This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2023-08159C

Sandia National Laboratories

Exceptional service in the national interest

Zero Trust

Strategizing and operating toward a Zero Trust model in the Cloud

Presenters

Ben Ybarra, *Enterprise Cloud Services* | *btybarr@sandia.gov*

SAND

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and wholly owned subsidiary of Honeywell International Inc. for the U.S. onal Nuclear Security Administration under contract DE-NA0003525.

Zero Trust Principals

Verify Explicitly

Always authenticate and authorize based on all available data points.

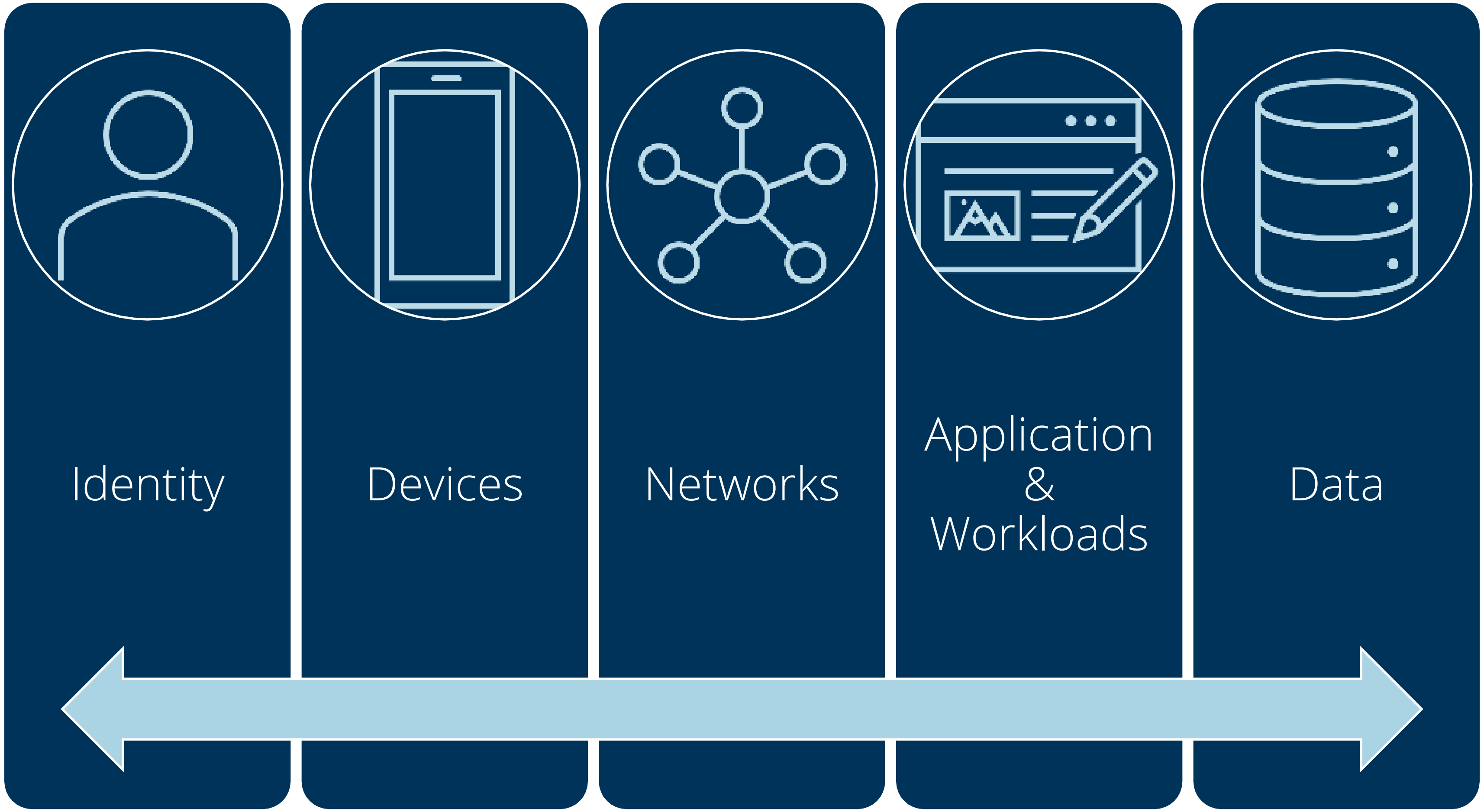
Enforce Least Privileged Access

Azure implementation leverages Azure RBAC for all services. Privileged roles are controlled and granted on a least privileged model. The Identity team validates a request before granting Just-Enough-Access (JEA) to Cloud Administrators. Azure AD Privileged Identity Management (PIM) is used for Just-In-Time (JIT) Administration to limit the attack surface.

Assume Breach

Minimize the surface attack for breaches and prevent lateral movement by segmenting access to network, users, devices, and applications. All access and services are segmented to prevent lateral movement including applications and services. Developers are required to segment out service principals based on level of graph permissions. If a portion of an application gets compromised the architecture minimizes the surface attack. Azure provides greater visibility into all services and resources. Events are fed directly into Azure Sentinel for analysis.

Zero Trust – Foundational Elements



Identity

Devices

Networks

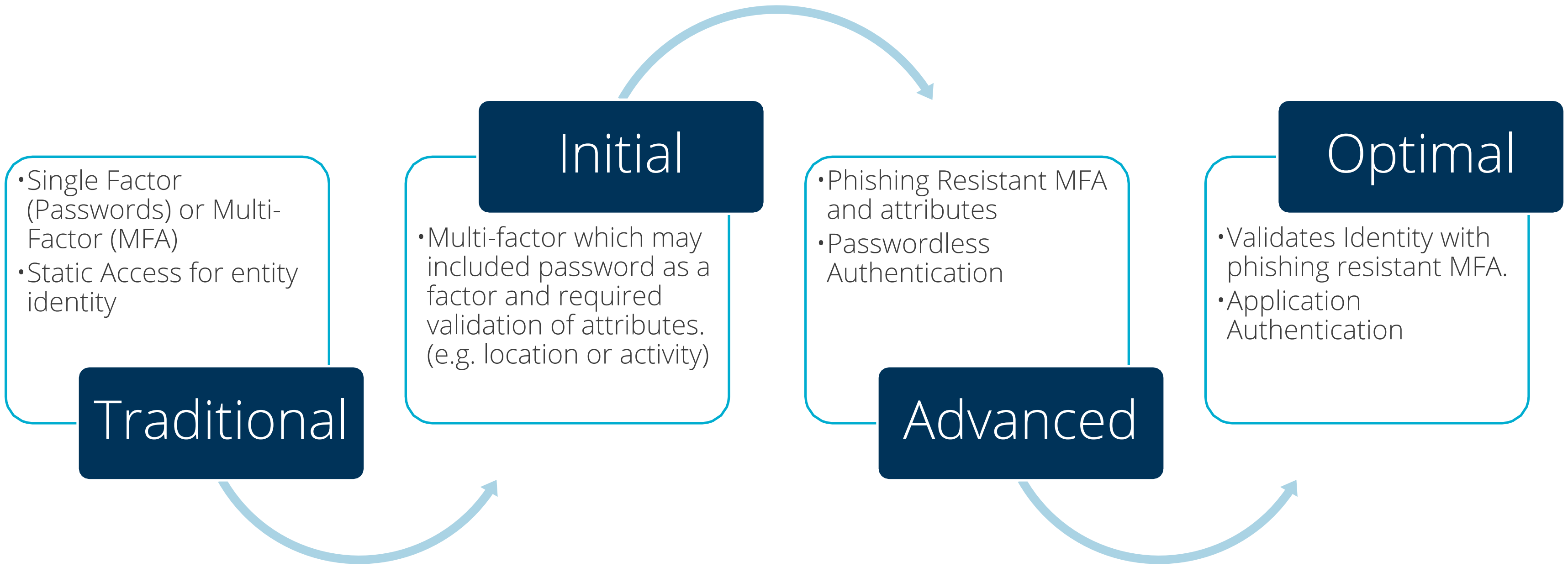
Application
&
Workloads

Data

Identity

<table>
<tr><th colspan="6">Maturity Area</th></tr>
<tr><td>Authentication</td><td>Identity Store</td><td>Risk Assessments</td><td>Access Management</td><td>Visibility and Analytics Capability</td><td>Automation and Orchestration</td></tr>
</table>

Identity - Authentication



Traditional

- Single Factor (Passwords) or Multi-Factor (MFA)
- Static Access for entity identity

Initial

- Multi-factor which may included password as a factor and required validation of attributes. (e.g. location or activity)

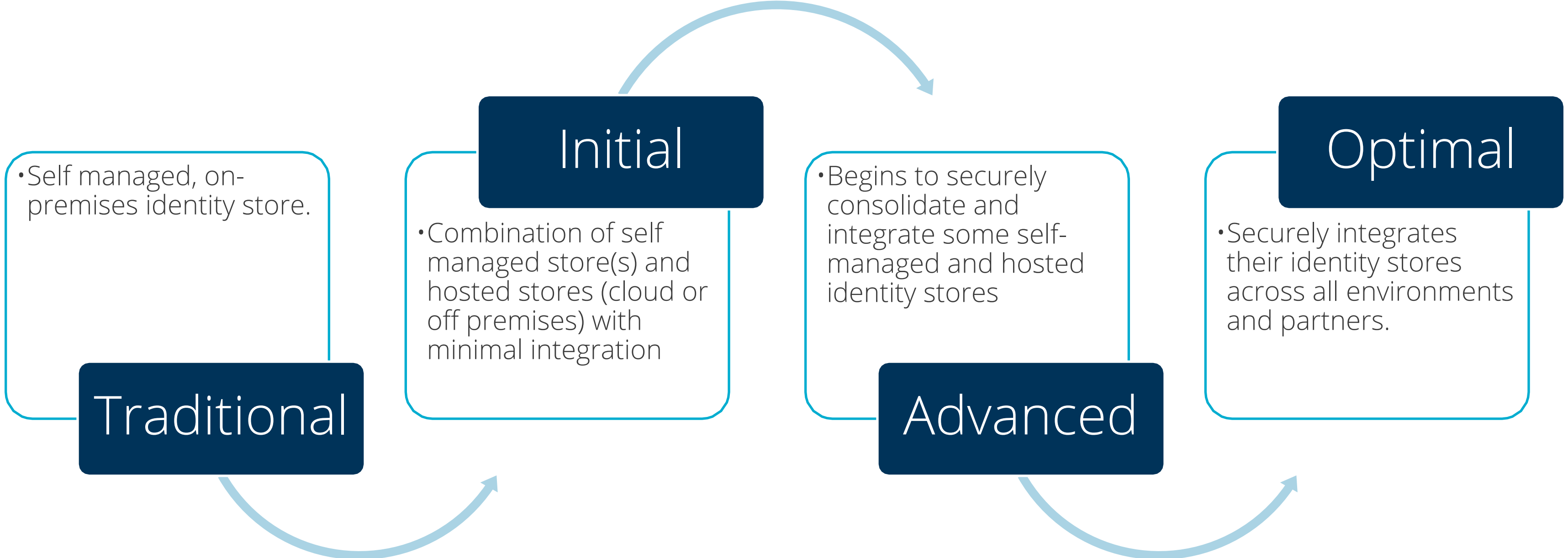
Advanced

- Phishing Resistant MFA and attributes
- Passwordless Authentication

Optimal

- Validates Identity with phishing resistant MFA.
- Application Authentication

Identity - Stores



Traditional

- Self managed, on-premises identity store.

Initial

- Combination of self managed store(s) and hosted stores (cloud or off premises) with minimal integration

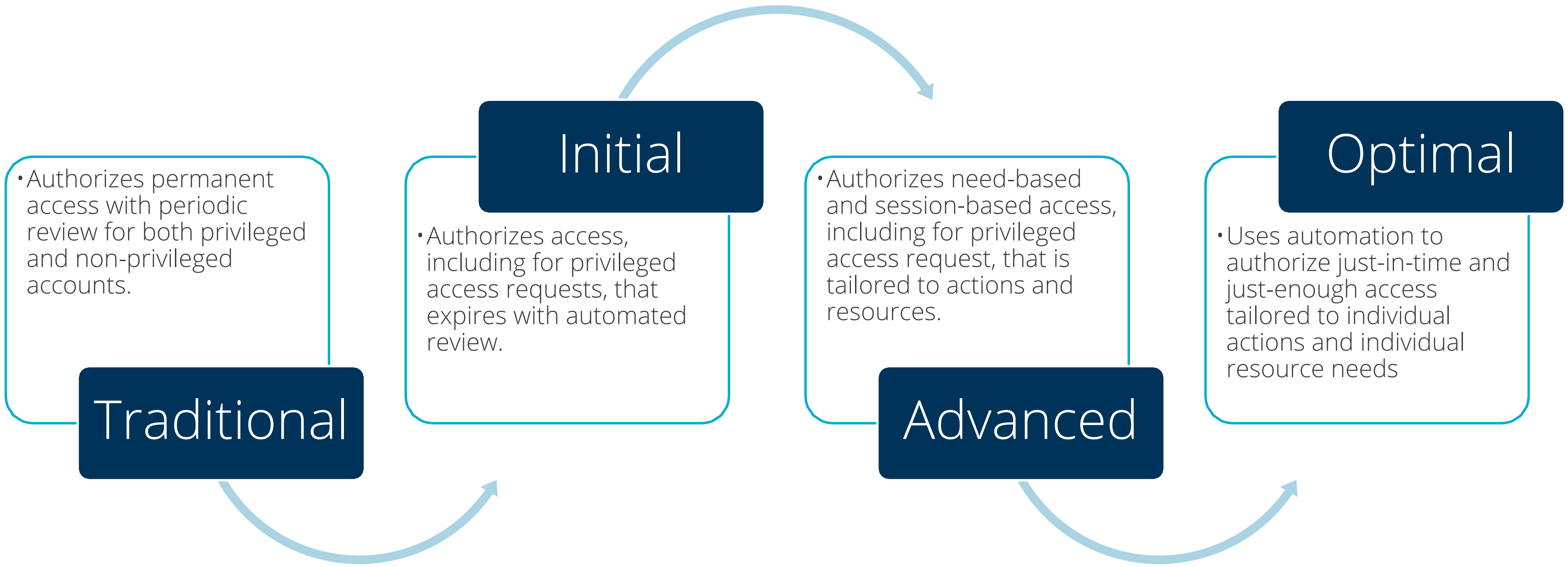
Advanced

- Begins to securely consolidate and integrate some self-managed and hosted identity stores

Optimal

- Securely integrates their identity stores across all environments and partners.

Identity – Access Management



Traditional

- Authorizes permanent access with periodic review for both privileged and non-privileged accounts.

Initial

- Authorizes access, including for privileged access requests, that expires with automated review.

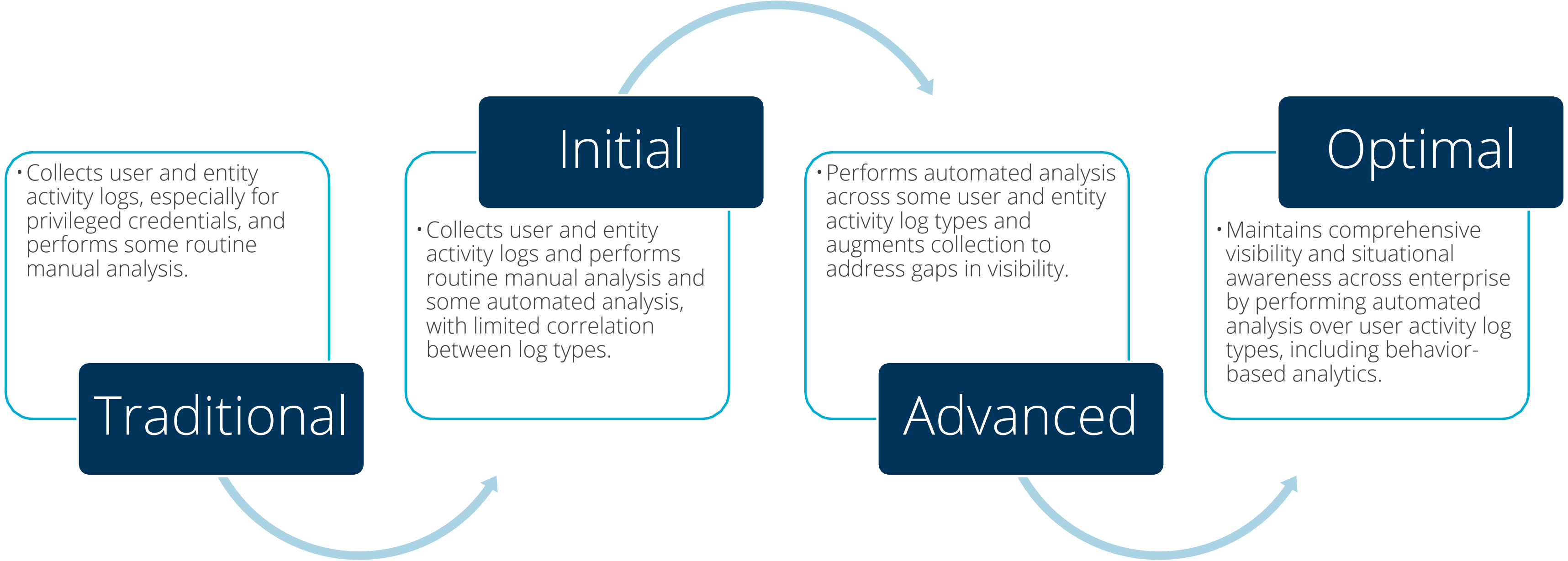
Advanced

- Authorizes need-based and session-based access, including for privileged access request, that is tailored to actions and resources.

Optimal

- Uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs

Identity – Visibility and Analytics Capability



Traditional

- Collects user and entity activity logs, especially for privileged credentials, and performs some routine manual analysis.

Initial

- Collects user and entity activity logs and performs routine manual analysis and some automated analysis, with limited correlation between log types.

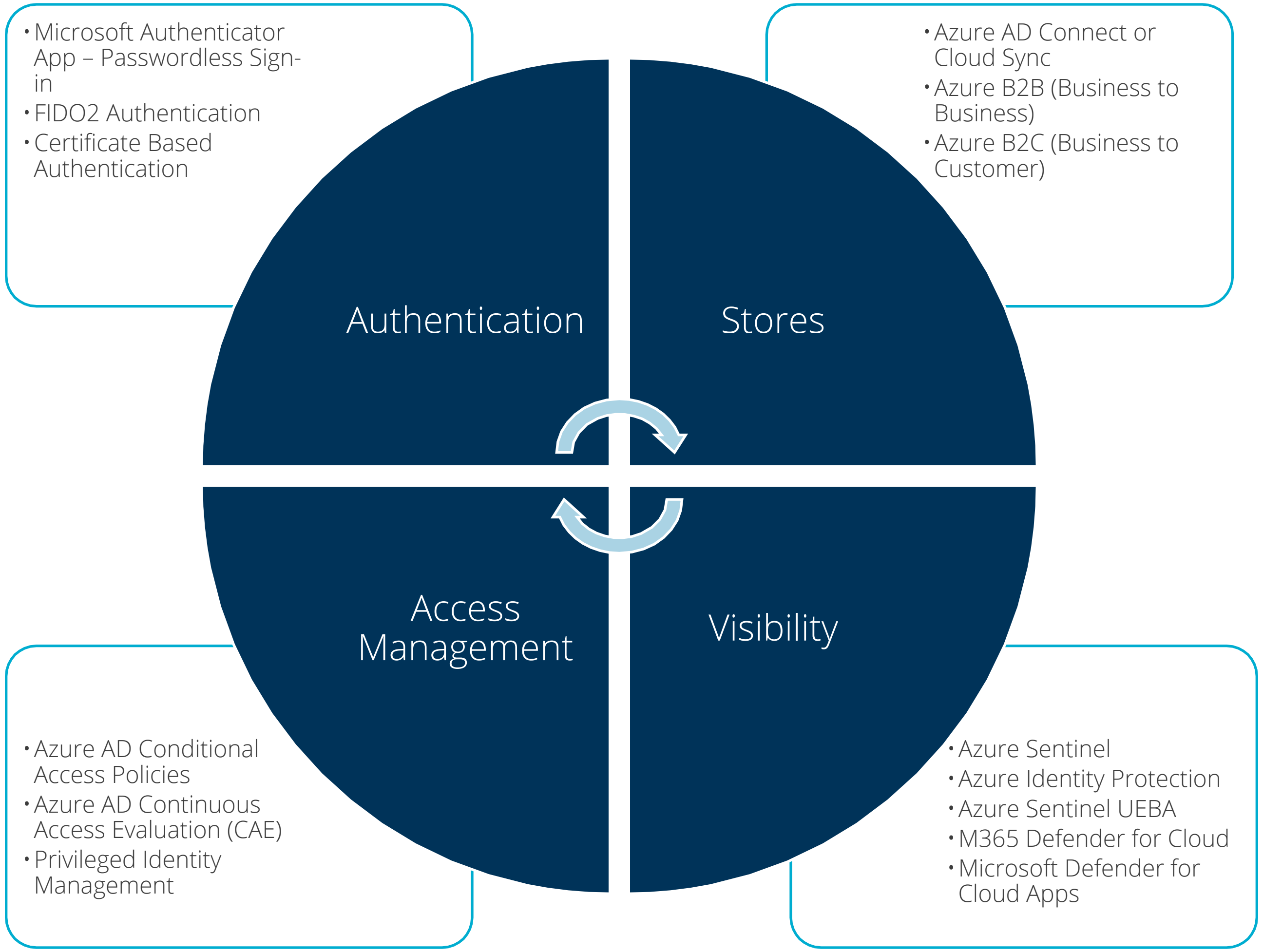
Advanced

- Performs automated analysis across some user and entity activity log types and augments collection to address gaps in visibility.

Optimal

- Maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behavior-based analytics.

Identity



Authentication

- Microsoft Authenticator App – Passwordless Sign-in
- FIDO2 Authentication
- Certificate Based Authentication

Stores

- Azure AD Connect or Cloud Sync
- Azure B2B (Business to Business)
- Azure B2C (Business to Customer)

Access Management

- Azure AD Conditional Access Policies
- Azure AD Continuous Access Evaluation (CAE)
- Privileged Identity Management

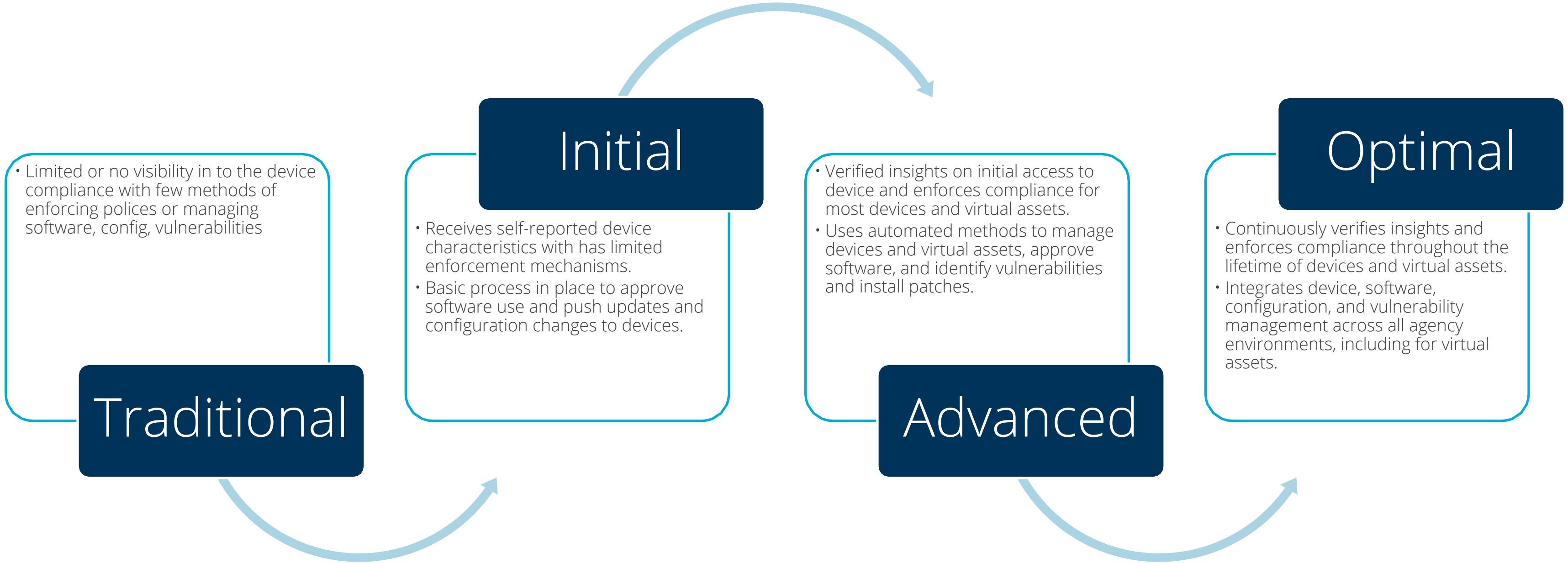
Visibility

- Azure Sentinel
- Azure Identity Protection
- Azure Sentinel UEBA
- M365 Defender for Cloud
- Microsoft Defender for Cloud Apps

Devices

Maturity Area						
Policy Enforcement & Compliance Monitoring	Asset & Supply Chain Risk Management	Resource Access	Device Threat Protection	Visibility and Analytics Capability	Automation and Orchestration Capability	Governance Capability

Devices – Policy Enforcement & Compliance Monitoring



Traditional

- Limited or no visibility in to the device compliance with few methods of enforcing polices or managing software, config, vulnerabilities

Initial

- Receives self-reported device characteristics with has limited enforcement mechanisms.
- Basic process in place to approve software use and push updates and configuration changes to devices.

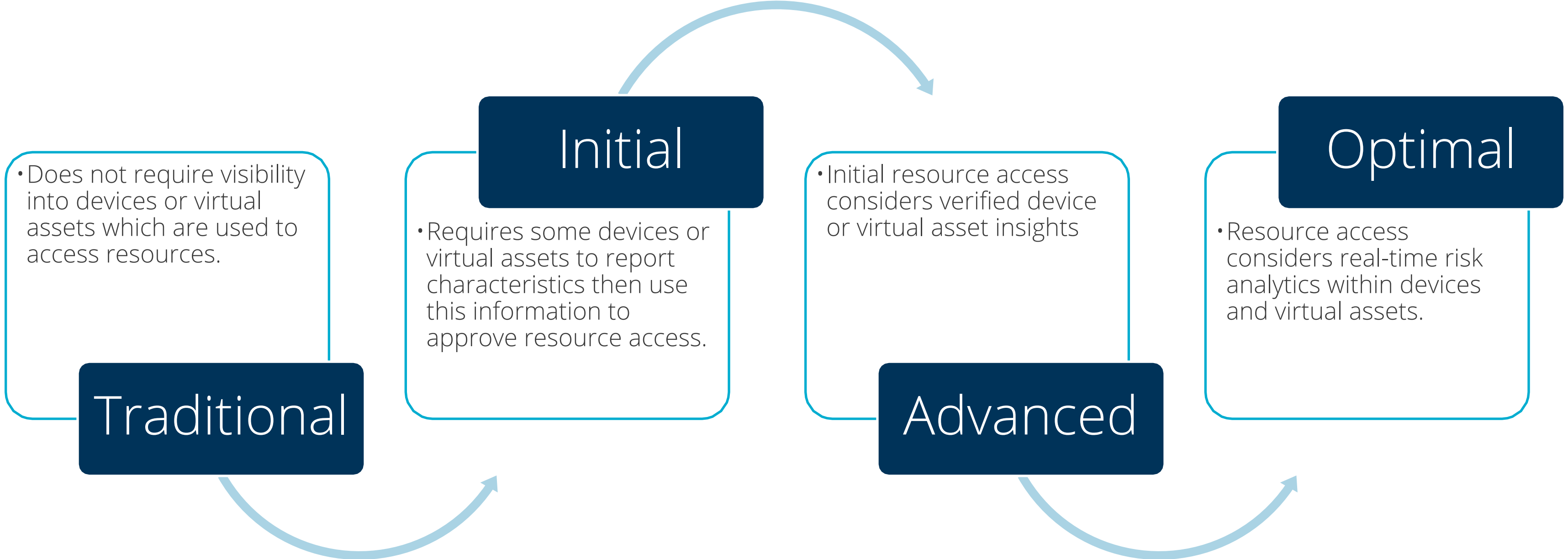
Advanced

- Verified insights on initial access to device and enforces compliance for most devices and virtual assets.
- Uses automated methods to manage devices and virtual assets, approve software, and identify vulnerabilities and install patches.

Optimal

- Continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets.
- Integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets.

Devices – Resource Access



Traditional

- Does not require visibility into devices or virtual assets which are used to access resources.

Initial

- Requires some devices or virtual assets to report characteristics then use this information to approve resource access.

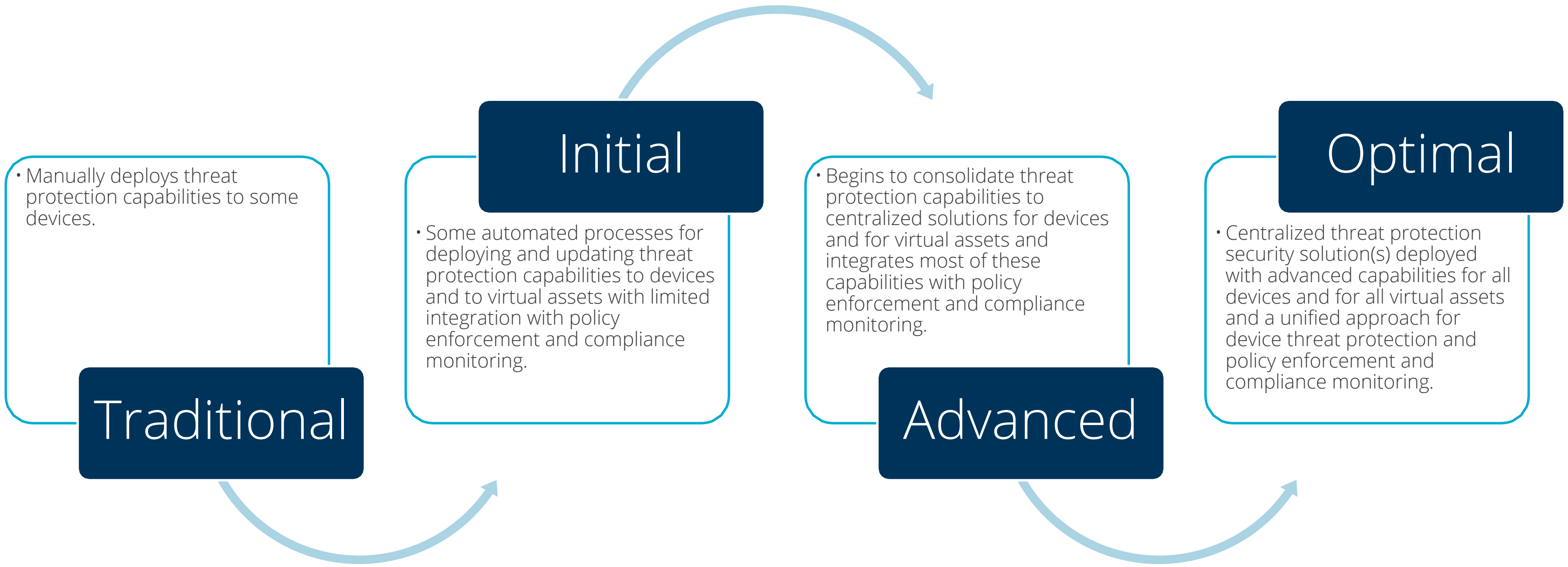
Advanced

- Initial resource access considers verified device or virtual asset insights

Optimal

- Resource access considers real-time risk analytics within devices and virtual assets.

Devices – Device Threat Protection



Traditional

- Manually deploys threat protection capabilities to some devices.

Initial

- Some automated processes for deploying and updating threat protection capabilities to devices and to virtual assets with limited integration with policy enforcement and compliance monitoring.

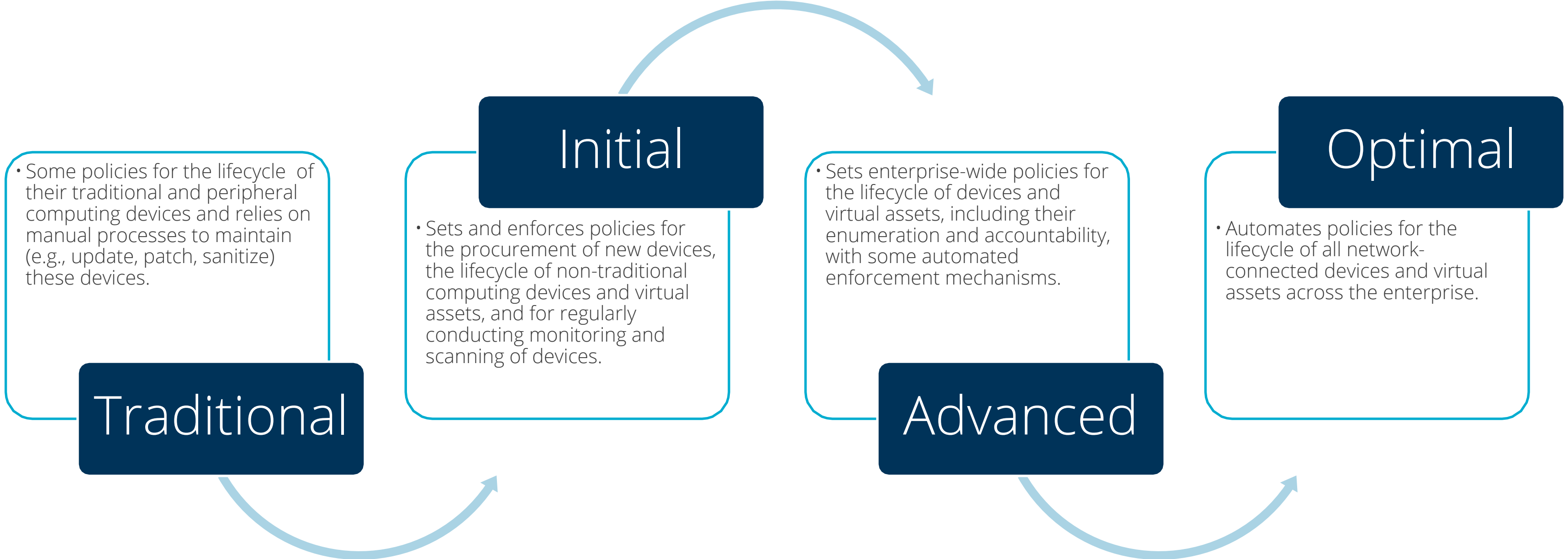
Advanced

- Begins to consolidate threat protection capabilities to centralized solutions for devices and for virtual assets and integrates most of these capabilities with policy enforcement and compliance monitoring.

Optimal

- Centralized threat protection security solution(s) deployed with advanced capabilities for all devices and for all virtual assets and a unified approach for device threat protection and policy enforcement and compliance monitoring.

Devices – Governance Capability



Traditional

- Some policies for the lifecycle of their traditional and peripheral computing devices and relies on manual processes to maintain (e.g., update, patch, sanitize) these devices.

Initial

- Sets and enforces policies for the procurement of new devices, the lifecycle of non-traditional computing devices and virtual assets, and for regularly conducting monitoring and scanning of devices.

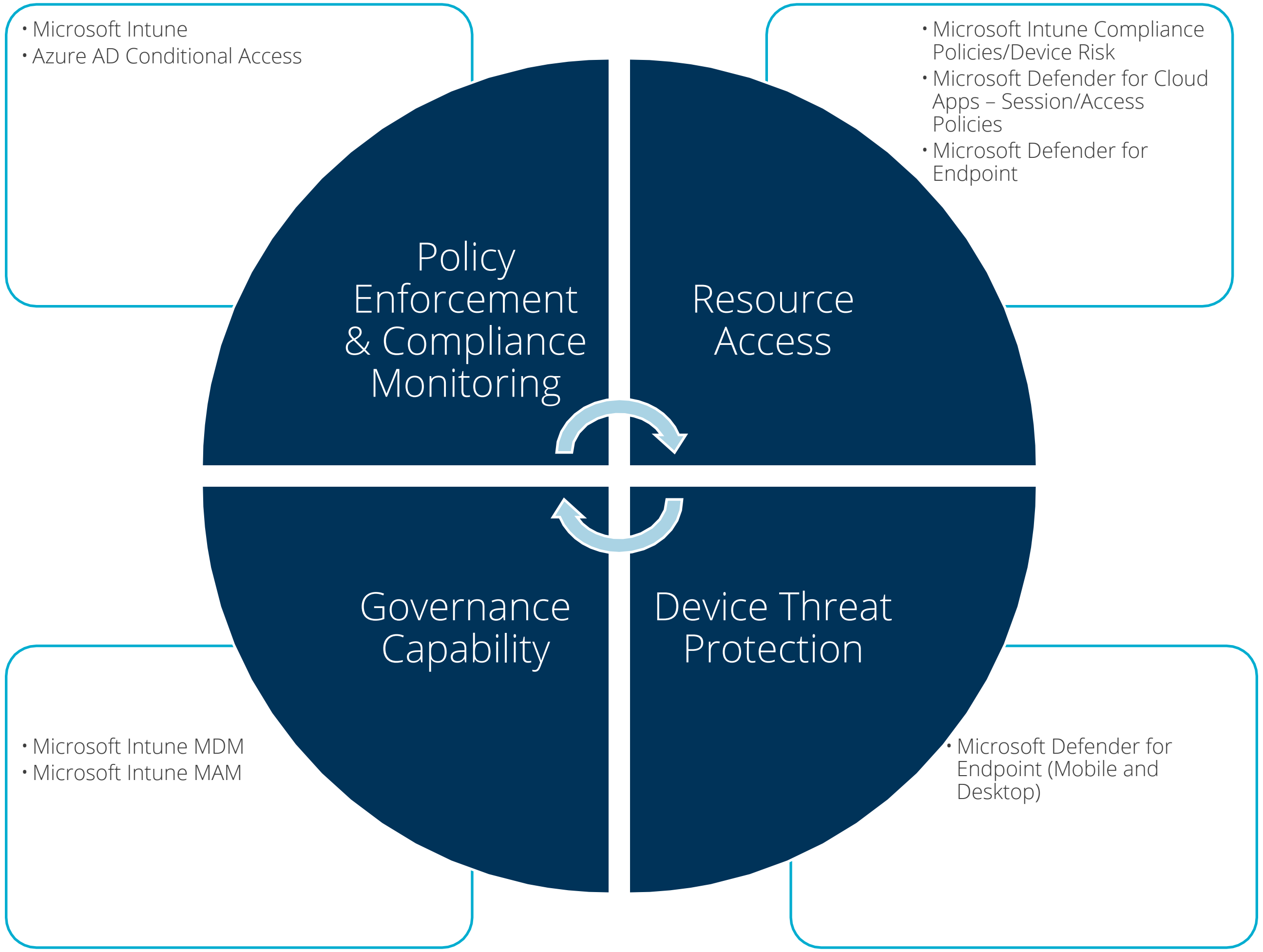
Advanced

- Sets enterprise-wide policies for the lifecycle of devices and virtual assets, including their enumeration and accountability, with some automated enforcement mechanisms.

Optimal

- Automates policies for the lifecycle of all network-connected devices and virtual assets across the enterprise.

Devices



Policy Enforcement & Compliance Monitoring

- Microsoft Intune
- Azure AD Conditional Access

Resource Access

- Microsoft Intune Compliance Policies/Device Risk
- Microsoft Defender for Cloud Apps – Session/Access Policies
- Microsoft Defender for Endpoint

Governance Capability

- Microsoft Intune MDM
- Microsoft Intune MAM

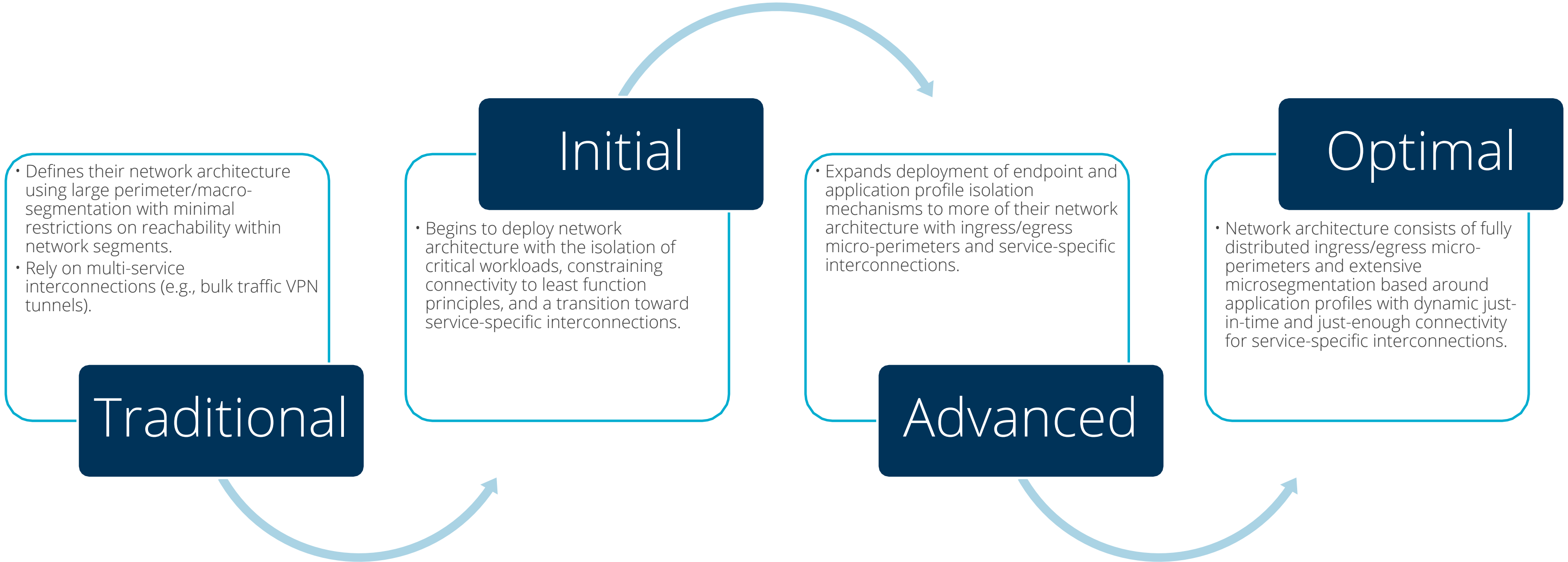
Device Threat Protection

- Microsoft Defender for Endpoint (Mobile and Desktop)

Network

Maturity Area						
Network Segmentation	Network Traffic Management	Traffic Encryption	Network Resilience	Visibility and Analytics Capability	Automation and Orchestration Capability	Governance Capability

Network - Segmentation



Traditional

- Defines their network architecture using large perimeter/macro-segmentation with minimal restrictions on reachability within network segments.
- Rely on multi-service interconnections (e.g., bulk traffic VPN tunnels).

Initial

- Begins to deploy network architecture with the isolation of critical workloads, constraining connectivity to least function principles, and a transition toward service-specific interconnections.

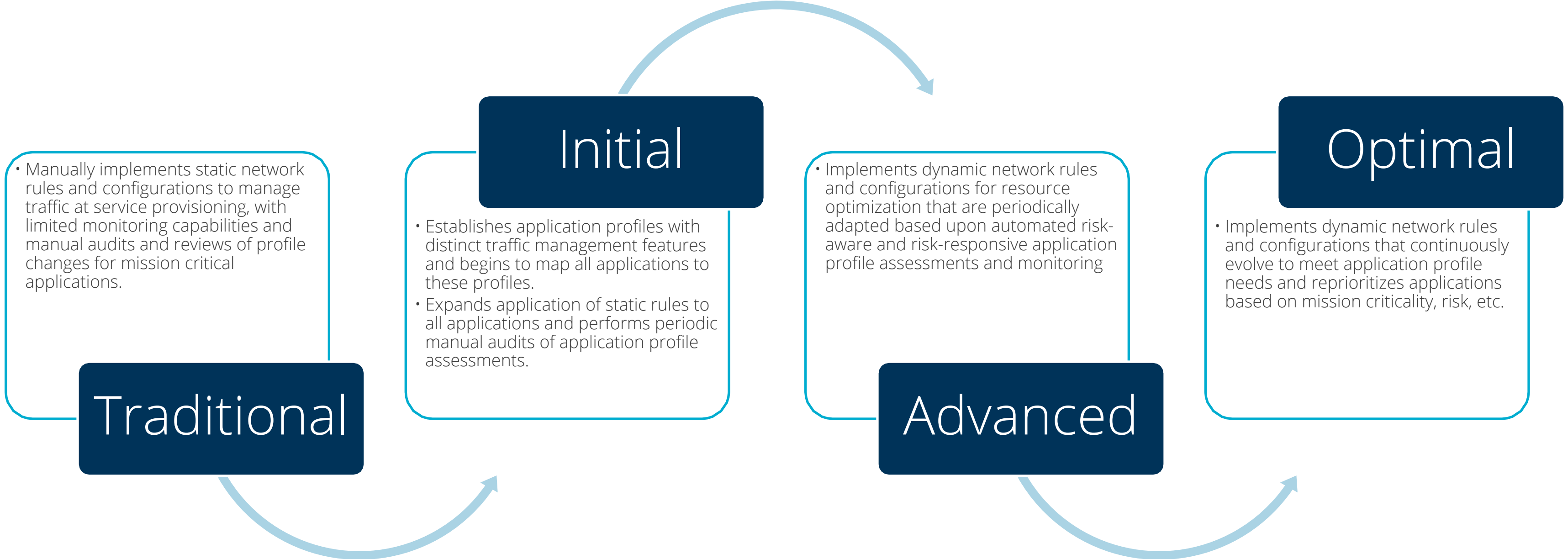
Advanced

- Expands deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress micro-perimeters and service-specific interconnections.

Optimal

- Network architecture consists of fully distributed ingress/egress micro-perimeters and extensive microsegmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections.

Network – Traffic Management



Traditional

- Manually implements static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities and manual audits and reviews of profile changes for mission critical applications.

Initial

- Establishes application profiles with distinct traffic management features and begins to map all applications to these profiles.
- Expands application of static rules to all applications and performs periodic manual audits of application profile assessments.

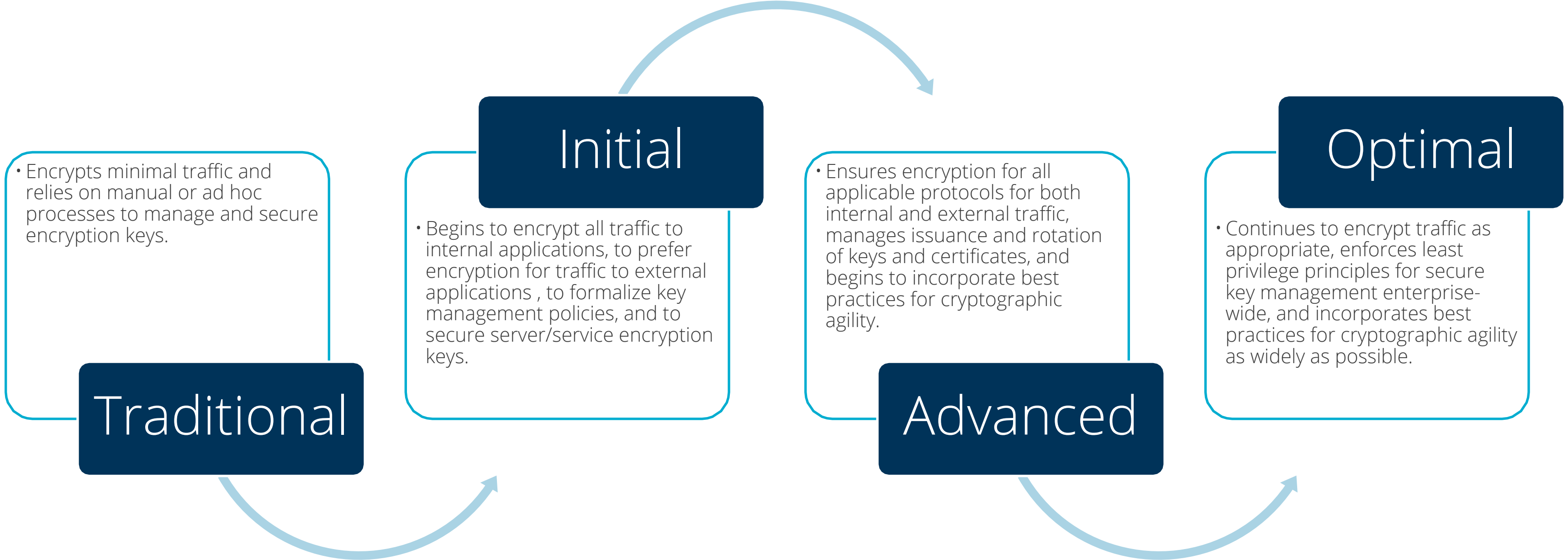
Advanced

- Implements dynamic network rules and configurations for resource optimization that are periodically adapted based upon automated risk-aware and risk-responsive application profile assessments and monitoring

Optimal

- Implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritizes applications based on mission criticality, risk, etc.

Network – Traffic Encryption



Traditional

- Encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.

Initial

- Begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications , to formalize key management policies, and to secure server/service encryption keys.

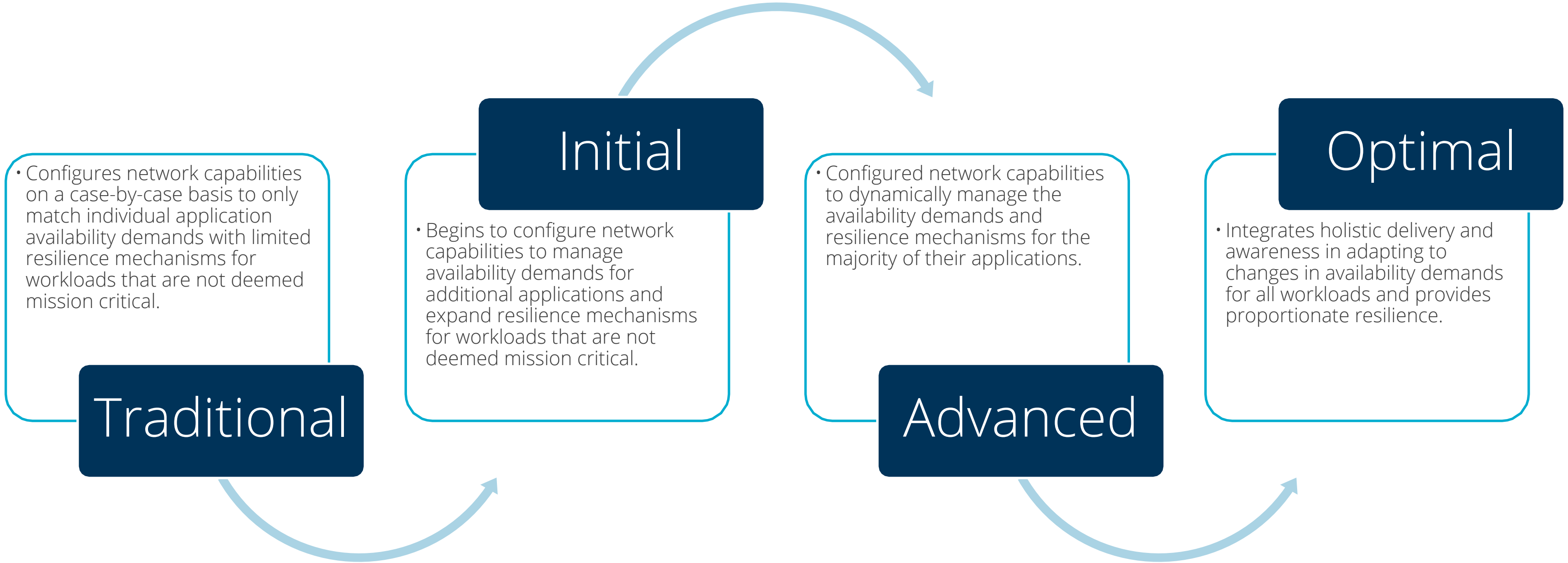
Advanced

- Ensures encryption for all applicable protocols for both internal and external traffic, manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.

Optimal

- Continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprise-wide, and incorporates best practices for cryptographic agility as widely as possible.

Network – Resilience



Traditional

- Configures network capabilities on a case-by-case basis to only match individual application availability demands with limited resilience mechanisms for workloads that are not deemed mission critical.

Initial

- Begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms for workloads that are not deemed mission critical.

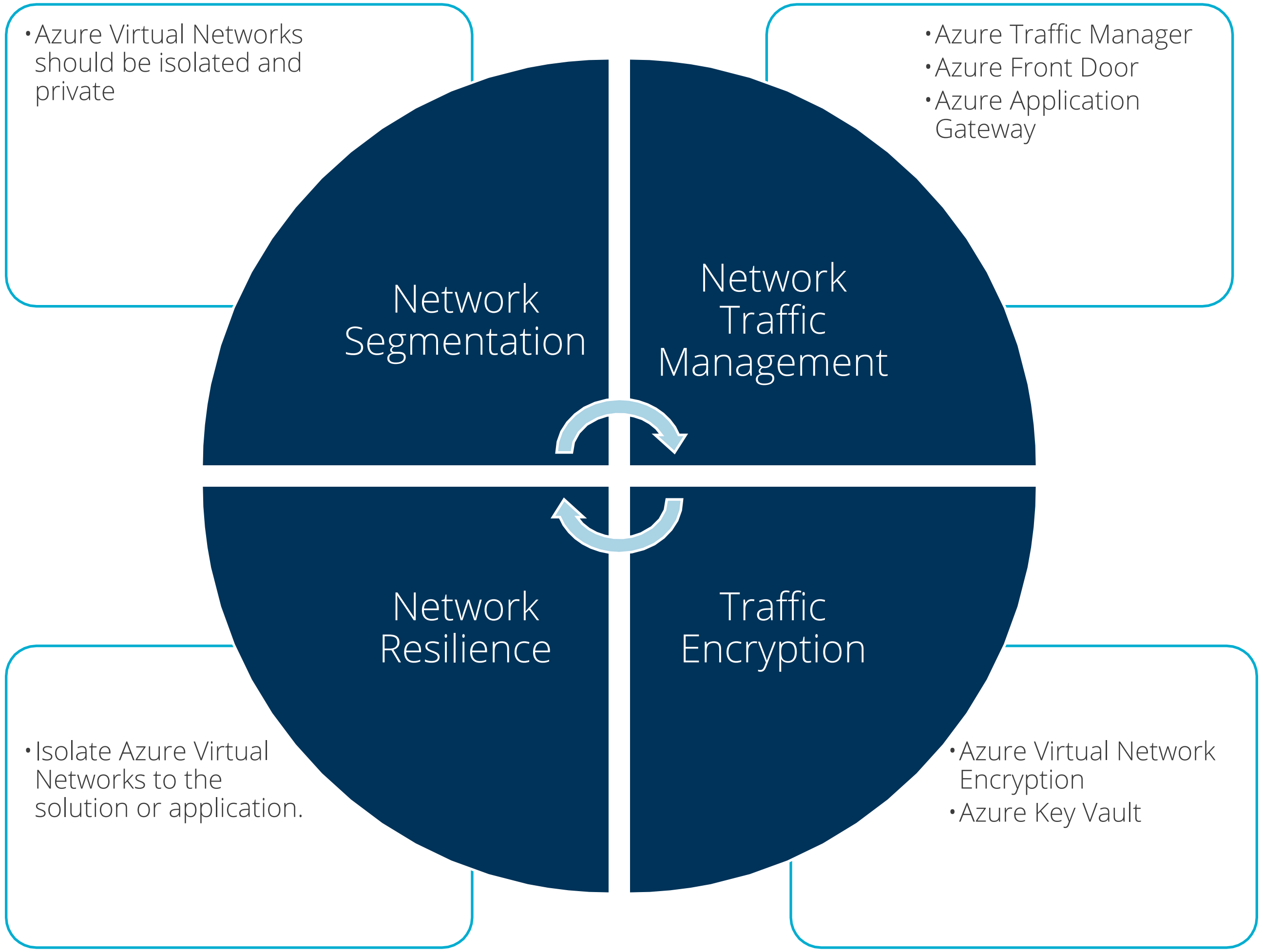
Advanced

- Configured network capabilities to dynamically manage the availability demands and resilience mechanisms for the majority of their applications.

Optimal

- Integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.

Network



Network Segmentation

- Azure Virtual Networks should be isolated and private

Network Traffic Management

- Azure Traffic Manager
- Azure Front Door
- Azure Application Gateway

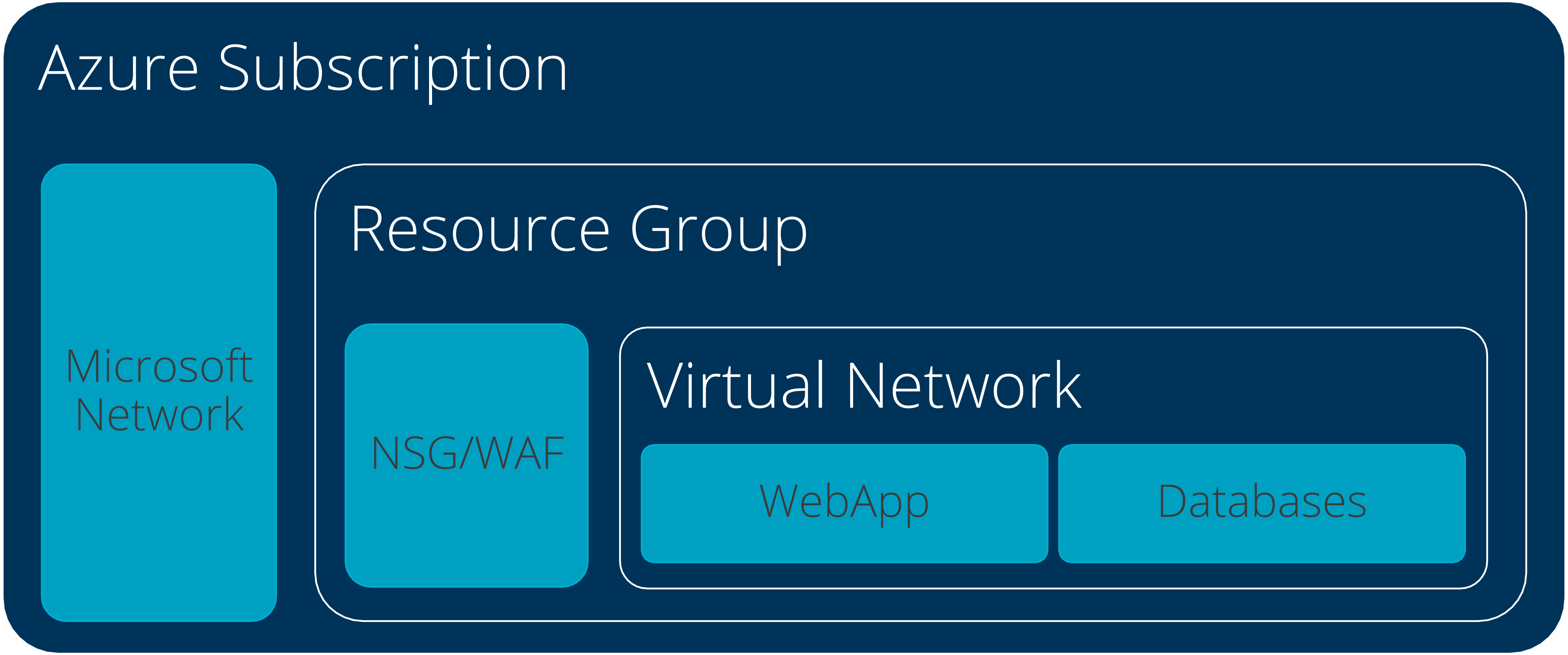
Network Resilience

- Isolate Azure Virtual Networks to the solution or application.

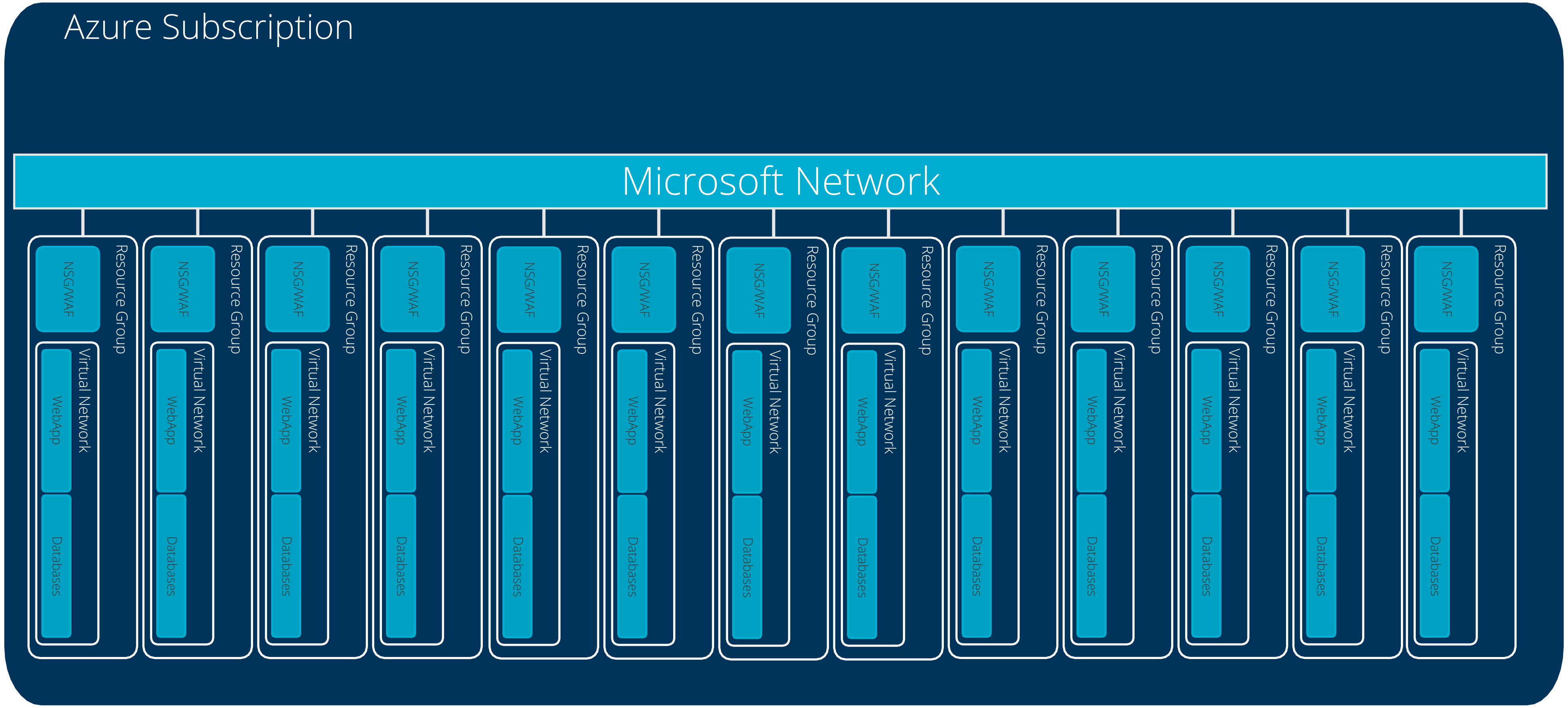
Traffic Encryption

- Azure Virtual Network Encryption
- Azure Key Vault

Network


Azure Subscription
Microsoft Network
Resource Group
NSG/WAF
Virtual Network
WebApp
Databases

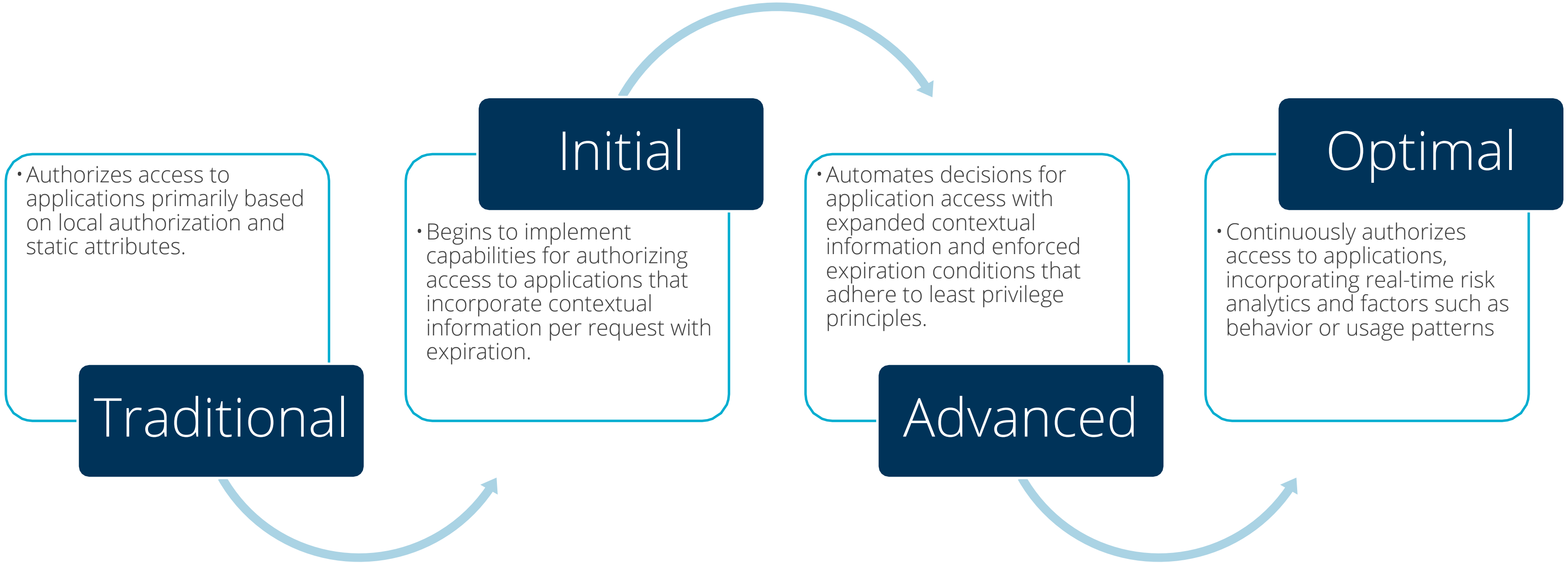
Network Segmented



Application and Workloads

Maturity Area							
Application Access	Application Threat Protections	Accessible Applications	Secure Application Development and Deployment Workflow	Application Security Testing	Visibility and Analytics Capability	Automation and Orchestration Capability	Governance Capability

Application – Application Access



Traditional

- Authorizes access to applications primarily based on local authorization and static attributes.

Initial

- Begins to implement capabilities for authorizing access to applications that incorporate contextual information per request with expiration.

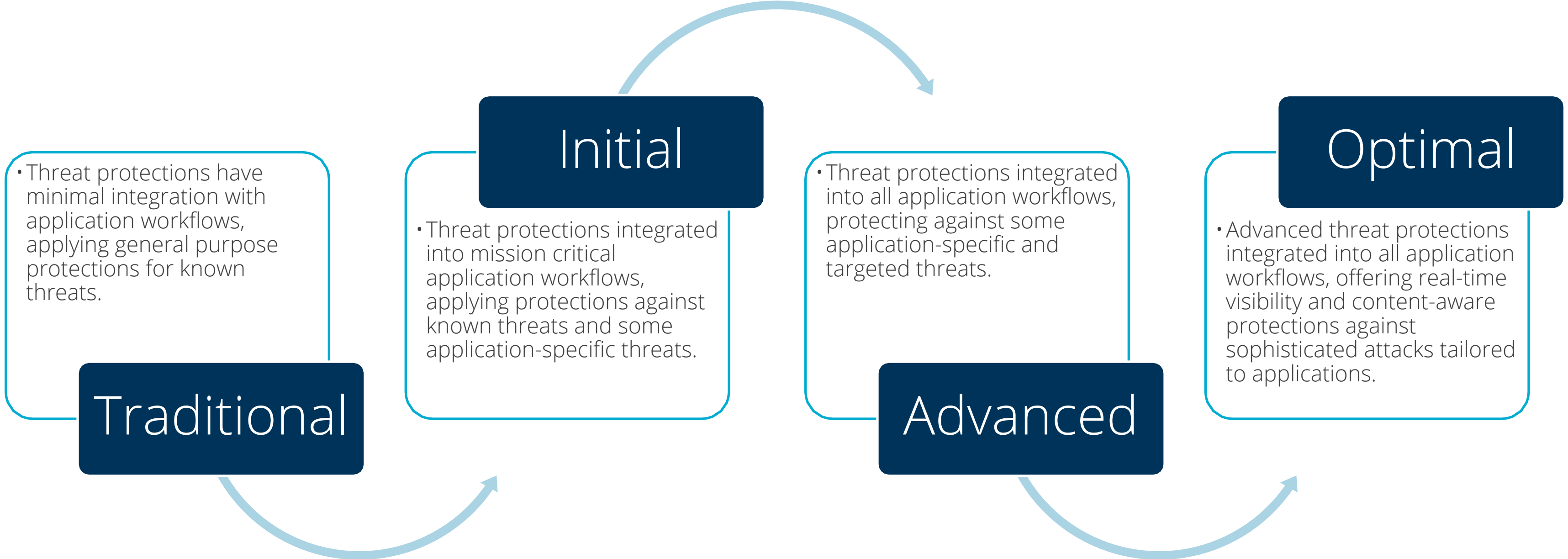
Advanced

- Automates decisions for application access with expanded contextual information and enforced expiration conditions that adhere to least privilege principles.

Optimal

- Continuously authorizes access to applications, incorporating real-time risk analytics and factors such as behavior or usage patterns

Application – Threat Protections



Traditional

- Threat protections have minimal integration with application workflows, applying general purpose protections for known threats.

Initial

- Threat protections integrated into mission critical application workflows, applying protections against known threats and some application-specific threats.

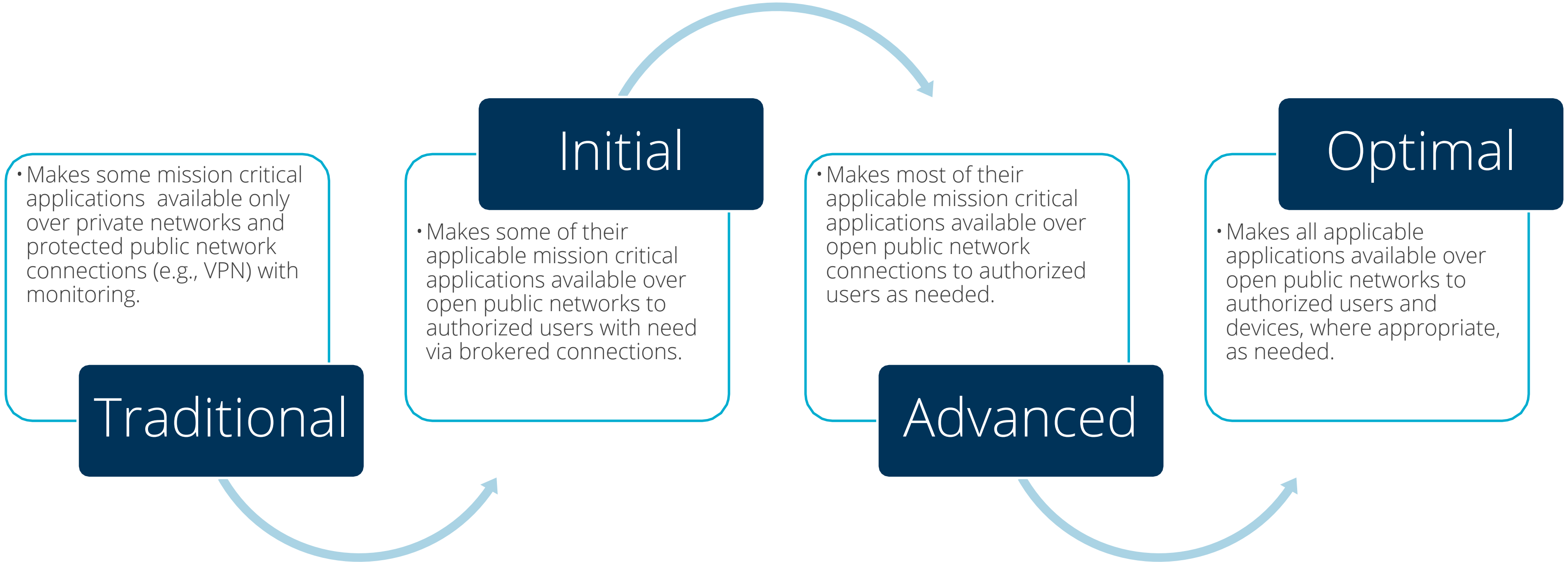
Advanced

- Threat protections integrated into all application workflows, protecting against some application-specific and targeted threats.

Optimal

- Advanced threat protections integrated into all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.

Application – Accessible Applications



Traditional

- Makes some mission critical applications available only over private networks and protected public network connections (e.g., VPN) with monitoring.

Initial

- Makes some of their applicable mission critical applications available over open public networks to authorized users with need via brokered connections.

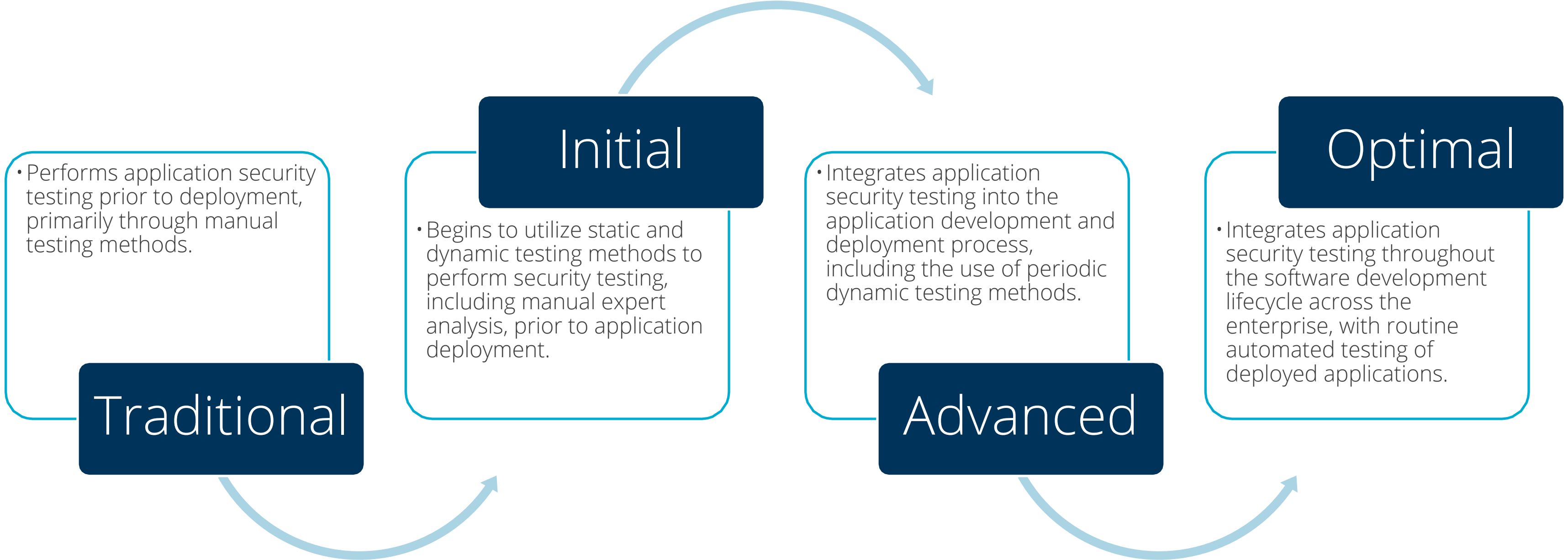
Advanced

- Makes most of their applicable mission critical applications available over open public network connections to authorized users as needed.

Optimal

- Makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.

Application – Application Security Testing



Traditional

- Performs application security testing prior to deployment, primarily through manual testing methods.

Initial

- Begins to utilize static and dynamic testing methods to perform security testing, including manual expert analysis, prior to application deployment.

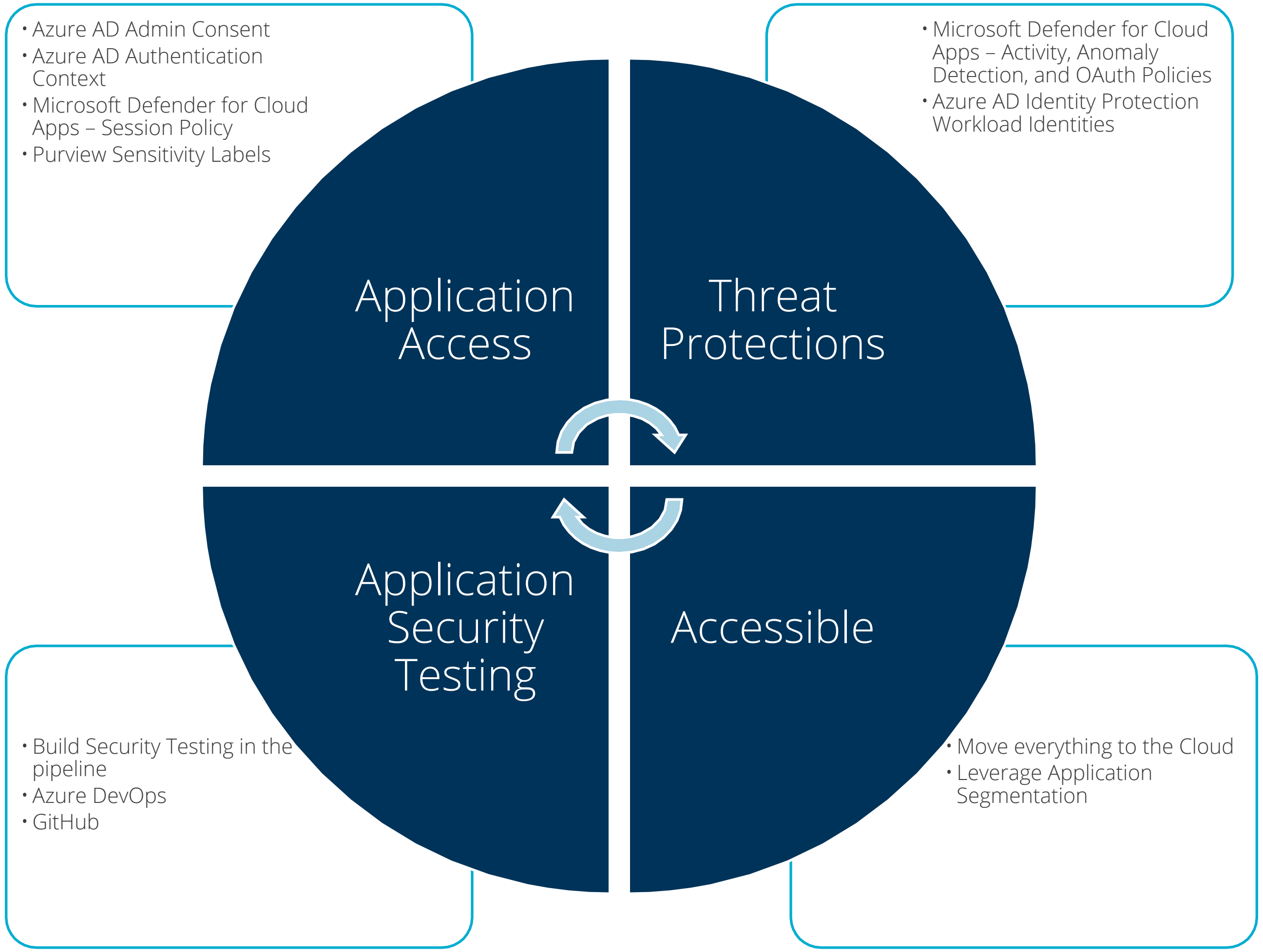
Advanced

- Integrates application security testing into the application development and deployment process, including the use of periodic dynamic testing methods.

Optimal

- Integrates application security testing throughout the software development lifecycle across the enterprise, with routine automated testing of deployed applications.

Application



Application Access

- Azure AD Admin Consent
- Azure AD Authentication Context
- Microsoft Defender for Cloud Apps – Session Policy
- Purview Sensitivity Labels

Threat Protections

- Microsoft Defender for Cloud Apps – Activity, Anomaly Detection, and OAuth Policies
- Azure AD Identity Protection Workload Identities

Application Security Testing

- Build Security Testing in the pipeline
- Azure DevOps
- GitHub

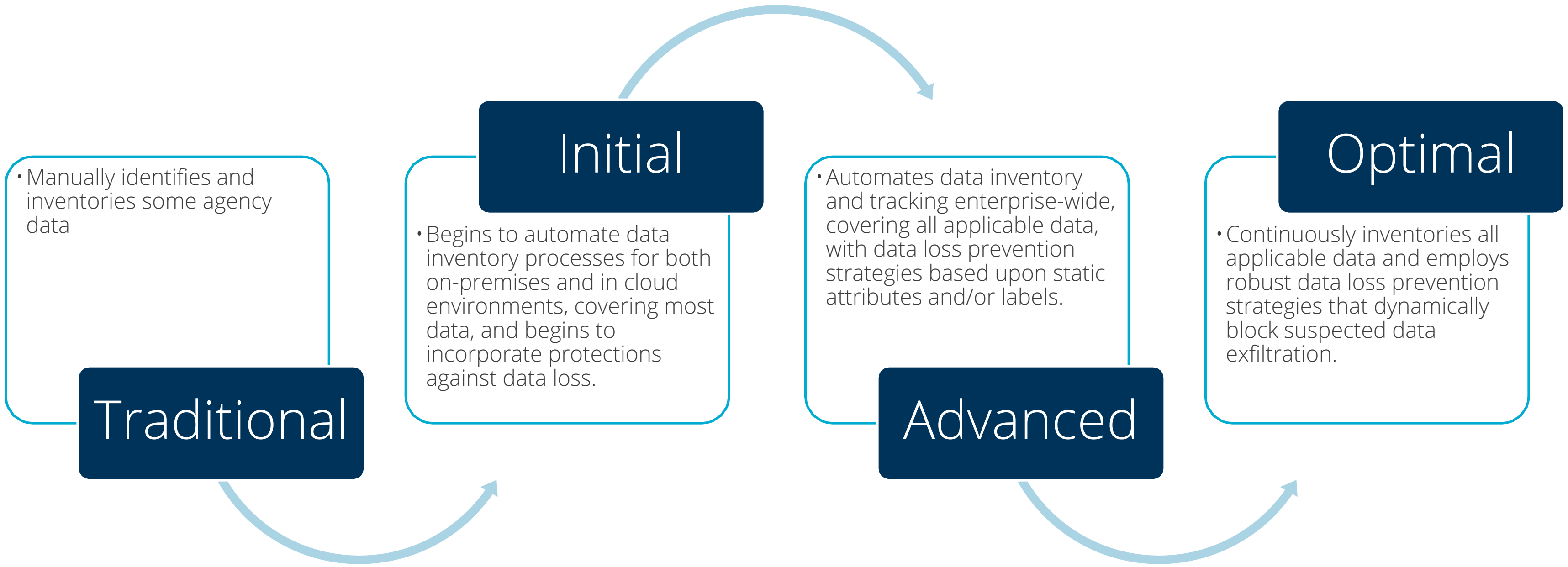
Accessible

- Move everything to the Cloud
- Leverage Application Segmentation

Data

Maturity Area							
Data Inventory Management	Data Categorization	Data Availability	Data Access	Data Encryption	Visibility and Analytics Capability	Automation and Orchestration Capability	Governance Capability

Data - Inventory Management



Traditional

- Manually identifies and inventories some agency data

Initial

- Begins to automate data inventory processes for both on-premises and in cloud environments, covering most data, and begins to incorporate protections against data loss.

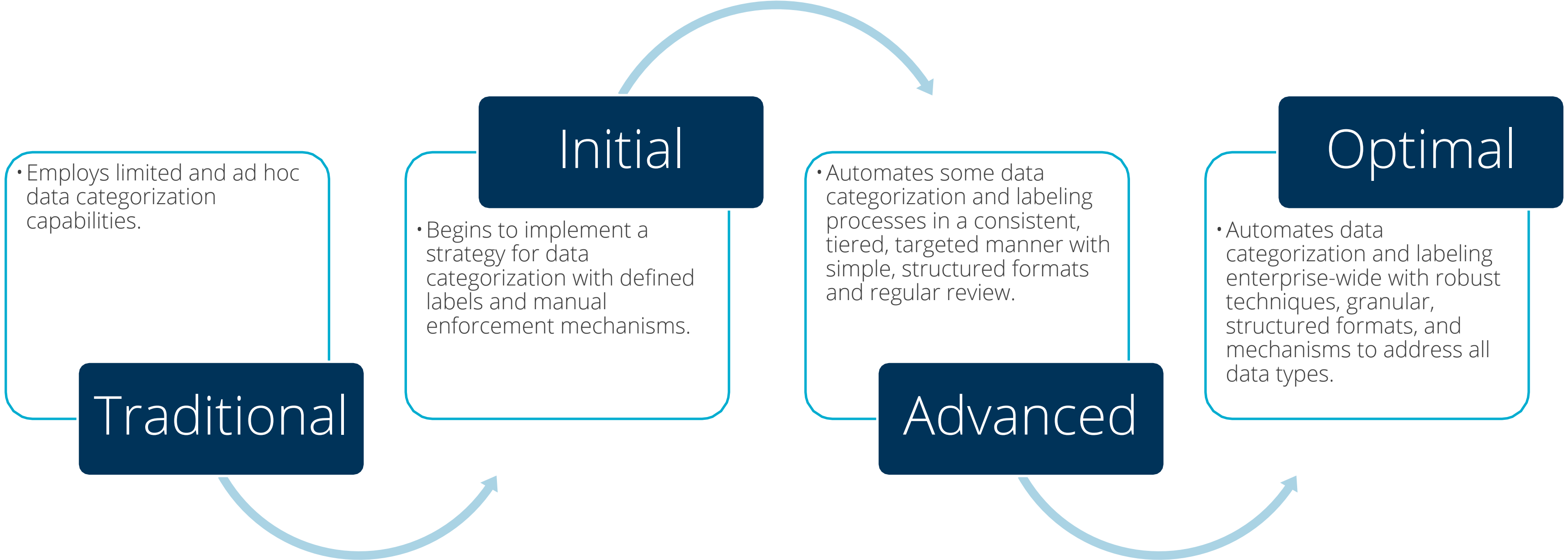
Advanced

- Automates data inventory and tracking enterprise-wide, covering all applicable data, with data loss prevention strategies based upon static attributes and/or labels.

Optimal

- Continuously inventories all applicable data and employs robust data loss prevention strategies that dynamically block suspected data exfiltration.

Data - Categorization



Traditional

- Employs limited and ad hoc data categorization capabilities.

Initial

- Begins to implement a strategy for data categorization with defined labels and manual enforcement mechanisms.

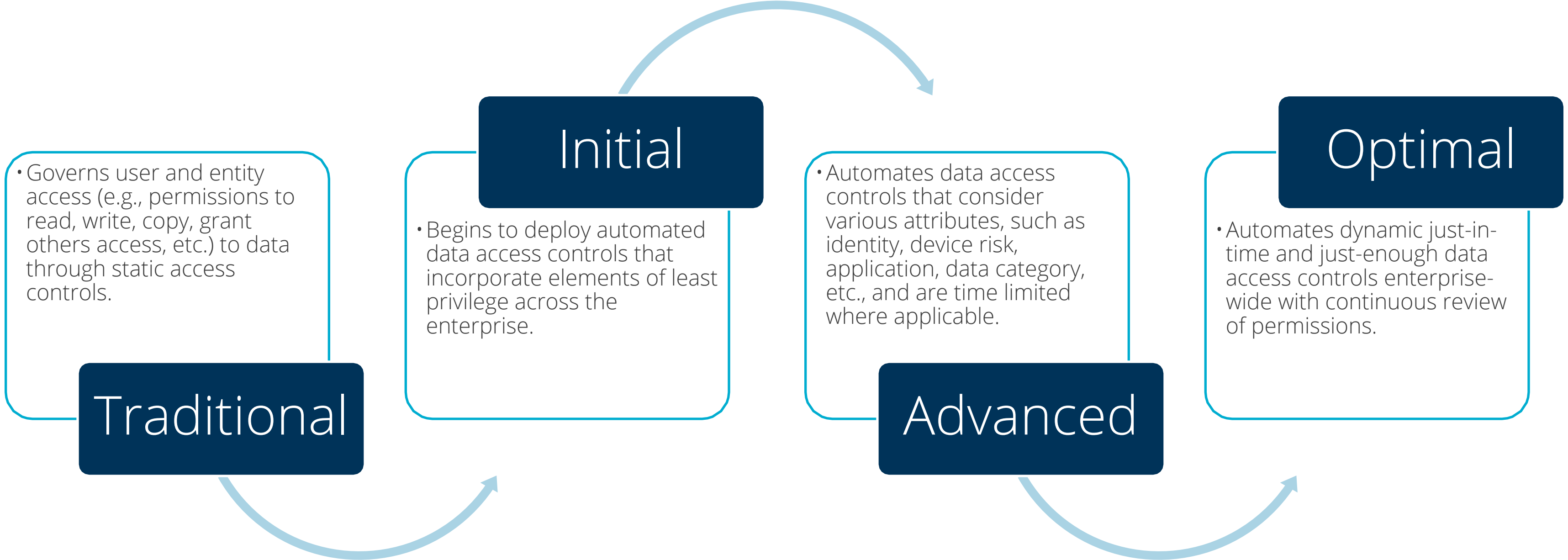
Advanced

- Automates some data categorization and labeling processes in a consistent, tiered, targeted manner with simple, structured formats and regular review.

Optimal

- Automates data categorization and labeling enterprise-wide with robust techniques, granular, structured formats, and mechanisms to address all data types.

Data - Access



Traditional

- Governs user and entity access (e.g., permissions to read, write, copy, grant others access, etc.) to data through static access controls.

Initial

- Begins to deploy automated data access controls that incorporate elements of least privilege across the enterprise.

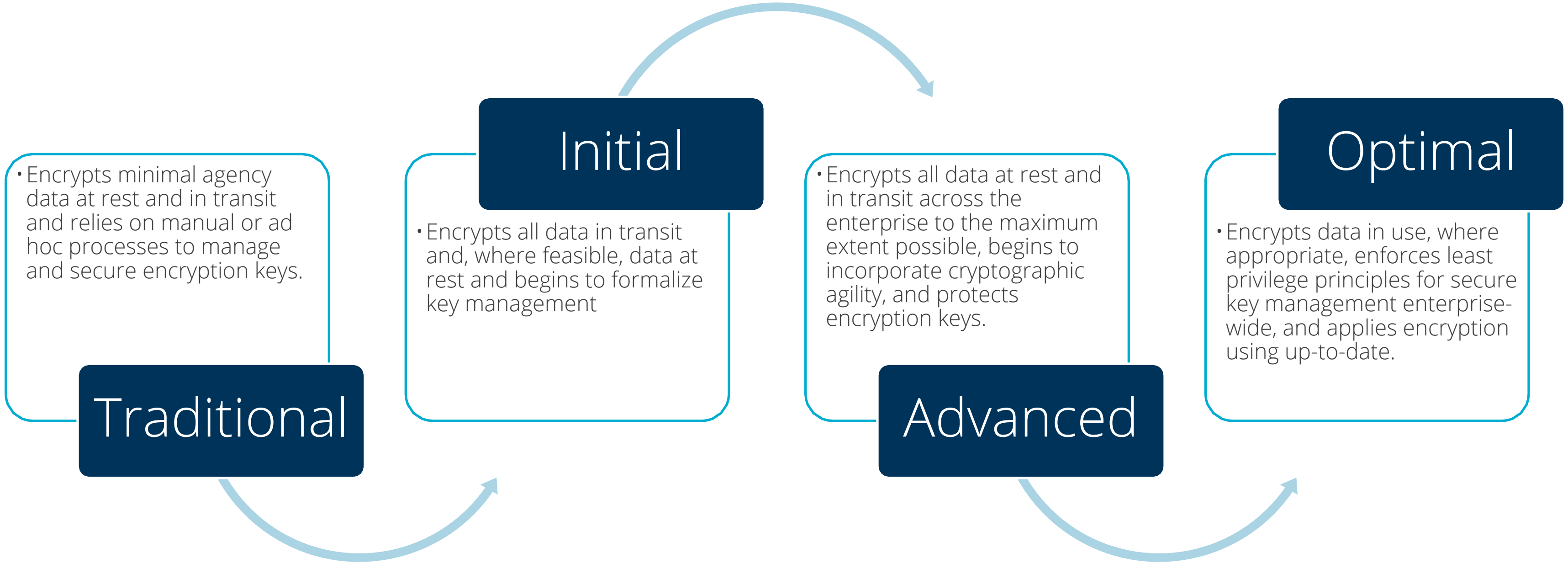
Advanced

- Automates data access controls that consider various attributes, such as identity, device risk, application, data category, etc., and are time limited where applicable.

Optimal

- Automates dynamic just-in-time and just-enough data access controls enterprise-wide with continuous review of permissions.

Data - Encryption



Traditional

- Encrypts minimal agency data at rest and in transit and relies on manual or ad hoc processes to manage and secure encryption keys.

Initial

- Encrypts all data in transit and, where feasible, data at rest and begins to formalize key management

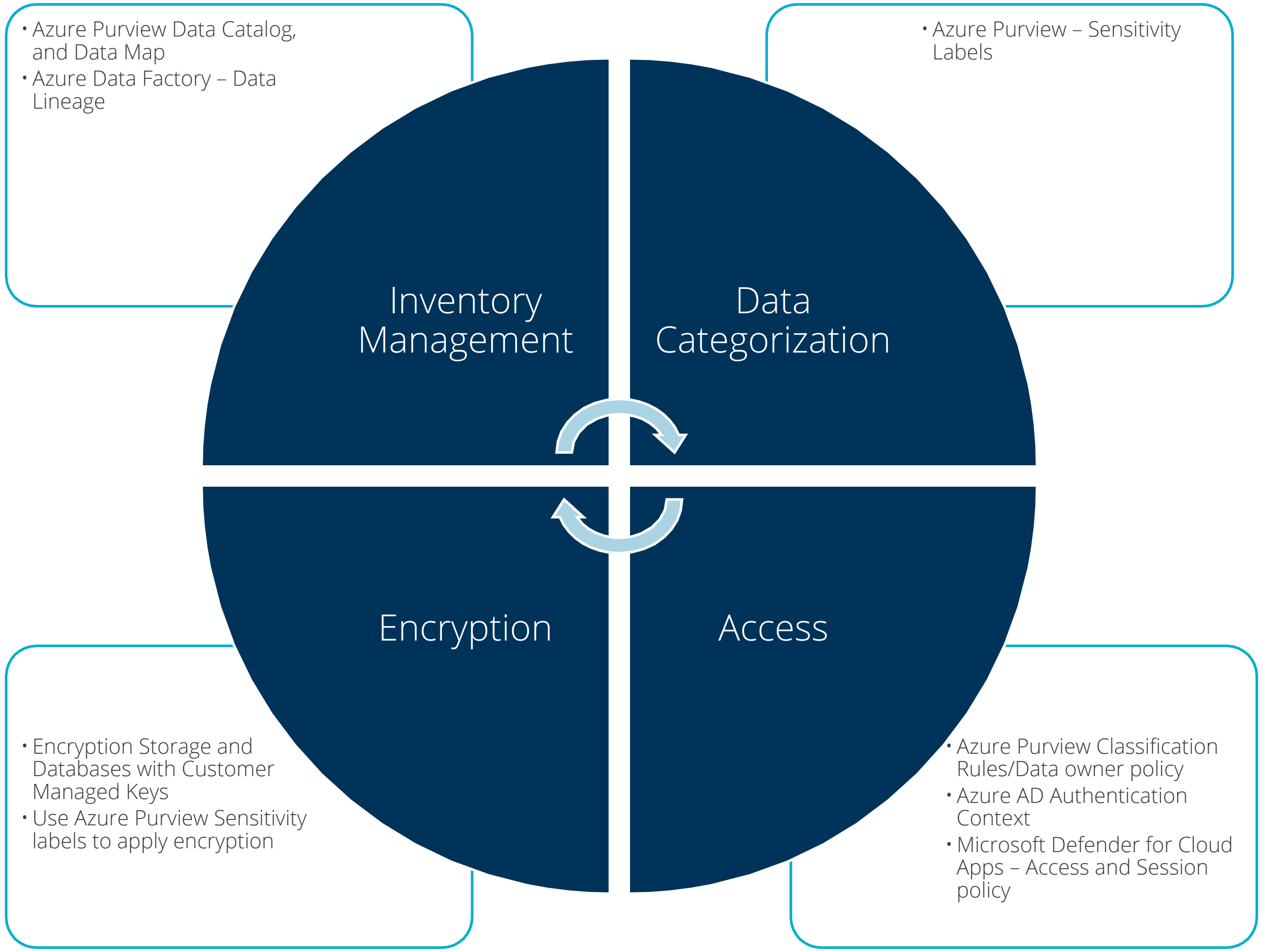
Advanced

- 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.

Optimal

- Encrypts data in use, where appropriate, enforces least privilege principles for secure key management enterprise-wide, and applies encryption using up-to-date.

Data



Inventory Management

- Azure Purview Data Catalog, and Data Map
- Azure Data Factory – Data Lineage

Data Categorization

- Azure Purview – Sensitivity Labels

Encryption

- Encryption Storage and Databases with Customer Managed Keys
- Use Azure Purview Sensitivity labels to apply encryption

Access

- Azure Purview Classification Rules/Data owner policy
- Azure AD Authentication Context
- Microsoft Defender for Cloud Apps – Access and Session policy

Reference

- CISA Zero Trust Maturity Model

https://www.cisa.gov/zero-trust-maturity-model

- Microsoft Zero Trust Guide

https://www.microsoft.com/en-us/security/business/zero-trust

Questions