern DevOps invites into the process to create shorter feedback loops and better customer experiences.

Infrastructure abstraction

- Cloud native applications built from the ground up **optimized for cloud**: resiliency,
- Global scale
- Agility
- Security
- Autoscaling

Innovate: refactor

- Refactoring an application to fit a **PaaS/Serverless-based model** or refactoring code to deliver on new business opportunities.
- **Drivers:** faster and shorter updates, code portability, greater cloud efficiency (resources, speed, cost)

Innovate: rearchitect

- Modify existing applications into managed **containers** to take advantage of cloud native benefits
- **Drivers:** application scale and agility, easier adoption of new cloud capabilities, mix of technology stacks

Innovate: rebuild

- A new code base is created to align with a **cloud-native** approach. **App Data and AI Services**
- **Drivers:** accelerate innovation, build apps faster, reduce operational cost

DevOps

- Culture
- Development
- Testing
- Release
- Monitoring
- Management

Govern

Policy definition ensures consistency across adoption efforts. Alignment to governance/compliance requirements is key to maintain a well-managed cross-cloud environment.

Business risk

- **Document** evolving business risk
- Document risk tolerance based on **data classification**, and **application criticality**

Policy & compliance

- Convert risk decisions into **policy statements**
- Establish cloud adoption boundaries

Processes

- Establish processes to **monitor violations**
- Adhere to corporate policies
- **Cloud Center of Excellence**

Cost management

- Evaluate and monitor cost
- Limit IT spend
- Scale based on business demand
- Create cost accountability

Security baseline

- Compliance with IT Security requirements
- Apply security baseline to all adoption efforts

Resource consistency

- Consistency in resource configuration
- Enforce on boarding, recovery and discoverability practices

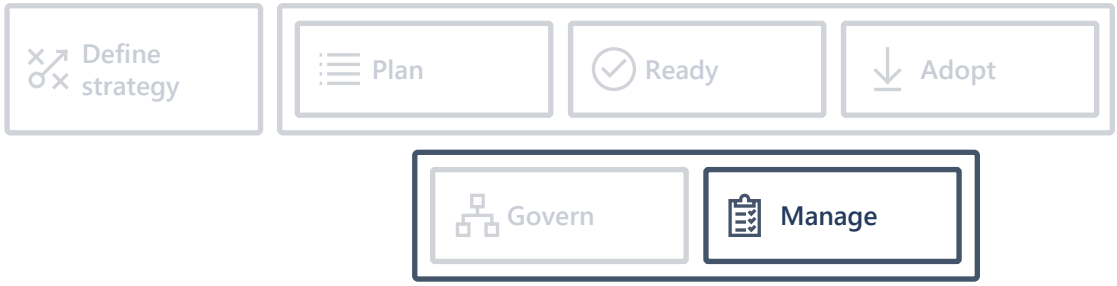
Identity baseline

- Enforce identity and access baseline
- Apply role definitions and assignments

Deployment acceleration

- Centralize templates
- Drive consistency and standardization

Manage and operations



Manage and operations enumerates, implements, and iteratively reviews related to the expected operational behavior of the service.

Management

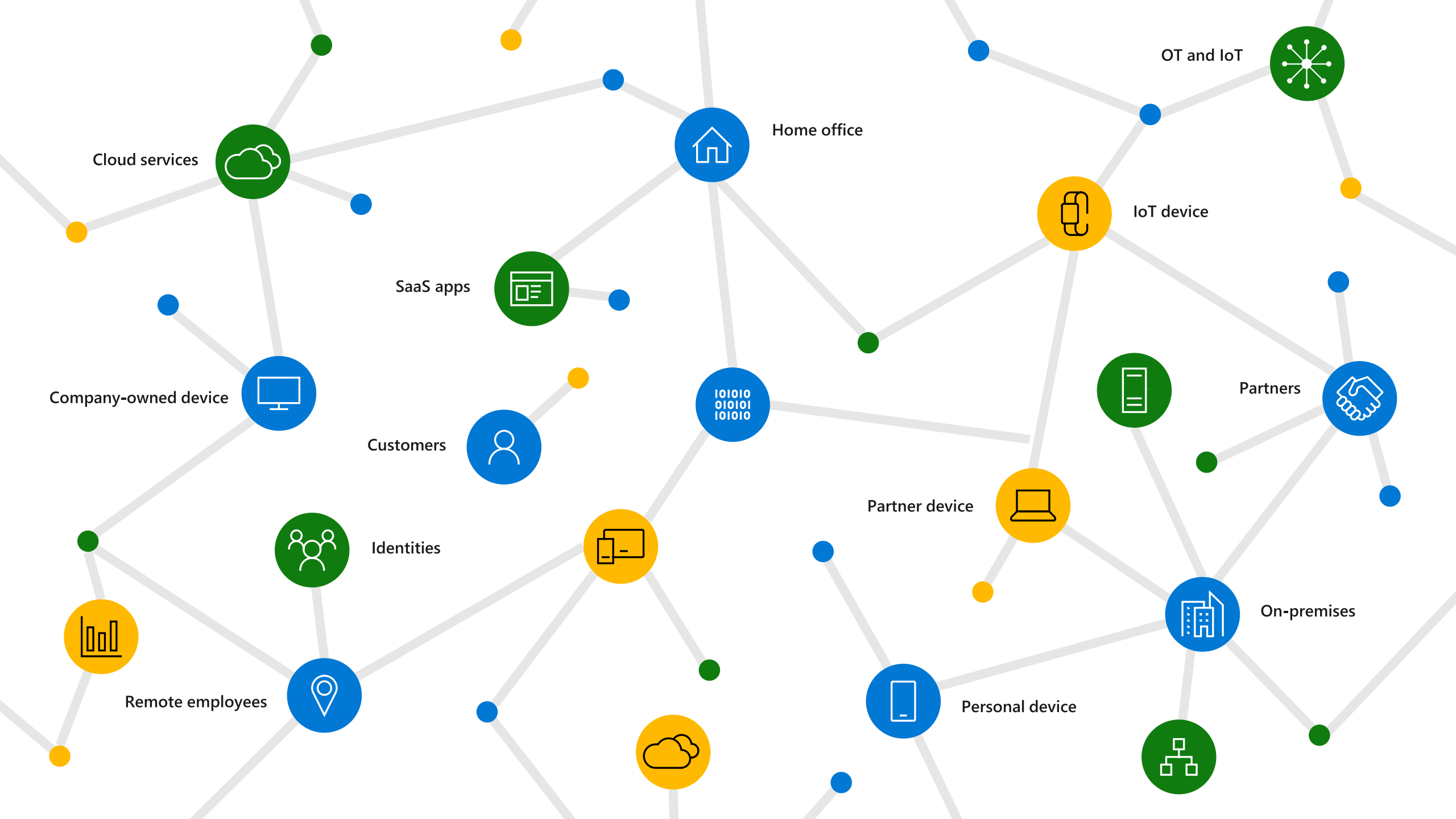
- Identify critical operations for business operations
- Map operations to services
- Analyze services dependencies
- Create high level view service dashboards

Monitoring

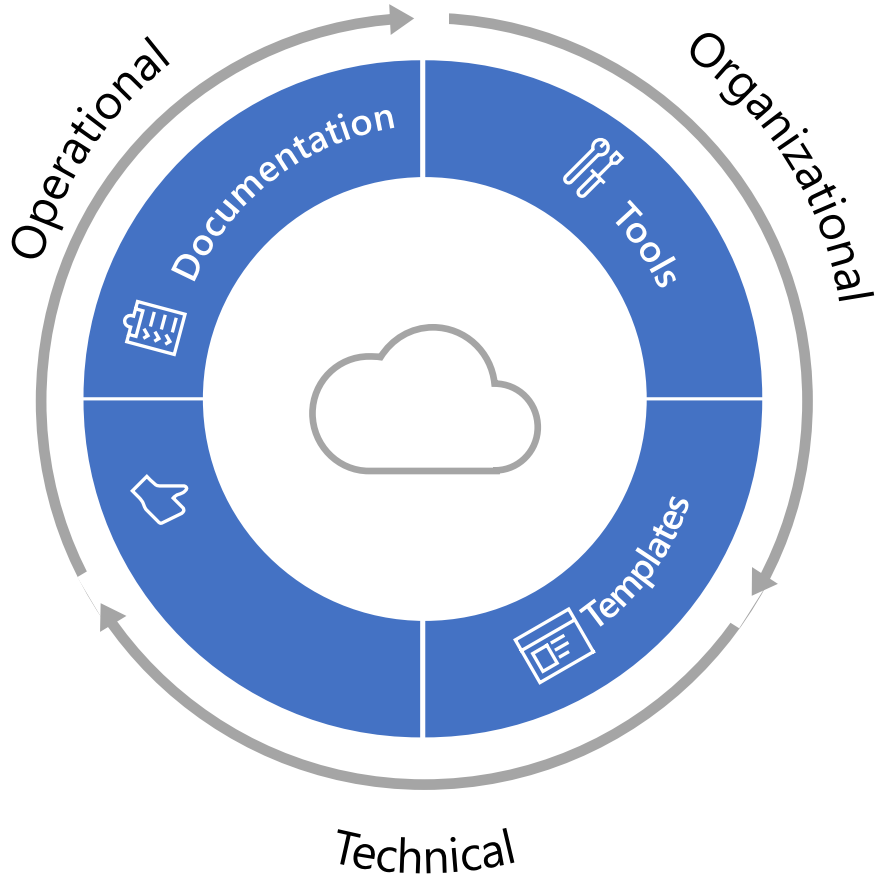
- Enable data collection
- Identify operations baseline
- Generate alerts
- Measure Service Metrics and generate SLAs

Resiliency

- **Enable a resilient** platform
- Recover from failures with minimal downtime and minimum data loss before
- **Evolve to a highly available platform**


OT and IoT
Cloud services
Home office
IoT device
SaaS apps
Partners
Company-owned device
Customers
Partner device
Identities
On-premises
Remote employees
Personal device

A Holistic Framework



Align **Organizational Framework, Operational Controls and the Technical strategy** to achieve business goals with **actionable, efficient, and comprehensive** guidance to deliver fast results with control and stability.

Focused Security

Comprehensive visibility, automation, and intelligence

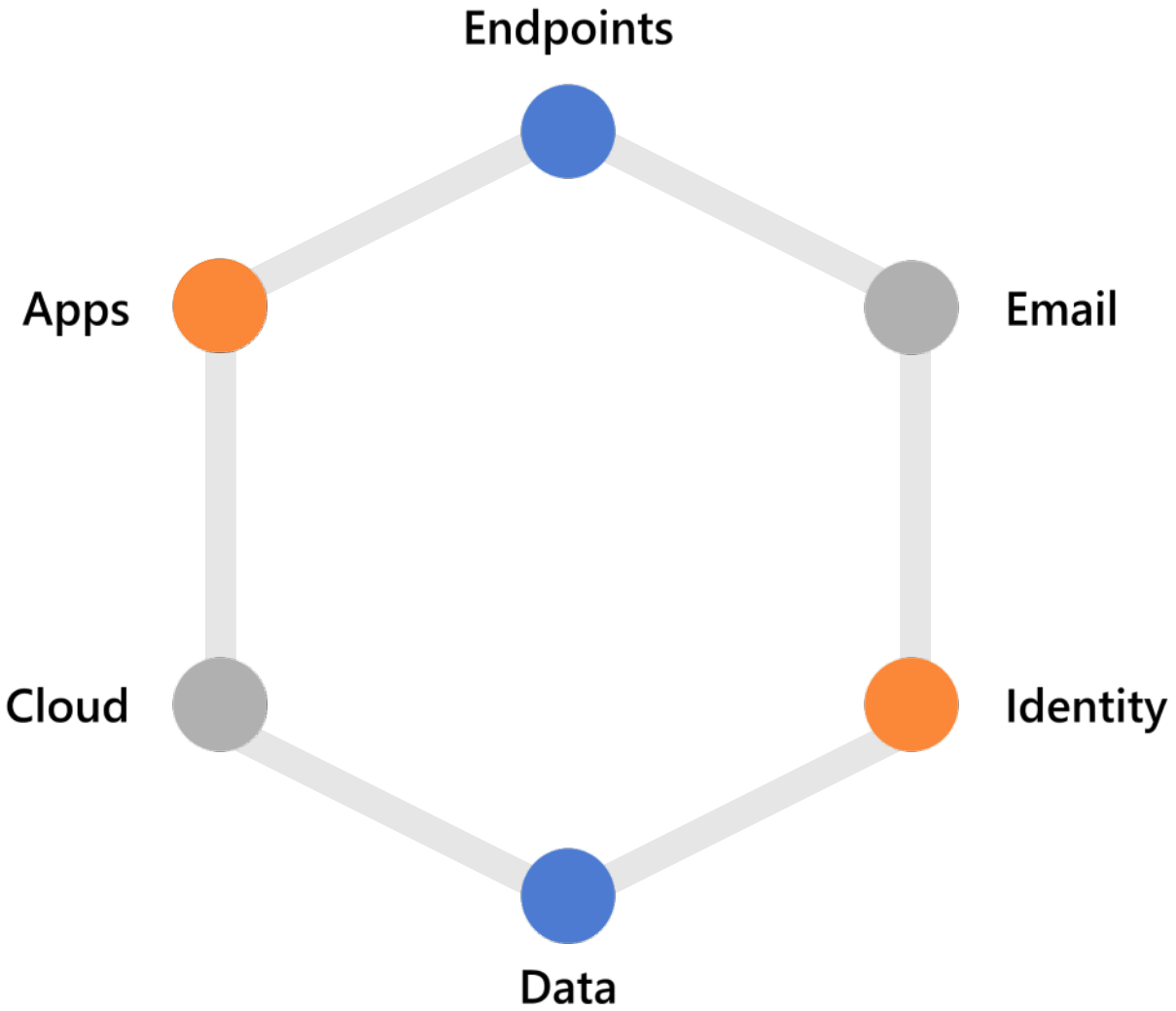
Protect
everything

Simplify
the complex

Catch
what others miss

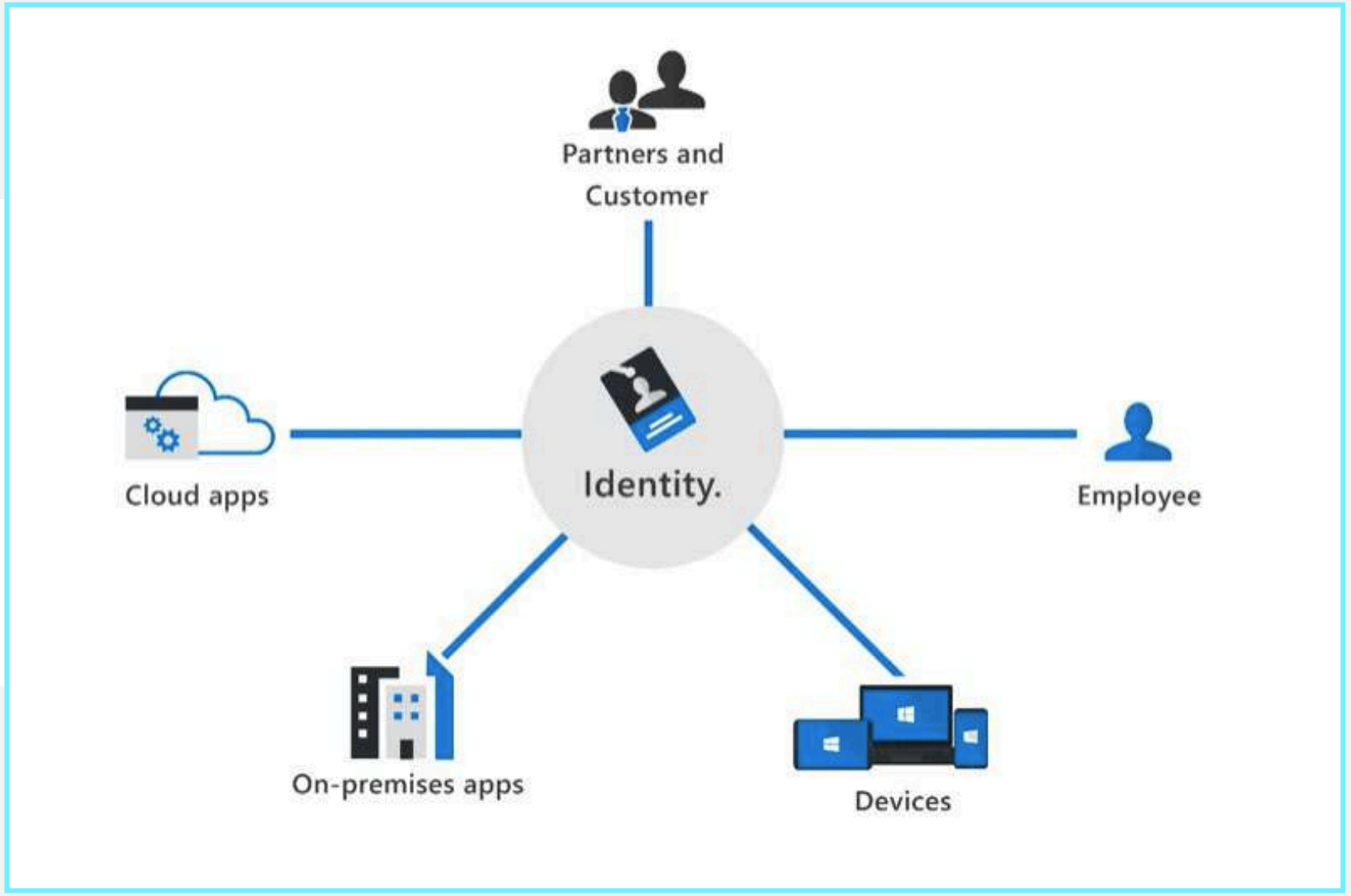
Grow
your future

Holistic Approach to the Protection Levels

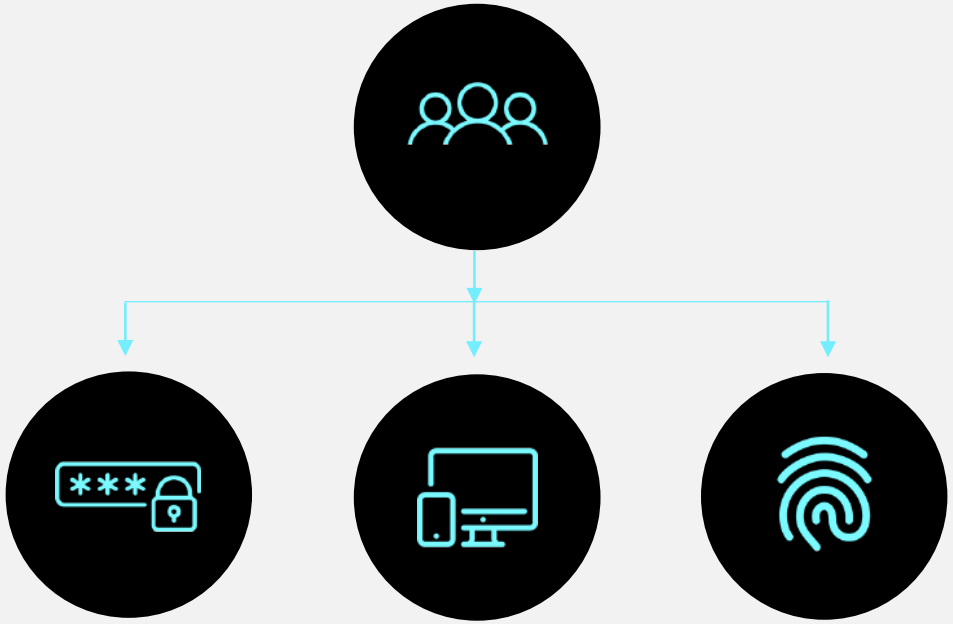


Identity as a security Perimeter

- Identity enables organizations to secure their assets
- An identity may be associated with a user, an application, a device, or something else



Authentication

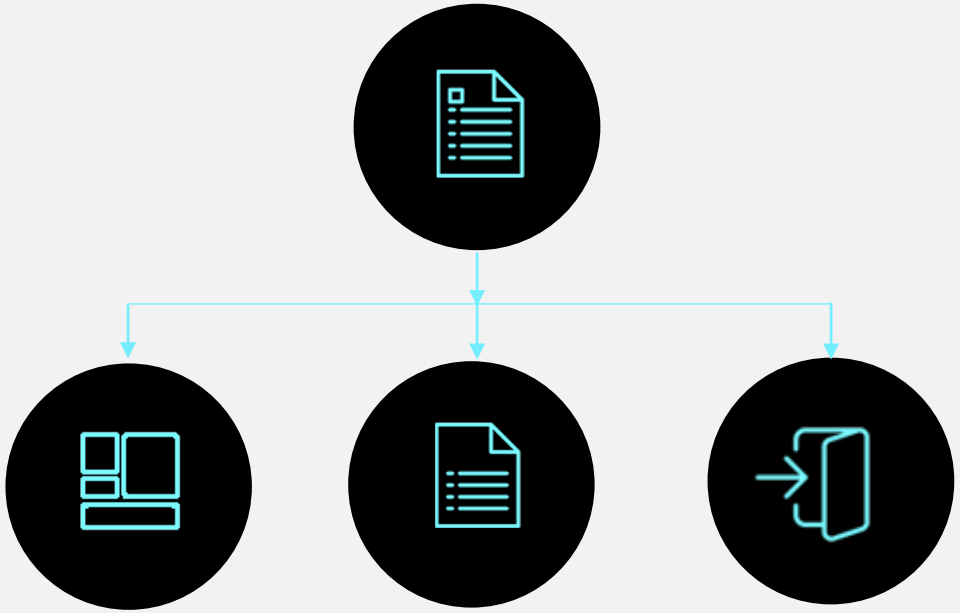


Something you know

Something you have

Something you are

Authorization



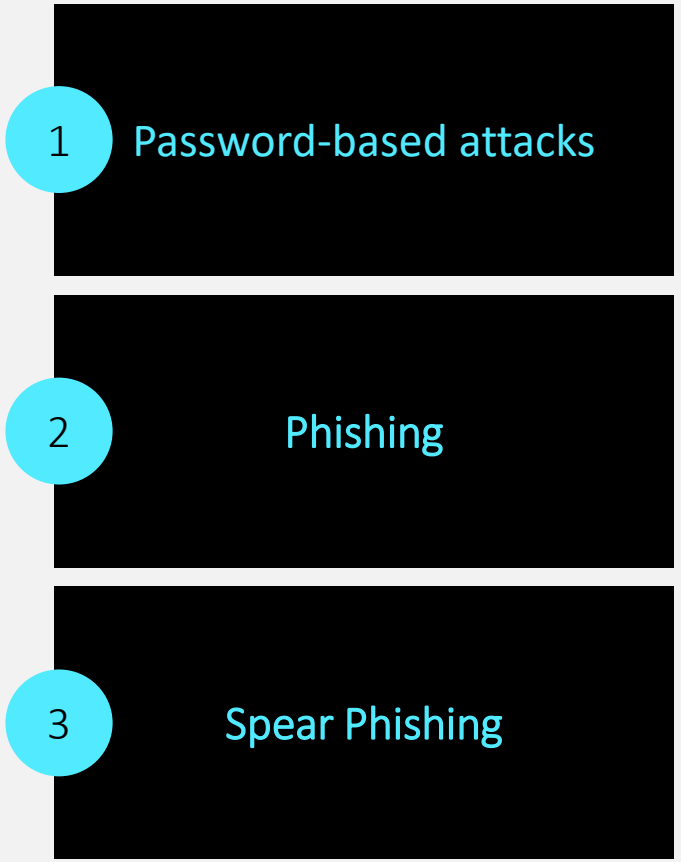
Apps & resources

Data

Access level

Common Identity Attacks

- Attacks are designed to steal the credentials
- The result is identity theft



Moving from Implicit Trust to Zero Trust

Unauthenticated Network Identifiers

Request context

Implicit Trust

Allowed

Static policy

Full Access

No Access

Level of access permitted

Identity

Device

Application

Network

Infrastructure

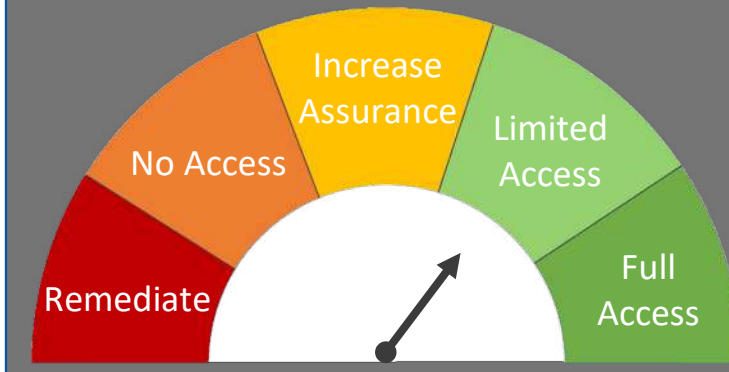
Data

Request context

Zero Trust

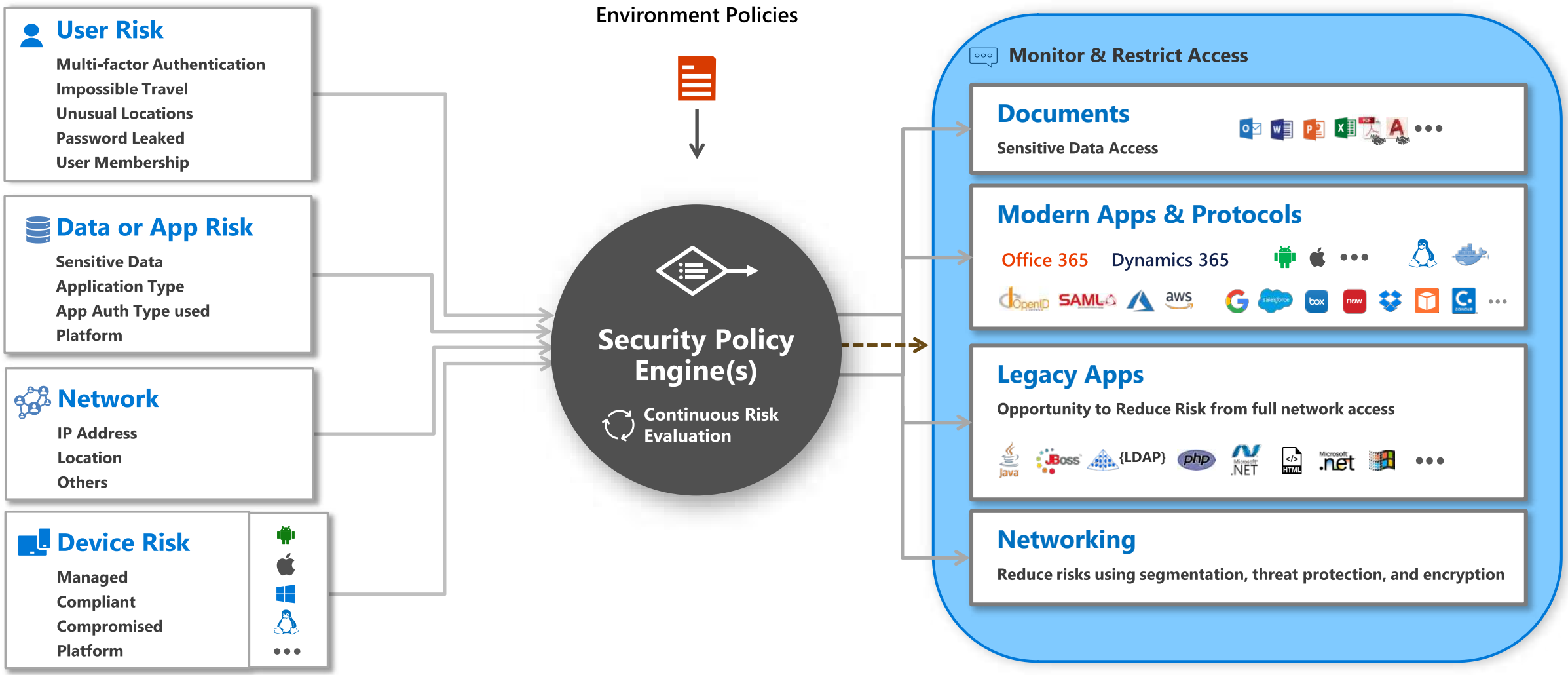
Known **Trusted** **Allowed**

Dynamic policy with continuous monitoring

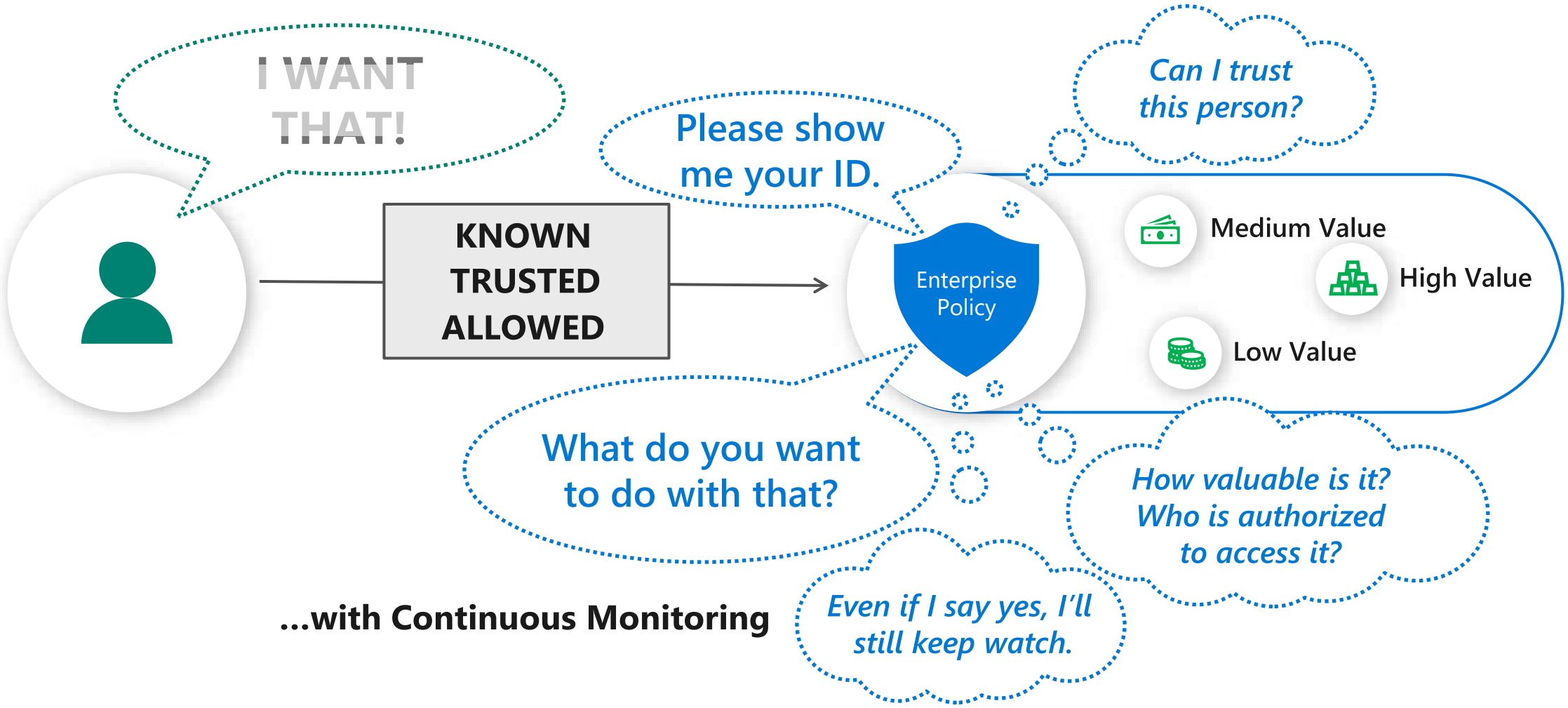


Level of access permitted

Zero Trust Architecture (ZTA)

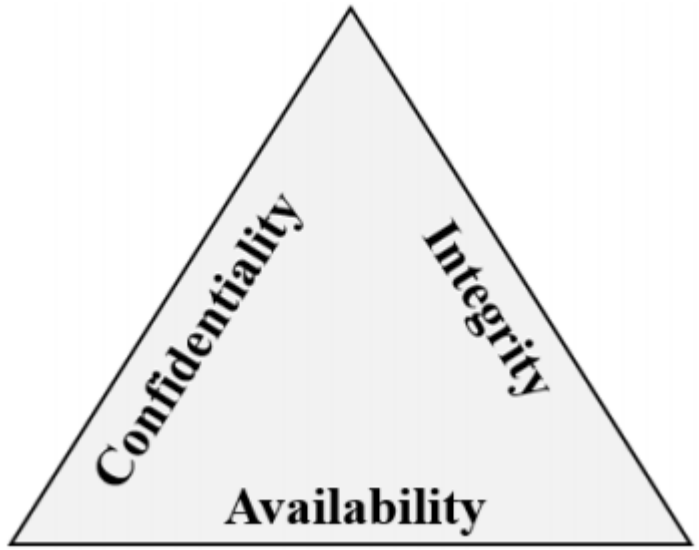


How Zero Trust works



Confidentiality, Integrity, Availability(CIA)

- Confidentiality, Integrity, Availability, or CIA, is a way to think about security trade-offs
- This is not a Microsoft model, but is common to all security professionals



Thank you!