



A Deeper Look at Microsoft Defender for Business

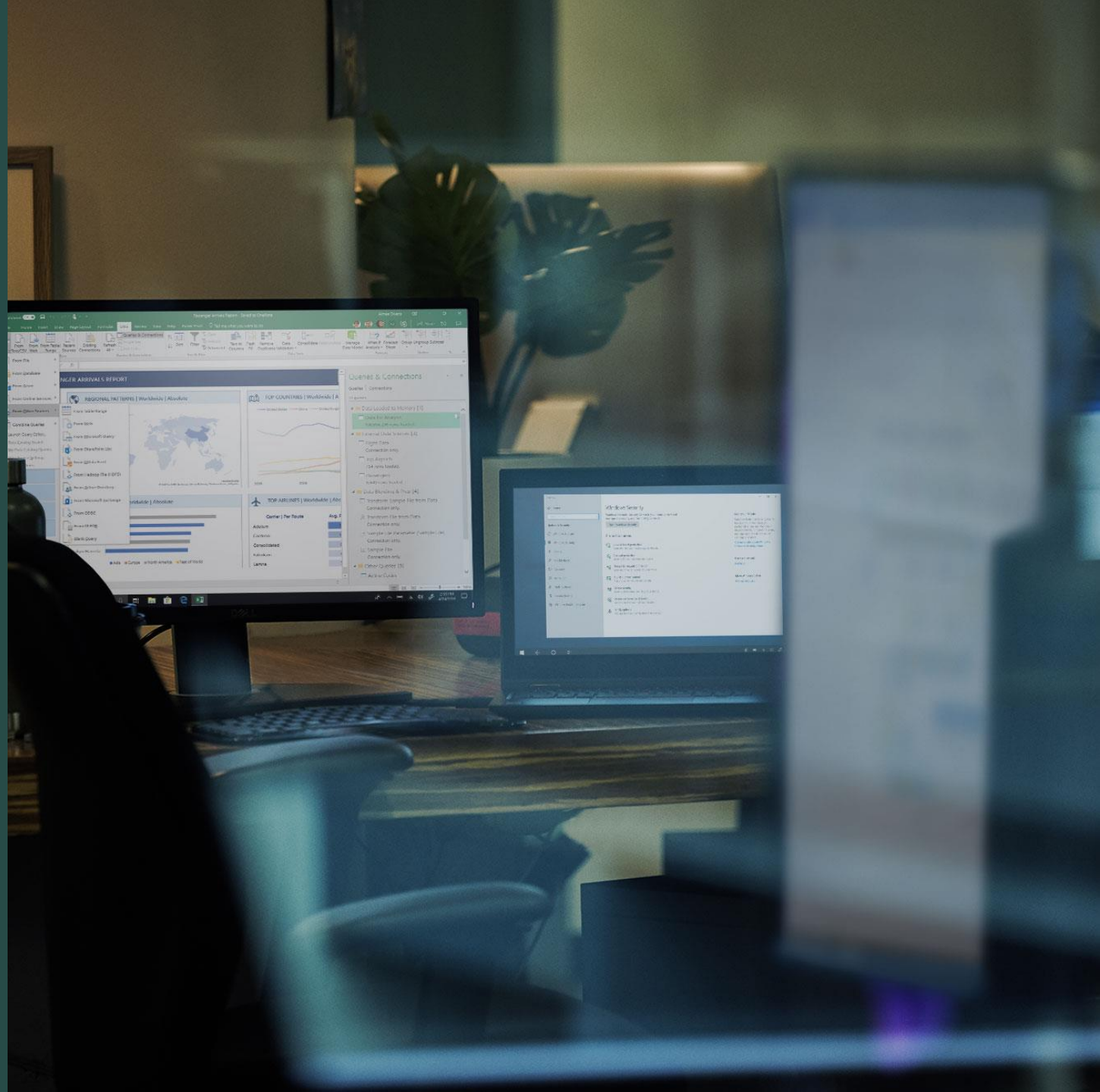
Peter Schmidt

MVP: Office Apps & Services

MCM: Exchange

Twitter: @petsch

Blog: www.msdigest.net



Microsoft Defender for Business

Elevate your security

Elevate your security with enterprise-grade endpoint protection specially built for businesses with up to 300 employees.



Enterprise-grade protection

Security for all your devices with next-gen protection, endpoint detection and response, and threat and vulnerability management.



Easy to use

Streamline onboarding with wizard-driven set up and recommended security policies activated out-of-the-box to quickly secure devices.



Cost-effective

Endpoint security that keeps you productive and works with your IT without compromising budget.

Read the preview blog: <https://aka.ms/MDB-PreviewBlog>

Microsoft Defender consistently rated top AV

- 1 **AV-TEST:** Protection score of 6.0/6.0 in the latest test
- 2 **AV-Comparatives:** Protection rating of 99.7% in the latest test
- 3 **SE Labs:** AAA award in the latest test
- 4 **MITRE:** Industry-leading optics and detection capabilities



6.0/6.0

**Protection score
in AV-TEST**

Achieved perfect protection
score in the past 8 cycles



99.7%

**Real-world protection
in AV-Comparatives**

Scored consistently high in
Real-World Protection Rates



AAA

**Award from SE Labs
in past 4 cycles**

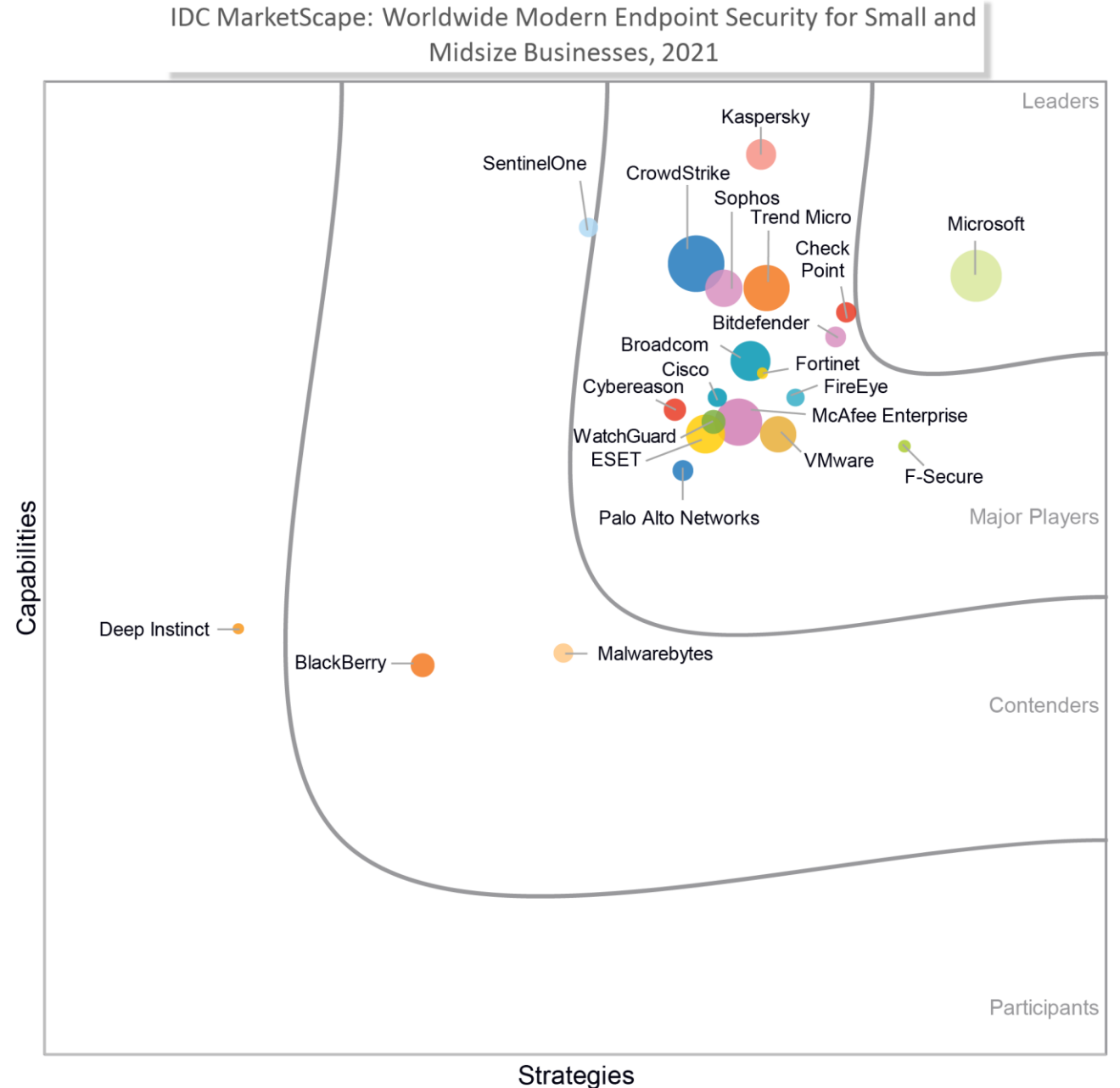
Achieved 97% cycles total
accuracy in latest cycle

Microsoft named a Leader in IDC MarketScape for Modern Endpoint Security for Enterprise and Small and Midsize Businesses

IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessment <https://idcdocserv.com/US48304721>

IDC MarketScape vendor analysis model is designed to provide an overview of the competitive fitness of information and communication technology (ICT) suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each vendor's position within a given market. The Capabilities score measures vendor product, go-to-market, and business execution in the short term. The Strategy score measures alignment of vendor strategies with customer requirements in a three to five-year timeframe. Vendor market share is represented by the size of the icons.

[Microsoft named a Leader in IDC MarketScape for Modern Endpoint Security for Enterprise and Small and Midsize Businesses - Microsoft Security Blog](#)



Source: IDC, 2021

Delivering endpoint security across platforms



 Windows





macOS

Endpoints



iOS

Mobile device OS*

 Windows 365
 Azure Virtual Desktop

Virtual desktops

*Requires Microsoft Endpoint Manager

Defender for Business Licensing options

Microsoft 365 Business Premium

(\$22pupm)^{1,2}

Comprehensive productivity and security solution
Per user license

Microsoft Defender Business

(\$3pupm)¹

Enterprise-grade
endpoint security

Per user license

- ✓ Next generation protection
- ✓ Cross Platform support (iOS, Android, Windows, MacOS)
- ✓ Endpoint Detection and Response
- ✓ Threat and Vulnerability Management
- ✓ ...and more



Microsoft 365 Business Standard (\$12.50)¹
Office apps and services, Teams



Coming soon! Microsoft Defender for Business

Microsoft Defender for Office 365 Plan 1

Intune

Azure AD Premium Plan 1

Azure Information Protection Premium P1

Exchange Online Archiving

Autopilot

Azure Virtual Desktop license

Windows 10/11 Business

Shared Computer Activation

1) As standalone SKU, for up to 300 users

Entitlement for use on up to 5 devices

2) Included as part of Microsoft 365 Business Premium, for up to 300 users

Microsoft Defender for Business will roll out to new and existing Microsoft 365 Business Premium customers at GA

General availability H1 CY 2022

¹price is subject to change based on subscription term, currency and region

Note that not all capabilities may be available in preview.

²Microsoft 365 Business Premium price changes to \$22pupm beginning March 1, 2022.



Microsoft Defender for Business

Elevate your security



Threat & Vulnerability
Management



Attack Surface
Reduction



Next Generation
Protection



Endpoint Detection
& Response



Auto Investigation
& Remediation

Identify

Protect

Detect & Respond

Recover

Enterprise-grade protection for SMBs

Cross platform and enterprise grade protection with next-gen protection, endpoint detection and response, and threat and vulnerability management

Available as a standalone offering and as part of Microsoft 365 Business Premium

Standalone offering will serve non-Microsoft 365 customers. No licensing prerequisites

Supports multi-customer viewing of security incidents with Microsoft 365 Lighthouse for partners in preview

Customer size	< 300 seats	> 300 seats	
Endpoint capabilities\SKU	Microsoft Defender for Business	Microsoft Defender for Endpoint Plan 1	Microsoft Defender for Endpoint Plan 2
Centralized management	✓	✓	✓
Simplified client configuration	✓		
Threat and Vulnerability Management	✓		✓
Attack Surface Reduction	✓	✓	✓
Next-Gen Protection	✓	✓	✓
Endpoint Detection and Response	✓ ²		✓
Automated Investigation and Response	✓ ²		✓
Threat Hunting and 6-months data retention			✓
Threat Analytics	✓ ²		✓
Cross platform support for Windows, MacOS, iOS, and Android	✓	✓	✓
Microsoft Threat Experts			✓
Partner APIs	✓	✓	✓
Microsoft 365 Lighthouse for viewing security incidents across customers	✓ ³		

Note that not all capabilities may be available in preview

¹Limited. ²Optimized for SMB. ³Additional capabilities planned

Detailed product comparison

Capabilities	MDB	MDE P1	MDE P2
Threat & Vulnerability			
Microsoft secure score	●		●
Vulnerability management (visibility into software and vulnerabilities)	●		●
Vulnerability remediation based on Intune integration	●		●
Attack Surface Reduction			
Advanced vulnerability and zero-day exploit mitigations	●	●	●
Attack Surface Reduction rules	●	●	●
Application Control	●	●	●
Network Firewall	●	●	●
Device Control (e.g.: USB)	●	●	●
Network protection	●	●	●
Device-based conditional access	●	●	●
Web Control / Category-based URL Blocking	●	●	●
Ransomware mitigation	●	●	●
Next Gen Protection			
Advanced cloud protection (deep inspection and detonation) BAFS	●	●	●
Monitoring, analytics and reporting for Next Generation Protection capabilities	●	●	●
Endpoint Detection and Response			
Behavioral-based detection (post-breach)	●		●
Rich investigation tools			●
Custom detections			●
6-month searchable data per endpoint			●
Advanced hunting			●
Evaluation Lab			●
Manual response actions - (Run AV scan, Machine isolation, File stop and quarantine)	●	●	●
Live response	●		●

*Not all capabilities available at time of preview

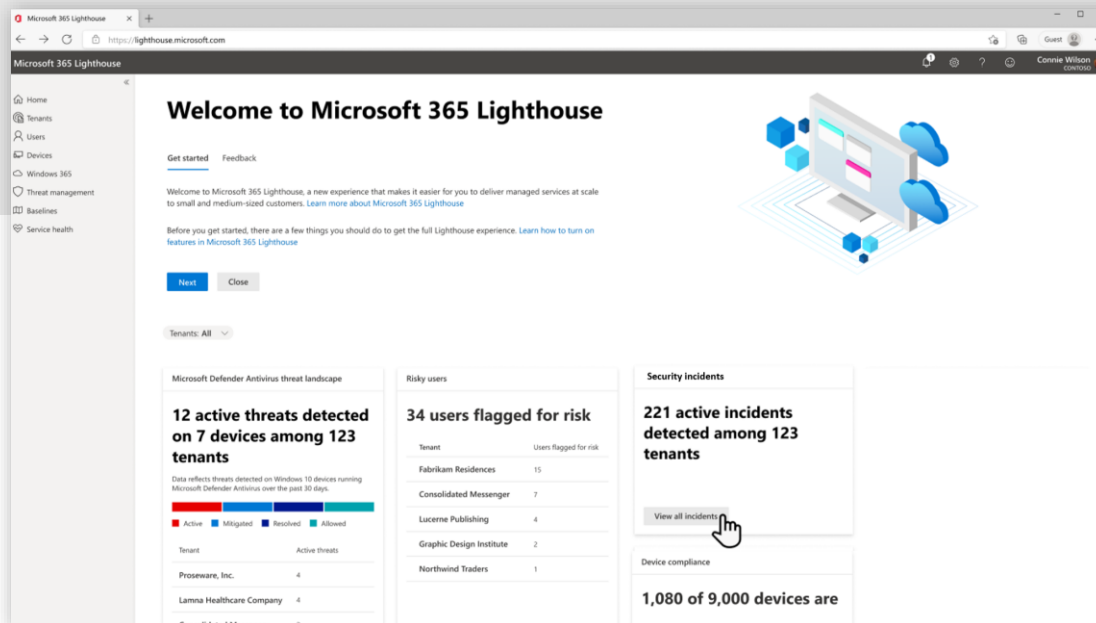
Detailed product comparison

Capabilities	MDB	MDE P1	MDE P2
Automatic Investigation and Remediation			
Default automation levels	•		•
Customized automation levels			•
Centralized Management			
Role-based access control	•	•	•
Simplified client configuration	•		
Reporting	•	•	•
API's			
SIEM Connector		•	•
API's (Response, Data collection)		•	•
Partner applications		•	•
Threat Intelligence			
Threat Analytics	•		•
Custom Threat Intelligence	•	•	•
Sandbox			•
3rd party Threat Intelligence Connector			•
Partner Support			
APIs (For Partners)	•	•	•
RMM Integration	•		
MSP Support (Multi-tenant API, multi tenant authentication)	•	•	•
Microsoft Threat Expert			
Targeted attack notification			•
Collaborate with Experts, on demand			•
Platform support			
Windows Client	•	•	•
MacOS	•	•	•
Mobile (Android, iOS)	•	•	•

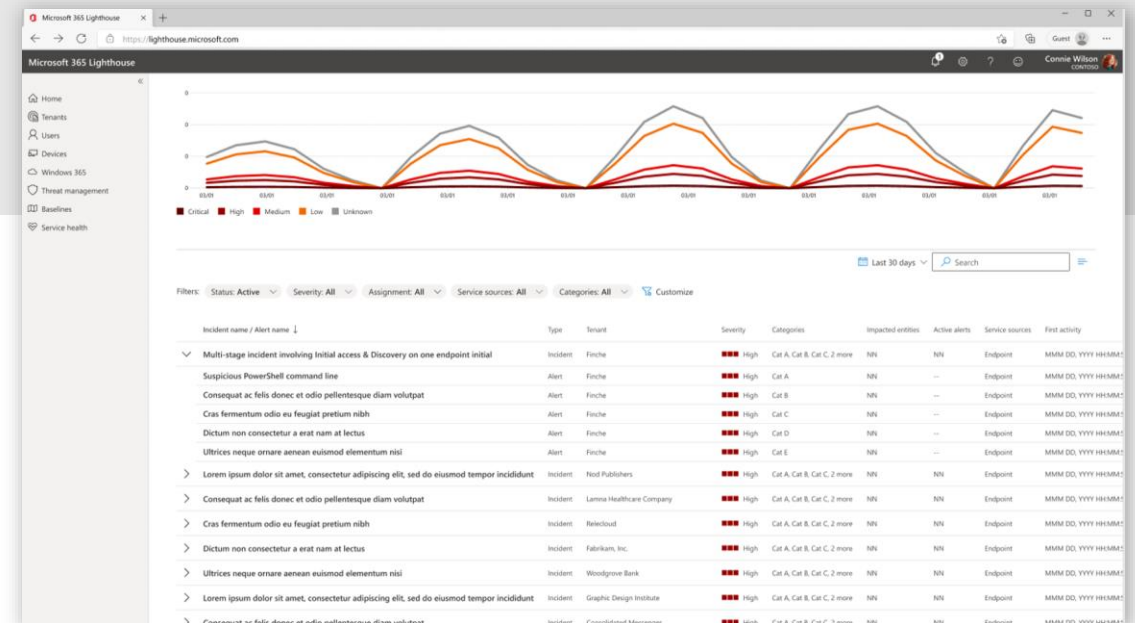
*Not all capabilities available at time of preview

Microsoft 365 Lighthouse with Defender for Business and Microsoft Business Premium

View security incidents and alerts from **Defender for Business** in the dashboard and get the detail from the Incidents queue. Additional security management capabilities are planned on the roadmap.



Security incident summary on the Home dashboard



Incident queue highlighting security incidents and alert details

MDB Recommended Security Policies

Next Generation Protection

- Antivirus
- Antimalware
- Scanning of removable drives
- Daily quick scans
- Security intelligence updates
- Security intelligence checks

Firewall

- Outbound connections from devices are allowed
- Devices connected to org network, all inbound connections are blocked
- Devices connected to public or private network, all inbound connections are blocked

DEMO

Microsoft Defender for Business



Provides layered protection – more than just antivirus



Brings enterprise grade security to customers and partners who manage customer security



Is well awarded and considered best-in-class by third-party testers and influential analysts



Creates a security solution whose experience is tailored to SMBs



Integrates with Microsoft 365 Lighthouse



Exposes partner APIs



Has a compelling partner opportunity story