Microsoft Security

Secure Multicloud & Microsoft's Defender for Cloud Strategy

Brian Stockbrugger – Senior Cloud Solution Architect, Security
Harry Rossoff – Senior GTM Manager – Cloud Security

Microsoft Security

Flow of Presentation

- **Overview**:
  - Exec. speaker from Microsoft to set the stage – 10 mins. – Im going to FU here
  - E2E Security platform – 5 mins. - @Brian
  - Our Secure Multicloud GTM Perspective & FY24 Focus – 10 mins. - Harry
  - Who are our sellers & What do our sellers care about 10 mins. - Harry
  - What are our key partner programs and how do they connect to the MSFT sales cycle – 10 mins. - Harry
  - What is the opportunity size for partners? 5 mins. - Brian
  - What is an example of a partner that has done this - @Brian Stockbrugger is looking into the potential to bring in a partner or to talk about anonymously a success story – 10 mins. - Brian
  - Next 3-4 Days - Brian
  - Summary & Recap – 5 mins. - Harry

"Security is our top priority and we are committed to working with others across the industry to protect our customers."

Satya Nadella
Chief Executive Officer, Microsoft Corporation

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships

Microsoft empowers you to Do More With Less

"No company is better positioned than Microsoft to help organizations deliver on their digital imperative so that they can **do more with less.** From infrastructure and data to business applications, hybrid work and security, we provide unique differentiated value to our customers."

– Satya Nadella, CEO

Businesses worldwide trust Microsoft security solutions

Scale and Protection of Microsoft Security

Over **24 trillion** daily security signals

AI powered detections and automated actions

8,500+ security engineers & researchers

9B
Endpoint threats blocked

31B
Identity threats blocked

32B
Email threats blocked

July 1, 2020, through June 30, 2021

Protecting

715K

organizations in 120 countries

Source: Microsoft Digital Defense Report

Exec Speaker from Microsoft

Microsoft E2E Security Pitch

Navigating a shifting world

Conventional security tools
have not kept pace

Attacks growing
more sophisticated

Regulatory landscape
becoming **more complex**

Secure your organization with Zero Trust

Verify **explicitly** | Use **least-privileged access** | Assume **breach**

Microsoft Security

Protect
everything

Simplify
the complex

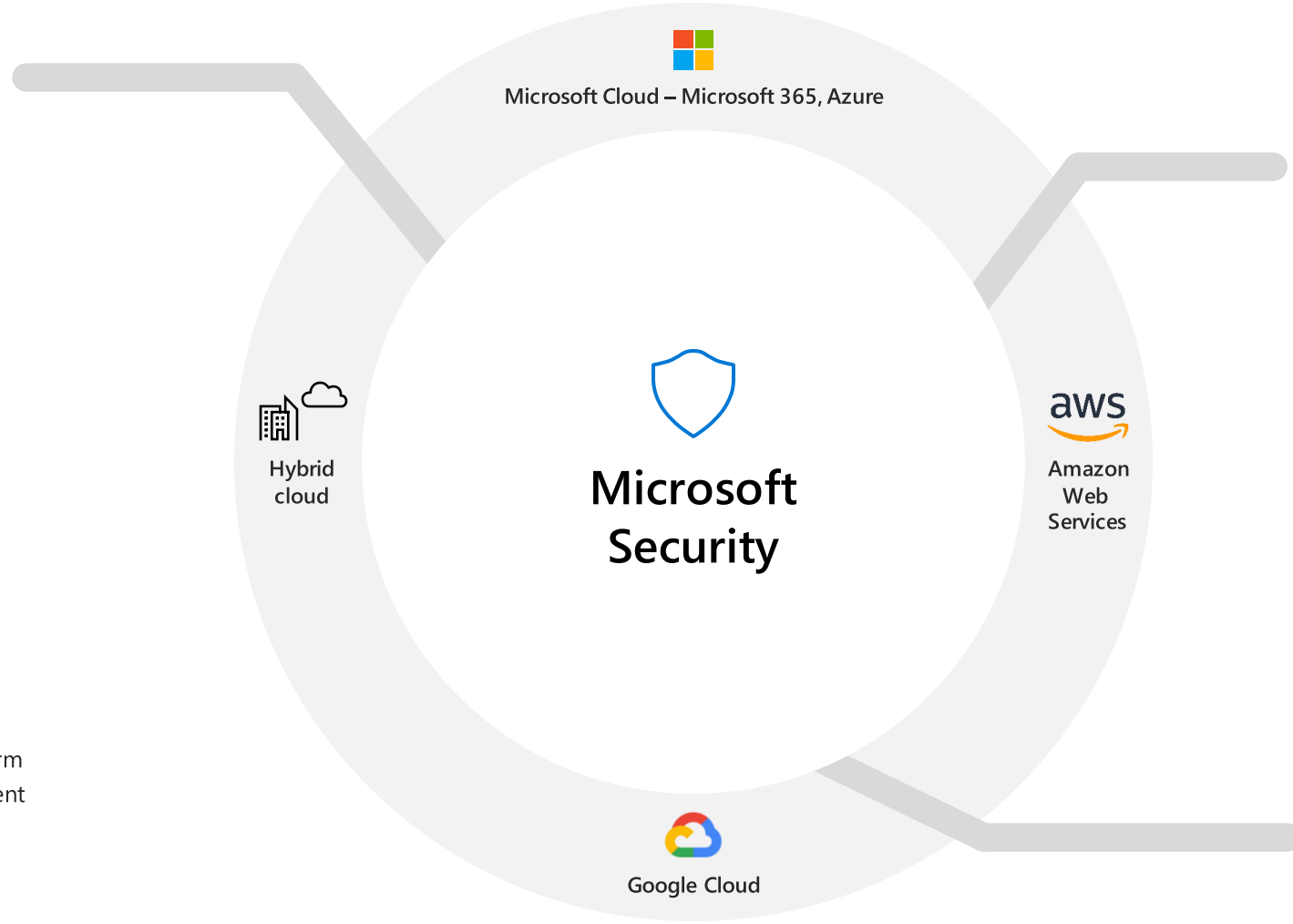
Catch
what others miss

Grow
your future

Microsoft's end-to-end security

Integrate over 40 categories

Endpoint detection and response
Endpoint protection platform
Forensic tools
Intrusion prevention system
Threat vulnerability management
Anti-phishing
User and entity behavior analytics
Threat intelligence feeds
App and browser isolation
Attachment sandboxing
Application control
End-user training
Network firewall (URL detonation)
Host firewall
Secure email gateway
Security assessment
SIEM
SOAR
Cloud access security broker
Cloud workload protection platform
Cloud security posture management
Incident response services
DDOS protection
IoT protection



Data discovery
Data classification
Data loss prevention
Insider risk management
Data retention
Data deletion
Records management
eDiscovery
Audit
Risk assessment
Privileged access management
Compliance management
Information and messaging encryption

Identity and access management
Single sign-on
User provisioning
Multi-factor authentication
Passwordless authentication
Risk-based conditional access
Identity protection
Self-service password reset
Identity governance
Priviledged identity management
Endpoint management
Mobile application management
Mobile device management

Microsoft—a Leader in Gartner Magic Quadrant reports

Access Management

Cloud Access Security Brokers

Enterprise Information Archiving

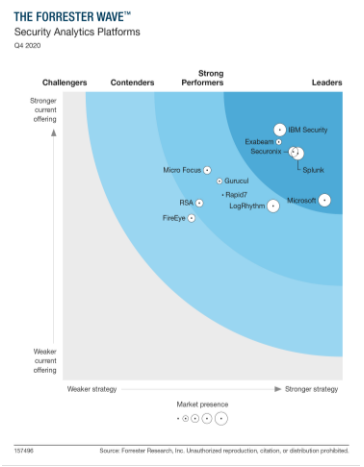
Endpoint Protection Platforms

Unified Endpoint Management

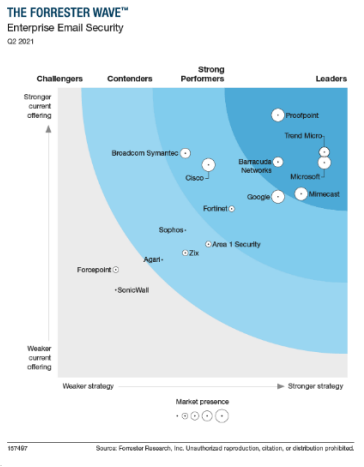
*Gartner "Magic Quadrant for Access Management," by Michael Kelley, Abhyuday Data, Henrique, Teixeira, November 2020
*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Craig Lawson, Steve Riley, October 2020
*Gartner "Magic Quadrant for Enterprise Information Archiving," by Michael Hoech, Jeff Vogel, October 2020
*Gartner "Magic Quadrant for Endpoint Protection Platforms," by Paul Webber, Rob Smith, Prateek Bhajanka, Mark Harris, Peter Firstbrook, May 2021
*Gartner "Magic Quadrant for Unified Endpoint Management ," by Dan Wilson, Rich Doheny, Rob Smith, Chris Silva, Manjunath Bhat, August 2020

FORRESTER®

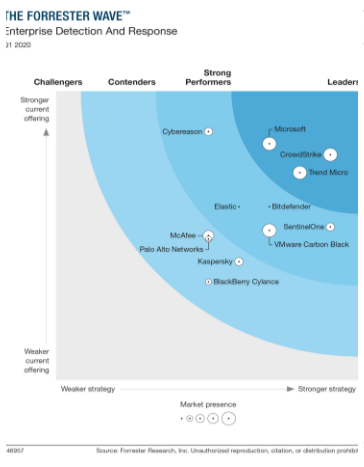
Microsoft Security—a Leader in 7 Forrester Wave reports



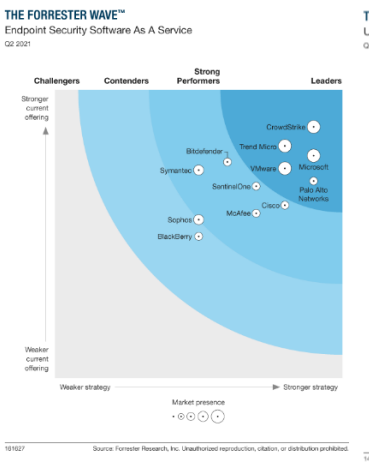
Security Analytics Platform



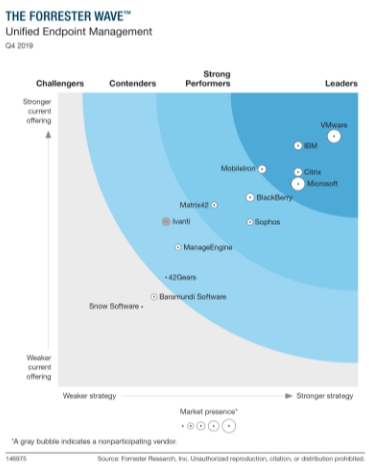
Enterprise Email Security



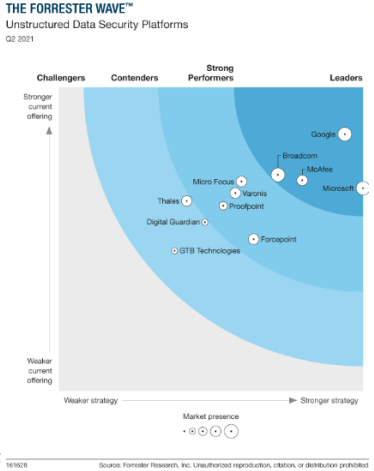
Enterprise Detection & Response



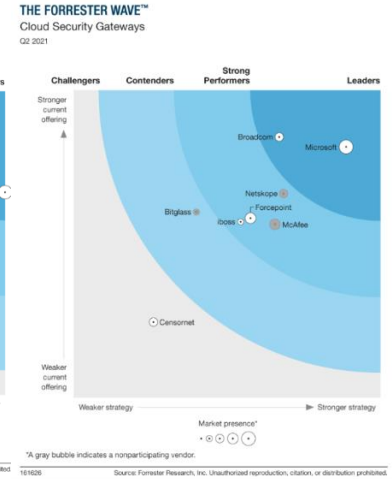
Endpoint Security Software as a Service



Unified Endpoint Management



Unstructured Data Security Platforms



Cloud Security Gateways

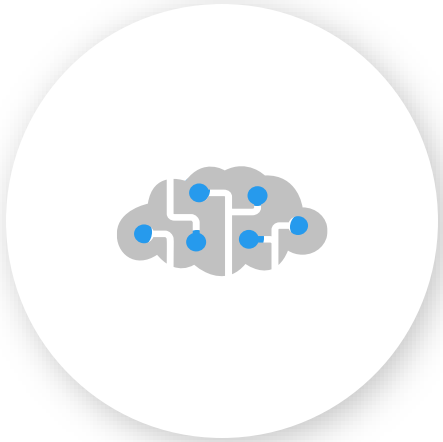
1. The Forrester Wave™: Security Analytics Platforms, Q4 2020, Joseph Blankenship, Claire O'Malley, December 2020
2. The Forrester Wave™: Enterprise Email Security Q2 2021 Joseph Blankenship, Claire O'Malley, April 2021
3. The Forrester Wave™: Enterprise Detection And Response, Q1 2020, Josh Zelonis, March 2020
4. The Forrester Wave™: Endpoint Security Software as a Service, Q2 2021, Chris Sherman, May 2021
5. The Forrester Wave™: Unified Endpoint Management, Q4 2019, Andrew Hewitt, November 2019
6. The Forrester Wave™: Unstructured Data Security Platforms, Q2 2021, Heidi Shey, May 2021
7. The Forrester Wave™: Cloud Security Gateways, Q2 2021, Andras Cser, May 2021

Microsoft Security

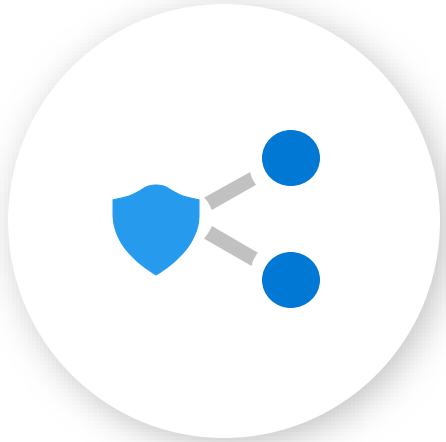
Our unique solution

Microsoft currently operates a $10B security business with $20B investment in security over the next 5 years.

Built-in experiences that work across platforms



AI and automation to secure your future



Integrated across people, devices, apps, and data

Microsoft protecting Microsoft

Hardening (Physical, OS App/Data, etc.)
Whitelisting
Auto-Patching
and more...

Traditional Defenses

Corporate Infrastructure

Cloud Infrastructure

Continual Scanning
Penetration Testing
Red Team Ops
Bug Bounties
One Hunt

Attackers View

People

Background Checks
Security Training
Conferences

Least Privilege

Least Privilege Access
Just-in-time Access
and more...

Authentication

Multi-factor Auth
Anomaly Detection

Privileged Access Workstations

Secure Access Workstations
isolation from web/email risks

Rigorous Security For Privileged Access

Automated Assessments
Secure DevOps toolkit
and more...

Security Development Lifecycle

Continuous Logging & Monitoring
Incident Response
CDOC (24x7 SOC)

Monitoring & Vigilance

Microsoft Defender For Cloud

Cloud native application protection across clouds and on-prem environments

Harden and manage your Security Posture

Secure configuration of resources

Management of compliance requirements

Detect threats and protect your workloads

Full-stack threat protection

Vulnerability assessment & management

Respond & Automate

Assess and resolve security alerts and incidents

Automate response

Automate with the tools of your choice

Microsoft Azure

Amazon Web Services

Google Cloud Platform

On-prem

How we're different

Built-in with Azure

- No deployment, just enable
- Built into the resource provisioning process
- Broadest protection coverage
- Remediate with a click

Multi-cloud and hybrid support

- Agentless onboarding for AWS and GCP posture management
- Auto provisioning for new resources
- Onboard on-prem resources with Azure Arc

Secure Score

- Birds-eye view of the security posture of all your clouds
- Prioritized security recommendations
- Track and manage your security posture state over time

Advanced Threat Protection

- Workload-specific signals and threat alerts
- Deterministic, AI, and anomaly-based detection mechanisms
- Leverages the power of Microsoft Threat Intelligence with 24 trillion signals daily

Make Microsoft Defender for Cloud work for you

Chief Information Security Officer

Responsibilities

Create an overall security strategy that creates resilience against cyber attacks and track performance over time

Product use cases

- Top level view of the multicloud security state
- Create dashboards to visualize progress over time

Security Admin

Responsibilities

Reduce the attack surface of the organization's cloud environments

Product use cases

- Harden the cloud environment with recommendations
- Set security policies for the environment, monitor implementation, track down vulnerabilities
- Manage the multicloud asset inventory

Security Operations

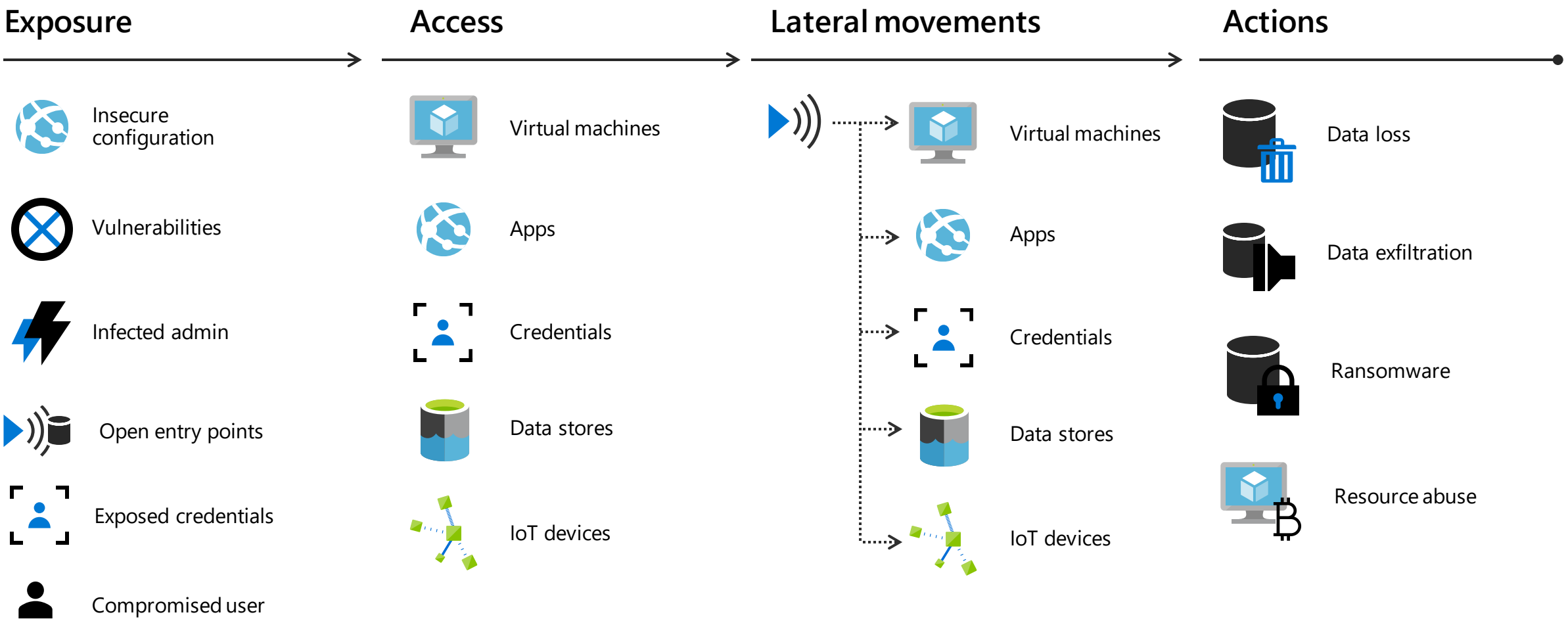
Responsibilities

Around the clock threat hunting, investigation of breaches, and mitigation of incidents

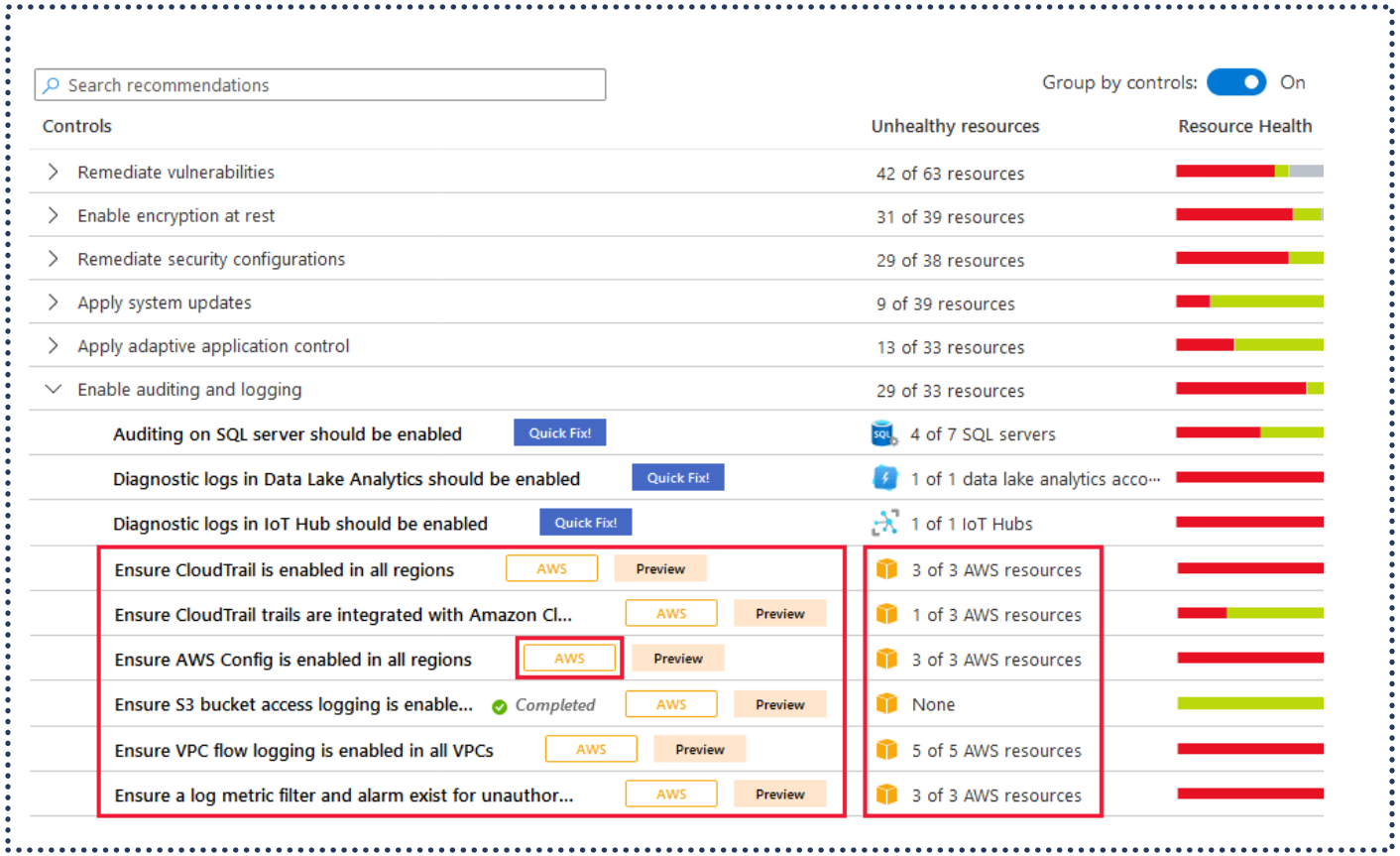
Product use cases

- Leverage workload-specific threat detections and response mechanisms to identify attacks, investigate alerts and incidents, and quickly mitigate threats

The cloud kill chain model



Microsoft Defender with AWS



Automatic agent provisioning (Security Center uses Azure Arc to deploy the Log Analytics agent to your AWS instances)

Policy management

Vulnerability management

Embedded Endpoint Detection and Response (EDR)

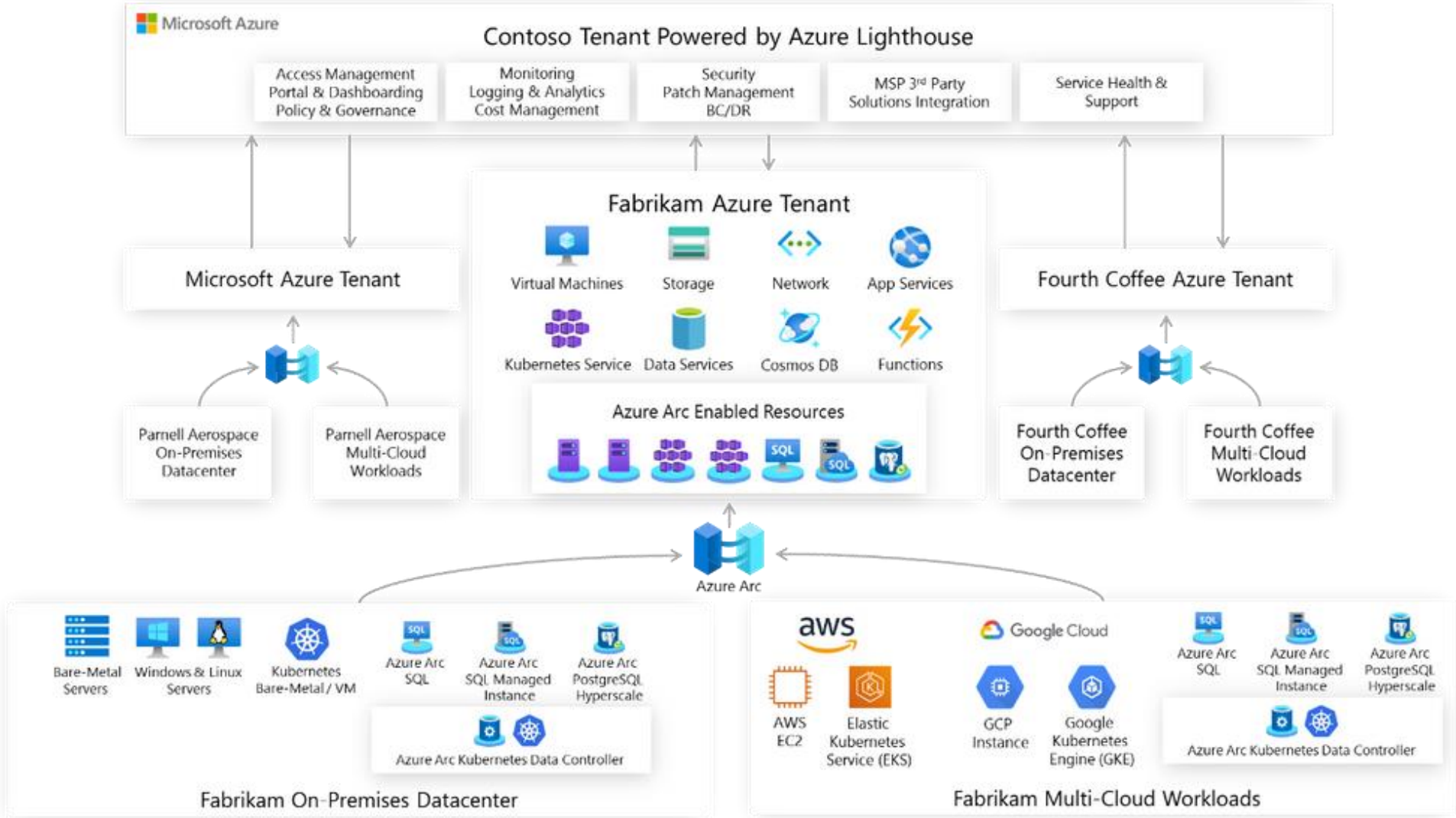
Detection of security misconfigurations

A single view showing Security Center recommendations and AWS Security Hub findings

Incorporation of your AWS resources into Security Center's secure score calculations

Regulatory compliance assessments of your AWS resources

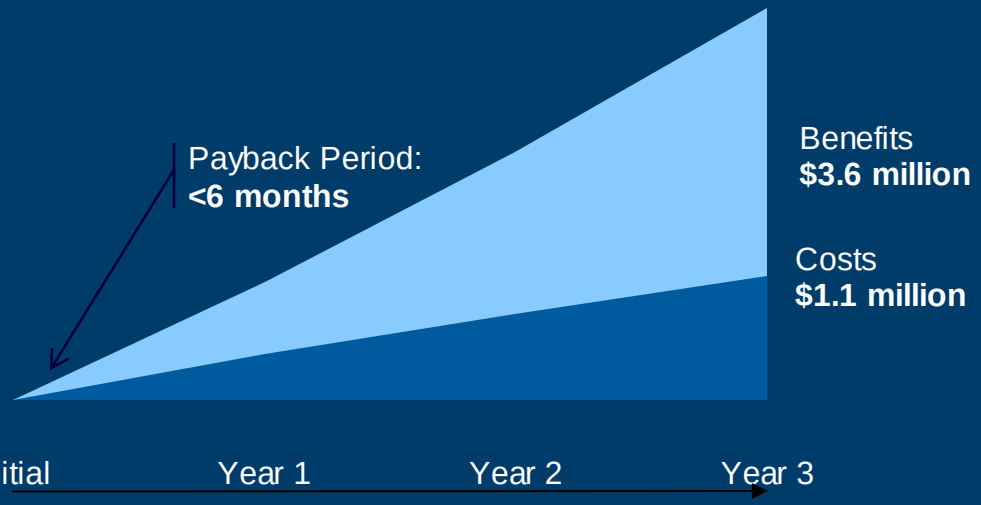
Using Azure to Secure and Manage Everything



The Total Economic Impact™ of Microsoft Defender for Cloud

Financial Summary

ROI	BENEFITS PV	NPV	PAYBACK
219%	**3.56M**	**$2.44M**	**<6 months**



Read the full study

COST SAVINGS AND BUSINESS BENEFITS

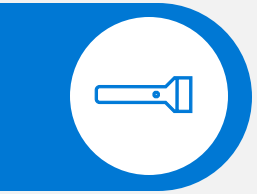
25%
reduction in risk of a security breach

50%
reduction in time to threat mitigation

30%
reduction in security policy and compliance management time

$216K
annual reduction in security tool spend

Solution Play Spotlight



Security-ACR & Secure Multi-cloud Environments

Partner Opportunity

Built-in Azure Security vs. bolt on after migration
Opportunity to expand infra. Opportunities
AWS, GCP On-prem extensibility

Securing multi-cloud environments

What's top of mind

Visibility into security and compliance

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

Protect against increasing, sophisticated attacks

$4.24M is the average cost of a breach, 2021.[2]

Manage access and permissions for users and applications

1,295 different cloud services are used by enterprises, on average.[3]

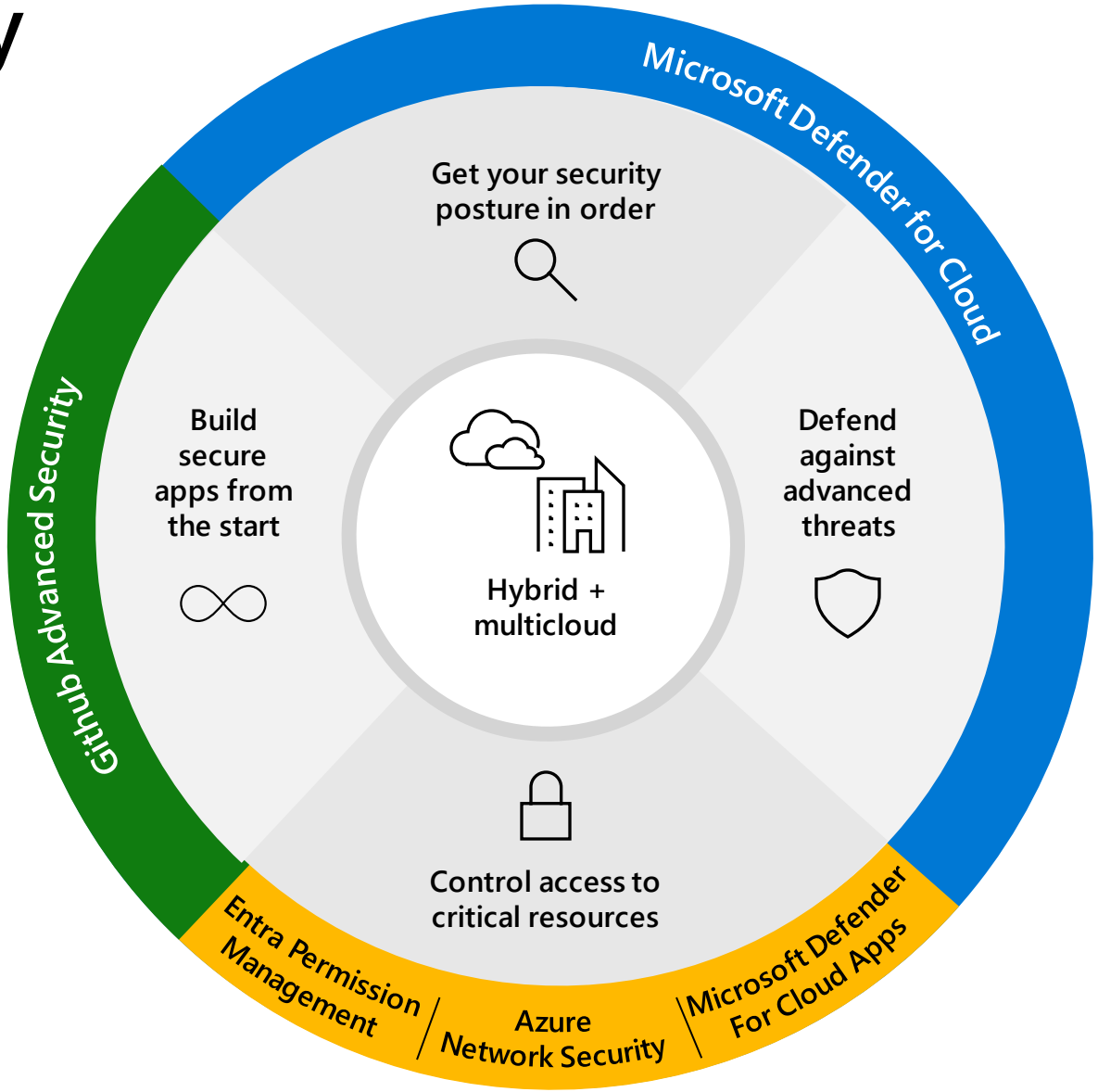
Develop and operate secure apps in the cloud

83% of code vulnerabilities are caused by developer error.[4]

1. 451 Research
2. Ponemon Institute, Cost of a Breach Report
3. Netskope Cloud Report.
4. https://www.ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-statistics-2019

Cloud security

Integrated protection for your customers multi-cloud resources, apps, and data



Defender for Cloud: Secure More With Less

More Cost Savings, Better Results from Azure Security

More than just security posture management, with Defender for Cloud, protecting Azure, hybrid & multi-cloud workloads, organizations saw a 25% reduction in risk of a security breach to cloud workloads. Organizations experienced 50% decrease in time to mitigation of cloud-based threats, up to 30% increase in speed of security policy and compliance-related workloads; and reduced their spending on third-party security tools and services resulting in over $200,000 savings annually.

- Reduce spend on third party security tools
- Enhance visibility into security posture & reduce risk of cloud security breaches
- Improve productivity of security teams responsible for threat detection, remediation and regulatory compliance.

Why US Secure Migration & Why now?

As we enter H2, Secure Migrations is a priority: Leadership has called US Secure Migration out as a **mainstream play** to focus on and drive both our Windows Server business and our Defender for Cloud business

Microsoft's Opportunity

To secure & grow our Azure business through both Windows Server and Defender for Server

- **XXXM in S-ACR of US Secure Migration** not yet enabled across migration targets
- $X.XB in ACR opportunity for WS ($X.XB) and SQL ($X.XB) has not yet been enabled across migrations
- Attaching Defender for Cloud to our Windows Server migration to Azure increase deal size 7%-10% & reduce cost for our customers

Our Customer's Opportunity

To enable digital transformation & Do more with Less in a secure and compliant way

- Reduce the effort required to provision and secure new infrastructure by 80% according to IDC
- Shifts security from a blocker to an accelerator for enabling digital transformation and closing out data centers and ensure quick and secure migrations
- Using Microsoft Defender for Cloud has been found to have a 219% ROI over 3 years & reduce risk by up to 25%

ATU/STU/CSU Roles at Microsoft

Security STU

STU Sales Roles

- Modern Work Specialist
- Project Specialist
- Surface Specialist

STU Technical Roles

- Teams Technical Specialist

Apps & Infrastructure

STU Sales Roles

- Azure Infrastructure Specialist
- Azure App Dev Specialist
- Azure SAP Specialist
- Azure (Hunter) Specialist

Data & AI

STU Sales Roles

- Azure Data & AI Specialist
- Azure Specialist

Business Applications

STU Sales Roles

- Customer Engagement Specialist (CRM)
- Finance & Operations Specialist (ERP)

STU Technical Roles

- Customer Engagement Technical Specialist
- Finance & Operations Technical Specialist

Security

STU Sales Roles

- Security Specialist

STU Technical Roles

- Security Technical Specialist
- Compliance Technical Specialist
- Cloud Endpoint Technical Specialist

Support

STU Sales Roles

- Support SSP

FY23 Microsoft Cloud Security | Partner GTM Opportunity

Pre-sales			Post-sales	
Generate interest	**Create intent**	**Build technical case**	**Deploy**	**Drive adoption**
Security Immersion Workshop *Shadow Hunter*	Build Intent Sales Workshop *Secure Multi-Cloud Environments* Solution Assessment - *Cloud Security*	Security ECIF ACO	Build Intent Usage Workshops AMMP ACO	Build Intent Usage Workshops WANI
Corporate paid events	Workshop - $5k USD Assessment - $ Varies	Varies by engagement	Workshop - $5k USD AMMP & ACO - $ Varies	Workshop - $5k USD WANI – Acquisition Bounty and Nurture $

Microsoft Security Immersion Workshop | Shadow Hunter

Our **Microsoft Security Immersion Workshop: Shadow Hunter is a gamified learning experience** that tests your cybersecurity skills. You are the cybersecurity analyst; it is up to you to find the attacker that has gained network access through a security camera in your office's building.

Business Objectives:

- Acquire new Security customers
- Attach Security to Azure migration customers

Customers will learn how to:

- Use Defender for Cloud to check the security posture of your cloud resources
- Protects workloads running in Azure, hybrid, and multi-cloud Linux and Windows environments
- Monitor risky workloads that you may not have visibility into, such as Enterprise IoT, Containers, and Storage services
- Detects threats to your hybrid and multi-cloud workloads
- Use Microsoft Sentinel to detect and resolve incidents

Microsoft Technologies:

- Defender for Cloud
- Azure Network Security
- Microsoft Sentinel
- Hybrid cloud workloads
- Defender for IOT
- Azure storage
- Azure Arc

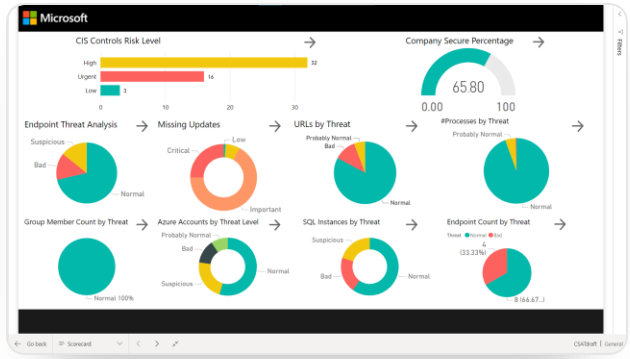
Learn More at Shadow Hunter (microsoft.com)

Cloud Security Assessment

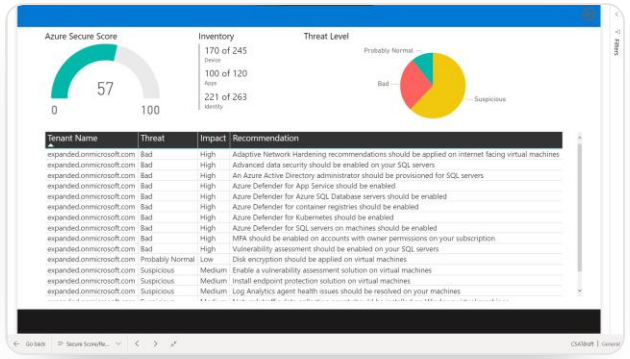
Provides organizations with a comprehensive look at their security posture by evaluating & addressing immediate vulnerabilities, identifying unmanaged devices, analyzing current software deployment & usage, discussing policies and controls to reduce risk, and delivering remediation recommendations to help establish processes for cyber-risk reduction in the cloud.

Sample Outputs

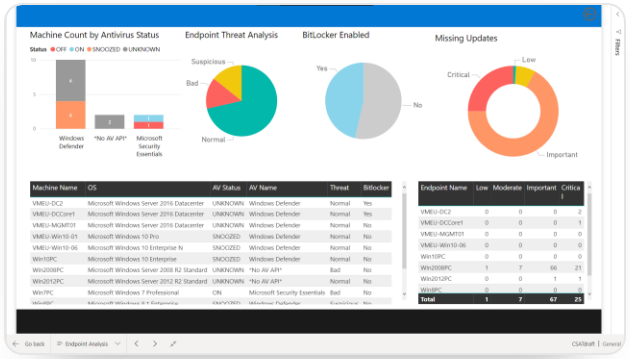
Cloud Security Scorecard



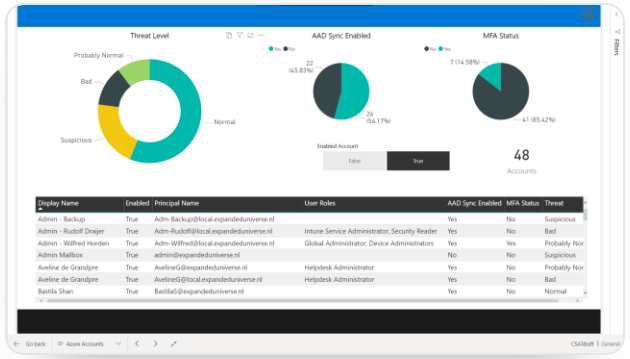
Azure Secure Scores & Recommendations



Endpoint Exposure, Antivirus & Encryption



Azure Account Threat Exposure



Assessment Details

- **Tool Used:** Cloud Security Assessment Tool
- **Timeline:** 2 weeks
- **Microsoft Scope:** Data discovery & analysis
- **Partner Scope (Optional):** Migration plan, program & workshop enrollment, architecture design, competitive analysis
- **Included Insights:** Cloud Security Scorecard, Azure Account Threat Exposure, Azure Secure Scores & Recommendations, Browser History Threat Analysis, Endpoint Exposure, Antivirus & Encryption, Firewall Exposure, Operating Systems & SQL Server Analysis
- **Programs:** Azure Migrate and Modernization Program, FastTrack for Azure, Cloud Adoption Framework Workshop, Digital Skilling

Partner Resources

- Partner Eligibility Requirements for the Solution Assessment Incentives Program

Secure Multi-Cloud Environments Workshop: Overview

Designed as a three-day engagement, the **Secure Multi-Cloud Environments Workshop** enables partners to build intent for sales and deployment of Microsoft Defender for Cloud and optionally, Azure Network Security. The engagement involves showcasing Microsoft Defender for Cloud features, discovering real threats to selected hybrid and multi-cloud workloads, and analyzing security vulnerabilities across existing hybrid and multi-cloud workloads in the customer's production environment. It also includes an optional exploration of Azure Network Security capabilities in a demonstration environment.

Audience

Customers

Senior BDMs – CISO, CSO, CIO, etc.
and TDMs – IT Security, IT Operations

Workshop

Partner Participants

Consultants, Solution Architects,
Dev and Design Leads

Envision

Value Conversation

- Customer priorities & requirements
- Product feature showcase

Discover

Security Assessment

- Threat Exploration
- Demonstrate Threat Investigation & Response
- Vulnerability Assessment

Plan

Next Steps Discussion

- Microsoft Defender for Cloud pilot/deployment
- Azure Network Security pilot/deployment [optional]
- Cost and economic value conversation

Cloud Adoption Framework – Secure methodology

End state for managing your overall security posture

Secure

Business alignment

Risk insights

Integrate security insights into risk management framework and digital initiatives.

Security integration

Integrate security insights and practices into business and IT processes

Operational resilience

Ensure organization can operate during attacks and rapidly regain full operational status.

Security disciplines

Access control

Establish Zero Trust access model. Extend modern protection to legacy assets.

Security operations

Detect, respond, and recover from attacks; hunt for hidden threats; lead through data-driven decision

Asset protection

Protect sensitive data and systems. Continuously discover, classify & secure assets.

Security governance

Continuously identify, measure, and manage security posture to correct deviation and reduce risk.

Innovation security

Integrate security into DevSecOps processes. Align security, development, and operations practices.

Business alignment

Establish cross-org processes to scale cloud security throughout your business

Security disciplines

Implement proven security processes built on modern, cloud-based security tools

Cloud security team

Establish team with expertise and experience for security and cloud. Often a cross-functional security team(s) that includes members of security team, cloud center of excellence (CCoE), Cloud operations, IT operations, and others.

CAF – Security Best Practices: Getting started

Deploy the Azure landing zone accelerator

- Rich, mature, scaled-out implementation
- 4 implementations: Start small to Enterprise-scale
- Includes full set of products and controls
- Intended to get organizations to security at scale, quickly
- Customizable implementation
- Deploy through portal or integrate with GitHub
- Opinionated guidance based on best practices and lessons learned

Deployment includes:

- Dedicated subscriptions for specific functions (optional)
- Management Group structure
- Network topology (hub and spoke or vWAN)
- Azure Policy – enforcement options
- Azure Firewall (optional)
- Azure Security Center
- Azure Defender (optional)
- Azure Sentinel (optional)
- Azure Network Security Groups (optional)
- Azure Monitor (Log Analytics, Audit Logging)

Implement Azure security services

- Small footprint, starter feature-set
- Develop and iterate at your own pace
- Work with partners to customize the iterations, based on your specific requirements (e.g. scale-out, or enhanced policy controls)

Deployment includes:

- Upgrade to Azure Defender - Azure Security Center
- Web Application Firewall deployment tutorial
- Deploy and configure Azure Firewall Premium
- Manage Azure DDoS Protection Standard using the Azure portal
- Overview of the Azure Security Benchmark V2
- CIS Microsoft Azure Foundations Benchmark v1.3.0 blueprint sample
- Azure Security Benchmark blueprint sample overview
- Cloud Adoption Framework - Security Methodology
- Enterprise-Scale/policies.json

CAF Security Resources:

- Review the Cloud Adoption Framework Documentation
- Review the Cloud Adoption Framework Security Documentation
- Learn with the Cloud Adoption Framework Learn Modules
- Watch the CAF Security Video on Azure Enablement Show

AMMP Security Opportunity

- **Safeguard your customers' digital transformation**
- **Become a trusted advisor**
- **Accelerate ACR growth ***
- **Develop new managed security services offerings**

AMMP Partner-led

When Partners sell and nominate customers directly

Recommended path when the following apply:

- ✓ Partner is leading the customer engagement
- ✓ Partner is already an Azure Expert MSP and/or Advanced Specialized
- ✓ Project is a Migrate & Modernize engagement
- ✓ Project size is $25K - $1M/year estimated Azure consumption

How to nominate

- ✓ Go to aka.ms/AMMPpartnerled to get started

***Partners investing in Cloud Security are seeing over 130% YoY growth.**

Source: Forrester 2021 Partner Opportunity Around Microsoft Security, Compliance, And Identity Solutions TEI study commissioned by Microsoft

AMMP helps with common Migration and Modernization scenarios

Infrastructure and database migration

Move your workloads to Azure to enhance operational efficiency, business continuity, disaster recovery, and optimize costs

[for Windows Server, SQL Server, Linux, OSS-databases, DevTest, migrating to VMware to Azure VMware Solution, hybrid deployment with Arc-enabled servers and data]

Virtual desktop infrastructure

Quickly migrate Windows desktops and apps to Azure with Azure Virtual Desktop and access your desktop and applications from virtually anywhere

[for Windows 10 and 11 based virtual desktops, incl. VMware and Citrix solutions]

App and data modernization

(incl. cloud native)

Modernize your web apps and innovate with new cloud-native apps on a highly productive platform with fully managed services

[for all application languages and frameworks (.NET, Java, PHP, etc.) and supporting database backends, including hybrid deployment options]

SAP

Migrate SAP landscapes to Azure and add complementary cloud services to accelerate innovation

[for SAP native environments, SAP HANA migration and greenfield SAP deployments]

Azure security foundations

Enhanced support within all AMMP offers to help you establish a highly secure cloud environment

NEW!

Hybrid and multicloud with Azure Arc

New AMMP offers and support so you can innovate anywhere

Assess & Plan

Arc Envisioning Workshop NEW OFFER

- Overview of Azure Arc capabilities
- Get hands-on experience with Azure Arc onboarding suited to your scenario (e.g. VMs, Azure SQL Managed Instance or a Kubernetes cluster).
- Understand management scenarios, including security with Microsoft Defender for Cloud

Pilot/Proof of Concept

- AMMP's pilot/POC offering extended to support all Arc-enabled scenarios
- Up to **$20K** partner funding + up to **$5K** Azure Access sandbox

Migrate & Modernize

Standard and Advanced offers EXPANDED SUPPORT

- Azure Arc supported in both Infrastructure/Database Migration and App & Data Modernization scenarios
- AMMP benefits are aligned to Standard and Advanced offers:
  - ✓ Assistance from partners + FastTrack for Azure guidance in Advanced offer
  - ✓ Partner funding at **20%** of 1st year Azure consumption estimates
  - ✓ Azure credits
  - ✓ Technical skilling

Guidance – include the Arc-enabled services in the overall project estimate

An example

Azure services	1st year Azure consumption estimate	AMMP Partner funding
Azure VMs and data services	$800K	$160K
Arc-enabled infrastructure and services	$100K	$20K
Total	**$900K**	**$180K**

Azure services in scope: Azure Arc-enabled Virtual Machines (Windows and Linux), Azure Arc-enabled SQL Managed Instance/SQL Server, Azure Arc-enabled Kubernetes

MCI Build Intent Usage Workshop

Secure Multi-Cloud Environments

Improve security posture and protection of multi-cloud environments

Focus Workloads & Objectives

Focus Workloads:

Microsoft Defender for Cloud (Servers, Storage, Containers, Databases)

Leave the customer in a better place:

- Microsoft Defender for Cloud enabled for additional resources using a documented limited scope and set of agreed design decisions
- Guidance on how to integrate Microsoft Defender for Cloud into security operations
- 30-60-90 day roadmap and checklist to improve customer's multi-cloud security posture

Workshop Name	Customer Criteria	Partner Criteria	Payment
Usage : Secure Multi-Cloud Environments	• Annual Azure consumption must be greater than $100,000 USD. (Annual Azure consumption = Azure consumption in last 12 months) • Microsoft Defender for Cloud consumption >4% of total Azure consumption	• Co-sell ready	• **$5K USD**

[Learn More About the Secure Multi-Cloud Environments Usage Workshop]

Why are partners so crucial to Cloud Security?

Build Practice	Qualify Lead 10%	Develop Strategy 20%	Present Value 40%	Prove Value 60%	Secure Work 80%	Drive Consumption
Build Solutions & Skilling	Listen & Consult/ Inspire & Design	Empower & Achieve/Realize Value			Realize Value	Manage & Optimize

AMMP (Azure Migration & Modernization Program): **Field OR Partner-led**

Solution Assess: For assessment of live env & recommendations

Solution Assess as a Service

MSSP: MXDR **Workshop** for onboard to POC of Managed Security Service

NEW ACO (Azure Credit Offer)

DfS P2 Targeted Empowerment: Discount on Server Security

New Usage **Workshops**

MSSP/MCI Workshops for Live-production Demo Payout #1

Managed Security **POC** PIE for 30-90-day POC of MDR service

MSSP: Payout #2

MSSP Compete **ECIF** for onboarding and X mos of full MDR service

MSSP: MXDR **Workshop** for onboard to MDR (E5, low usage)

Managed Security **POC** PIE for 30-90-day POC of MDR (E5, low usage)

OSU/CPOR, PAL

AMMP-funding levers

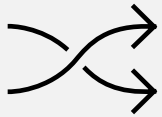
Can be stacked with both programs

MSSP Program-funding levers

Go-dos for Partner Success in Security

Building new-age Technical Capabilities	Attend Technical Trainings to Build new Security Service Offerings
Power Up with Microsoft Programs	**MCI Workshop:** Pre-sales & Usage/Consumption **Security Solution Assessment:** or Assessment as a Service **Partner-led AMMP:** Submissions with Security Included
Specialization	Puts your solution at the **top** of the MSFT field partner list; **Attain at least one Security Specialization**
Sell in Verticals	Like **retail, healthcare, financial services, manufacturing, education, State & Local Gov** create value for our customers
Go-to-Market Offers	Familiarize yourself with new Campaign Content: • **XDR + SIEM: Secure More with Less** • **Forrester study: The Total Economic Impact™ of Azure Defender for Cloud**

Trends from the past year



1. Transition to Hybrid Work

2. Navigating Multi-Cloud complexity

3. Increase of Ransomware Attacks

4. Demand for Security experts

The Partner Opportunity Around Microsoft Security, Compliance and Identity Solutions, a Total Economic Impact™ study commissioned by Microsoft and conducted by Forrester Consulting, 2022

Partner Testimonials

Forrester 2022 Partner Opportunity Research

"We are still helping some clients revisit decisions made hastily during the COVID work-from-home rush, but most of our effort is around helping customers formulate **better hybrid-working strategies**."

"**Ninety percent of the companies** we talk to need to outsource their IT security if they want to be properly protected. We are bundling together the E5 and Azure pieces into a single managed services offering."

"**We continue to bet on Microsoft as the go-to-market leader for security**. We will continue to invest in our Microsoft 365 and Azure security practices to take advantage of this growth."

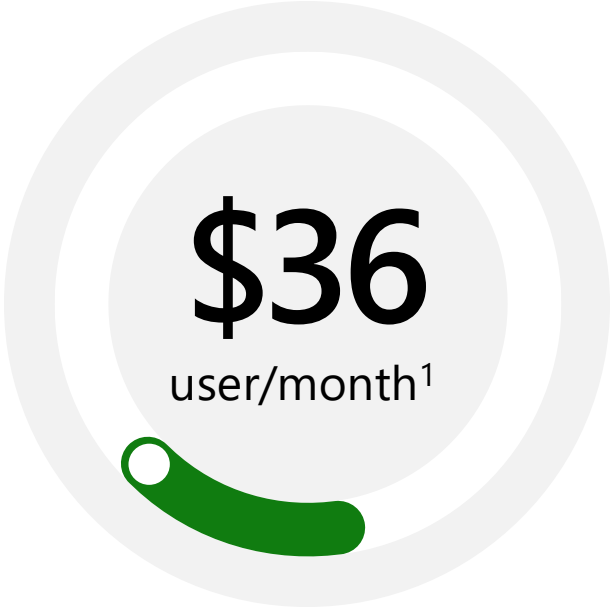
The Partner Opportunity Around Microsoft Security, Compliance and Identity Solutions, a Total Economic Impact™ study commissioned by Microsoft and conducted by Forrester Consulting, 2022

Microsoft Security

Partner revenue opportunity

2022
Microsoft Security Services

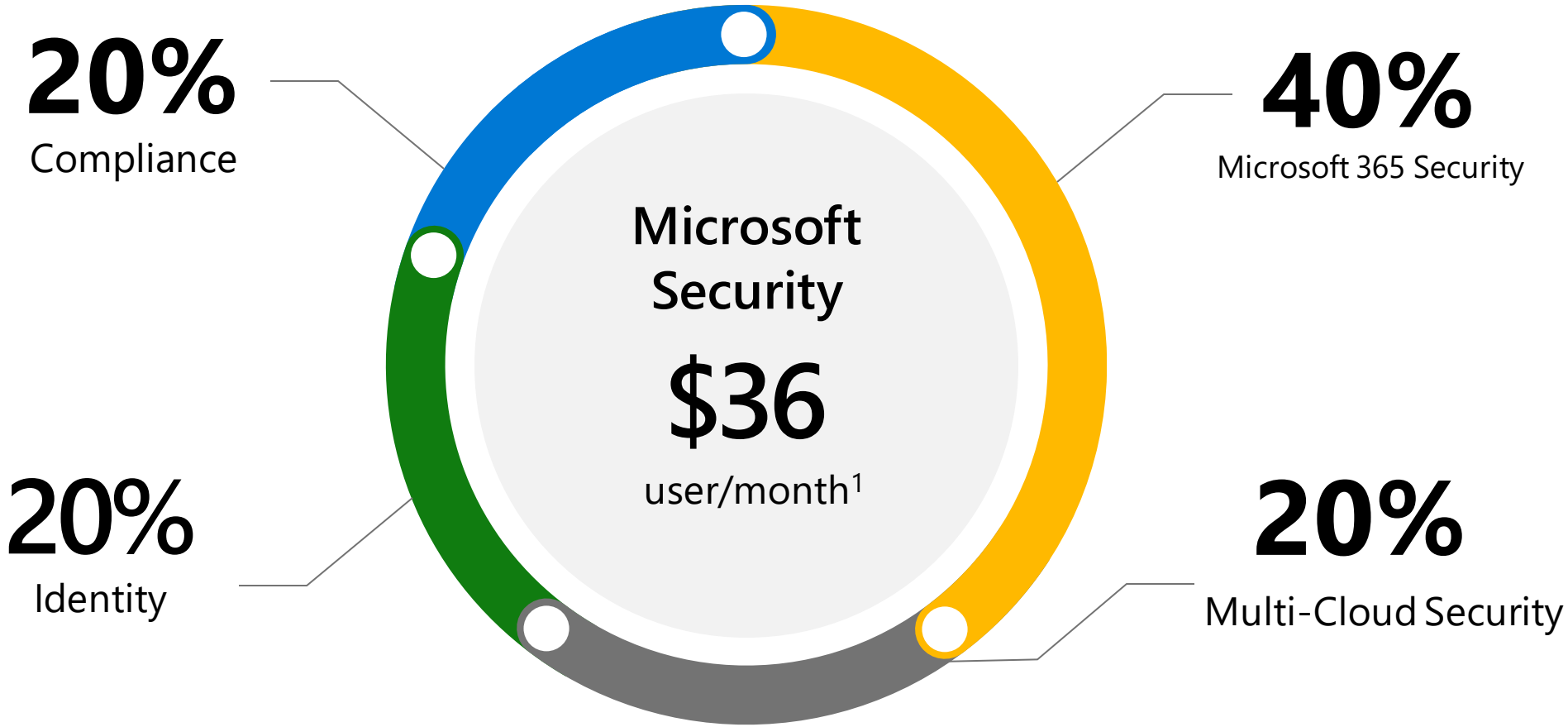
2022
Microsoft Security



Forrester 2022 The Partner Opportunity Around Microsoft Security, Compliance, And Identity Solutions TEI study commissioned by Microsoft

Microsoft Security

Partner revenue opportunity mix



Forrester 2022 The Partner Opportunity Around Microsoft Security, Compliance, And Identity Solutions TEI study commissioned by Microsoft

“We are helping a lot of customers in their digital transformations of moving to the cloud. This includes infrastructure, data, and applications. Multi-cloud makes these initiatives bigger for us.”

Senior managing director – Microsoft Security partner

Forrester 2022 Partner Opportunity Around Microsoft Security, Compliance, And Identity Solutions TEI study commissioned by Microsoft

SECURITY PARTNER SUCCESS STORY

Partner Opportunity	Investment	Results

• IT Services Company
• Established security practice but very little of it was Microsoft
• We convinced them to make a big bet on Microsoft security after seeing growth of Microsoft security capabilities in recent years
• Championed internally by their VP of Security Services, who led security strategy and offering development for the company
	• PTS and CSA engaged to help modify their security practice with a new focus on Microsoft security capabilities
	• Worked together to understand current capabilities of the partner's security team and their strategic big bets
	• Built a plan that focused on solution building activities that included technical trainings, workshop deliveries, and the development of solutions to publish in the marketplace.
	• After a 1+ year long effort, solutions now developed and Co-Sell activities in full pursuit, the team has started to see a return on their dedicated investment
		Capacity
		• Launched 4 new LSE security offerings in H1FY23
		  • Securing Identities Workshop
		  • Data Protection Workshop
		  • Defender for Endpoint Advisory Workshop
		  • Managed Microsoft Defender for Cloud Implementation (Co-Sell Prioritized)
		Capability
		• High attendance in recent Security Rockstar Bootcamps
		• In queue to join Managed Security Service Partner (MSSP) Program
		• Attained MCPP Solutions Partner for Security Designation and IAM Specialization
		Co-sell
		• These solutions have already generated several million dollars in pipeline, with notable customers
		• Tripled their Security ACR in the past 12 months

Microsoft Security

Thank you

laurabrick@microsoft.com