Partner Introduction

Microsoft Security

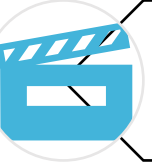InvokeLLC.com | Hello@InvokeLLC.com

Agenda

Introductions

Solution Portfolio

Solution Plays - Pre-Sales & Adoption

Call to Action

INVOKE your organization's digital journey with Microsoft Cloud solutions

With over one million licenses deployed Invoke is within the top 10 Microsoft Security partners in the United States

Top 10 Microsoft Security Partner

8 partner specializations earned through extensive Microsoft audits

Microsoft Partner Specializations

Multiple Solution partner designations & specializations from Microsoft for Modern Work, Security, and Azure

Solution Partner Designations

Invoke has been recognized by the Microsoft Entra team for its impact on Identity Governance

Microsoft Product Group Recognition

Designated Microsoft MVPs in Security, Azure, Modern Work, and other areas

Microsoft MVP Experts

Out of 100k partners Invoke is one of 190 Microsoft National Solution Providers (NSPs)

Microsoft NSP

Security

- **Identity & Access Management**
- **Defend Against Threats with SIEM plus XDR**
- **Secure Multi-Cloud Environments**
- **Protect and Govern Sensitive Data**
- **Mitigate Compliance and Privacy Risks**
- **Intune Device Management**

Azure

- **Well Architected**
- **Cloud Adoption Framework**
- **Migrate and Modernize your Infrastructure**
- **Protect your Data and Ensure Business Resiliency with BCDR**
- **Digital and Application Innovation**
- **Modernize Enterprise Applications**
- **Accelerate Innovation with Low Code**
- **Innovate and Scale with Cloud Native Apps**

Modern Work

- **Digital Workforce**
- **Frontline Worker**
- **Teamwork Deployment**
- **Teams Meetings & Phone**
- **Employee Experience with Microsoft Viva**
- **Windows 365**
- **Adoption & Change Management**

USA TOP 10
Microsoft Security

GLOBAL TOP 15
Microsoft Security

#1 Microsoft Entra
Identity Governance

Invoke | InvokeLLC.com | hello@InvokeLLC.com | +1 (713) 909-0411 | 118 Vintage Park Blvd. #W700 Houston, TX 77070

INVOKE Microsoft Partner Designations and Specializations

Microsoft Solutions Partner
Security

Specialist
Identity and Access Management
Information Protection and Governance
Threat Protection

Microsoft Solutions Partner
Modern Work

Specialist
Adoption and Change Management
Calling for Microsoft Teams
Meetings and Meeting Rooms for Microsoft Teams

Microsoft Solutions Partner
Infrastructure Azure

Specialist
Infra and Database Migration

Microsoft Solutions Partner
Digital & App Innovation Azure

Specialist
Migrate Enterprise Applications to Microsoft Azure

Azure Migrate & Modernize Ready Partner

Security & Management Elite

Microsoft FastTrack Ready Partner

Gold **Microsoft Partner**
Microsoft

USA TOP 10
Microsoft Security

GLOBAL TOP 15
Microsoft Security

#1 Microsoft Entra
Identity Governance

Invoke **Services**

Invoke Advisor
- *Journey management & advisory*

Invoke Advantage
- *On-demand consultative sessions and guidance*

Staff Augmentation
- *Additional or temporary IT staff*

Hypercare
- *Short-term post-implementation engagement*

Project Services
- *Structured engagement with scope, deliverables, and a timeline.*

Is my digital security transformation on the right track?

How do I measure success and identify the next steps?
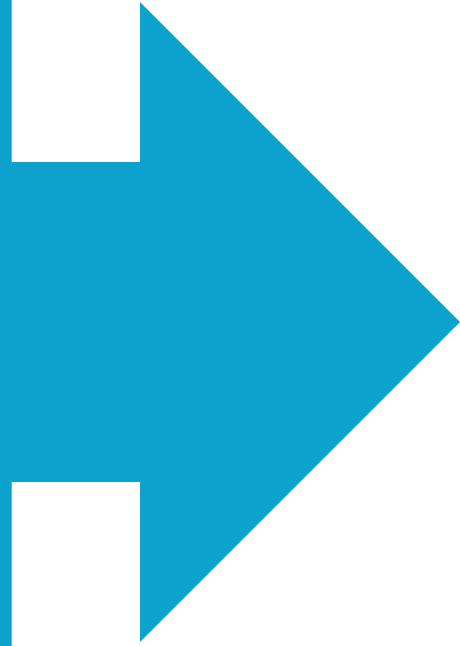
Solution Journeys - Roadmaps that guide you through the recommended practices and milestones of digital security transformation.

Solution Journey

Assess
Build Intent

Current State Assessment

Risk assessments

Proof of concepts

Plan
Map use cases from legacy solution to modern solution

Strategic & Technical Roadmaps

Enable
Implement the solution

Migrate use cases

Team skilling

Innovate
Continuous adoption of new features

Assessment cadence

1-3 Weeks

Variable (1-6 Months)

Business as usual

Funding Vehicles

- **Cyber Security Investment**
- **Microsoft Commerce Incentive**

- **Cyber Security Investment**
- **End Customer Investment Funds**
- **Azure Migrate & Modernize**
- **Customer**

- **Customer**

Microsoft 365 Threat Check Assessment

USA TOP 10

Microsoft Security

Stage 1

Engagement Setup

- Pre-Engagement Call
- Questionnaire
- Pre-requisites and scope

Stage 2

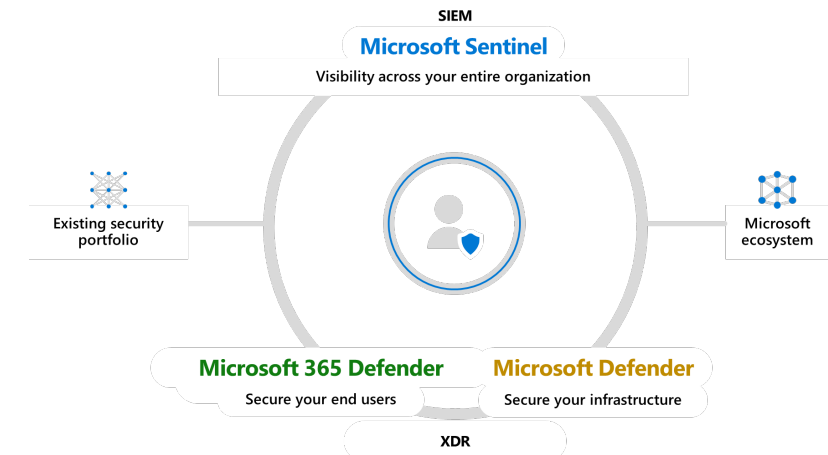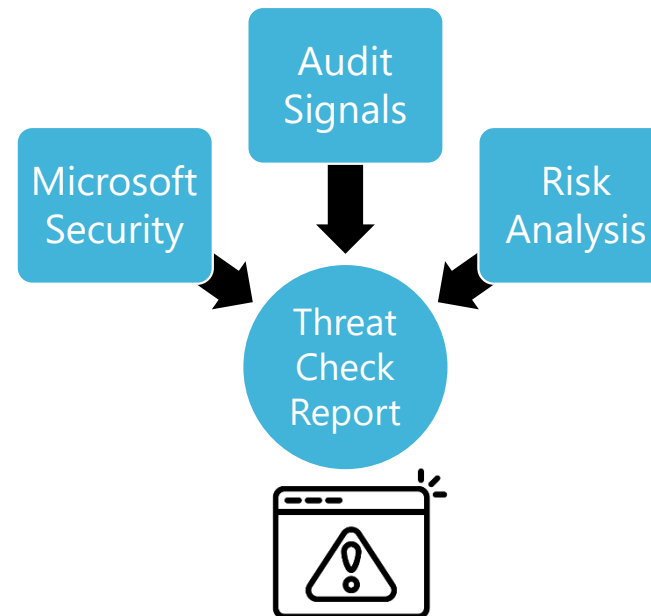**Kick-Off, Onboarding & Discovery**

- Kick-off meeting with all stake holders
- Configuration and onboarding
- Microsoft 365 Defender Overview and Demonstrations

Stage 3

Findings Presentation & Closeout

- Data collection & Documentation
- Write up and recommendations
- Assessment report presentation
- Recommended Next Steps
- Engagement Closeout

Value proposition

The Microsoft 365 Threat Check Assessment offering is designed to understand customers' security goals and objectives, identify security threats across M365 services and provide recommendations to mitigate those risks using Microsoft Security solutions.

Workloads

- Entra ID (AAD) Identity Protection
- Entra Workload ID
- Microsoft Defender Office & Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Sentinel

Engagement Outcomes

- Microsoft 365 Risk assessment report deliverable
- High-level roadmap to mitigate security risk across your Microsoft 365 ecosystem.
- 11 hours of collaborative sessions scheduled over 2-3 weeks

Assessment offers

- *Microsoft funding for Invoke-led Assessment may be available upon request*
- **Invoke-led trial licensing for qualified customers*

Audit Signals

Microsoft Security

Risk Analysis

Threat Check Report

SIEM

Microsoft Sentinel

Visibility across your entire organization

Existing security portfolio

Microsoft ecosystem

Microsoft 365 Defender

Secure your end users

Microsoft Defender

Secure your infrastructure

XDR

Microsoft Sentinel PoC

USA TOP 10

Microsoft Security

Value proposition

Modern security operations needs to be intelligent, adaptive and make best use of automation and machine learning to keep pace with today's threats. Traditional SIEM solutions gather and present security alerts but the increasingly frequent and sophisticated attacks, volume of alerts and need for rapid detection and remediation has led to a shift to more modern solutions. Microsoft Sentinel is a cloud native SIEM and SOAR solution backed by Microsoft's advanced telemetry, providing a single solution for alert detection, investigation, remediation, and proactive hunting across Microsoft and 3rd party signals through a vast ecosystem of native connectors & integrations.

Workloads

- Microsoft Sentinel
- Azure Logic Apps (Playbooks)
- First & third-party workload native connectors

Engagement Outcomes

- Review your security goals and objectives
- Identify real threats in your cloud or PoC environment
- Map identified threats to specific solution recommendations
- Automate incident response to reduce mean time to detect (MTTD) and mean time to respond (MTTR)
- Showcase security scenarios with product demos
- Develop joint plans and next steps

Who should participate

- CISO, CIO, CSO, IT Security, IT Security Operations
- 11 hours of collaborative sessions scheduled over 2-3 weeks

Assessment offers

- Microsoft funding for Invoke-led Assessment may be available upon request
- Engagement length and cost will vary, depending upon scenarios explored

Stage 1

Engagement Setup

- Pre-Engagement Call
- Pre-Requisites and Scope
- Align on SIEM use cases
- Microsoft Sentinel Overview
- Technical Setup

Stage 2

Monitoring & Response

- Remote incident monitoring
- Automated Incident Response
- Threat Exploration
- Integration with Defender (Optional)

Stage 3

Exploration and Report Generation

- Report Generation
- Results Presentation
- Customer Conversation
- Build the Plan & Next Steps Discussion

Understand the features and benefits of Microsoft Sentinel

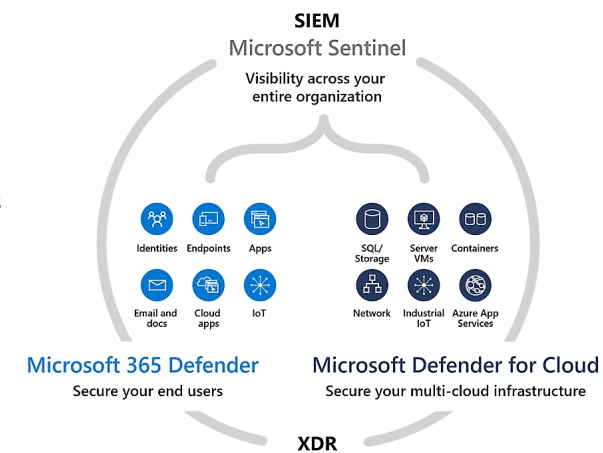Gain visibility into threats across email, identity, and data

Better understand, prioritize, and mitigate potential threat vectors

Create a defined deployment roadmap based on your environment and goals

Develop joint plans and next steps

SIEM
Microsoft Sentinel
Visibility across your entire organization

Identities Endpoints Apps

SQL/Storage Server VMs Containers

Email and docs Cloud apps IoT

Network Industrial IoT Azure App Services

Microsoft 365 Defender
Secure your end users

Microsoft Defender for Cloud
Secure your multi-cloud infrastructure

XDR

Hybrid & Multi-Cloud Threat Check

USA TOP 10

Microsoft Security

INVOKE

Timeline & Scope – Customer customizable (**minimal customer effort**)

Stage 1

Engagement Setup

- Pre-Engagement Call
- Questionnaire
- Pre-requisites and scope

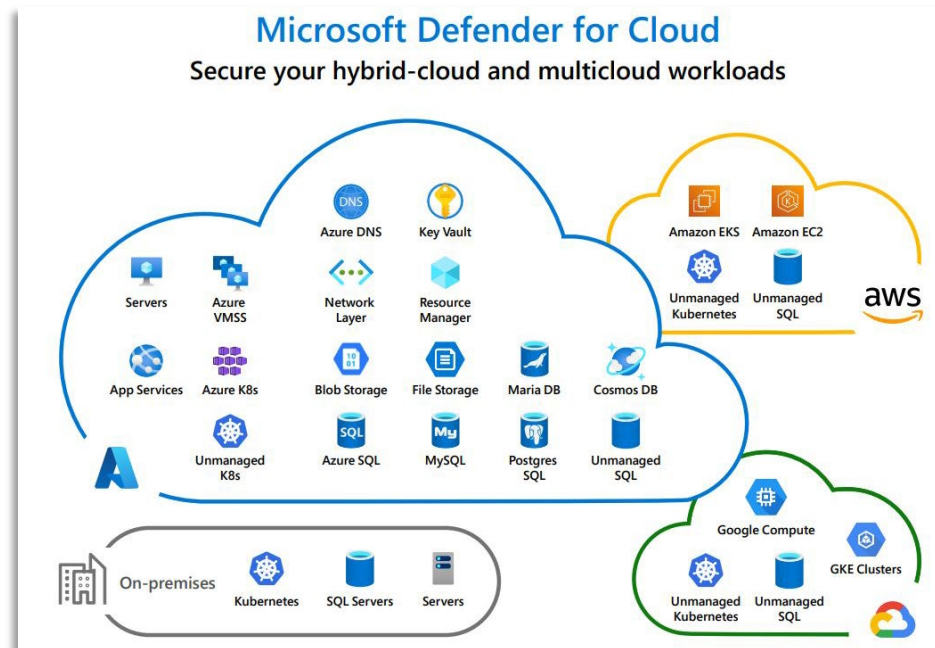**Stage 2**

Kick-Off, Onboarding & Discovery

- Kick-off meeting with all stake holders
- Configuration and onboarding
- Azure Network Security Overview and Demo

Stage 3

Findings Presentation & Closeout

- Threat data collection & Documentation
- Write up and recommendations
- Threat Assessment report presentation
- Recommended Next Steps
- Engagement Closeout

Value proposition

The Cloud Threat Check Assessment is an engagement allowing you to gain insights on active threats and vulnerabilities related to your Azure, multi-cloud, and/or hybrid workloads using Microsoft Defender for Cloud, Azure Arc, and other Azure security capabilities.

Workloads

- Microsoft Defender for Cloud
- Microsoft Sentinel
- Azure Arc
- Azure Firewall, Firewall Manager, & WAF
- Azure DDoS Protection
- Multi-Cloud Support - Azure and AWS, and/or GCP

Engagement Outcomes

- Assessment risk report deliverable
- High-level roadmap to remediate permission risk across all major cloud platforms
- Up to 17 hours of collaborative sessions scheduled over 2-3 weeks

Assessment offers

- *Microsoft funding for Invoke-led Assessment may be available upon request*
- **Invoke-led trial licensing for qualified customers*

Microsoft Defender for Cloud
Secure your hybrid-cloud and multicloud workloads

Invoke Data Risk Assessment

USA TOP 10
Microsoft Security

INVOKE

Timeline & Scope – Customer customizable (**minimal customer effort**)

Stage 1

Engagement Setup

- Pre-Engagement Call
- Questionnaire
- Pre-requisites and scope

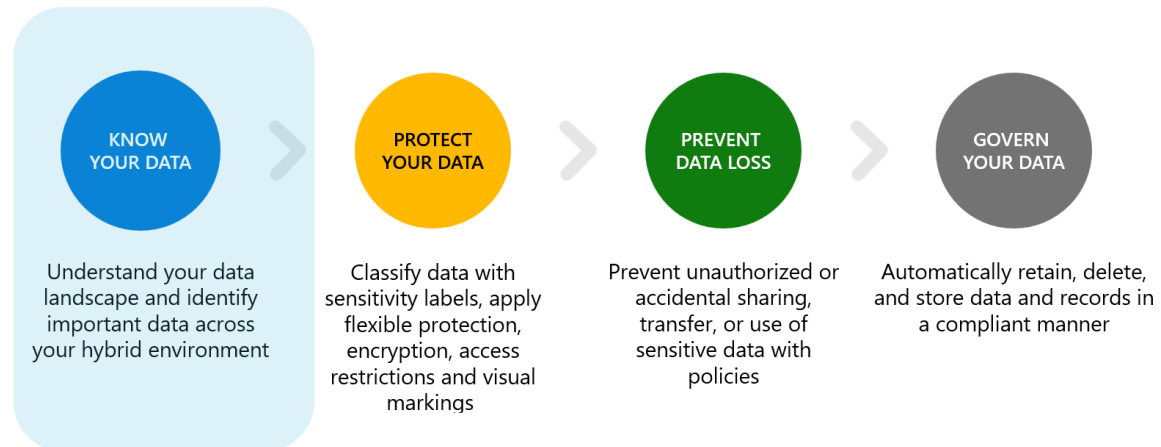### Stage 2

Kick-Off, Onboarding & Discovery

- Kick-off meeting with all stake holders
- Configuration and onboarding

Stage 3

Findings Presentation & Closeout

- Data risk data collection & Documentation
- Write up and recommendations
- Understand how to mitigate data risk using Microsoft integrated compliance solutions.
- Data Assessment report presentation
- Recommended Next Steps
- Engagement Closeout

Value proposition
The Invoke Data Risk Assessment offering is designed to Identify privacy and regulatory risks in Dark Data present in Microsoft 365 and on-premises repositories to help mitigate using Microsoft 365 compliance solutions.

Workloads
- Exchange Online
- SharePoint Online
- Windows Data Loss Prevention
- Microsoft Purview Information Protection
- Microsoft Purview Compliance Manager

Engagement Outcomes
- Data assessment risk report deliverable
- High-level roadmap to remediate data risk
- Understand how to mitigate data risk using Microsoft integrated compliance solutions

Participation
- 15 hours of collaborative sessions scheduled over 2-3 weeks
- Project Executive Sponsor (CSO, CISO, CEO, CFO, CIO or CTO), Enterprise/Compliance Architects, Privacy & Compliance Specialists, and Microsoft 365 Administrator

Assessment offers
- *Microsoft funding for Invoke-led Assessment may be available upon request*
- **Invoke-led trial licensing for qualified customers*

KNOW YOUR DATA

Understand your data landscape and identify important data across your hybrid environment

PROTECT YOUR DATA

Classify data with sensitivity labels, apply flexible protection, encryption, access restrictions and visual markings

PREVENT DATA LOSS

Prevent unauthorized or accidental sharing, transfer, or use of sensitive data with policies

GOVERN YOUR DATA

Automatically retain, delete, and store data and records in a compliant manner

Identity Governance Assessment - Microsoft Entra

USA TOP 10

Microsoft Security

Stage 1

Stage 2

Stage 3

Engagement Setup

- Introductions & engagement walk-through
- Gather key business scenarios through a questionnaire
- Identify business stakeholders
- Kick off
- Microsoft Entra ID Governance overview
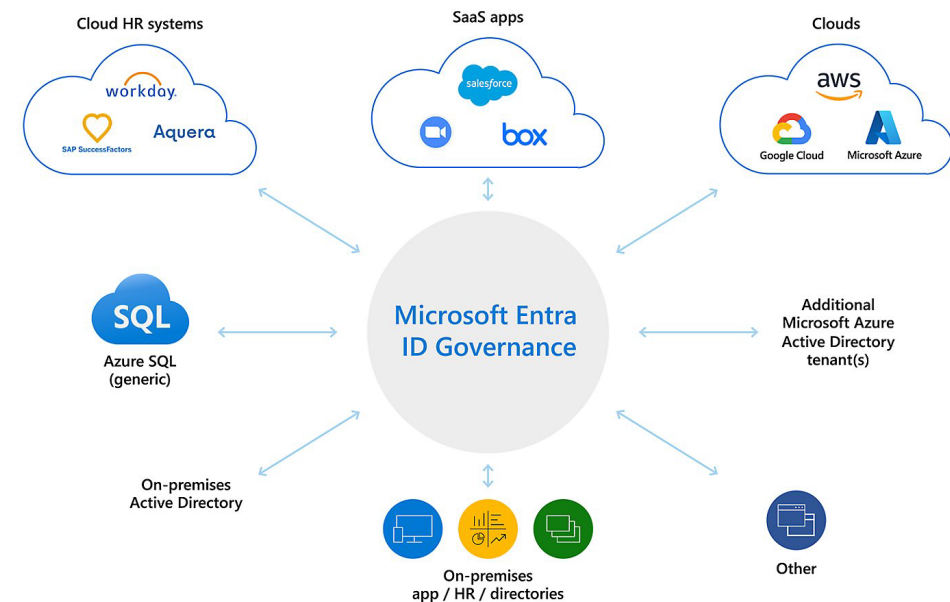- Assessment workload provisioning

Assessment Activities

- Tenant analytics for Identity Governance
- Authentication & authorization
- Assess guest access risk
- Cloud HR Provisioning
- Identity Lifecycle automation (JML)
- Identify primary use cases
- Demonstrations

Recommendations & Next Steps

- Business Value Discussion (BVD)
- Prioritize customer's top use cases and scenarios
- Key results, recommendations, and next steps
- Closeout

Value proposition

Microsoft Entra ID Governance: Transform your IAM processes and achieve your business goals. Learn how to simplify, secure, and improve your identity and access management (IAM) processes with a cloud-powered AI-based solution. Invoke will assess your current IAM processes, where we will analyze your IAM infrastructure, identify your IAM challenges and opportunities, and provide you with a customized report and recommendations on how to improve your IAM processes with Microsoft Entra ID Governance.

Workloads

- Microsoft Entra Azure Active Directory
- Microsoft Entra ID Governance

Engagement Outcomes

- Evaluation of current identity and access management processes
- Identity compliance, risk, and productivity opportunities identified
- Recommendations for improving identity and access management practices
- Identity governance use cases prioritized, and next steps established

Participation

- 18 hours of collaborative sessions scheduled over 2-3 weeks.
- Who should attend – CIO, CISO, CSO, Identity and/or App owners/decision makers, IT Security, IT Operations, Security Architect, Security Engineers, and Application business owners.

Assessment offers

- *Microsoft funding for Invoke-led Assessment may be available upon request*
- **Invoke-led trial licensing for qualified customers*

Cloud HR systems

workday.

SAP SuccessFactors   Aquera

SaaS apps

salesforce

box

Clouds

aws

Google Cloud   Microsoft Azure

SQL

Azure SQL (generic)

Microsoft Entra ID Governance

Additional Microsoft Azure Active Directory tenant(s)

On-premises Active Directory

On-premises app / HR / directories

Other

Okta to Microsoft Entra Migration Assessment

USA TOP 10

Microsoft Security

Value proposition
Knowing current state is critical to managing engagement risk for any migration. Specific to identity, there are foundational components that must be in place to support Okta to Azure AD migration success. Invoke will develop a remediation plan, and a preliminary migration plan for your applications in Okta with the ultimate destination being Azure AD. Eligible workloads - Azure Active Directory (SSO, Conditional Access, Identity protection, MFA, SSPR, IGA), Microsoft Endpoint Manager, and Microsoft 365 E3 or E5.

Workloads
- Microsoft Entra ID (formerly Azure Active Directory)
- Microsoft Entra ID Governance
- Microsoft Entra External Access

Engagement Outcomes
- Securely work anywhere, anytime, and on any device (Zero Trust)
- Understand how you can reduce complexity and save up to millions in licensing cost
- Discover current applications estate and bucketized migration work effort estimate
- Have a clear vision of understanding of your tailored journey to Microsoft Entra through a migration Statement of Work and executive presentation

Participation
- 15 hours of collaborative sessions scheduled over 3-4 weeks.
- Who should participate – CIO, CISO, CSO, Identity and/or App owners/decision makers, IT Security, IT Operations, Security Architect, Security Engineers, and Application business owners.

Assessment offers
- *Microsoft funding for Invoke-led Assessment may be available upon request*
- **Invoke-led trial licensing for qualified customers*

Timeline & Scope – Customer customizable (**minimal customer effort**)

Stage 1

Engagement Setup
- Introductions & engagement walk-through
- Gather key business scenarios through a questionnaire
- Identify business stakeholders
- Kick off
- Microsoft Entra overview
- Assessment workload provisioning
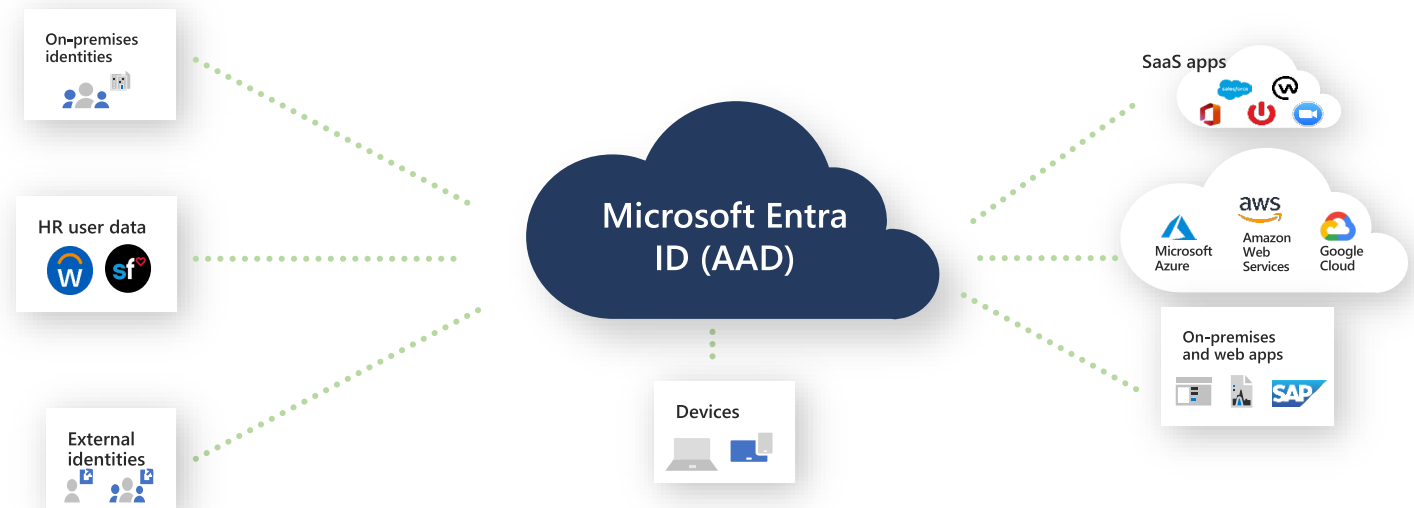
Stage 2

Assessment Activities
- Current State Assessment of Microsoft Entra ID & Okta
- Identify primary use cases
- Inventory 3rd party IdP apps
- Normalize & Rationalize App details & Owners
- Bucketize apps by migration work effort
- Demonstrations

Stage 3

Recommendations & Next Steps
- Business Value Discussion (BVD)
- Prioritize customer's top use cases and scenarios
- Develop migration Statement of Work
- Key results, recommendations, and next steps
- Closeout

On-premises identities

HR user data

External identities

Microsoft Entra ID (AAD)

Devices

SaaS apps

Microsoft Azure • Amazon Web Services • Google Cloud

On-premises and web apps

Cloud Permissions Management Risk Assessment

Timeline & Scope – Customer customizable (**minimal customer effort**) →

Stage 1
Engagement Setup
- Pre-Engagement Call
- Questionnaire
- Pre-requisites and scope

Stage 2
Kick-Off, Onboarding & Discovery
- Kick-off meeting with all stakeholders
- Configuration and onboarding
- Entra Permission Management Overview and Demo

Stage 3
Findings Presentation & Closeout
- Data collection & Documentation
- Write up and recommendations
- Assessment report presentation
- Recommended Next Steps
- Engagement Closeout

Value proposition

Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility into permissions assigned to all identities – users and workloads – actions, and resources across cloud infrastructures and identity providers. It detects, right-sizes, and monitors unused and excessive permissions and enables Zero Trust security through least privilege access in Multi-Cloud - Microsoft Azure, AWS, and GCP.

Workloads
- Azure Active Directory
- Entra Permissions Management*
- Multi-Cloud - Azure, AWS, and/or GCP

Engagement Outcomes
- Assessment risk report deliverable
- High-level roadmap to remediate permission risk across all major cloud platforms

Participation
- 17 hours of collaborative sessions scheduled over 2-3 weeks.
- Who should participate – CISO, CSO, Identity and/or App owners/decision makers, IT Security, IT Operations, Security Architect, Security Engineers, and Cloud Platform Architects.

Assessment offers
- *Microsoft funding for Invoke-led Assessment may be available upon request*
- **Invoke-led trial licensing for qualified customers*

Microsoft Entra Permissions Management

USA TOP 10

Microsoft Security

Value proposition

This offering is designed for customers taking either their first steps in exploring the use cases for, and benefits of, Microsoft Intune, or for customers that have already started their endpoint management modernization journey to the "North Star" of enabling a cloud-powered and scalable solution for hybrid work. The Good-Better-Best approach to operationalization enables organizations to rapidly consume the entire journey, or to incrementally consume over time to meet budgetary and organizational change management needs.

Workloads
- Microsoft 365 E3 / E5
- Windows / Windows 365
- Microsoft Intune

Engagement Outcomes
- Discover endpoint management goals and objectives to support a roadmap
- Customer endpoint management use cases evaluated in a live environment
- Accelerate your endpoint management journey
- Defined next steps based on your needs and objectives

Participation
- 18 hours of collaborative sessions scheduled over 2-3 weeks.
- Who should attend – Endpoint managements owners/decision makers, IT Security, IT Operations, Endpoint Architects, Security Engineers, and desktop engineering.

Engagement Offer*
- *Microsoft funding for Invoke-led Journey may be available upon request*

Timeline & Scope – Customer customizable (**minimal customer effort**)

Stage 1
Assess the Customer
- Pre-Engagement Call
- Questionnaire
- Pre-requisites and scope
- Microsoft Intune Overview
- Managing Endpoints

Stage 2
Art of the Possible
- Entra ID
- Microsoft Devices
- Microsoft 365 Apps and Edge
- Analytics and Reporting
- Migration

Stage 3
Build a Plan & Closeout
- Workload Analysis
- Report and Recommendations
- Engagement Closeout & Next Steps

Azure AD
- ❑ Azure AD Overview
- ❑ Secure, Seamless Access to all Your Apps with Azure AD

Microsoft Devices
- ❑ Microsoft Surface
- ❑ Surface Hub
- ❑ Microsoft Teams Rooms
- ❑ HoloLens

Microsoft 365 Apps and Edge
- ❑ Microsoft 365 Apps for Enterprise
- ❑ Microsoft Edge

Analytics and Reporting
- ❑ Endpoint Analytics
- ❑ Intune Reporting and Graph API

Migration
- ❑ Migration Overview

Deploy with zero touch

Simplify and speed deployments

Manage digital estate health

Automate updates

Microsoft 365 Copilot Readiness Assessment

USA TOP 10 Microsoft Security

Microsoft Solutions Partner — Modern Work

Timeline & Scope – Customer customizable (**minimal customer effort**)

Value proposition

Grounded in business data, Microsoft 365 Copilot is designed to help organizations unleash creativity, unlock productivity, and level up skills. With this readiness assessment, customers will work through various demos on copilot in action, relevant user scenarios challenges and pain points to identify top prioritized scenarios for their workforce.

Workloads
- Microsoft 365 Copilot
- Microsoft Entra
- Microsoft Purview

Engagement Outcomes
- Identify technical requirements for Microsoft 365 Copilot
- Identify participants for Microsoft 365 Copilot
- Select Microsoft 365 Copilot scenarios
- Deliver a prioritized, actionable plan to quickly address your worker needs by implementing and adopting Microsoft 365 Copilot

Participation
- Up to 10 hours of collaborative sessions scheduled over 2-3 weeks
- Who should participate – CIO, Enterprise Architects, Executive Sponsor, LOB leaders, Project Manager, Key Knowledge workers, and IT Decision Makers.

Assessment offers
- *Microsoft funding for Invoke-led Assessment may be available upon request*

Stage 1

Engagement Setup & Assess
- Pre-Engagement Call
- Questionnaire
- Readiness Assessment
- Scorecard & Guidance

Stage 2

Kick-Off, Art of the Possible
- Kick-off meeting with all stake holders
- Art of the Possible Kick-Off
- AI-powered organization
- Responsible AI commitment
- Microsoft 365 Copilot Overview
- Unleash Productivity, Unlock Creativity, Uplevel Skills
- Better together with Teams
- Microsoft 365 Copilot Personas

Stage 3

Findings Presentation & Closeout
- Build the Plan Kick-Off
- Identify scenarios based on customer's Business Decisions pain points
- Discover personas and map them to customer's business challenges
- Provide a summary of prioritized scenarios
- Deliver an overall plan for pilot of Microsoft 365 copilot, next steps and identified risks
- Engagement Closeout
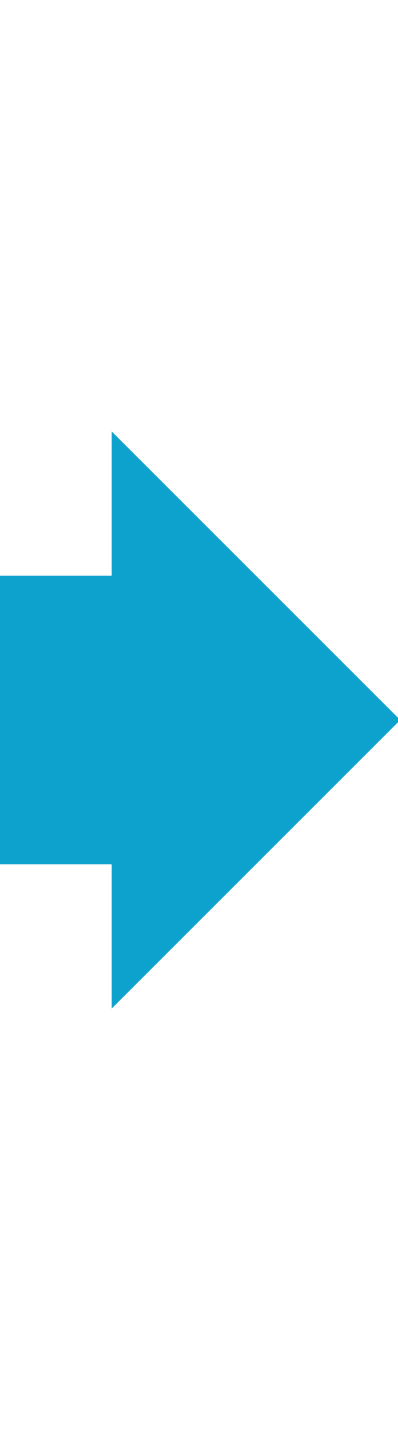
Your AI assistant at work

Assess → Art of the Possible → Build the Plan

Do you require expert engagement outside of Project Services?

Invoke Advisor - Get a customized and data-driven plan for your digital landscape, with annual assessments, monthly updates, and insights from our experts.

Invoke Advisor for Microsoft 365 Security

USA TOP 10

Microsoft Security

Timeline & Scope

Annual
Assessment & Road Mapping

- Current State Assessment
- Baseline of the customers environment within the designated Solution Journey
- Solution Road mapping
- Based on the outcome of the assessment and designated Solution Journey Invoke develops a Solution Roadmap

Monthly
Road Map Checkpoint & Solution Updates

- Measure actual progress against the roadmap and vision
- Highlight any roadblocks faced and successes celebrated
- Highlight new features or capabilities and how they can benefit your organization
- Discuss recent features and trends relevant to the solution area

Bi-Weekly
Proactive Advisory Sessions

- Data-driven understanding of environment health based on tenant signals to assist with prioritization and risk management
- Support prioritization motion of potential risks or issues
- Suggest strategies or actions to optimize the solution's performance

Reactive
Advisory Sessions

- On-demand advisory for addressing risks, issues, business opportunities OR expert guidance for implementing specific features or controls

Value proposition

Cyberattacks are becoming more sophisticated and frequent, and they can cause serious damage to your business reputation, productivity, and profitability. You need a security solution that can advise you on how to prevent, detect, and respond to threats, as well as comply with industry and regional regulations. Microsoft 365 Security Advisor is a comprehensive security solution that helps you protect your users, devices, data, and applications from cyberthreats.

Workloads

- Microsoft 365 Defender

Engagement Outcomes

- Assess your current security posture and identify gaps and risks.
- Solution implementation guidance by Invoke's security expertise and Microsoft recommended practices.
- Monitor and manage your threat protection use cases across Microsoft 365 services and other cloud platforms.
- Access advanced security features such as identity protection, endpoint protection, Microsoft 365 Apps, and cloud application security.
- Access on-demand advisory and consultation from Microsoft-certified security experts.
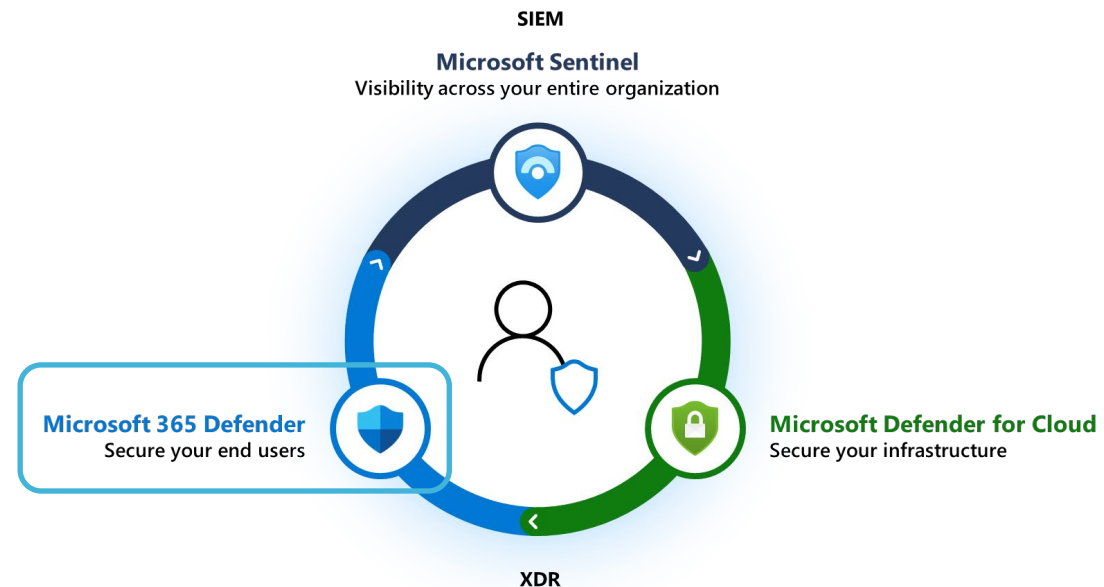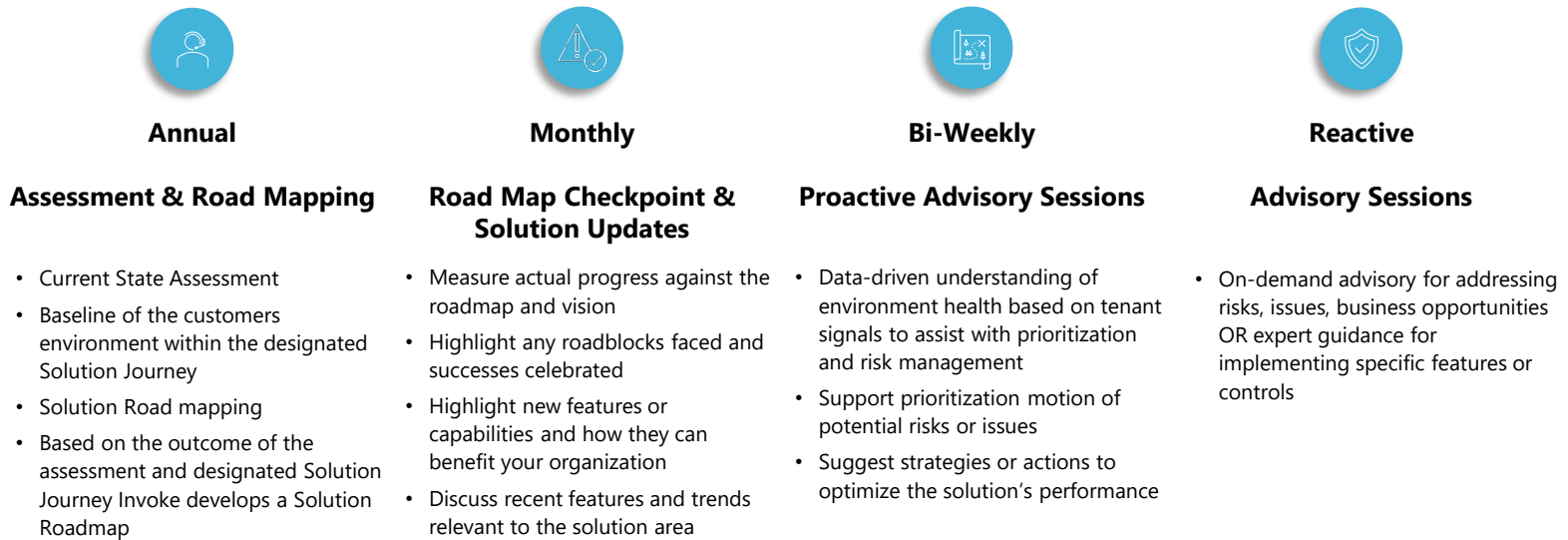
Participation

- Collaborative advisory & consultative sessions scheduled over a 12-month period.
- Who should participate – CIO, CISO, CSO, information security owners/decision makers, IT Security, Security Architect, and Security Engineers.

Assessment offers

- *Investment offers may be available upon request*

SIEM

Microsoft Sentinel
Visibility across your entire organization

Microsoft 365 Defender
Secure your end users

Microsoft Defender for Cloud
Secure your infrastructure

XDR

Invoke Advisor for Modern Security Operations

INVOKE | USA TOP 10
Microsoft Security

Timeline & Scope

Annual	Monthly	Bi-Weekly	Reactive

Value proposition
Modernizing Security Operations helps you leverage the power of Microsoft Sentinel, a cloud-native SIEM solution, to simplify and enhance your security operations. With our expert guidance, you can collect, analyze, and respond to security threats across your enterprise, using AI and automation. You can also integrate Microsoft Sentinel with additional Microsoft and other security solutions, such as Microsoft Defender, Azure Security Center, and Microsoft 365 Defender, to create a unified and comprehensive security platform. Whether you are new to Microsoft Sentinel or looking to optimize your existing deployment, Invoke Advisor can help you achieve your security goals and maximize the return on your Microsoft Sentinel investment.

Workloads
• Microsoft Sentinel

Engagement Outcomes
• Assess your current security posture and identify gaps and risks.
• Solution implementation guidance by Invoke's security expertise and Microsoft recommended practices.
• Establish & reach your Modern Security Operations vision.
• Improved security posture, reduced risk, and increased compliance with Microsoft Sentinel's cloud-native capabilities and threat intelligence.
• Access on-demand advisory and consultation from Microsoft-certified security experts.
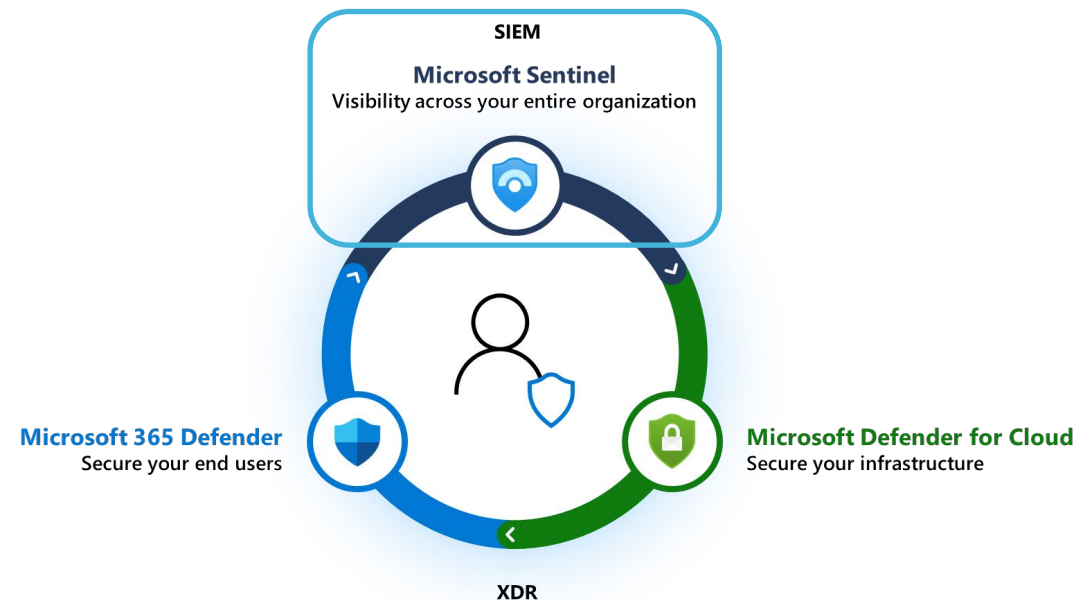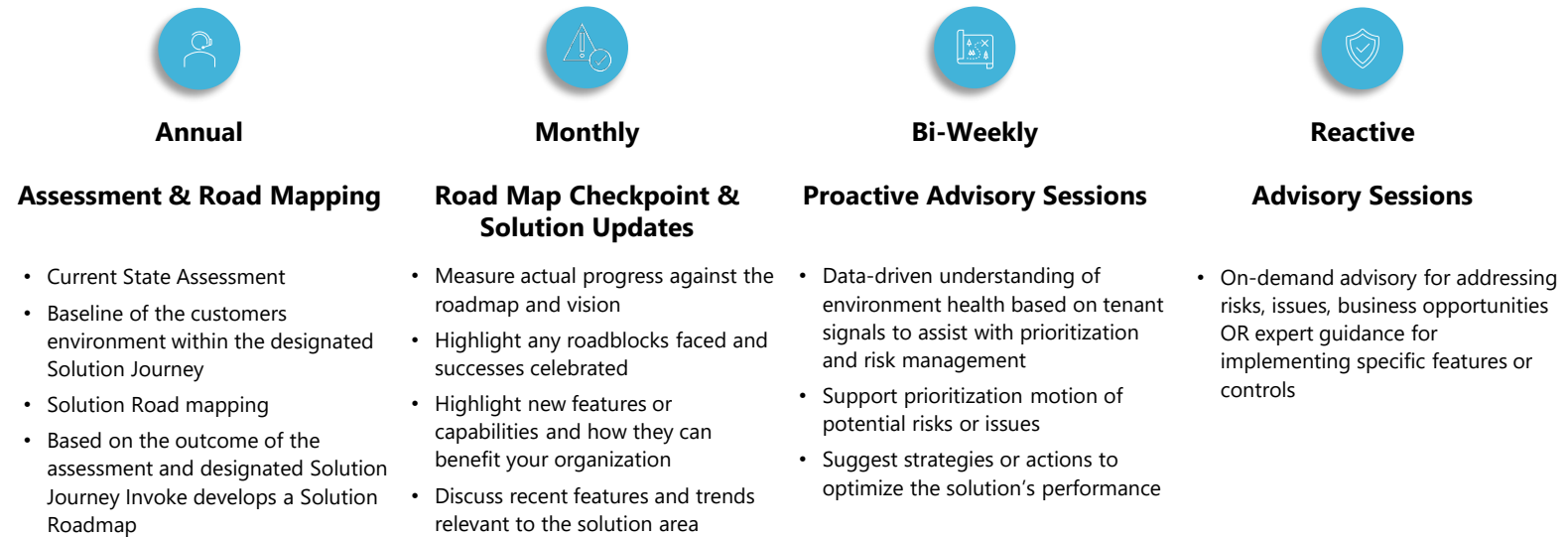
Participation
• Collaborative advisory & consultative sessions scheduled over a 12-month period.
• Who should participate – CIO, CISO, CSO, information security owners/decision makers, IT Security, Security Architect, SOC Manager, and Security Engineers.

Assessment offers
• *Investment offers may be available upon request*

Assessment & Road Mapping

• Current State Assessment
• Baseline of the customers environment within the designated Solution Journey
• Solution Road mapping
• Based on the outcome of the assessment and designated Solution Journey Invoke develops a Solution Roadmap

Road Map Checkpoint & Solution Updates

• Measure actual progress against the roadmap and vision
• Highlight any roadblocks faced and successes celebrated
• Highlight new features or capabilities and how they can benefit your organization
• Discuss recent features and trends relevant to the solution area

Proactive Advisory Sessions

• Data-driven understanding of environment health based on tenant signals to assist with prioritization and risk management
• Support prioritization motion of potential risks or issues
• Suggest strategies or actions to optimize the solution's performance

Advisory Sessions

• On-demand advisory for addressing risks, issues, business opportunities OR expert guidance for implementing specific features or controls

SIEM
Microsoft Sentinel
Visibility across your entire organization

Microsoft 365 Defender
Secure your end users

Microsoft Defender for Cloud
Secure your infrastructure

XDR

Next steps

- Schedule a meeting

Q&A

Stephen Leuthold / Director of Modern Work & Security
Stephen.Leuthold@InvokeLLC.com

Ryan Durbin / Director of Operations
Ryan.Durbin@InvokeLLC.com

Denny Singleton / Director of Service Delivery
Denny.Singleton@InvokeLLC.com

118 Vintage Park Blvd, Suite W7000
Houston, TX 77070
+1 (713) 909-0411

Services Comparison

Service	Project Services	Hypercare	Staff Augmentation	Invoke Advantage	Invoke Advisor
Comprehensive project management with a team of delivery resources	X				
Outcome-focused service delivering specific products via defined scope & deliverables	X				X
Service following predefined procedures		X		X	X
Provides extra support after a launch or implementation		X			X
Expert IT consultation service providing guidance and advice				X	X
Provision of additional or temporary IT staff as per your needs			X		