

Microsoft Defender Security Solutions for Microsoft 365 and Azure

Wade Walker
VP Cloud Services

wadew@biggreenit.com

Lindsay Cowan
Account Manager

lindsayc@biggreenit.com

Austin Kelly
Account Manager

austink@biggreenit.com



Microsoft
Partner



Gold Data Analytics
Gold Data Platform
Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices

Today's Agenda

Introduction: Wade Walker / Lindsay Cowan / Austin Kelly

Microsoft Defender Security Solutions for Microsoft 365 and Azure

- Overview
- Microsoft Defender Services in Microsoft 365
- Microsoft Defender Services in Azure
- Microsoft 365 Defender + Azure Defender + Sentinel
- Defender Licensing

Q & A / Wrap Up



Connecting Enterprise Businesses to the Microsoft Cloud Ecosystem

- Business is moving to the Cloud at a rapid pace
- We help companies develop a comprehensive Cloud strategy that delivers the right technology at the right time
- Build upon the Microsoft Cloud platform
- Leverage our expertise for Microsoft Cloud consulting, licensing, implementation and support
- Together we can help you develop a modern infrastructure with an ecosystem of products and services that are:
 - Secure
 - Built to work together
 - Supported
 - Able to grow and pivot as business needs change



Azure regions

Azure has more global regions than any other cloud provider—offering the scale needed to bring applications closer to users around the world, preserving data residency, and offering comprehensive compliance and resiliency options for customers.

Azure is “*The World's Computer*”

55 regions worldwide **140** available in 140 countries



* Two Azure Government Secret region locations undisclosed

Azure / Microsoft 365: Trusted

Global



ISO 27001



ISO 27018



ISO 27017



ISO 22301



SOC 1 Type 2



SOC 2 Type 2



SOC 3



CSA STAR
Self-Assessment



CSA STAR
Certification



CSA STAR
Attestation

Regional



Argentina
PDPA



EU
Model
Clauses



UK
G-Cloud



China
DJCP



China
GB 18030



China
TRUCS



Singapore
MTCS



Australia
IRAP/CCSL



New
Zealand
GCIO



Japan My
Number Act



ENISA
IAF



Japan CS
Mark Gold



Spain
ENS



Spain
DPA



India
MeitY



Canada
Privacy Laws



Privacy
Shield



Germany IT
Grundschutz
workbook

Industry



PCI DSS
Level 1



CDSA



MPAA



FACTUK



Shared
Assessments



FISC Japan



HIPAA/
HITECH Act



HITRUST



GxP
21 CFR Part 11



MARS-E



IG Toolkit UK



FERPA



GLBA



FFIEC

Us Gov



Moderate
JAB P-ATO



High
JAB P-ATO



DoD DISA
SRG Level 2



DoD DISA
SRG Level 4



DoD DISA
SRG Level 5



SP 800-171



FIPS 140-2



Section 508 VPAT



ITAR



CJIS



IRS 1075

Overview



Microsoft
Partner



Gold Cloud Platform
Gold Data Platform
Gold Windows and Devices
Silver Cloud Productivity
Silver Small and Midmarket Cloud Solutions

Five Best Practices for Cloud Security



Cloud security is a fundamentally new landscape for many companies.

While many of the security principles remain the same as on-premises, the implementation is often very different. This overview provides a snapshot of five best practices for cloud security: identity and access control, security posture management, apps and data security, threat protection, and network security.



Strengthen access control

Traditional security practices are not enough to defend against modern security attacks. Therefore, the modern security practice is to “assume breach”: protect as though the attacker has breached the network perimeter. Today, users work from many locations with multiple devices and apps. The only constant is user identity, which is why it is the new



Institute multifactor authentication

Provide another layer of security by requiring two or more of the following authentication methods:

- Something you know (a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics)



Take advantage of conditional access

Master the balance between security and productivity by factoring how a resource is accessed into an access control decision. Implement automated access control decisions for accessing your cloud apps that are based on conditions.



Operate in a zero-trust model

Verify the identity of everything and anything trying to authenticate or connect before granting access.



Improve your current posture

Use a tool like [Secure Score](#) in [Azure Security Center](#) to understand and improve your security posture by implementing best practices.



Educate stakeholders

Share progress on your secure score with stakeholders to demonstrate the value that you are providing to the organization as you improve organizational security.



Collaborate with your DevOps team on policies

To get out of reactive mode, you must work with your DevOps teams up front to apply key security policies at the beginning of the engineering cycle as secure DevOps.



Improve security posture

With more and more recommendations and security vulnerabilities identified, it is harder to triage and prioritize response. Make sure you have the tools you need to assess your current environments and assets and identify potential security issues.



Secure apps and data

Protect data, apps, and infrastructure through a layered, defense-in-depth strategy across identity, data, hosts, and networks.



Encryption

Encrypt data at rest and in transit. Consider encrypting data at use with confidential computing technologies.

Follow security best practices

Ensure your open source dependencies do not have vulnerabilities. Additionally, train your developers in security best practices such as [Security Development Lifecycle \(SDL\)](#).



Share the responsibility

When a company operates primarily on premises, it owns the whole stack and is responsible for its own security. Depending on how you use the cloud, your responsibilities change, with some responsibilities moving to your cloud provider.

- IaaS: for applications running in virtual machines, more of the burden is on the customer to ensure that both the application and OS are secure.
- PaaS: as you move to cloud-native PaaS, cloud providers like Microsoft will take more of the security responsibility at the OS level itself.
- SaaS: at the SaaS level, more responsibility shifts away from the customer. See the [shared responsibility model](#).





Enable detection for all resource types

Ensure threat detection is enabled for virtual machines, databases, storage, and IoT. [Azure Security Center](#) has built-in threat detection that supports all Azure resource types.



Integrate threat intelligence

Use a cloud provider that integrates threat intelligence, providing the necessary context, relevance, and prioritization for you to make faster, better, and more proactive decisions.



Modernize your security information and event management (SIEM)

Consider a [cloud-native SIEM](#) that scales with your needs, uses AI to reduce noise and requires no infrastructure.



Mitigate threats

Operational security posture—protect, detect, and respond—should be informed by unparalleled security intelligence to identify rapidly evolving threats early so you can respond quickly.



Protect the network

We're in a time of transformation for network security. As the landscape changes, your security solutions must meet the challenges of the evolving threat landscape and make it more difficult for attackers to exploit networks.



Keep strong firewall protection

Setting up your firewall is still important, even with identity and access management. Controls need to be in place to protect the perimeter, detect hostile activity, and build your response. A web application firewall (WAF) protects web apps from common exploits like SQL injection and cross-site scripting.



Enable Distributed Denial of Service (DDoS) Protection

Protect web assets and networks from malicious traffic targeting application and network layers, to maintain availability and performance, while containing operating costs.



Create a micro-segmented network

A flat network makes it easier for attackers to move laterally. Familiarize yourself with concepts like virtual networking, subnet provisioning, and IP addressing. Use micro-segmentation, and embrace a whole new concept of micro perimeters to support zero trust networking.

Microsoft Defender Services in Microsoft 365

Lindsay Cowan

Account Manager

lindsayc@biggreenit.com



Microsoft
Partner



Gold Data Analytics
Gold Data Platform
Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices

Microsoft 365 Defender

Prevent and detect attacks across your identities, endpoints, apps, email, data, and cloud apps with XDR capabilities. Investigate and respond to attacks with out-of-the-box, best-in-class protection. Hunt for threats and easily coordinate your response from a single dashboard.



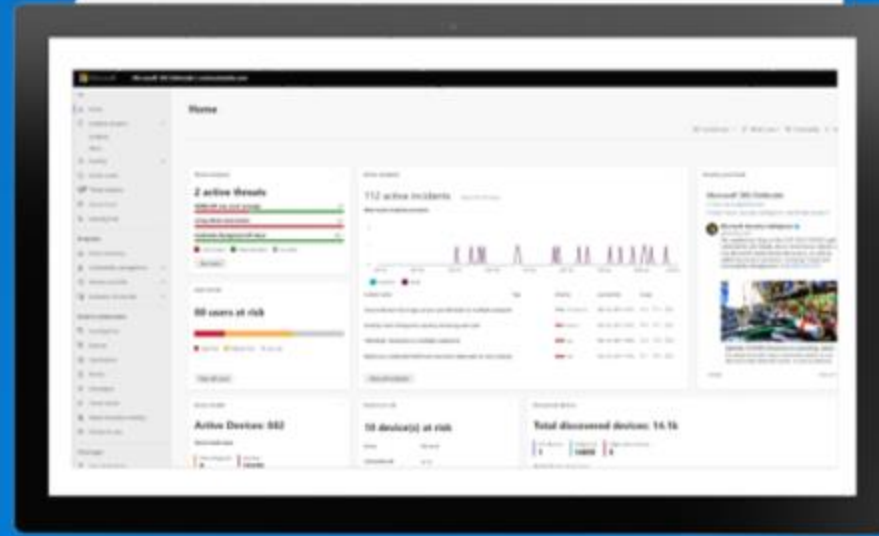
1 Stop attacks before they happen
Reduce your attack surface and eliminate persistent threats.



2 Detect and automate across domains
Integrate threat detection data for rapid and complete response.



3 Hunt across all your data
Leverage time saved to apply your unique expertise.



Microsoft 365 Defender Portal for All Products:



Incidents > Multi-stage incident involving Initial access & Exfiltration on one endpoint reported by multiple sources

Multi-stage incident involving Initial ...

Manage incident Consult a threat expert Comments and history

Summary Alerts (95) Devices (1) Users (2) Mailboxes (38) Investigations Evidence and Response (8.17k)

Alerts and categories
94/95 active alerts
5 MITRE ATT&CK tactics
1 other alert categories

Scope
1 impacted device
2 impacted users
38 impacted mailboxes

Top impacted entities

Entity type	Risk level/investigation priority	Tags
[Device]	High	asdf tag
[User]	0	
[User]	0	Office 365 ad
[Mailbox]	No data available	
[Mailbox]	No data available	

Incident Information
 This incident might be associ...
 Associated Incidents

Microsoft 365 Defender Portal for Specific Incident:

Incidents > Multi-stage incident involving Initial access & Exfiltration on one endpoint reported by multiple sources

Multi-stage incident involving Initi...

Manage incident Consult a threat expert

Summary Alerts (95) Devices (1) Users (2) Mailboxes (38) Investigations (24) Evidence and Response (8.17k)

1-30 of 95 Choose columns 30 items per page Filters

Title	Tags	Severity	Status	Linked by	Category
Email was delivered but it recognized as a threat		Medium	New	4 reasons	Initial acce
![[Uh oh...]](https://www.example.com/image.png?onload="alert('XSS'))	asdf tag +1	High	New	Same device	Exploit
Custom detection - move mail to inbox		Medium	New	33 reasons	Execution
Custom detection - move mail to inbox		Medium	Resolved	Same user credentials	Execution



Gold Data Analytics
 Gold Data Platform
 Gold Cloud Platform
 Gold Cloud Productivity
 Gold Windows and Devices

Microsoft 365 Defender Services/Licensing

- Microsoft Defender for Business
- Microsoft Defender for Endpoint Plan 1 / Plan 2
 - *Defender Vulnerability Management (add on to Plan 2)
- Microsoft Defender for Endpoint Servers
- Microsoft Defender for Office 365 Plan 1 / Plan 2
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps



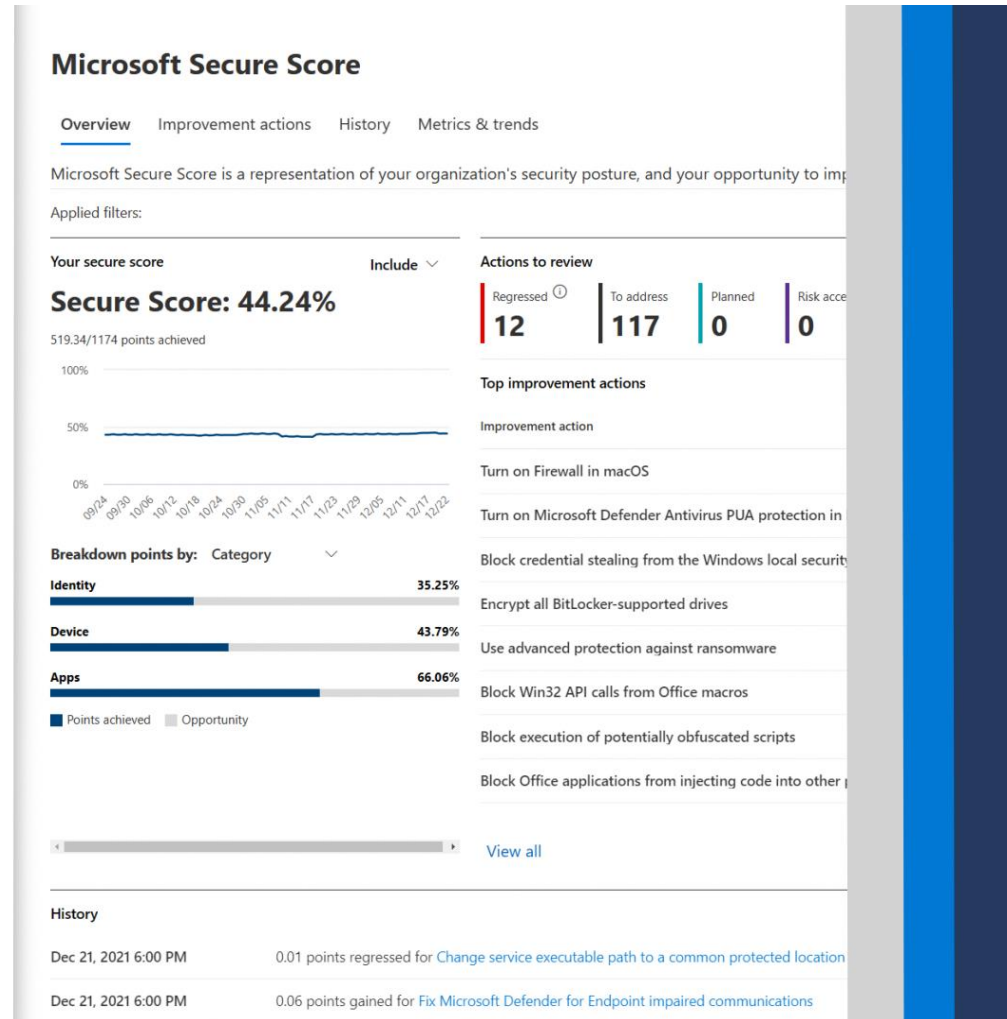
Microsoft
Partner



Gold Cloud Platform
Gold Data Platform
Gold Windows and Devices
Gold Data Analytics
Gold Cloud Productivity

Microsoft 365 Defender

Microsoft Secure Score



Secure Score helps organizations:

- Report on the current state of the organization's security posture.
- Improve their security posture by providing discoverability, visibility, guidance, and control.
- Compare with benchmarks and establish key performance indicators (KPIs).

Microsoft Defender Services in Azure

Austin Kelly

Account Manager

austink@biggreenit.com



Microsoft Defender for Cloud / Azure Defender

Microsoft Defender for Cloud

Protect your multi-cloud and hybrid cloud workloads with built-in XDR capabilities. Secure your servers, storage, databases, containers, and more. Focus on what matters most with prioritized alerts.



1 Assess and strengthen the security configuration of your cloud resources.



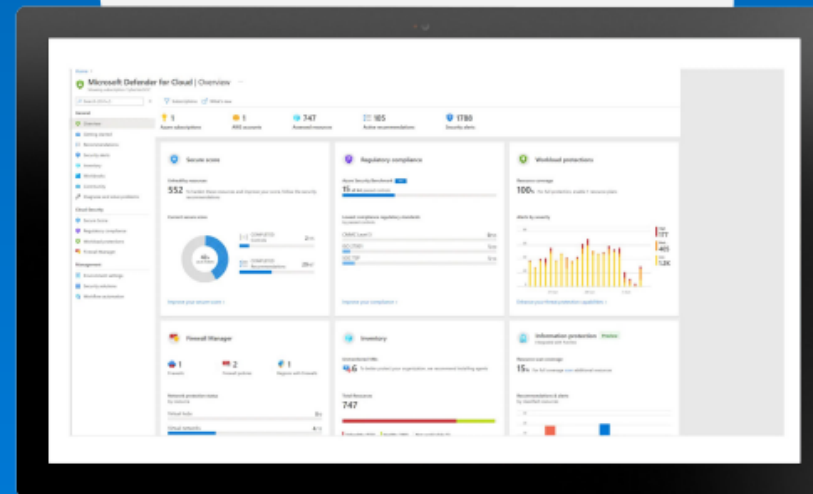
2 Manage compliance against critical industry and regulatory standards.



3 Enable threat protection for workloads running in Azure, AWS, Google Cloud Platform, & on premises.



4 Detect vulnerabilities to protect your multicloud and hybrid workloads against malicious attacks.



Azure Defender Services

Microsoft Defender for Cloud / Azure Defender

- Microsoft Defender for App Service
- Microsoft Defender for Azure Cosmos DB
- Microsoft Defender for Containers / Container Registries
- Microsoft Defender for DNS
- Microsoft Defender for IoT (Monitored Devices, Agentless OT)
- Microsoft Defender for Key Vault
- Microsoft Defender for Kubernetes
- Microsoft Defender for MariaDB

Microsoft Defender for Cloud / Azure Defender

- Microsoft Defender for MySQL
- Microsoft Defender for PostgreSQL
- Microsoft Defender for Azure Resource Manager (ARM)
- Microsoft Defender for Servers Plan 1 / Plan 2
- Microsoft Defender for SQL (On Azure / Outside Azure)
- Microsoft Defender for Storage
- Microsoft Defender Percentage Model
- Microsoft Defender External Attack Surface Management (EASM)



Microsoft
Partner



Gold Cloud Platform
Gold Data Platform
Gold Windows and Devices
Gold Data Analytics
Gold Cloud Productivity

Azure Security Center

Security Center | Azure Defender

Showing 64 subscriptions

Search (Cmd+/) Subscriptions What's new

- General
 - Overview
 - Getting started
 - Recommendations
 - Security alerts
 - Inventory (Preview)
 - Community
- Cloud Security
 - Secure Score
 - Regulatory compliance
- Azure Defender**
- Management
 - Pricing & settings
 - Security policy
 - Security solutions
 - Workflow automation
 - Coverage

Azure Defender coverage

1,055 TOTAL

- Fully covered (659)
- Agent not installed (12) [Install](#)
- Not covered (384) [Upgrade all](#)

Virtual Machines: 266/330	Kubernetes Service: 6/20	Container registry: 2/7	App Services: 66/94
SQL Server Virtual Machines: 0/7	Key vaults: 5/46	SQL servers: 28/37	Storage accounts: 286/502

Security alerts

High severity	20
Medium severity	63
Low severity	7

Advanced protection

VM Vulnerability Assessment: 132 Unprotected	Just-in-time VM access: 11 Unprotected	Adaptive application control: 43 Unprotected	Container image scanning: 2 Unprotected	Adaptive network hardening: 12 Unprotected
SQL vulnerability assessment: 27 Unprotected	File integrity monitoring	Network map	IoT security	

Insights

Most prevalent security alerts

Suspicious authenticatio...	8
PREVIEW - User accesse...	5
Traffic detected from IP ...	3

Most attacked resources

ec2amaz-f4e0ns5	19 Alerts
ch-victimvm00	19 Alerts
ch-victimvm00-dev	19 Alerts

High severity VM vulnerability alerts

- Microsoft Windows Security Update...
- Microsoft Internet Explorer Remote ...
- Microsoft Windows Security Update...

[View all in ARG >](#)

Azure Secure Score

Secure score recommendations

All recommendations

Secure score ⓘ

71%

Active items

Controls 6/15
Recommendations 10/39

Resource health

Unhealthy (13) Healthy (5) Not applicable (17)

Governance (preview)

Azure AWS GCP

Overdue recommendations 0/0 ⓘ
Unassigned recommendations 10/10 ⓘ

Recommendation status == None

Severity == None

Resource type == None

Recommendation maturity == None

Show my items only: Off

Name <input type="button" value="↑↓"/>	Max score <input type="button" value="↑↓"/>	Current score <input type="button" value="↑↓"/>	Potential score increase <input type="button" value="↑↓"/>	Status <input type="button" value="↑↓"/>	Unhealthy resources	Insights
> Secure management ports	8	8.00		Completed	0 of 7 resources	
> Apply system updates	6	2.00	+ 11%	Unassigned	8 of 12 resources	
> Encrypt data in transit	4	4.00		Completed	0 of 3 resources	
> Manage access and permissions	4	4.00		Completed	0 of 11 resources	
> Remediate security configurations	4	1.45	+ 7%	Unassigned	7 of 12 resources	
> Restrict unauthorized network access	4	4.00		Completed	0 of 13 resources	
> Apply adaptive application control	3	0.50	+ 7%	Unassigned	5 of 7 resources	
> Enable endpoint protection	2	1.17	+ 2%	Unassigned	5 of 12 resources	
> Enable auditing and logging	1	0.29	+ 2%	Unassigned	5 of 7 resources	

Microsoft Defender + Azure Defender + Sentinel

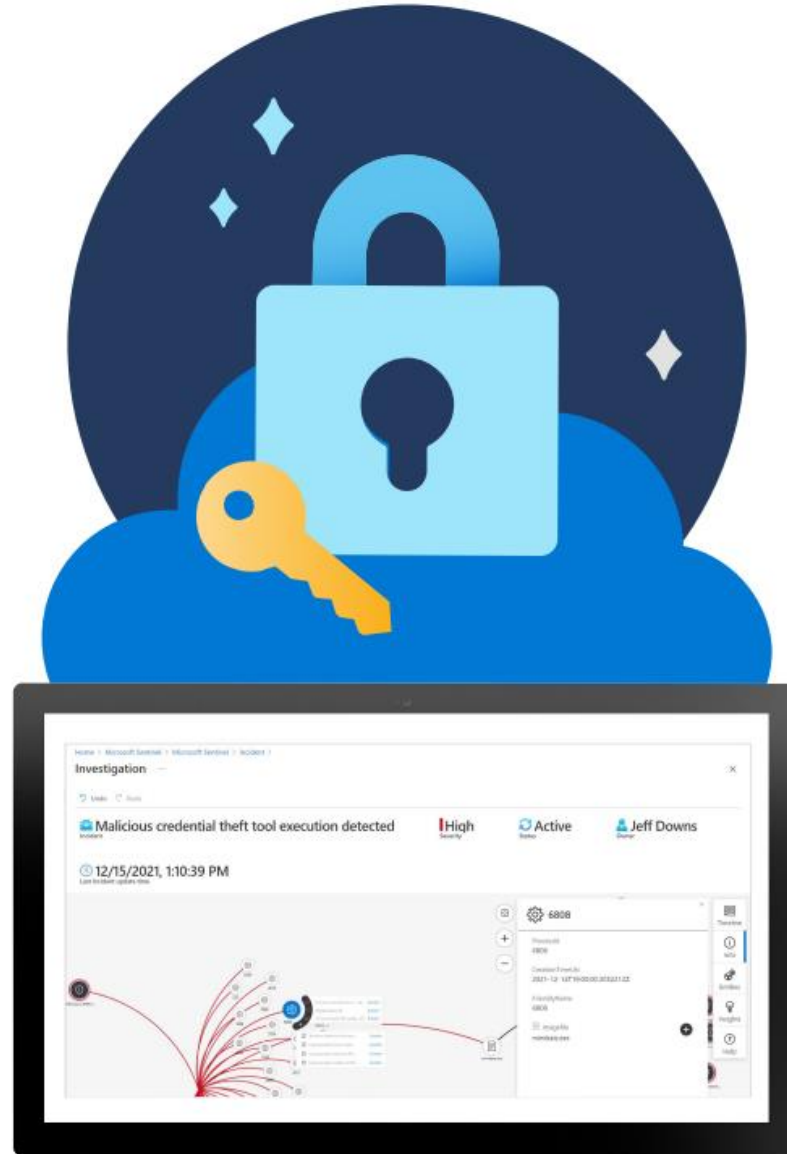


Microsoft
Partner



Gold Data Analytics
Gold Data Platform
Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices

Azure Sentinel



Microsoft Sentinel

Get a bird's-eye view across the enterprise with the cloud-native security information and event management (SIEM) tool from Microsoft. Aggregate security data from virtually any source and apply AI to separate noise from legitimate events, correlate alerts across complex attack chains, and speed up threat response with built-in orchestration and automation.



Collect Data at cloud scale across all users, devices, application, and infrastructure, both on-premises and in multiple clouds.



Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft.



Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.



Respond to incidents rapidly with built-in orchestration and automation of common tasks.

SIEM

Azure Sentinel



Multi-cloud



Partnerships

Cloud native, any data, any entity



Cloud native



Any data



AI



Automation



Identities



Devices



Data



Infrastructure



Apps









Network







Microsoft 365 Defender & Azure Defender

← Cross-domain protection →

Microsoft 365 Defender

-  Identities
-  Endpoints
-  Apps
-  E-mail
-  Cloud Apps
-  Docs

Azure Defender

-  SQL
-  Server VMs
-  Containers
-  Network
-  IoT
-  Azure App Services

Microsoft 365 Defender & Azure Defender

Microsoft Defender Licensing



Microsoft
Partner



Gold Cloud Platform
Gold Data Platform
Gold Windows and Devices
Silver Cloud Productivity
Silver Small and Midmarket Cloud Solutions

Security Operations / SOC

Threat Experts | Detection and Response Team (DART) | MSSP/MDR

Microsoft Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

Microsoft Defender – Extended Detection and Response (XDR)
Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting

Other Tools, Logs, & Data Sources

Cloud Azure, AWS, GCP, On Premises & other 3rd party clouds	Endpoint & Server/VM	Office 365 Email and Apps	Identity Cloud & On-Premises	SaaS Cloud Apps	+ More OT, IoT, SQL, and more
---	---------------------------------	-------------------------------------	--	---------------------------	---



Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

December 2021 – <https://aka.ms/MCRA>

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. [Security Documentation](#)
2. [Microsoft Best Practices](#)
3. Azure Security [Top 10](#) | [Benchmarks](#) | [CAF](#) | [WAF](#)

Software as a Service (SaaS)

Microsoft Defender for Cloud Apps

- App Discovery & Risk Scoring (Shadow IT)
- Threat Detection & Response
- Policy Audit & Enforcement
- Session monitoring & control
- Information Protection & Data Loss Prevention (DLP)



Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

Endpoints & Devices

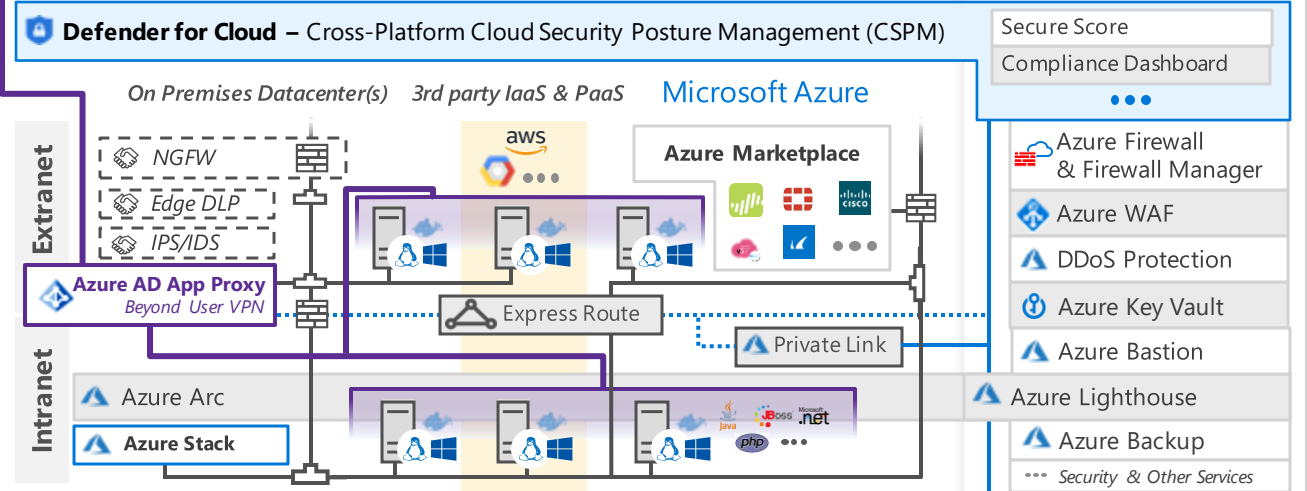
Microsoft Endpoint Manager
Unified Endpoint Management (UEM)

Intune | Configuration Manager

Microsoft Defender for Endpoint
Unified Endpoint Security

- Endpoint Detection & Response (EDR)
- Web Content Filtering
- Threat & Vuln Management
- Endpoint Data Loss Protection (DLP)

Hybrid Infrastructure – IaaS, PaaS, On-Premises



Information Protection

Azure Purview

Microsoft Information Protection (MIP)

Monitor | Discover | Classify | Protect

File Scanner
(on-premises and cloud)

Data Governance

Advanced eDiscovery

Compliance Manager

Azure Active Directory

Passwordless & MFA

- Hello for Business
- Authenticator App
- FIDO2 Keys

Identity Protection
Leaked cred protection
Behavioral Analytics

Azure AD PIM

Identity Governance

Azure AD [B2B](#) & [B2C](#)

Defender for Identity

Active Directory

Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

Privileged Access Workstations (PAWs) – Secure workstations for administrators, developers, and other sensitive users

Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance

Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls

Windows 10 & 11 Security

- Network protection
- Credential protection
- Full Disk Encryption
- Attack surface reduction
- App control
- Exploit protection
- Behavior monitoring
- Next-generation protection

IoT and Operational Technology (OT)

Azure Sphere

Microsoft Defender for IoT

- ICS, SCADA, OT
- Internet of Things (IoT)
- Industrial IoT (IIoT)
- Asset & Vulnerability management
- Threat Detection & Response

Defender for Cloud – Cross-Platform, Cross-Cloud XDR

Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses

People Security

Attack Simulator | Insider Risk Management | Communication Compliance

GitHub Advanced Security – Secure development and software supply chain

Threat Intelligence – 8+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)


Next Steps



Cloud Consultation



[Contact us for a free consultation](#)




(916) 787-3223

Cloud Services ▾ Solutions ▾ About Us ▾ Knowledge Center ▾

[Client Portal](#) [Contact Us](#)

30-minute Microsoft Cloud Consultation



Sometimes 30 minutes is all it takes to get the answers you need. Gather up your specific questions and discussion topics and we will connect you with one of our Microsoft experts for a 30-minute 1:1 call.

During this call, the floor is yours. You ask your questions, and we will provide you with answers.

Let's sync calendars. Please fill out the form to the right and we will get back with you right away to schedule a meeting.

Please provide us with a brief description of what you would like to discuss so we can get the right Microsoft expert on the call.

Schedule your 30-minute consultation

First Name **

Last Name **

Job Title **

Company Name **

Company Email **

Phone Number

Please tell us what you would like to discuss **

Secure Score / BGIT Support



Big Green IT M365 Support

Sometimes even the most experienced IT teams need help. Microsoft is continually making changes and improvements to Microsoft 365 products and services. This constant change makes it challenging for IT teams to keep up and can sometimes overwhelm your help desk.

Big Green IT is a Tier 1, direct Microsoft Gold partner. We offer a range of Microsoft 365 support service plans to meet the varying needs of our customers.

Features	Standard	Most Popular Premium	Enterprise
Incident Support	Basic	Unlimited	Unlimited
Service Request	Basic	Unlimited	Unlimited
Response Times	4 Hours	2 Hours	1 Hour
Big Green IT Service Management Portal	●	●	●
Big Green Knowledge Base	●	●	●
Big Green License Management Portal	●	●	●
Support Service Hours ^{3,2}		2 Hours	4 Hours
Dedicated Account Manger ³		●	●
Microsoft 365 Critical Response Team		●	●
24 x 7 Support Access			●
Big Green M365 Training Portal			●



Big Green IT- Azure Support Plans

Sometimes even the most experienced IT teams need help. Microsoft is continually making changes and improvements to Azure products and services. This constant change makes it challenging for IT teams to keep up and can sometimes overwhelm your help desk.

Big Green IT is a Tier 1, direct Microsoft Gold partner. We offer a range of Azure support service plans to meet the varying needs of our customers.

Features	Standard <small>Less than \$5,000 monthly Azure Spend</small>	Most Popular Standard+	Premium <small>\$10,001-\$50,000 monthly Azure Spend</small>	Enterprise <small>\$50,001-\$100,000 monthly Azure Spend</small>	Enterprise+ <small>More than \$100,000 monthly Azure Spend</small>
Incident Support	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Service Request	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Response Time with SLA	2 Hours	2 Hours	2 Hours	1 Hour	1 Hour
Big Green IT Support Portal	●	●	●	●	●
Big Green IT Knowledge Base	●	●	●	●	●
Big Green IT License Management Portal	●	●	●	●	●
Support Service Hours ¹	1 Hour	2 Hours	2 Hours	4 Hours	8 Hours
Dedicated Account Manger ¹		●	●	●	●
Microsoft Azure Problem Resolution Support	●	●	●	●	●
Microsoft Azure Critical Response Team		●	●	●	●
24 x 7 Support Access		●	●	●	●
Microsoft Advisory Services Access ²		●	●	●	●
Big Green IT Azure Cost Optimization		●	●	●	●
Microsoft Training Service Access ¹		●	●	●	●

Relevant Links

Microsoft's Five Best Practices for Cloud Security: [Five Best Practices for Cloud Security | Microsoft](#)
Microsoft Digital Defense Report (October 2021): [Microsoft Digital Defense Report OCTOBER 2021](#)
Microsoft Security Best Practices: [Microsoft Security Best Practices | Microsoft Learn](#)

Microsoft Defender Product Family: [Microsoft Defender Product Family | Microsoft Security](#)
Microsoft 365 Secure Score: [Microsoft Secure Score | Microsoft Learn](#)
Microsoft 365 Defender Portal: [Microsoft 365 Defender portal | Microsoft Learn](#)

Microsoft Defender for Cloud: [Microsoft Defender for Cloud - CSPM & CWPP | Microsoft Azure](#)
Microsoft Defender for Cloud Secure Score: [Security posture for Microsoft Defender for Cloud | Microsoft Learn](#)

Microsoft Cloud for Servers: [Integration with Microsoft Defender for Cloud | Microsoft Learn](#)
Azure Sentinel: [Azure Sentinel – Cloud-native SIEM Solution | Microsoft](#)



Gold Cloud Platform
Gold Data Platform
Gold Windows and Devices
Gold Data Analytics
Gold Cloud Productivity

Questions?

- **LinkedIn**
 - <https://www.linkedin.com/in/waderwalker/>
 - <https://www.linkedin.com/in/lindsaybcowan/>
 - <https://www.linkedin.com/in/a1k/>
- **Big Green IT: Free Microsoft Security Consultation**
- **Microsoft Data Center Optimization (DCO)**
- **Microsoft Premier Support**
- **Microsoft Partner Advisory Council**
- **Microsoft Co-Partner / Partner-to-Partner**
- **International Association of Microsoft Channel Partners (IAMCP)**



Microsoft
Partner



Gold Data Analytics
Gold Data Platform
Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices