Cyber Threat Defense

Cognizant Microsoft Business Group

Agenda

01 Cognizant Microsoft Business Group Overview

02 Business Landscape and Drivers

03 Point of View

04 Value Proposition

05 Proof Points

06 Pricing Model

01

Cognizant Microsoft Business Group Overview

Advancing Cloud Modernization With Focus, Simplicity and Scale

Cognizant Microsoft Business Group is an end-to-end Microsoft-centric **cloud solutions and managed services provider** that leverages **extensive experience and IP** to deliver constant innovation and business value to our clients, **powered by the Microsoft Cloud platform.**

Our Value to Clients

Focus

Dedicated specialists creating agility for clients exclusively through the Microsoft Cloud platform.

Simplicity

An intelligent blueprint, built from experience that offers a tested business transformation prescription.

Scale

Unmatched impact on client organizations based on our global scale, reach and ambition.

Cognizant’s Extensive Microsoft Expertise

ONE OF THE WORLD’S MOST CERTIFIED MICROSOFT CLOUD PARTNERS

20 Years of Partnership

20 Advanced Specializations

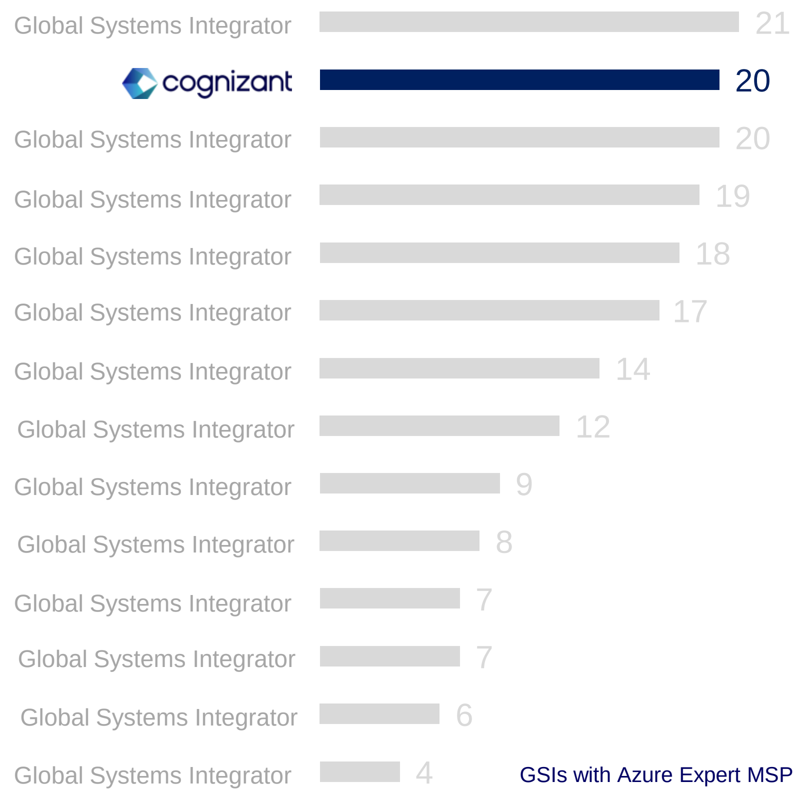
6 Solution Partner Designations

25+ Partner of the Year Awards

20,000+ Microsoft Certified Consultants

610+ Clients

A GLOBAL PARTNER WITH ENTERPRISE SCALE



ADVANCED SPECIALIZATIONS

Intelligent Automation	Low Code Application Development	Build and Modernize AI Apps with Microsoft Azure	AI and Machine Learning in Azure	Analytics on Microsoft Azure
Infra and Database Migration to Azure	Kubernetes on Microsoft Azure	Microsoft Azure Virtual Desktop	Migrate Enterprise Applications to Microsoft Azure	SAP on Azure
Adoption and Change Management	Calling for Microsoft Teams	Custom Solutions for Teams	Meetings and Meeting Rooms	Modernize Endpoints
Business Intelligence	Cloud Security	Id and Access Management	Information Protection and Governance	Threat Protection

RECENT MICROSOFT AWARDS

2023

Microsoft Global Partner of the Year
Intelligent Automation (Business Applications)

Microsoft Global Partner of the Year Finalist
Low Code Application Development

2022

Microsoft US Partner of the Year
Media and Communications Industry

Microsoft US Partner of the Year
Dynamics 365 Customer Insights and Marketing

AFFILIATIONS

2023/2024 INNERCIRCLE for Microsoft Business Applications

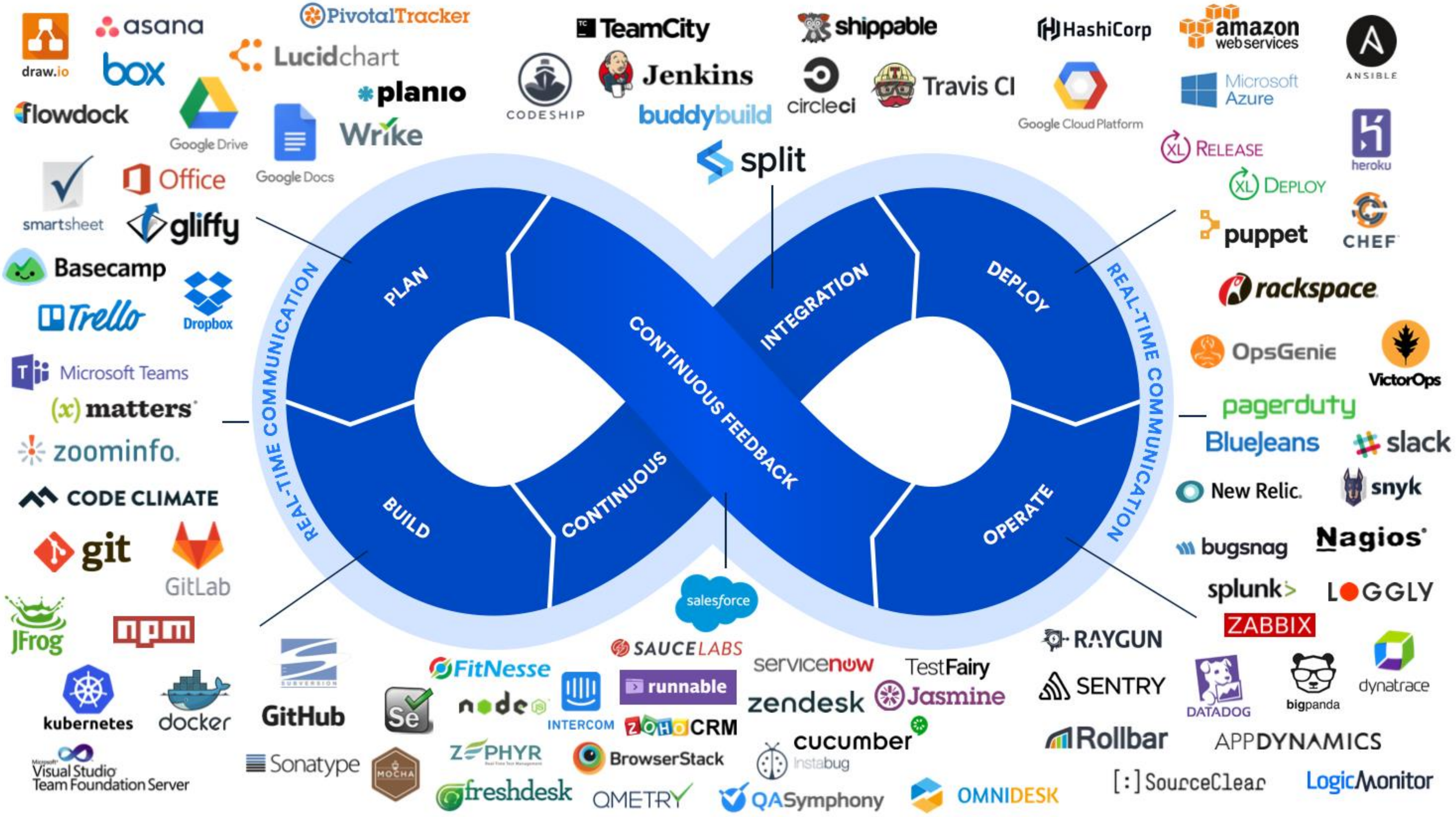
Microsoft Partner Microsoft | Azure Expert MSP

Member of Microsoft Intelligent Security Association Microsoft

Microsoft Solutions Partner
Microsoft Cloud

Modern Work
Business Applications
Azure Infrastructure
Data & AI
Digital & App Innovation
Security

Complexity Stifles Innovation



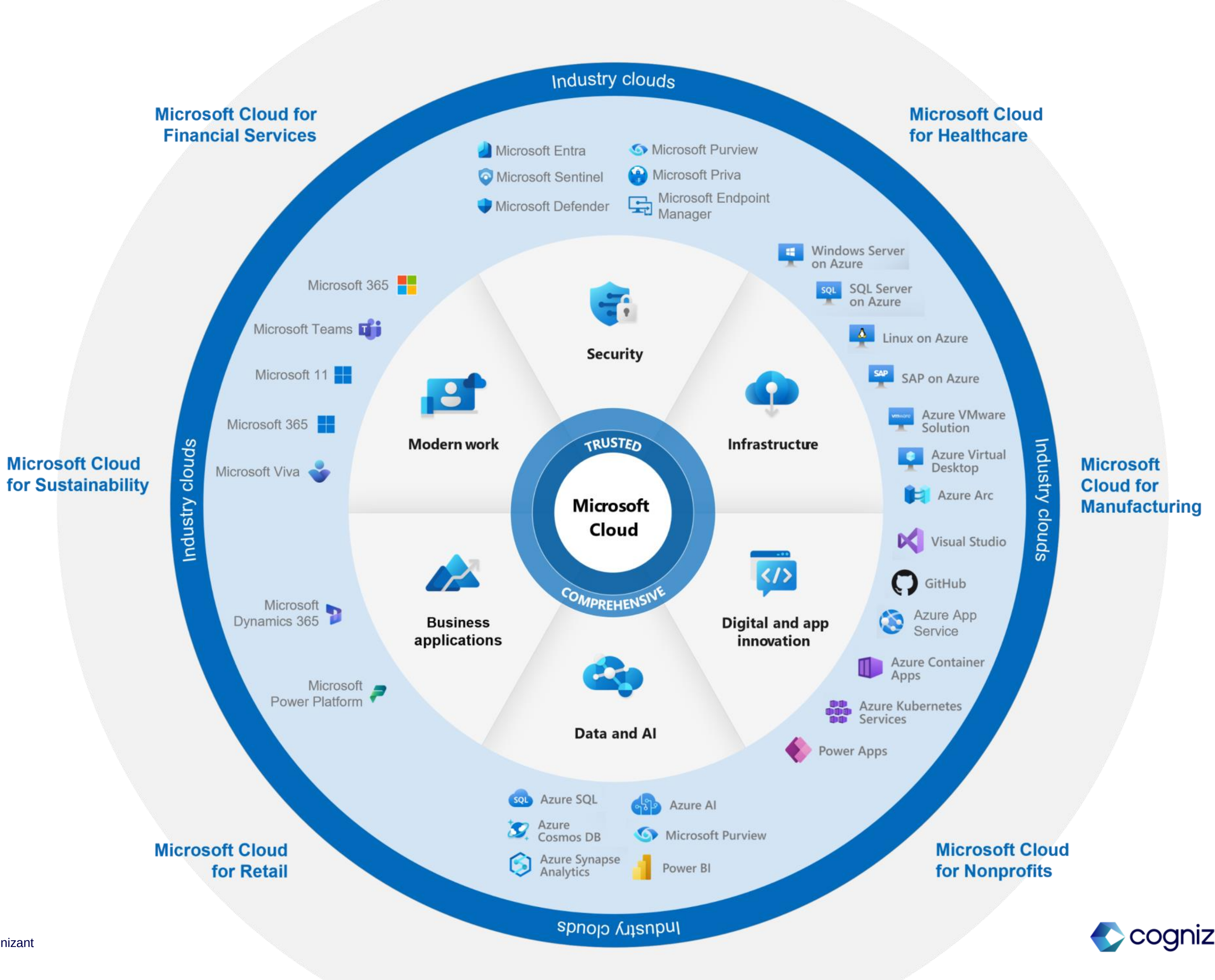
Seamless Integration

Across the Microsoft Cloud

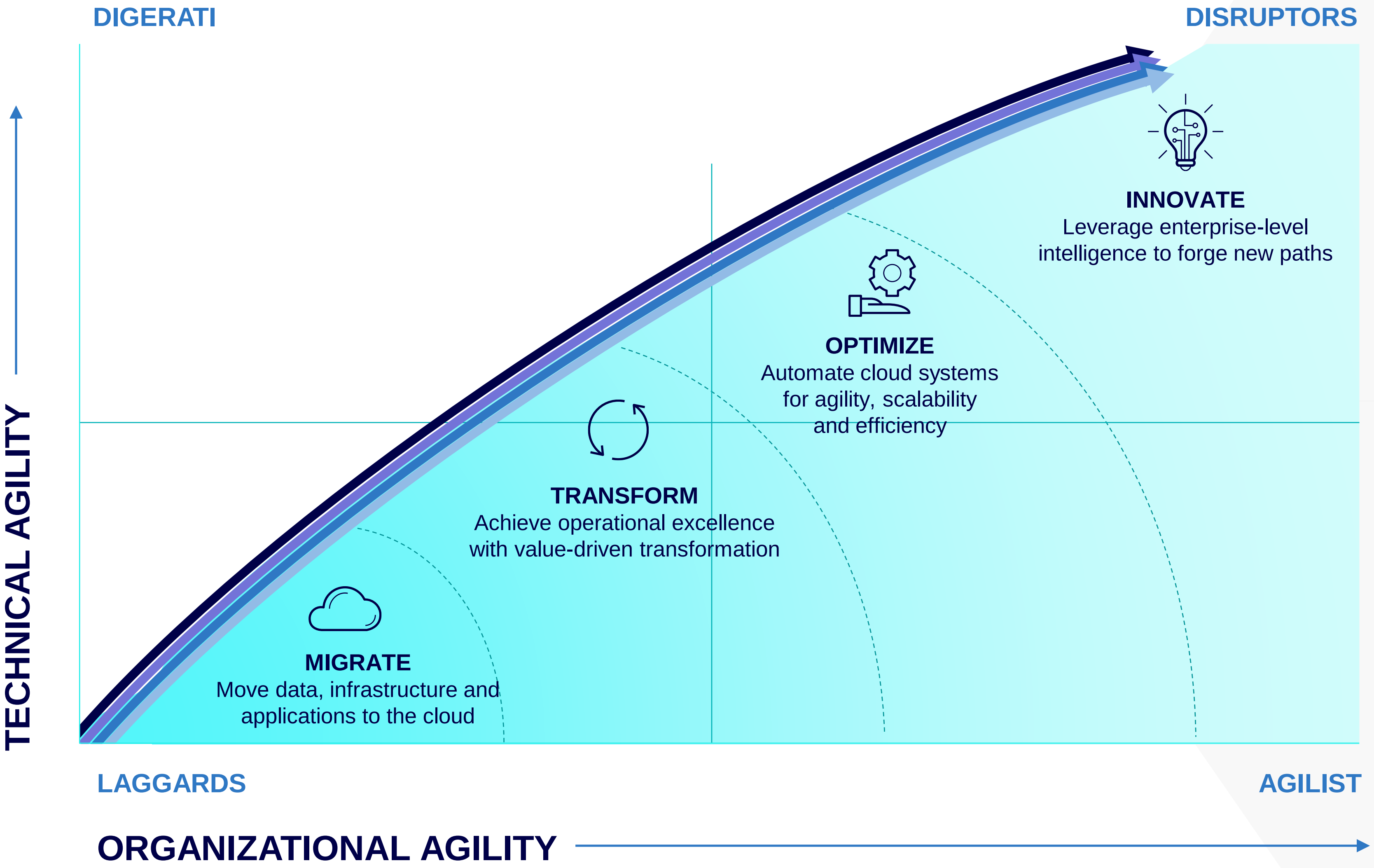
Native integrations and tools combined with robust and extendable low-code applications unlock **business value** with

- Less risk,
- Lower cost, and
- Increased security

for a faster time to production.



We Meet You Where You Are on the Journey...



DIGERATI
DISRUPTORS
TECHNICAL AGILITY
INNOVATE
Leverage enterprise-level intelligence to forge new paths
OPTIMIZE
Automate cloud systems for agility, scalability and efficiency
TRANSFORM
Achieve operational excellence with value-driven transformation
MIGRATE
Move data, infrastructure and applications to the cloud
LAGGARDS
AGILIST
ORGANIZATIONAL AGILITY

Agility Quadrant

Be the Leader.

Drive Industry Change.

Innovate.

MODERN ENTERPRISE FRAMEWORK

- PLATFORM
- DATA + AI
- APPLICATIONS
- MANAGED SERVICES

02

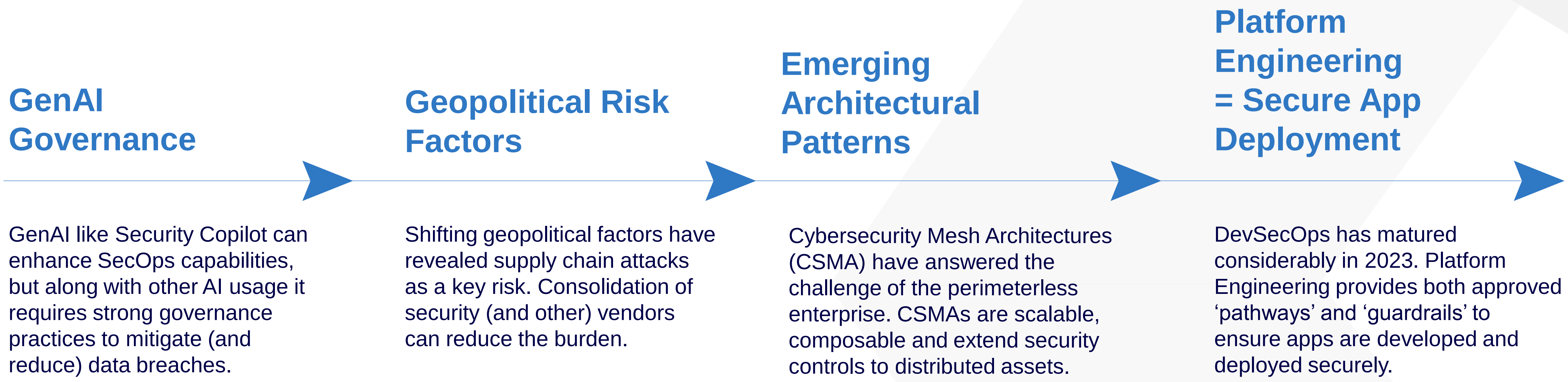
Business Landscape and Drivers

“

Cybercrime is the number one threat facing every business today.

Satya Nadella
CEO, Microsoft

Security and Risk Management Trends - 2024



GenAI Governance

GenAI like Security Copilot can enhance SecOps capabilities, but along with other AI usage it requires strong governance practices to mitigate (and reduce) data breaches.

Geopolitical Risk Factors

Shifting geopolitical factors have revealed supply chain attacks as a key risk. Consolidation of security (and other) vendors can reduce the burden.

Emerging Architectural Patterns

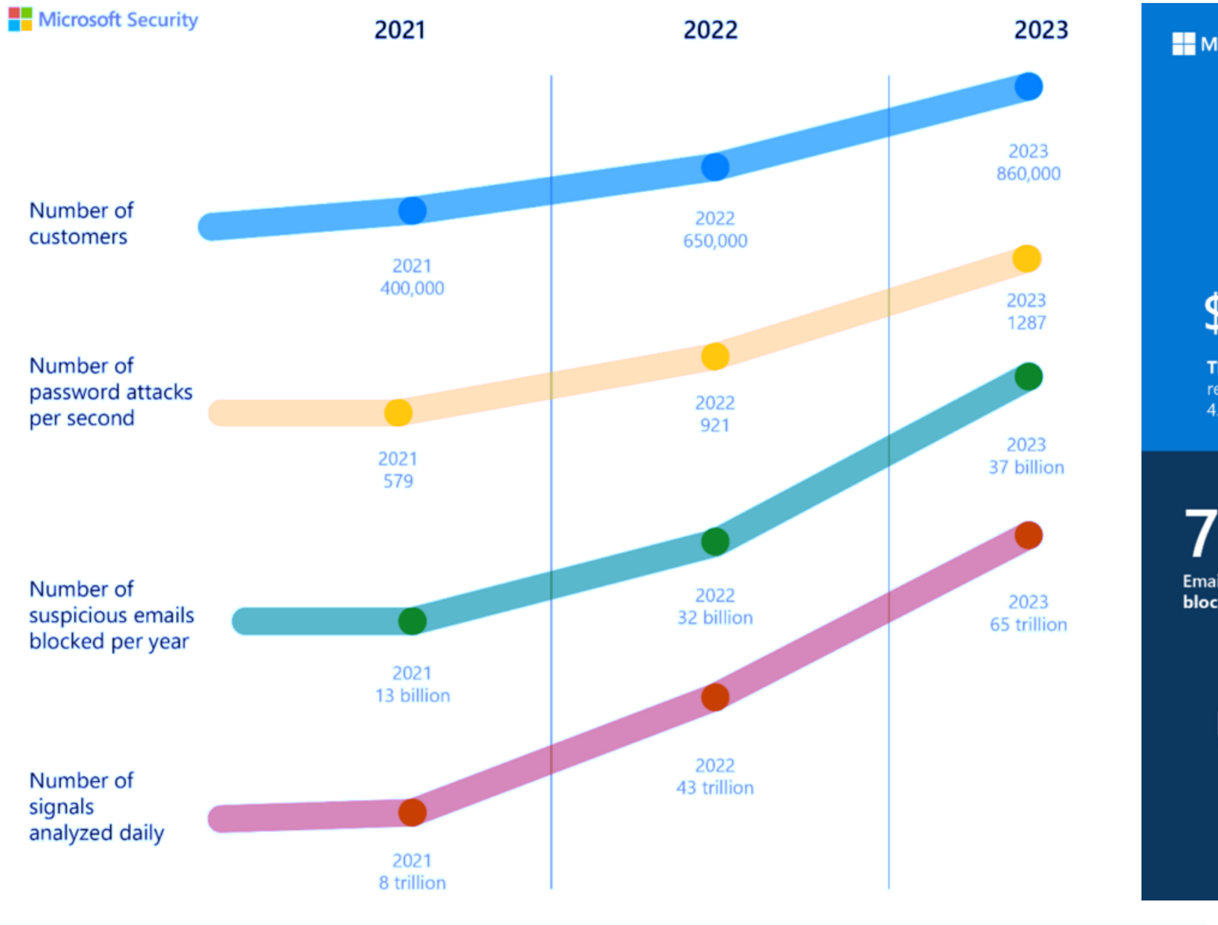
Cybersecurity Mesh Architectures (CSMA) have answered the challenge of the perimeterless enterprise. CSMAs are scalable, composable and extend security controls to distributed assets.

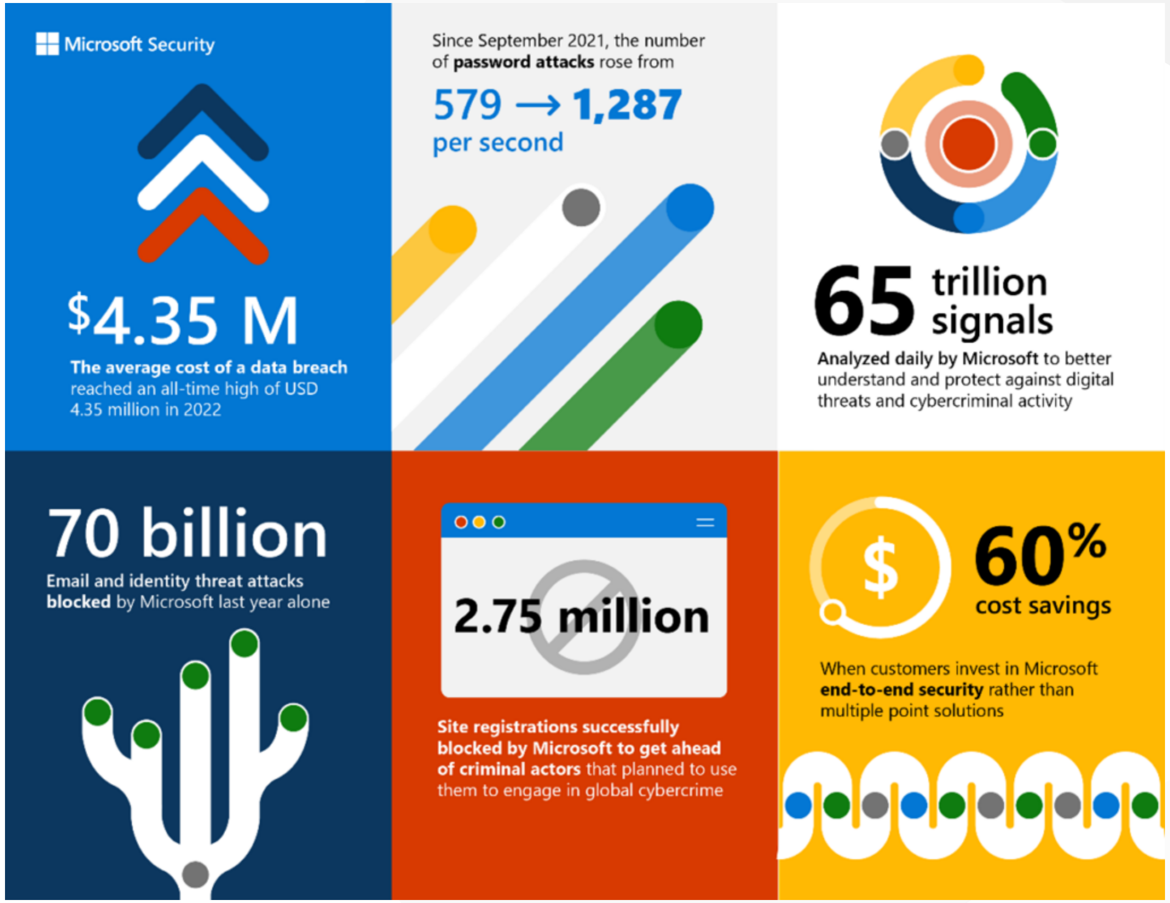
Platform Engineering = Secure App Deployment

DevSecOps has matured considerably in 2023. Platform Engineering provides both approved ‘pathways’ and ‘guardrails’ to ensure apps are developed and deployed securely.

Microsoft Security enables you to capitalize on these trends, and many more…

Microsoft: The Biggest Security Company You've Never Heard Of





$4.35 M

The average cost of a data breach reached an all-time high of USD 4.35 million in 2022

Since September 2021, the number of **password attacks** rose from

579 ⟶ **1,287** per second

65 trillion signals

Analyzed daily by Microsoft to better understand and protect against digital threats and cybercriminal activity

70 billion

Email and identity threat attacks blocked by Microsoft last year alone

2.75 million

Site registrations successfully blocked by Microsoft to get ahead of criminal actors that planned to use them to engage in global cybercrime

60% cost savings

When customers invest in Microsoft **end-to-end security** rather than multiple point solutions

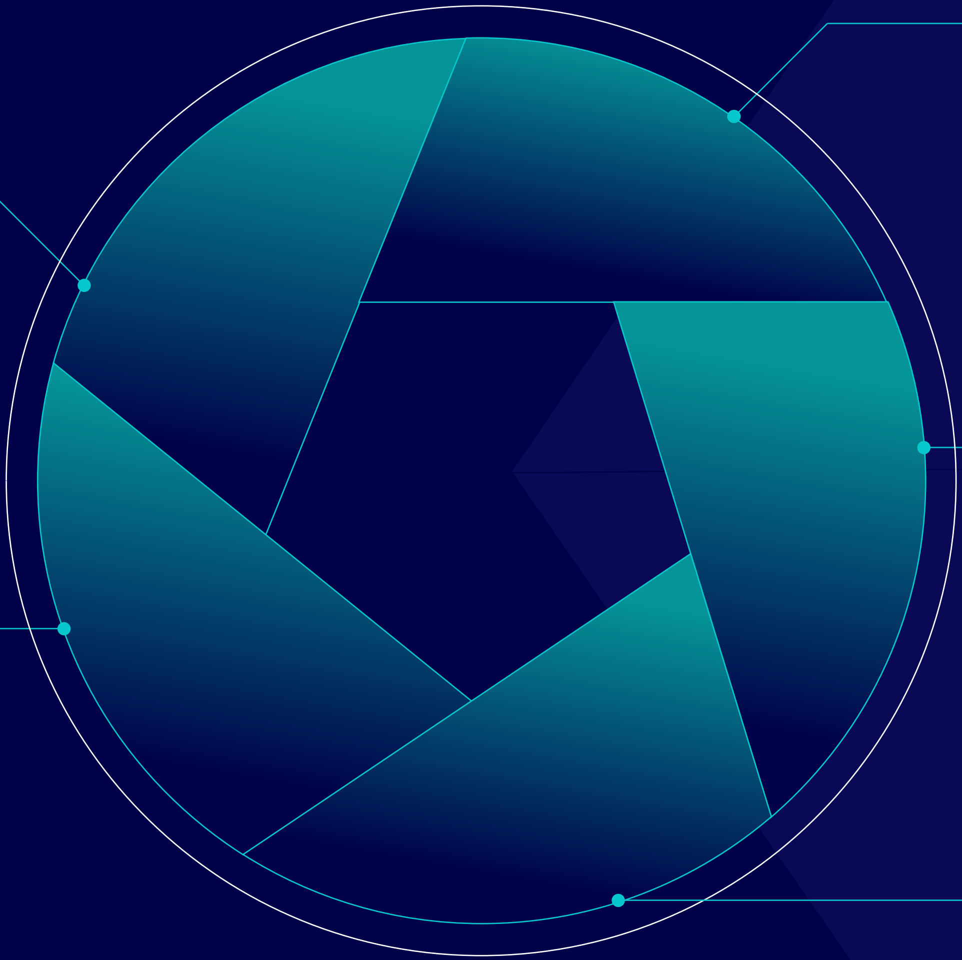
Maximize The Business Value of Security

SecOps

- Reduce MTTD and MTTR with unprecedented visibility across the kill-chain.
- SOAR and XDR capabilities stop threats in their tracks.
- GenAI copilots allow the SOC structure to evolve.

Scalability

- Cloud-native logging platform, no need to manage storage.
- Efficient scaling with increase in workloads.
- Multi-vendor, multi-cloud, hybrid, on-premises coverage.



Innovation

- Reducing Legacy Debt.
- Faster experimentation.
- Faster time-to-value.
- Take advantage of GenAI before the attackers do.

Security

- Reduced customer responsibility for physical security.
- Cloud-native compliance.
- Eliminates need to import customer data for managed services.

Agility

- Faster time to market.
- Simple integration.
- Enterprise-grade security orchestration.

Are You At Risk Of Getting Left Behind and Becoming a Target?

Current Software Supply Chain

How secure is your supply chain really?

What is the impact of a breach at a key vendor?

Organizational Structure

Is your security team optimally structured to meet your business goals?

Collaboration and Innovation

Is your security team as productive and collaborative as you’d like?

Are you innovating as fast as you would like?

Security & Compliance

Are you able to rapidly detect threats and ensure ongoing legal and security compliance obligations are met?

Scale and Reliability

Are you taking advantage of cloud-native services?

FinOps

How do you ensure financial accountability and reduce the total cost of ownership?

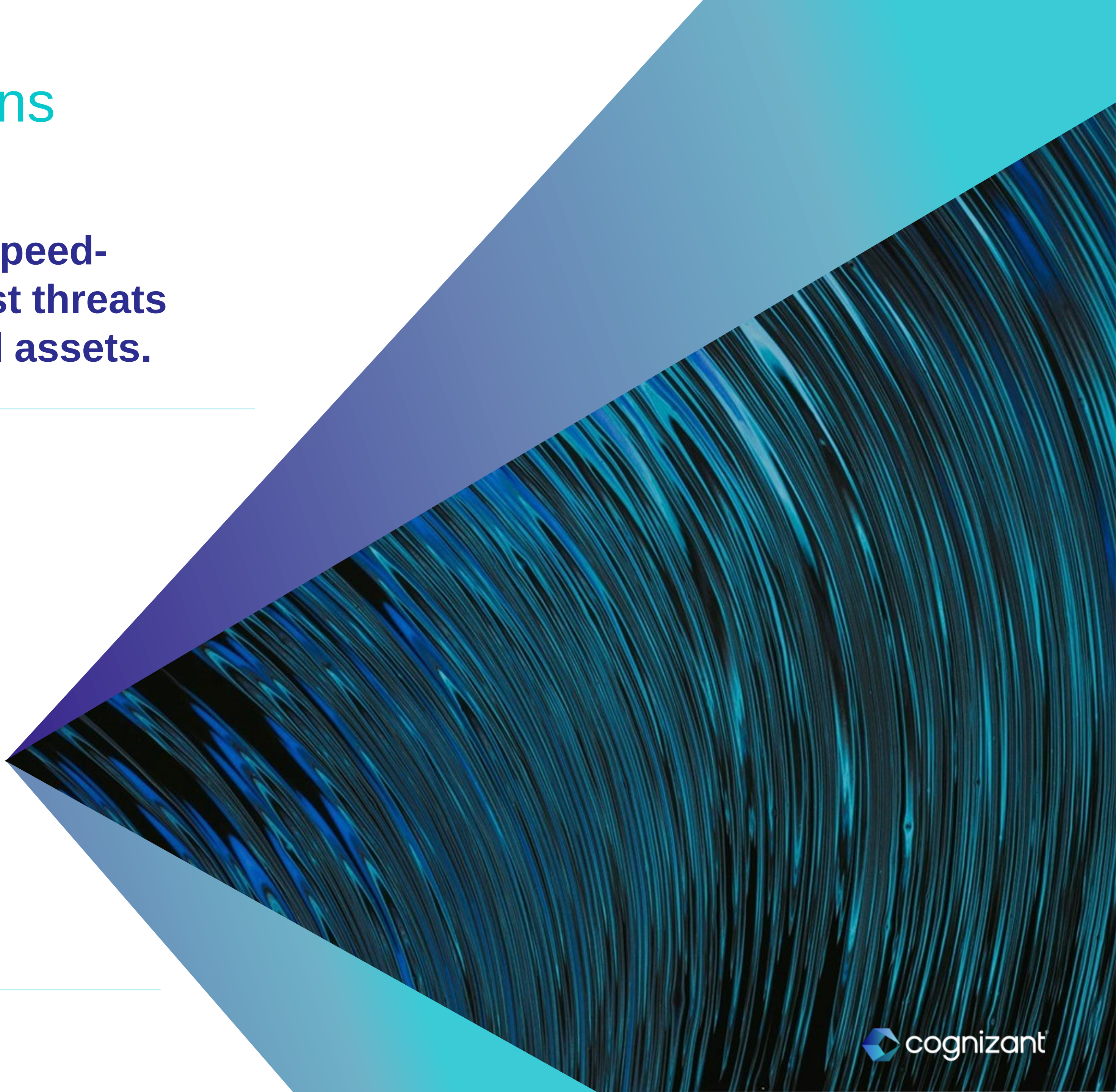
Reimagine Security Operations

Optimised with Microsoft Security

Modern SecOps defends at machine speed- allowing you to stay ahead of the latest threats and protect your organizations critical assets.

The right solution;

- Turns your SOC into an agile, flexible and relentless threat detection and eradication engine.
- Is able to rapidly adapt to new business imperatives driven by technology.
- Allows you to provide assurance and be an enabler, rather than stifling innovation.
- Moves your business along the Agility Quadrant – your path to digital transformation.



A CISO’s Objectives Frequently Include…

- Risk Reduction
- Cost Optimization
- Zero Trust
- Secure App and Systems Modernization
- Data Governance and Privacy
- Secure Business Growth and Scale
- CAPEX reduction and consolidation of 3rd party vendors
- Keeping Cyber Risk on the Board Agenda

> **The most important part is you have to be enablers of your business.**

Noopur Davis

Chief Information Security and Product Privacy Officer, Comcast

03

Point of View

Cyber Threat Defense

Cognizant MBG's Cyber Threat Defense offering provides a set of structured methodologies and tools to assess, migrate, modernize and even manage your Security Operations Center (SOC). We break down the barriers between Cloud Apps and Infrastructure (including Hybrid and Multicloud) and your modern workplace providing unparalleled threat visibility backed up by action.

Infrastructure Modernization

Comprehensive and defined approach to modernizing core security tools like XDR platforms and centralized logging.

SOC Modernization

Unique and highly automated approach to modernizing security operations, infused with GenAI insights and XDR response capabilities.

IR Excellence

We work hand-in-hand with Microsoft Security Services for Incident Response to get you back in action in the event of a breach.

Microsoft Copilot for Security- Improving Cyber Threat Defense

✓ Triage alerts with enriched threat intelligence

✓ Hunt for threats with natural language queries

✓ Generate reports and summaries with AI

✓ Seamless Integration with products in Microsoft’s broader security portfolio

✓ monitoring AI usage, tracking data leaks, and monitoring which users are accessing high-risk applications.

✓ Retaining and logging all interactions with AI apps across the organization and investigating new incidents..

Copilot for Security

Microsoft Copilot for Security represents a groundbreaking advancement in the realm of security technology, as it empowers defenders to harness the agility and adaptability of artificial intelligence. The solution combines OpenAI’s GPT-4 generative AI with a security-specific model from Microsoft, informed by global threat intelligence and an extensive database of daily signals. Security Copilot enables defenders to move at the speed and scale of AI, delivering critical step-by-step guidance, context and prioritize threat detection in real time.

Reducing burn-out among human defenders

With vast threat intelligence, and more than 78 million security signals, Copilot for Security could change how we manage risk in the modern world. In particular, it could help address the security skill gap at a time when more than 3.4 million security roles are currently left unfilled.

Identifying high-fidelity, high-priority incidents

The most crucial decision in the security event lifecycle has been which incidents are to be escalated to a senior resource by the organization's most junior members. Now, more seasoned engineers can zero-in on the incidents that matter most, and junior resources can get help instantly

Increasing capacity of the modern SOC

Organizations have relied on hiring entry-level security specialists to analyse the bulk of low priority security events at a manageable cost, while a select group of senior, highly-skilled security specialists handle escalated incidents. introducing Gen AI into the SOC should not be viewed as an opportunity to reduce staffing costs, rather as a way to become more effective with the resources at hand.

Performing advanced analysis in a fraction of the time

By monitoring AI usage, tracking data leaks, and monitoring which users are accessing high-risk applications.

Use Case

Security Copilot – Integration with Defender XDR

Business Drivers

- Summarize the recent threat intelligence.
- Show me the latest threat articles.
- Get threat articles associated with the finance industry.
- IP address and host contextual information in relation to threat intelligence

Solution Highlights

- Investigating incidents with multiple alerts can be a daunting task.
- To immediately understand an incident, you can tap Security Copilot in Microsoft Defender XDR to summarize an incident for you.
- Security Copilot creates an overview of the attack containing essential information for you to understand what transpired in the attack, what assets are involved, and the timeline of the attack.
- Security Copilot automatically creates a summary when you navigate to an incident's page.

Benefits

- Enhanced information security and threat protection.
- Timely and effective addressing of alerts.
- Improved discovery and assessing the risks of Shadow IT.
- Security teams who use advanced hunting to proactively hunt for threats in their network can now use a query assistant that converts any natural-language question in the context of threat hunting, into a ready-to-run KQL query.
- The query assistant saves security teams time by generating a KQL query that can then be automatically run or further tweaked according to the analyst needs.

Scale & Complexity

- Most attackers rely on sophisticated malware when launching attacks to avoid detection and analysis.
- These files are usually obfuscated and arrive as scripts, Powershell, batch, and bash.
- Security Copilot can quickly analyze these file types, reducing the time for script or code analysis and helping security teams decide on the next action steps using information from the analysis.

Cyber Threat Defense

Approach

Discover & Assess

Assess the current state of your critical security infrastructure, gaining deep knowledge of your needs and threat model.

Envision

Envision the ideal future state of your SOC, identify key risk mitigations and technical problems to solve.

Migrate

Migrate security workloads with business priorities in mind, in-building CI/CD pipelines and DevOps best practices.

Manage

Implement operational and management best practices, enabling Cognizant Cyber Threat Defence to take security operations off your plate.

Optimize

Optimize continuously, utilizing machine learning and predictive analytics to help you scale faster and keep risk down.

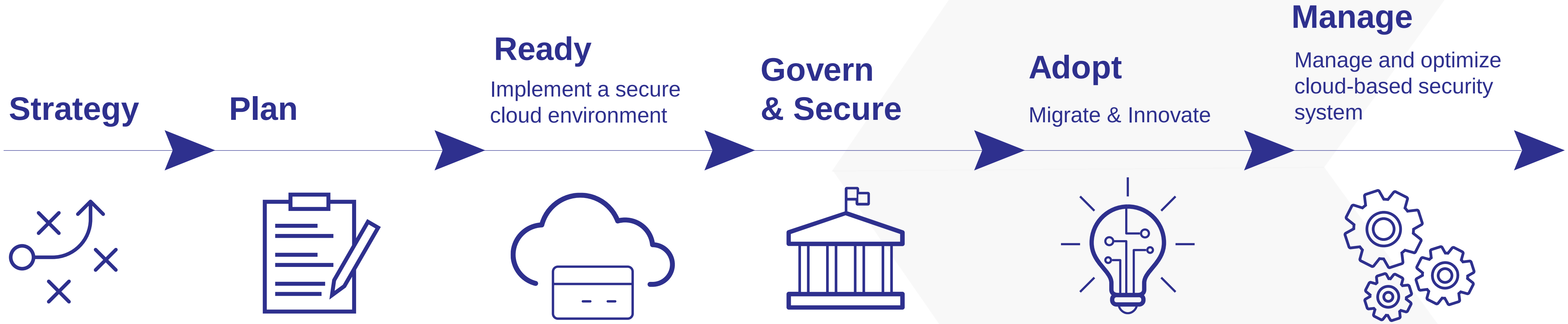
Cyber Threat Defense

What We Do

- ✓ Design security infrastructure around current best-practice architectural patterns like Zero Trust and CSMA.
- ✓ Deploy XDR components across apps, data, infrastructure, collab and endpoints.
- ✓ Integrate XDR and 3rd party data sources to cloud-native SIEM & SOAR platform.
- ✓ Embed DevOps Practices and Tooling to Improve Time to Market and Delivery.
- ✓ Operational Modernization services with custom ITSM integrations (including GenAI).
- ✓ Optional: Leverage and extend Microsoft Security Copilot capabilities with custom extensions.

We help organizations ensure they are ready to meet the challenge of today's threat landscape with the strength of the Microsoft Cloud.

Built on Microsoft’s Cloud Adoption Framework



Strategy

Plan

Ready

Implement a secure cloud environment

Govern & Secure

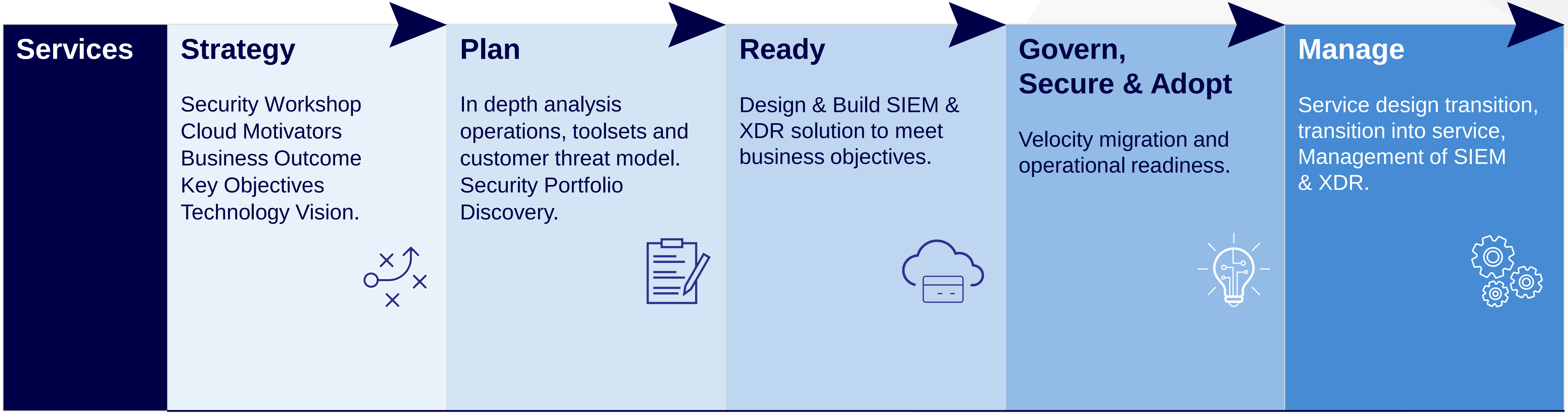
Adopt

Migrate & Innovate

Manage

Manage and optimize cloud-based security system

Cyber Threat Defense Client Journey



Services

Strategy

Security Workshop
Cloud Motivators
Business Outcome
Key Objectives
Technology Vision.

Plan

In depth analysis operations, toolsets and customer threat model.
Security Portfolio Discovery.

Ready

Design & Build SIEM & XDR solution to meet business objectives.

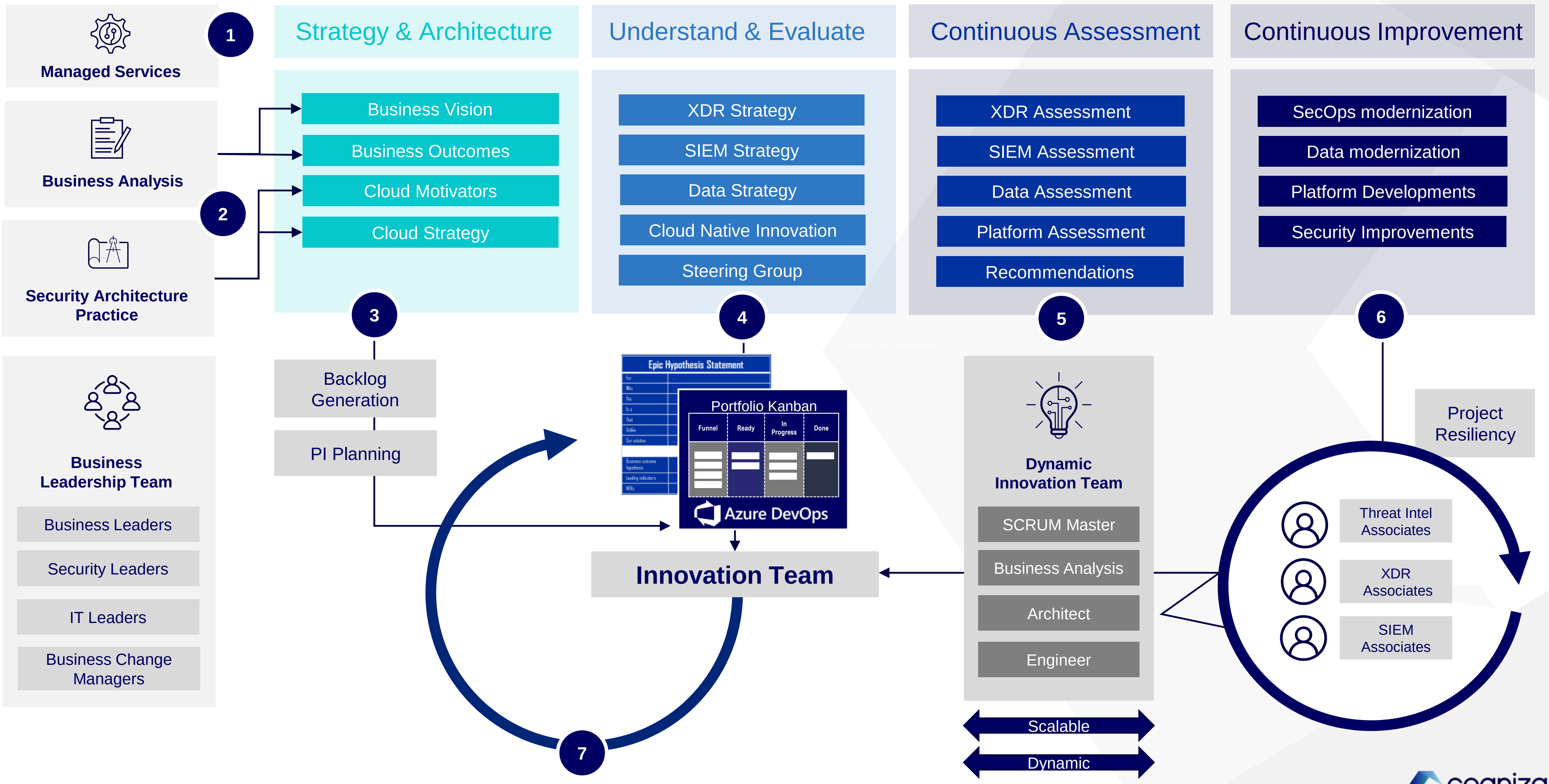
Govern, Secure & Adopt

Velocity migration and operational readiness.

Manage

Service design transition, transition into service, Management of SIEM & XDR.

Innovate From Within



1 Managed Services

Business Analysis

2

Security Architecture Practice

Business Leadership Team

- Business Leaders
- Security Leaders
- IT Leaders
- Business Change Managers

Strategy & Architecture

- Business Vision
- Business Outcomes
- Cloud Motivators
- Cloud Strategy

3

- Backlog Generation
- PI Planning

Understand & Evaluate

- XDR Strategy
- SIEM Strategy
- Data Strategy
- Cloud Native Innovation
- Steering Group

4

Epic Hypothesis Statement

Portfolio Kanban

Innovation Team

Continuous Assessment

- XDR Assessment
- SIEM Assessment
- Data Assessment
- Platform Assessment
- Recommendations

5

Dynamic Innovation Team

- SCRUM Master
- Business Analysis
- Architect
- Engineer

Scalable

Dynamic

Continuous Improvement

- SecOps modernization
- Data modernization
- Platform Developments
- Security Improvements

6

Project Resiliency

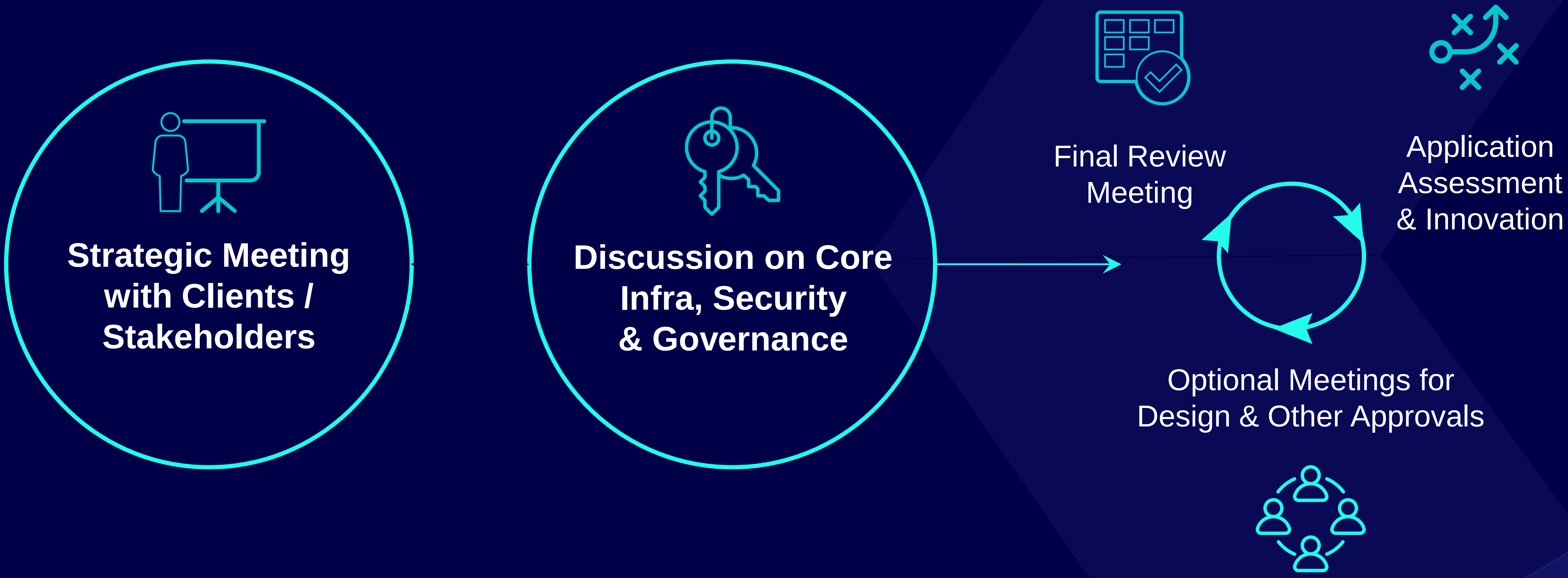
- Threat Intel Associates
- XDR Associates
- SIEM Associates

7

04

Value Proposition

Customer Engagement Journey Touchpoints



Strategic Meeting with Clients / Stakeholders

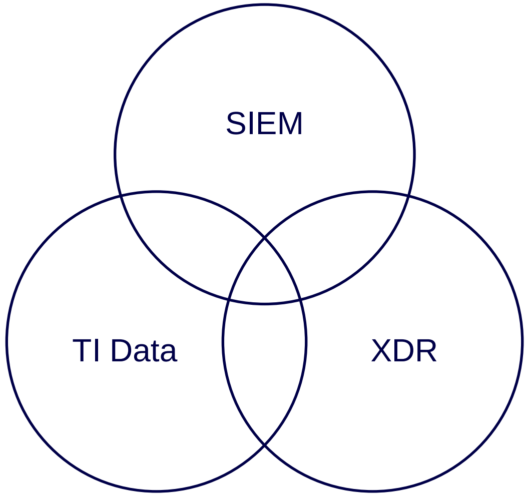
Discussion on Core Infra, Security & Governance

Final Review Meeting

Application Assessment & Innovation

Optional Meetings for Design & Other Approvals

Cyber Threat Defense: Approach



Assessment

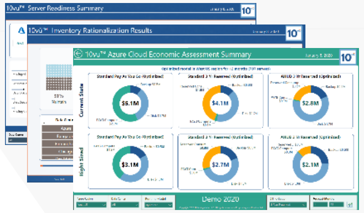
Rationalization & Cloud Suitability

Cloud Viability Analysis

Identifying Migration Strategy

- Infra & App dependencies
- Business criticality
- Security & compliance
- Business plan
- Foundation architecture and design
- Data usage pattern
- Anti-patterns details
- Migration complexity
- Tech stack suitability
- License portability

Design & Build

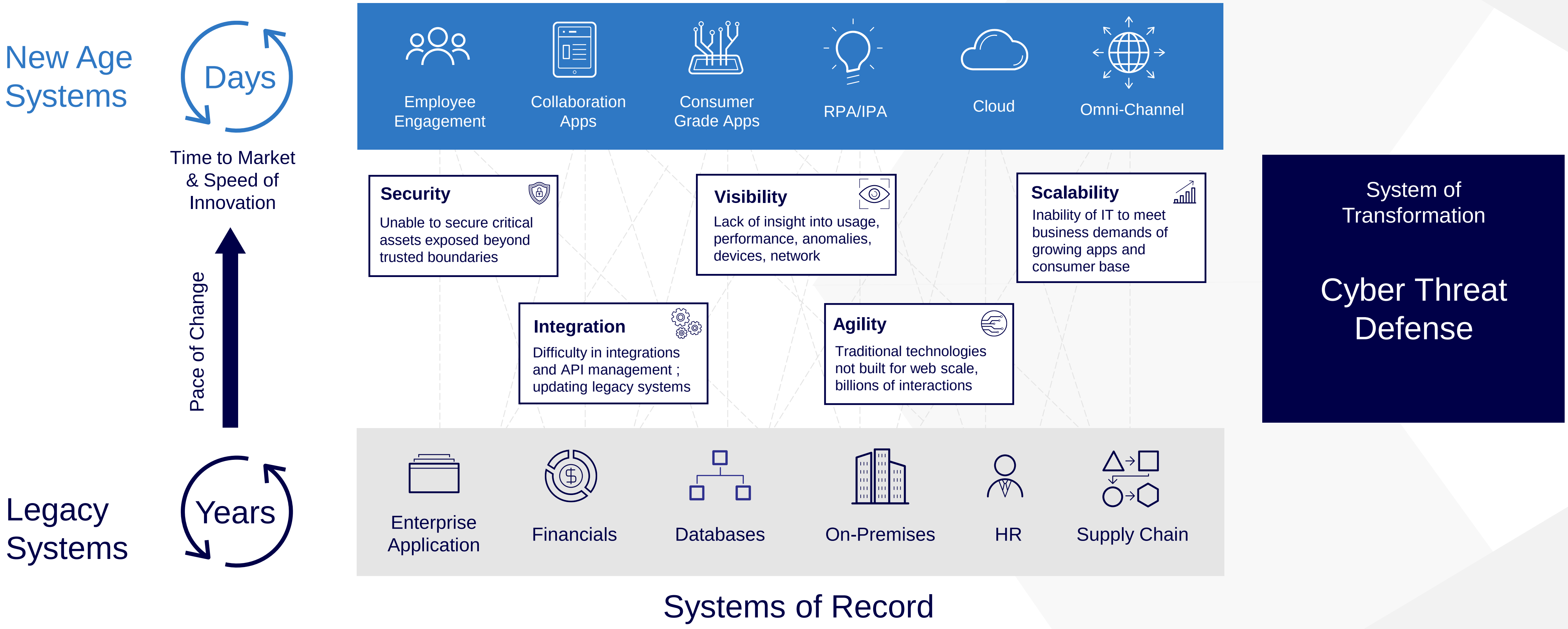

10vu™ Server Readiness Summary
10vu™ Inventory Rationalization Results
10vu™ Azure Cloud Economic Assessment Summary
10
Current State
Right Sized
Standard Pay As You Go (Optimized)
$5.1M
$4.1M
$2.8M
$3.1M
$2.7M
$2.1M
Demo 2020

Modernize

The 7 Rs Modernization

Refactor	Rearchitect	
Rehost	Replatform	
Replace	Retire	Retain

Ready to Start your Modernization Journey?



New Age Systems

Days

Time to Market & Speed of Innovation

Pace of Change

Legacy Systems

Years

Employee Engagement

Collaboration Apps

Consumer Grade Apps

RPA/IPA

Cloud

Omni-Channel

Security
Unable to secure critical assets exposed beyond trusted boundaries

Visibility
Lack of insight into usage, performance, anomalies, devices, network

Scalability
Inability of IT to meet business demands of growing apps and consumer base

Integration
Difficulty in integrations and API management ; updating legacy systems

Agility
Traditional technologies not built for web scale, billions of interactions

Enterprise Application

Financials

Databases

On-Premises

HR

Supply Chain

Systems of Record

System of Transformation

Cyber Threat Defense

05

Proof Points

Case Study 1

SIEM Migration From IBM QRadar to Microsoft Sentinel & Management For a Leading Healthcare Customer in NA

Business Drivers

- Design & Build of MS Sentinel Solution.
- Migration from IBM Qradar to Microsoft Sentinel SIEM.
- 24x7x365 SOC Operations support on Microsoft Sentinel.
- Improving the IT infrastructure and application suite to better support business needs.

Solution Highlights

- Seamless migration from IBM Qradar to Microsoft Sentinel.
- Integration of all log types / systems.
- Improved MITRE ATT&CK coverage.
- Reduction in false positives & log optimization.

Scale & Complexity

- Multi-vendor ecosystem with technologies such as: Next Gen Firewalls, WAF, Endpoint Security, File Integrity Monitoring, DLP, Vulnerability Scanner, Web Security Gateways, Identity and Access Management and Azure Cloud Security Services.

Benefits

- End to end to security operations.
- Increased visibility via a single pane of glass.
- Deliver high compliance monitoring and immediate remediation methodologies.
- Incident and threat detection worked accurately in purple team exercise.
- Adherence for higher SLA %
- Deliver intelligent threat detection and hunting features.
- Deliver cost benefits in designing & managing SIEM services.
- Adherence to HIPAA compliance & data protection regulations/ laws that needs to be followed during data transfer/access outside client location or country.

Case Study 2

Implementation of Microsoft Defender for Endpoint and Provide an Assessment Report on M365 Tenant Security For a Financial Company Based in France.

Business Drivers

- Complete Tenant Assessment and provide remediation plan for current security.
- Provide remediation plan to mitigate current security issues and improve overall security of M365 tenant.

Solution Highlights

- Solution design for Microsoft Defender for Endpoints for Servers, VDi and Windows 10 Machines.
- Implementation of Defender for Endpoint.
- Approximately 1500 Endpoints and 400+ Servers onboarded to Defender for Endpoint.
- Shadow IT discovery and alerting on risky cloud usage.
- Improved detection and remediation of Cyber security threats.

Benefits

- Enhanced information security and threat protection.
- Timely and effective addressing of alerts.
- Improved discovery and assessing the risks of Shadow IT.
- Improved protection for Endpoints.
- Improved security and compliance.
- 24/7 monitoring and support for alerts.
- Reduced downtime for business.

Scale & Complexity

- On board in scope servers, windows 10 machines to Microsoft Defender using GPO or Configuration Manager.
- Enable Extended Detection and Response (EDR), Attack surface reduction (ASR) and Next generation protection (NGP).
- 200 + recommendations have been provided along with remediation plan.

Case Study 3

Implementation of Microsoft Cloud App Security at a World Leading Life and Pension Insurance Services Provider

Business Drivers

- Securing sensitive information and enforcing compliance.
- Visibility over Microsoft and Non-Microsoft Cloud technologies.
- Information protection for Cloud apps.
- Effective detection and remediation of cybersecurity threats.
- Timely addressable of security threats and business critical alerts.

Solution Highlights

- Implementation of MCAS and Integration of MS and Non-MS Clouds (AWS & GCP).
- Improved protection for Cloud Apps.
- Improved Security and Compliance.
- Shadow IT discovery and Alert on Risky Cloud Usage.
- Improved detection and remediation of cybersecurity threats.

Benefits

- Revenue to Cognizant for SOC implementation.
- Enhanced security and compliance.
- Improved discovery and assessing the risks of Shadow IT.
- Improved protection for Endpoints.
- Improved security and compliance.
- 24/7 monitoring and support for alerts.
- Reduced downtime for business.

Scale & Complexity

- Dispersed split of Cloud technologies across multiple Cloud hosted services and Vendors.
- 400+ Servers scattered across multiple Clouds.

Case Study 4

Implementation of Microsoft Purview (IP & DLP) and Azure AD Conditional Access and MFA on M365 Tenant Security For a Philippines Based Banking Client.

Business Drivers

- Greenfield Solution design for Microsoft Purview Information Protection and Data Loss Prevention including sensitivity labeling, client-based and service-based auto-labeling. Also, data loss prevention policies required with customized regular expressions and built-in functions.
- Greenfield Azure AD conditional access and multi-factor authentication (MFA) design in M365.
- Need for auditing and alerts management.

Benefits

- Enhanced information protection and data loss prevention.
- Enhanced security and compliance.
- Improved email spoofing resistance.
- Improved security and compliance.
- 24/7 monitoring and support for alerts.
- Reduced downtime for business.

Solution Highlights

- Implementation of Microsoft Purview Information Protection.
- Configuration of retention policies, content search jobs & report and customize Purview alerts.
- Greenfield implementation of MFA along with Conditional Access polices for securing Azure AD tenant from internal and external threats.
- Implementation of DKIM onto Azure AD customized domain.

Scale & Complexity

- Approximately 9000 users and 9000+ devices including Windows 10, Android and iOS mobile devices.

06

Pricing Model

Pricing Model

Subscription Cost

Service Cost

Implementation

Managed Services

About Cognizant

Cognizant (Nasdaq-100: CTSH) engineers modern businesses. We help our clients modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast- changing world. Together, we're improving everyday life. See how at www.cognizant.com or @Cognizant

UK Headquarters

Cognizant Worldwide Limited
280 Bishopsgate
London RC2M 4RB
England
Phone: +44 207 297 7600
Contact: gcloud@cognizant.com

Thank You