

YES PLAYS

YOUR ENABLEMENT FOR SUCCESS

- Strengthen Security-



Connecting the 5 Lifecycle Stages of an opportunity across Data Security, Threat Detection & Response, Risk Management, and Secure Connectivity.

eGroup
ENABLING TECHNOLOGIES

Active, Consistent, & Frequent



What Is A YES (Your Enablement For Success) Play

At eGroup Enabling Technologies, the **YES Play** is designed to connect the 6 stages of the sales lifecycle into a consistent and repeatable sales motion that allows us to:

- ✓ Create consistent pipeline for solutions in our focus portfolio
- ✓ Convert that pipeline into qualified sales leads
- ✓ Deliver consistent and repeatable presales and post-sales engagements that encourage efficiency, automation, and high-quality outputs
- ✓ Connects valuable recurring services opportunities to everything we sell

All While Helping You To Understand The Following-

- ✓ “Who” would buy this, “Who” should I be speaking to?
- ✓ “Why” do organizations adopt or use these solutions?
- ✓ “What” are the features and benefits of these solutions?

Sales Lifecycle Stages



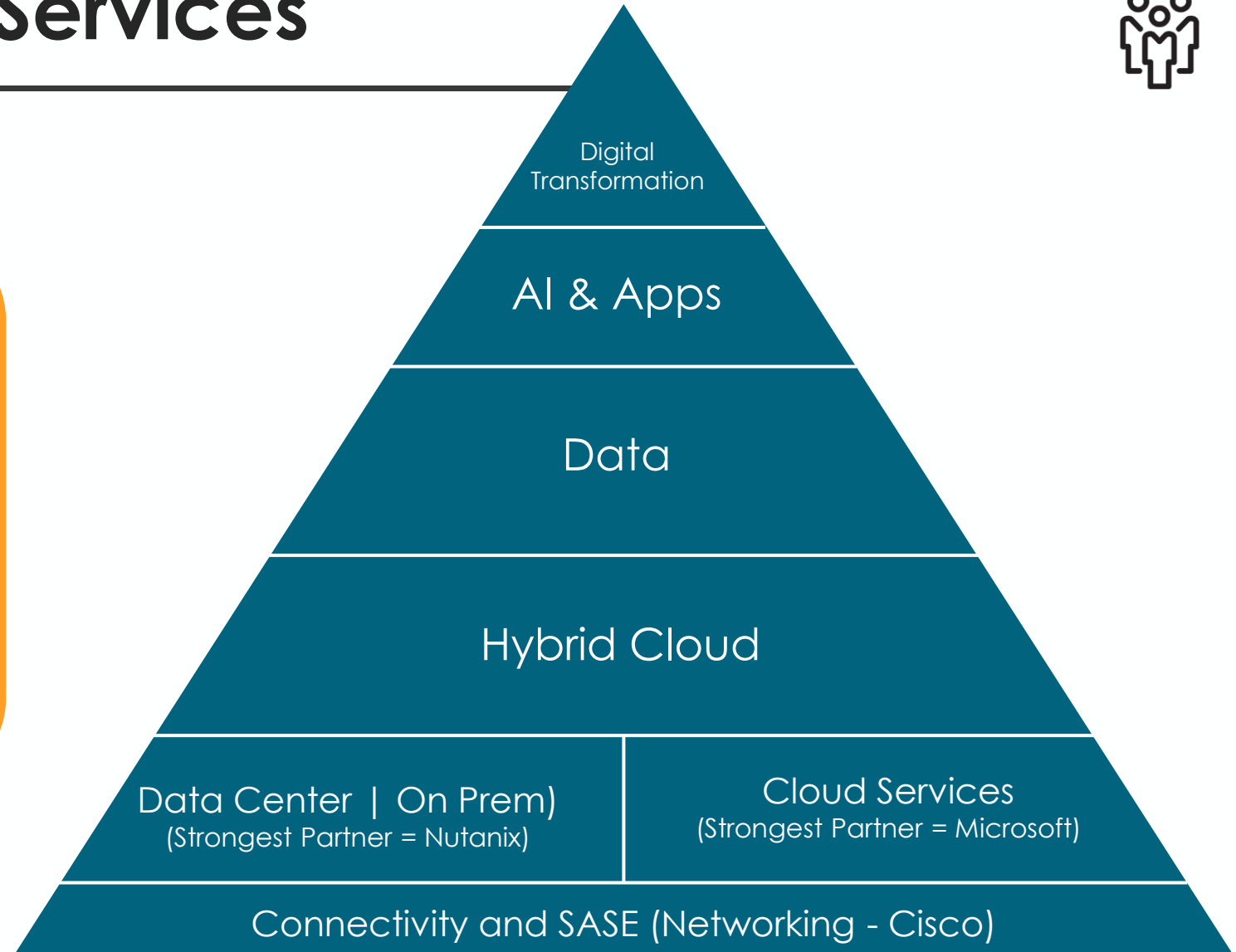
- **Generate Pipeline (MQLs)** - Create & Qualify a Lead
 - Generate marketing qualified leads (MQL) through our partner channel, eGroup events, social media, website, and digital presence.
 - Generate sales qualified leads (SQL) by further developing MQLs and our direct marketing efforts from our Sales Development Reps (SDR) through campaigns, direct dial, and social.
- **Readiness** - Assess, Plan & Present a Roadmap
 - Conduct standardized engagements with consistent outputs to assess customer needs and present valuable and actionable solutions.
 - Deliver a standardized presentation of findings that addresses the customer needs and includes:
 - Supporting data from the assessment
 - Actionable Next Steps – Statement of Work (SOW)
 - Summary Solution Cost / Total Cost of Ownership (TCO)
 - Summary of Managed Services including Scope and Price
- **Validate** - POC / Pilot a Solution
 - Test the value and capability of the solution with a pilot engagement. Skip directly to implementation if not required
- **Implementation**
 - Implement the solution for the client and confirm value
- **Manage & Optimize**
 - Secure Recurring Services, such as Managed Services Provider Agreement (MSPA), MSSP, Partner Support, and CSP

Selling Solutions + Services



Solutions & Services

- Artificial Intelligence (AI)
- Data
- Platform (Cloud / On Prem)
- Productivity (Microsoft 365)
- Security & Compliance
- Managed Services
- Organizational Change Management
- Strategic Advisory Services
- Strategic Roadmap Discussions
- Licensing Optimization
- Project Coordination



Customer Relevance = Customer Value = Services-led Solutions for Digital Transformation

YES Play Quick Links



- [Data Security & Risk Management](#)



- [Threat Detection & Response](#)



- [Microsoft Endpoint Management](#)



- [Secure Connectivity](#)



- [Secure Access Service Edge \(SASE\)](#)

Data Security & Risk Management



“Ask”

Key Asks:

1. How much money do you think you could save if you did a thorough comparison of tools, you might already have vs 3rd party tools you are using today?
2. How many different security solutions are you currently using?
3. Are there any known gaps in your current data security posture?

Follow up Asks:

1. Do you have a hybrid security plan for a hybrid (cloud + on prem) environment?
2. Are there any specific compliance or regulations that you need to follow?
3. Have you ever had a security breach? Outside of the recovery effort are their areas that you wish you were better equipped after the fact?
4. Is there a unified view for all of your data and security telemetry?

“Say”

What are common responses to this question?

1. I have a layered security solution in place already
2. The Microsoft Security licensing is too expensive
3. Don't want to put all my eggs in one basket

How do you handle these objections?

1. Microsoft has a vast intelligence spectrum – per month:
 - a. Scan 400 billion emails across outlook.com and Office 365 for phishing and malware
 - b. Process 450 billion authentications across all cloud services
 - c. Execute 18+ billion Bing webpage scans
 - d. Update 1+ billion Windows devices
2. Allow us to run a TCO looking for cost avoidance opportunities and overlap in solutions

“Do”

Key Do's - What talk track do you use to tee-up the next action?

1. Security Assessment
2. Microsoft MCI Security Engagement
3. Microsoft 365 Roadmap Workshop
4. Co-sell with the Microsoft Account team
5. ThreatDefender MXDR MSSP

Optional Do's:

1. FastTrack
2. Strategic Advisory Services

Data Security & Risk Management

YES PLAYS
YOUR ENABLEMENT FOR SUCCESS

Create Lead 0% Qualify Lead 10%
IDENTIFY VALUE

Assess, Plan, and Present Roadmap 20% - 40% Pilot Solution 60%
CREATE VALUE

Implement 80% Secure Recurring Services
REALIZE VALUE

Who = IT Manager, IT Architect, CIO, CSO, Security Director

Why = Defend against Phishing & Ransomware, Protect from Sign-in Risk, Management of Devices, Control Sensitive Information

What = Convenience of a Single Easy to Manage Workplace Application

Generate Pipeline (MQLs)

Readiness

Validate

Implementation

Manage & Optimize

- Targeted Data Security & Risk Management Offers:
 - [Microsoft Defender Suite](#)
 - [Microsoft Purview](#)
 - [Microsoft 365 Security](#)
 - [Microsoft Sentinel](#)
- Email Campaigns
- Events (Virtual / In-Person)
- [Blogs](#)
- Co-Selling with Microsoft Account Team
- Referral / Funnel Share with Microsoft
- [One-Pagers](#)
- [Microsoft Marketplace](#)
- [Events on Demand](#)
- FastTrack Ready Program

Success Stories

- [Case Studies](#)
- [Win Wires](#) (Confidential not customer facing)
- [Lookbooks](#)
- [Services Catalog](#)

Key Play Opportunities

- [Microsoft 365 Roadmap](#)
- [Threat Protection Workshop](#)
- [Modern SecOps Workshop](#)
- [Data Security Workshop](#)
- [Microsoft MCI Engagement](#)
- [Technology Strategy Review](#)
- FastTrack Ready Program
- [Incident Response Tabletop Exercise](#)
- [Cybersecurity Health Check](#)
- [Microsoft Security Transition Assessment](#)
- [Microsoft Compliance Purview Assessment](#)
- [Organizational Change Management](#)

Deliverables

- Licensing Requirements

Certifications

- Microsoft Advanced Specialization in Information Protection & Governance, Identity & Access Management, Threat Protection, Cloud Security
- Microsoft MISA & MXDR Partner
- Microsoft Security Solution Partner

- [Secure POC of Readiness Offers](#)

- OR -

- [Go straight to Implementation of Readiness Offers](#)

- [Present value of Manage & Optimize](#)

- [Organizational Change Management](#)

Documents

- SOW Templates
- Existing Designs & Documentation
- Executive Summary Presentation Template

- [CSP Deployment Accelerators \(MCI\)](#)

- [Implementation of Readiness Offers](#)

- Secure CSP Advantage

- Secure CPOR / FTP Association

- Secure PAL Association (Azure)

- [Organizational Change Management](#)

- Partnering with Microsoft AE to drive to close

- [Enabled IT \(MPSA\)](#)
- [ThreatDefender MXDR MSSP](#)
- [Arctic Wolf Security Services](#)
- [Unified Services Block \(USB\)](#)

Partner Certifications

- [Arctic Wolf Silver Pack](#)
- Microsoft Advanced Specialization in Information Protection & Governance, Identity & Access Management, Threat Protection, Cloud Security
- Microsoft MISA & MXDR Partner
- Microsoft Security Solution Partner

- Microsoft MCI Engagements

- ECIF Funding
- Microsoft MCI Engagements

- Azure Accelerate Sentinel Deployment Funding
- ECIF Funding

- CPOR / FTP incentives
- CSP Incentives
- [Arctic Wolf Deal Registration / Rebates](#)

Activity & Deliverables

Investments & Profitability

Data Security & Risk Management



Data Discovery: Automated Scanning, Sensitive Data Classification, and Data Mapping of your Data Estate

Data Governance: Centralized cataloging for all data assets, Data Lineage Tracking, and the ability to define and manage business terms

Compliance & Risk Management: Regulatory compliance, dashboards to provide risk insights, and audit trails

FEATURE



Enhanced Data Visibility: A unified view of your entire data estate across multiple environments

Streamlined Compliance: Simplifies meeting regulatory requirements to offer built-in compliance templates for audit-ready reporting

Reduced Risk of Data Breaches: Detects and prevents unauthorized access or sharing through DLP and sensitivity labels

BENEFIT



Risk Reduction: Helps prevent financial and reputational damage by securing business data and infrastructure.

Cost Savings: Offers a cost-effective solution by bundling various security features into one package.

Trust & Transparency: Builds confidence by ensuring data is handled securely and in compliance with regulations

VALUE

Threat Detection & Response



“Ask”

Key Asks:

1. What are your specific security goals and objectives? What is your current security posture?
2. What kind of data and assets do you need to protect? Do you have any compliance requirements?
3. Do you have an incident response plan in place?
4. What are your primary security concerns or threats you have faced in the past?

Follow up Asks:

1. What is your network architecture and cloud strategy?
2. What is your expected level of service availability and response time? How do you want to receive security alerts and reports?
3. Do you have an internal security team, and if so, what is their level of expertise and capacity?
4. Are there any third-party vendors or partners you are using for security monitoring?
5. Can you provide historical data on security incidents or breaches you have experienced?
6. Are there any specific industries or sectors you serve that may have unique security requirements?

“Say”

What are common responses to this question?

1. The cost for SOC services is too high.
2. We have the appropriate in-house expertise.
3. We are confident in our current security posture.
4. We do not feel comfortable sharing that information.

How do you handle these objections?

1. SOCaaS can actually save you money in the long run by preventing costly security incidents and data breaches.
2. Complementing your in-house expertise with a SOC can provide 24 / 7 coverage, access to advanced tools and threat intelligence.
3. We can customize our services to align with your specific compliance requirements. We can provide transparency in our operations and audit trails for peace of mind.
4. Share general insights and best practices related to security to demonstrate your expertise and the relevance of SOC services.
5. Explain that sharing information about their security posture is essential for tailoring a solution that truly addresses their vulnerabilities and risks.

“Do”

Key Do's - What talk track do you use to tee-up the next action?

1. Engage a presales resource
2. MCI Security Engagements
3. License Optimization Workshop
4. **Get the counts! - People, endpoints, AD DCs, M365 licensing level and counts**

Optional Do's:

1. Sentinel Workshop

Threat Detection & Response

YES PLAYS
YOUR **ENABLEMENT** FOR **SUCCESS**

Create Lead 0%	Qualify Lead 10%	Assess, Plan, and Present Roadmap 20% - 40%	Pilot Solution 60%	Implement 80%	Secure Recurring Services
IDENTIFY VALUE		CREATE VALUE		REALIZE VALUE	

Who = IT Manager, IT Architect, CIO, CSO, Security Director

Why = Prevent possible data breaches, Proactively hunt for Security threats, Respond to incidents rapidly

What = Single solution for attack detection, visibility, proactive hunting, & response

Generate Pipeline (MQLs)

Readiness

Validate

Implementation

Manage & Optimize

- Targeted Threat Detection Offers:
 - [Microsoft Sentinel](#)
 - [Microsoft Defender XDR](#)
 - [ThreatDefender](#) (Microsoft only solutions)
 - Arctic Wolf** (Any Microsoft or 3rd party solution)
- Email Campaigns
- Events (Virtual / In-Person)
- [Blogs](#)
- Co-Selling with Microsoft Account Team
- Referral / Funnel Share with Microsoft
- [One-Pagers](#)
- [Microsoft Marketplace](#)
- [Events on Demand](#)
- FastTrack Ready Program

Success Stories

- [Case Studies](#)
- [Win Wires](#) (Confidential not customer facing)
- [Lookbooks](#)
- [Services Catalog](#)

Key Play Opportunities

- [Threat Protection Workshop](#)
- [Modern SecOps Workshop](#)
- [Cloud Security Workshop](#)
- [Microsoft Sentinel Assessment](#)
- [Microsoft Defender XDR Assessment](#)
- [Microsoft MCI Engagement](#)
- [Technology Strategy Review](#)
- FastTrack Ready Program
- [Incident Response Tabletop Exercise](#)
- [Cybersecurity Health Check](#)
- [Microsoft Security Transition Assessment](#)
- [Organizational Change Management](#)

Deliverables

- Licensing Requirements

Certifications

- Microsoft Advanced Specialization in Information Protection & Governance, Identity & Access Management, Threat Protection, Cloud Security
- Microsoft MISA, & MXDR Partner
- Microsoft Security Solutions Partner
- Arctic Wolf** Silver Partner Pack

- [Secure POC of Readiness Offers](#)
- OR -
- [Go straight to Implementation of Readiness Offers](#)

- [Present value of Manage & Optimize](#)

- [Organizational Change Management](#)

Documents

- SOW Templates
- Existing Designs & Documentation
- Executive Summary Presentation Template

- [CSP Deployment Accelerators \(MCI\)](#)
- [Implementation of Readiness Offers](#)

- Secure CSP Advantage
- Secure CPOR / FTP Association
- Secure PAL Association (Azure)

- [Organizational Change Management](#)

- Partnering with Microsoft & **Arctic Wolf** AE to drive to close

- [ThreatDefender MXDR MSSP](#)
- Arctic Wolf** Security Services
- [Unified Services Block \(USB\)](#)

Partner Certifications

- Arctic Wolf** Silver Pack Partner
- Microsoft Advanced Specialization in Security
- Microsoft Security Solutions Partner
- Microsoft MISA & MXDR Partnership

Activity & Deliverables

Investments & Profitability

- ECIF Funding
- MCI Engagements
- Arctic Wolf** Deal Registration

- Azure Accelerate Sentinel Deployment Funding
- ECIF Funding

- CPOR / FTP / PAL incentives
- CSP Incentives
- Arctic Wolf** Deal Registration / Rebates

Threat Detection & Response



24 / 7 Monitoring: Continuous surveillance of your network to detect and respond to threats in real-time.

Threat Detection and Response: Advanced systems and expertise to identify and mitigate cyber threats.

Compliance Management: Ensures that your business meets industry standards and regulations.

FEATURE



Expertise on Demand: Access to a team of security professionals without the need for in-house hiring.

Cost-Effective: Reduces the need for significant investment in security infrastructure and personnel.

Focus on Core Business: Allows businesses to concentrate on their core activities while experts handle security.

BENEFIT



Risk Mitigation: Minimizes the risk of data breaches and cyber attacks, protecting the organization's reputation and finances.

Operational Efficiency: Streamlines security operations, saving time and resources that can be allocated elsewhere.

Scalability: Easily scales with your business, providing flexibility as your security needs change.

VALUE

Microsoft Endpoint Management



“Ask”

Key Asks:

1. How do you manage your workstations and servers today?
2. Can you control lost devices? Can you remotely wipe a device?
3. Do you have a BYOD policy? How do you enforce / protect use of the device?

Follow up Asks:

1. Do you have full visibility into how well your workstations and servers are updated?
2. Can you manage your clients outside of the network?
3. How do you onboard new devices?
4. What do you use for mobile device management?
5. Are your users using uncontrolled devices to access organizational information?

“Say”

What are common responses to this question?

1. We use Workspace One.
2. We tried it a while back and have not had a good experience.
3. We do not think it is ready for prime time.

How do you handle these objections?

1. How have things been going since the VMware acquisition of Workspace One?
2. What all are you using Workspace One to manage? Are you also using SCCM or Intune for any purpose?
3. What kind of discount do you get from the user list price? Intune is \$8 / month per user and is part of EMS and M365 E# which also provides Entra and some DLP capabilities. Is consolidating money on these services important?
4. We have seen things changing quickly with Microsoft 365.

“Do”

Key Do's - What talk track do you use to tee-up the next action?

1. FastTrack
2. Strategic Advisory Services
3. SOC as Service YES Play

Optional Do's:

1. Licensing Optimization

Microsoft Endpoint Management

YES PLAYS
YOUR ENABLEMENT FOR SUCCESS



Who = IT Manager, IT Architect, CIO, CSO, Security Director

Why = Defend against Phishing & Ransomware, Protect from Sign-in Risk, Management of Devices, Control Sensitive Information

What = Convenience of a Single Easy to Manage Workplace Application

	Generate Pipeline (MQLs)	Readiness	Validate	Implementation	Manage & Optimize
Activity & Deliverables	<ul style="list-style-type: none">Targeted Microsoft Endpoint Management Offers:<ul style="list-style-type: none">IntuneWindows AutoPilotConfiguration ManagerEmail CampaignsEvents (Virtual / In-Person)BlogsCo-Selling with Microsoft Account TeamReferral / Funnel Share with MicrosoftOne-PagersMicrosoft MarketplaceEvents on DemandFastTrack Ready Program <p>Success Stories</p> <ul style="list-style-type: none">Case StudiesWin Wires (Confidential not customer facing)LookbooksServices Catalog	<p>Key Play Opportunities</p> <ul style="list-style-type: none">Microsoft 365 RoadmapTechnology Strategy ReviewMicrosoft Endpoint Management AssessmentFastTrack Ready ProgramOrganizational Change Management <p>Deliverables</p> <ul style="list-style-type: none">Workshop / Assessment FindingsLicensing RequirementsActionable Plan and SOWManaged Services Summary <p>Certifications</p> <ul style="list-style-type: none">Microsoft Advanced Specialization in Modernize EndpointsMicrosoft Modern Work Solution PartnerMicrosoft Security Solution PartnerMicrosoft Advanced Specialization in Information Protection & Governance, Identity & Access Management, Threat Protection, Cloud Security	<ul style="list-style-type: none">Secure POC of Readiness Offers- OR -Go straight to Implementation of Readiness OffersPresent value of Manage & OptimizeOrganizational Change Management <p>Documents</p> <ul style="list-style-type: none">SOW TemplatesExisting Designs & DocumentationExecutive Summary Presentation Template	<ul style="list-style-type: none">CSP Deployment Accelerators (MCI)Implementation of Readiness OffersSecure CSP AdvantageSecure CPOR / FTP AssociationOrganizational Change ManagementPartnering with Microsoft AE to drive to close	<ul style="list-style-type: none">ThreatDefender MXDR MSSPUnified Services Block (USB) <p>Partner Certifications</p> <ul style="list-style-type: none">Microsoft Advanced Specialization in Modernize EndpointsMicrosoft Modern Work Solution PartnerMicrosoft Security Solution PartnerMicrosoft Advanced Specialization in Information Protection & Governance, Identity & Access Management, Threat Protection, Cloud SecurityMicrosoft MISA & MXDR Partner
Investments & Profitability		<ul style="list-style-type: none">ECIF Funding	<ul style="list-style-type: none">ECIF FundingMicrosoft Surface Distributor Managed Partner		<ul style="list-style-type: none">CPOR / FTP incentivesCSP Incentives

Microsoft Endpoint Management



Unified Endpoint Management:
Provides a single solution for managing multiple operating systems and devices, both on-premises and in the cloud.

Advanced Security: Utilizes Microsoft Security signals to ensure device health and compliance, mitigating cyber threats.

Automated Software Updates:
Enforces software updates automatically across all endpoints, reducing vulnerabilities.

FEATURE



Simplified Device Management:
Centralized control makes deploying, wiping, and repurposing devices simple and efficient.

Strengthened Security Posture:
Protects corporate data and ensures compliance with security policies.

Operational Efficiency: Increases IT efficiency by bringing together device visibility, endpoint security, and data-driven insights.

BENEFIT



Cost Reduction: Reduces overall costs by consolidating vendors and offering cost-effective licensing options.

Improved Productivity: Enhances end-user productivity and performance across devices, supporting a hybrid workforce.

Risk Mitigation: Helps prevent financial and reputational damage by securing business data and infrastructure.

VALUE

Secure Connectivity



“Ask”

Key Asks:

1. How do you currently manage user identities and access across your organization?
2. What challenges do you face with onboarding, offboarding, or managing user permissions?
3. Are you using multiple identity platforms?
4. What are your primary security concerns related to identity and access?
5. Do you have specific compliance requirements that impact identity management?

Follow up Asks:

1. Are you leveraging multi-factor authentication or passwordless authentication today?
2. What applications require secure access for employees, partners, or customers?
3. Are you interested in automating access reviews, lifecycle workflows or integrating HR systems?
4. How much time does your IT team spend managing access requests and troubleshooting identity issues?
5. Would you benefit from self-service tools for access requests, password resets, or compliance reporting?

“Say”

What are common responses to this question?

1. It's too expensive, we don't have the budget.
2. Microsoft Sentinel and Entra will increase our Azure Consumed Revenue costs.
3. We use multiple identity platforms; how will this integrate?
4. We don't trust completing using one vendor.

How do you handle these objections?

1. We can offer a Total Cost of Ownership (TCO) analysis to show cost savings from consolidating tools and reducing manual processes.
2. Cost avoidance opportunity by preventing breaches and reducing compliance penalties.
3. Automation and self-service capabilities will allow you to reduce IT workload.
4. Entra meets specific regulatory requirements.

“Do”

Key Do's - What talk track do you use to tee-up the next action?

1. Engage a presales resource
2. MCI Security Engagements
3. License Optimization Workshop

Optional Do's:

1. Microsoft Security Transition Assessment



Who = IT Manager, IT Architect, CIO, CSO, Security Director	Why = Prevent possible data breaches, Proactively hunt for Security threats, Respond to incidents rapidly	What = Single solution for attack detection, visibility, proactive hunting, & response
---	---	--



Activity & Deliverables

<ul style="list-style-type: none">Targeted Secure Connectivity Offers:<ul style="list-style-type: none">Microsoft EntraEmail CampaignsEvents (Virtual / In-Person)BlogsCo-Selling with Microsoft Account TeamReferral / Funnel Share with MicrosoftOne-PagersMicrosoft MarketplaceEvents on DemandFastTrack Ready Program <p>Success Stories</p> <ul style="list-style-type: none">Case StudiesWin Wires (Confidential not customer facing)LookbooksServices Catalog	<p>Key Play Opportunities</p> <ul style="list-style-type: none">Microsoft 365 RoadmapTechnology Strategy ReviewIdentity & Access Management Planning & DesignIdentity Governance Planning & DesignMicrosoft Sentinel AssessmentMicrosoft Security Transition AssessmentIncident Response Tabletop ExerciseOrganizational Change Management <p>Deliverables</p> <ul style="list-style-type: none">Licensing Requirements <p>Certifications</p> <ul style="list-style-type: none">Microsoft Advanced Specialization in Information Protection & Governance, Identity & Access Management, Threat Protection, Cloud SecurityMicrosoft MISA, & MXDR PartnerMicrosoft Security Solutions Partner	<ul style="list-style-type: none">Secure POC of Readiness Offers- OR -Go straight to Implementation of Readiness OffersPresent value of Manage & OptimizeOrganizational Change Management <p>Documents</p> <ul style="list-style-type: none">SOW TemplatesExisting Designs & DocumentationExecutive Summary Presentation Template	<ul style="list-style-type: none">CSP Deployment Accelerators (MCI)Implementation of Readiness OffersSecure CSP AdvantageSecure CPOR / FTP AssociationOrganizational Change ManagementPartnering with Microsoft AE to drive to close	<ul style="list-style-type: none">Enabled Data Protection (MSPA) (Rubrik & Cohesity)ThreatDefender MXDR MSSPArctic Wolf Security ServicesUnified Services Block (USB) <p>Partner Certifications</p> <ul style="list-style-type: none">Cohesity Professional Services Authorization for Data Protection PartnerCohesity Preferred PartnerRubrik Elite PartnerArctic Wolf Silver Pack PartnerMicrosoft Advanced Specialization in SecurityMicrosoft Security Solutions PartnerMicrosoft MISA & MXDR Partnership
---	---	--	---	---

Investments & Profitability

	<ul style="list-style-type: none">ECIF FundingMCI Engagements	<ul style="list-style-type: none">ECIF Funding	<ul style="list-style-type: none">CPOR / FTP incentivesCSP IncentivesArctic Wolf, Rubrik, Cohesity Deal Registration / Rebates
--	--	--	--

Secure Connectivity



Single Sign-On (SSO): Users can access multiple applications with one set of credentials.

Multifactor Authentication (MFA): Adds an extra layer of security by requiring users to verify their identity.

Conditional Access: Policies that allow or block access based on user, device, location, or risk level.

Identity Protection: Uses machine learning to detect suspicious sign-ins and compromised accounts.

FEATURE



Risk Mitigation: Minimizes the risk of data breaches and cyber attacks by enforcing strong authentication, access controls, and continuous monitoring.

Streamlines security operations, saving time and resources for IT teams.

Reduces overall costs by consolidating vendors, offering cost-effective licensing options, and preventing costly security incidents.

BENEFIT



Risk Mitigation & Security: With reduced data breaches, automated threat detection, and least privilege access.

Operational Efficiency: With simplified access management, centralized control, and automated workflows.

Compliance & Audit Readiness: With integrated compliance tools and access reviews.

VALUE

Secure Access Service Edge (SASE)



"Ask"

Key Asks:

Zero Trust Access

1. Are you using Cisco Duo or Microsoft Entra ID (Azure AD) to enforce conditional access and MFA?
2. How do you define and enforce trust for devices and users?

Secure Web Gateway / DNS Layer Security

1. Do you use Cisco Umbrella or Microsoft Defender for Endpoint/Web to block threats at the edge?
2. Are you managing multiple point products for web filtering and threat detection?

ZTNA vs VPN

1. Are you still using traditional VPNs for remote access?
2. Would users benefit from a more seamless, app-specific access experience?

Policy Consistency

1. How are policies enforced across corporate, BYOD, and mobile devices?
2. Are policies tied to user identity, device posture, or both?

Security Stack Consolidation

1. Are you using both Microsoft and Cisco tools today—any overlap or inefficiencies?
2. Would a unified SASE platform help simplify your current security operations?

"Say"

What are common responses to this question?

1. We don't want to be locked into a single vendor.
2. We don't want to rely on cloud-based services for our internet traffic
3. Cost and Time – both are in short supply here!

How do you handle these objections?

1. By leveraging cloud-based services and eliminating the need for on-premises hardware and infrastructure, organizations can reduce capital expenditures. Additionally, the pay-as-you-go model allows for more efficient resource allocation, ensuring that costs align with actual usage.
2. With a SASE unified solution, organizations can streamline their network management processes, reduce operational overhead, and achieve cost savings by consolidating and optimizing their network resources.
3. SASE provides centralized management and visibility across the entire network and security infrastructure. It enables organizations to enforce consistent security policies across all network traffic, regardless of the user's location or device, thus reducing potential security vulnerabilities.

"Do"

Key Do's - What talk track do you use to tee-up the next action?

1. Network Assessment
2. PEN Test
3. Technology Strategy Review
4. Cost / Capacity assessment

Optional Do's:

1. Strategic Advisory Services
2. FastTrack (Microsoft only)
3. Microsoft CSI Engagements (Microsoft Only)

Secure Access Service Edge (SASE)

YES PLAYS
YOUR **ENABLEMENT** FOR **SUCCESS**

Create Lead 0% Qualify Lead 10%
IDENTIFY VALUE

Assess, Plan, and Present Roadmap 20% - 40% Pilot Solution 60%
CREATE VALUE

Implement 80% Secure Recurring Services
REALIZE VALUE

Who = IT Manager, IT Architect, CIO, Data Center Manager, Infrastructure

Why = Data Locality, Increased System Performance, Continuity of Processes

What = Reduced IT Costs, Greater agility & scalability, Improved security

Generate Pipeline (MQLs)

Readiness

Validate

Implementation

Manage & Optimize

- Targeted SASE Offers:
 - [Cisco SD-Wan – Meraki](#)
 - [Cisco Umbrella](#)
 - [Cisco Secure Access by Duo](#)
 - [Cisco Secure Firewall](#)
 - Cisco Secure Internet Gateway (SIG)
- Email Campaigns
- Events (Virtual / In-Person)
- [Blogs](#)
- [One-Pagers](#)
- [Microsoft Marketplace](#)
- [Events on Demand](#)
- Co-Selling with **Cisco** Teams

Success Stories

- [Case Studies](#)
- [Win Wires](#) (Confidential not customer facing)
- [Lookbooks](#)
- [Services Catalog](#)

Key Play Opportunities

- [SASE Assessment](#)

Deliverables

- Assessment / Workshop Documentation
- Roadmap Plan(s)
- Hardware / Software Requirements
- Total Cost of Ownership (TCO)

Certifications

- Cisco** Provider Partner

- [Cisco Umbrella DNS POC](#)
- [Cisco Secure Client POC](#)
- Cisco Duo Security POC
- [Meraki AutoVPN & SD-WAN POC](#)
- [Cisco Secure Firewall POC](#)
- [Cisco Networking POC](#)
- [Go straight to Implementation of Readiness Offers](#)
- [Present value of Manage & Optimize](#)

Documents

- SOW Templates
- Existing Designs & Documentation
- Executive Summary Presentation Template

- Signed Product Quote
- [Implementation of Readiness Offers](#)
- Partnering with **Cisco** AE to drive to close

- [Enabled IT \(MSPA\)](#)
- [Enabled Networking \(MSPA\)](#)
- [Unified Services Block](#)

Partner Certifications

- Cisco** Provider Partner

- Cisco** / Ingram Enablement Credits

- Cisco** Deal Registration

- Cisco** Rebates

- Cisco** Rebates

Activity & Deliverables

Investments & Profitability

Secure Access Service Edge (SASE)



Converged Networking and Security: Integrates various functions like SD-WAN, SWG, CASB, and ZTNA into a single cloud service.

Simplified Policy Enforcement: Centralizes the control of security policies and access rules.

Flexible Deployment Models: Supports different deployment models to suit business needs.

Cloud-Native Capabilities: Build from the ground up to operate in the cloud, providing scalability and agility.

FEATURE



Reduced Complexity: Streamlines IT infrastructure by consolidating multiple security and networking functions.

Enhanced Security Posture: Improves security with consistent policy application and advanced threat protection.

Improved User Experience: Ensures seamless access for users regardless of their location, enhancing productivity.

Operational Efficiency: Simplifies management and optimizes application performance in real-time.

BENEFIT



Cost-Savings: By consolidating services, SASE can reduce overall IT costs and complexity.

Strategic Flexibility: Enables businesses to adapt quickly to changing work environments and business needs.

Scalability: Scales with the business, providing secure access for a growing number of users and devices.

VALUE

Who We Partner With



Microsoft

NUTANIX

Nutanix



Cisco / Meraki



Rubrik

COHESITY

Cohesity



Zerto



Arctic Wolf



Nerdio



AudioCodes



Enghouse



Intrado



Poly / HP



Quest



Broadcom / VMware



Omnissa



Pure Storage



EMC



Dell



Lenovo



Hewlett Packard
Enterprise

HPE



Veeam



Varonis

Term and Acronym Definitions

Term	Description
SMC	Small & Medium Corporate Accounts. Microsoft uses this to define businesses that are approximately 300-3,000 users and are “managed accounts”
EOU	Enterprise Accounts. Microsoft uses this to define the larger accounts in their portfolio. EOU accounts are “managed accounts” and have dedicated account teams
SMB	Small, Medium, Business Accounts. Microsoft uses this to define businesses that are smaller and not managed, sometimes also referred to as a Partner-Led account.
M365	Microsoft 365 – The suite of solutions that encompasses Office 365, Security, and Endpoint Management tools for the Microsoft Productivity Cloud
Co-Sell	A Microsoft engagement involving a third-party solution that drives Microsoft Cloud such as Rubrik, Cohesity, Zerto, etc. Co-Sell engagements are designated inside of Partner Center and Microsoft Sales Teams earn additional quota retirement based on them.
MQL	Marketing Qualified Lead - owned by Marketing that comes through the funnel as part of a unique HubSpot sequence.
SQL	Sales Qualified Lead - owned by our frontline sellers - our Account Executives - and it's a process that takes a new MQL that was produced by Marketing and begins shaking it down to evaluate it around the B/A/N/T (budget, authority, need, and the timeline) principles to ensure that we can move forward
SOW	Statement of Work – A document describing the work to be performed, the outcome, and the price for an eGroup services engagement
Advanced Specialization	Highest level Microsoft Certification Program that allows access to additional funding programs such as AMM
AMM	Azure Migration and Modernization Program – Additional funding, tools, and Azure credits for each of eGroup Enabling’s Advanced Specializations.
Modern Workplace	Microsoft Term utilized to describe Microsoft 365 sellers and the overall portfolio of end user productivity solutions
ECIF	End Customer Incentive Funds – Microsoft funding for select presales and post-sales initiatives that is available by working directly with the Microsoft account team. ECIF is often for engagements that do not have other programs clearly defined or where larger investments are needed for larger opportunities.
CSP	Cloud Solution Provider – This is a licensing program that allows eGroup Enabling to sell and support Microsoft Azure and Microsoft 365 licenses to the customer
CPOR	Claimed Partner of Record – This is a Microsoft attribution program that designates eGroup Enabling as the partner who assisted in the deployment of specific Microsoft 365 workloads. Attribution needs to be done prior to activation of licenses for incentives. Incentives are based on number of seats activated.
PAL	Partner Admin Link – Contrary to the name, this has nothing to do with admin access. PAL designation is a way for Microsoft to attribute specific workloads in Microsoft Azure to the partner that helped deploy them. This is required to receive scorecard credit as well as backend incentives.

Term and Acronym Definitions Cont...

Term	Description
SaaS	Software as a Service
Documentation Templates	Created and Managed by the eGroup Enabling Sales Engineering team. These are pre-built documentation templates that are used as deliverables for any engagement that has a SOW Template.
BANT	Budget, Authority, Need, and Timeline: Do they have the ability to spend? Do they have the authority to make the purchase? Does the lead (need) have an urgent problem? Do we know a timeframe?
FTOP	Fasttrack Orchestrations Operations Portal -
FRP / FTP	FastTrack Ready Partner Program - Microsoft Free benefit to qualifying customers that helps to drive adoption of Microsoft Office 365 Solutions
EA	Enterprise Agreement - This is a Microsoft licensing program where a Licensing Services Provider (LSP) resells Microsoft licensing on a 3-Year agreement.
MSPA	Managed Services Provider Agreement - An eGroup Enabling Managed Services Agreement that defines how and what responsibilities we will take in managing a client's environment on their behalf
Co-Op	Microsoft program that pays a percentage of CSP revenues back to the partner to use for technical enablement, solution development, and marketing/demand gen activities
CAF	Cloud Adoption Framework - a proven guidance that is designed to help you create and implement the business and technology strategies necessary for organizations to succeed in the cloud.
Success Engagement	A Microsoft engagement that is registered within partner center and is utilizing a formal program such as the solution assessment program. These are measured engagements where partners are scored based on volume. High volumes allow for the partner to be invited to future programs.
MFE	Manufacturer Funded Engagement - engagement funds that are provided by a manufacturer program, rebate, etc. Our goal is to convert MFE to CFE within 90 days of the MFE win date (the date the project was one, not finished).
CFE	Client Funded Engagement - engagement funds that are provided by the client.
Azure Landing Zone	The output of a multi-subscription Azure environment that accounts for scale, security governance, networking, and identity. Azure Landing Zones enable application migration, modernization and innovation at enterprise-scale in Azure.

Term	Description
HCI	Hyper-Converged Infrastructure - combines compute, virtualization, storage, and networking in a single cluster.
VLAN	Virtual Local Area Networks - VLANs allow for the segmentation and isolation of network traffic based on criteria such as function, department, or security requirements
Subnet	A portion of a larger network that has been divided or segmented into smaller networks.
SAN	Storage Area Network - A specialized network architecture that enables the connection of storage devices to servers and other computing resources
NAS	Network Attached Storage - A storage device or system that is dedicated to providing file-level data storage and access to multiple clients or users over a network.
FC	Fibre Channel - A high-speed network technology used to connect storage devices, such as dis arrays and tape libraries, to servers.
iSCSI	A network protocol that allows the transmission of SCSI (Small Computer System Interface) commands over an IP (Internet Protocol) network.
FWaaS	Firewall as a Service - moves firewall protection to the cloud instead of the traditional network perimeter.
IaaS	Infrastructure as a Service
SWG	Secure Web Gateway - is a web security service that filters unauthorized traffic from accessing a particular network.
CASB	Cloud access security broker - is a SaaS application that acts as a security checkpoint between on-premises networks and cloud-based applications and enforces data security policies.
ZTNA	Zero Trust Network Access - is a set of consolidated, cloud-based technologies that operates on a framework in which trust is never implicit and access is granted on a need-to-know, least-privileged basis across all users, devices, and applications.
SD-WAN	Software-defined wide area network - is an overlay architecture that uses routing or switching software to create virtual connections between endpoints, both physical and logical.
SASE	Secure Access Service Edge - an emerging cybersecurity concept that was first described by Gartner