

# Security for nonprofits

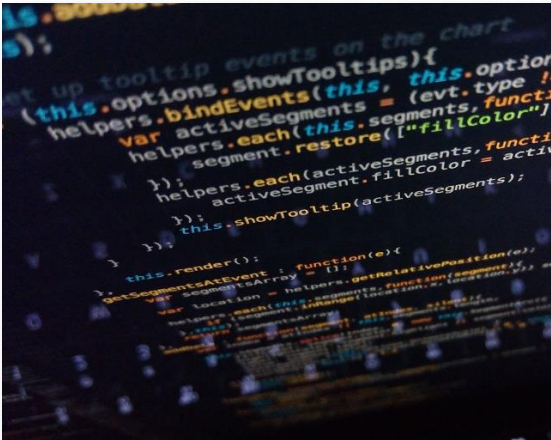
Safeguard your organization with a complete, intelligent solution that helps everyone work together, securely.

Author name  
Date

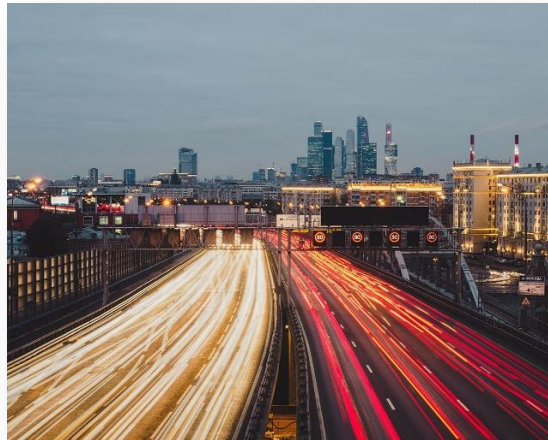


# The era of flux and transformation

Everyone is now in the technology business



Conventional security tools have not kept pace



Security professionals alone can't fill the gap

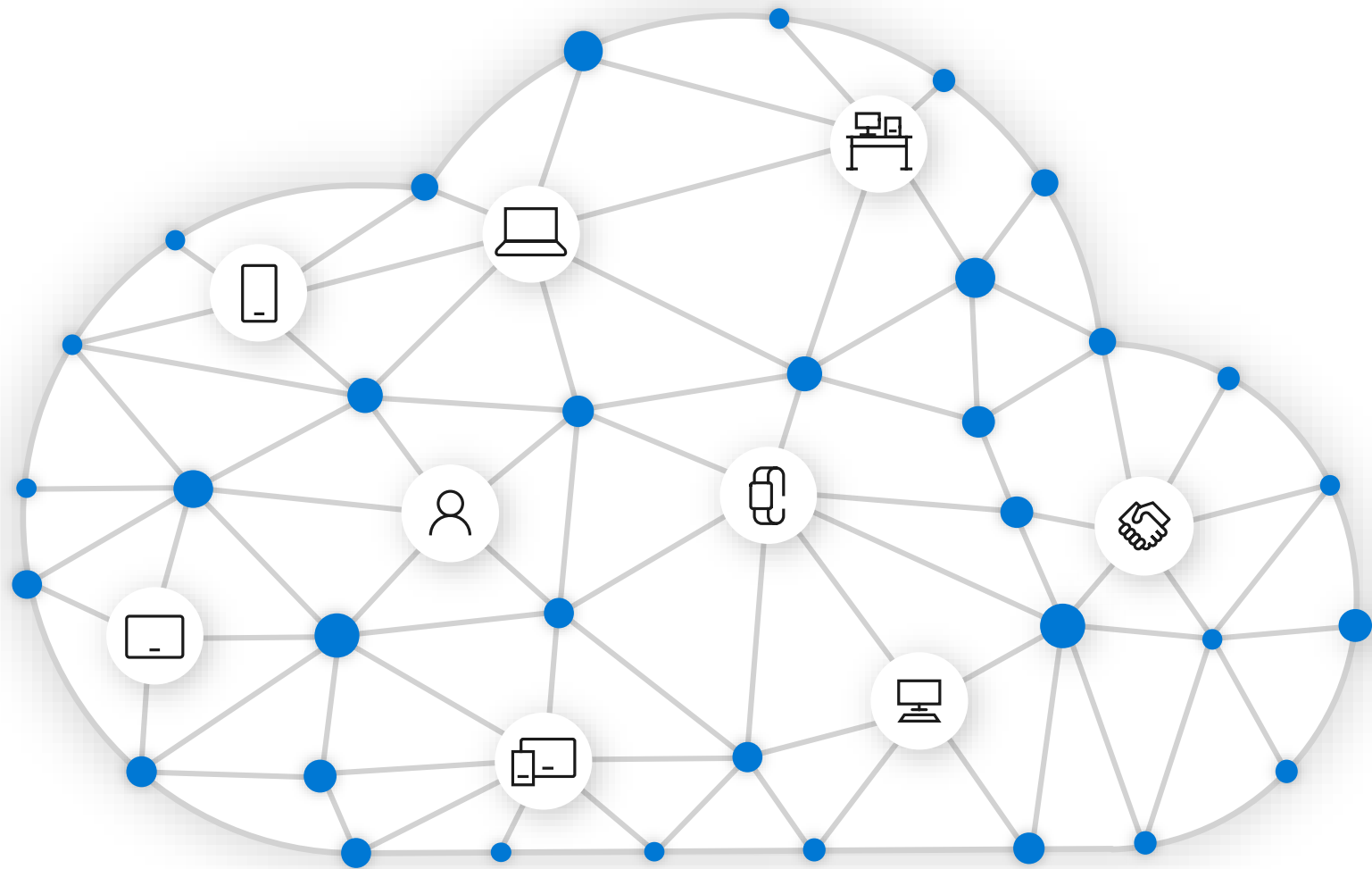


Regulatory requirements and costs are increasing









# Microsoft Security



## Identity and access management

Your universal platform to manage and secure identities.



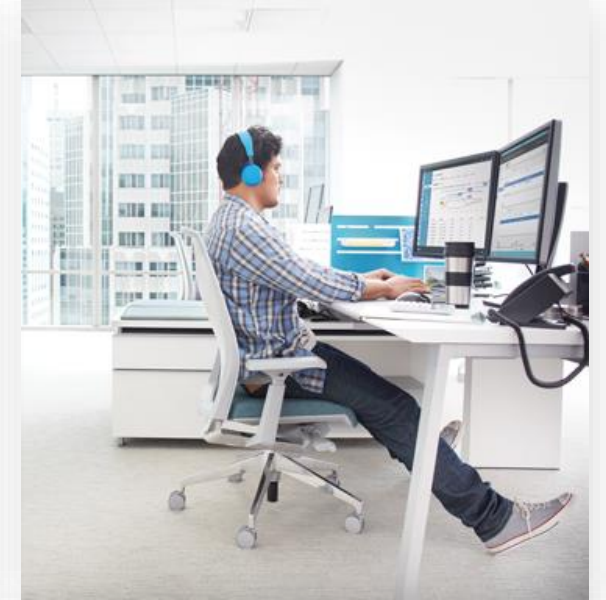
## Threat protection

Stop attacks with integrated and automated security.



## Information protection

Protect your sensitive data—wherever it lives or travels.



## Cloud security

Safeguard your cross-cloud resources.

# Identity and access management

Secure authentication, conditional access, identity protection.

Go beyond passwords and protect against identity compromise, while automatically identifying potential breaches before they cause damage.

- Risk-based Conditional Access and Multi-Factor Authentication
- Advanced security reporting
- Identify threats on-premises
- Identify high-risk usage of cloud apps, user behavior, detect abnormal downloads, prevent threats



Microsoft 365 products and services can help you develop solutions for identity-driven security.



### Azure Active Directory Premium — Manage and control access to resources

In a mobile-first, cloud-first world, IT professionals in nonprofits need to protect their organization's assets while empowering user productivity at any location, at any time.



### Cloud App Security — Provide security for your cloud apps

Bring security capabilities to SaaS cloud applications to gain better visibility and enhanced protection against cloud security issues.



### Windows Hello — Authenticate identities without passwords

Using facial recognition or a fingerprint reader is faster and more secure than standard password authentication, and there's no danger of users reusing or forgetting passwords.



### Credential Guard — Protect derived domain credentials

Systems are vulnerable to "pass the hash" attacks that exploit user credentials after users have logged in. Isolate credentials so that only privileged system software can access them.



### Conditional Access — Control access to apps based on specific conditions

Enterprises need control to allow the right people to access resources under certain conditions while blocking access under other circumstances.





# Information protection

**Discover and classify sensitive information, apply protection based on policy, monitor and remediate, accelerate compliance.**

Protect information in documents and emails with encryption that travels as they move inside and outside your organization.

- Shadow IT Detection: Discovering Apps and Risk Scoring
- Intelligent Classification and Tagging of content
- Document encryption, tracking, revocation
- Monitoring shared files and responding to potential leaks
- Data segregation at a device/app level



Microsoft 365 products and services can help you develop solutions for a security practice focused on protecting content at creation, in transit, and during consumption.



### Windows Information Protection — Integrated protection against accidental data leaks

Maintain control of the organization's data without degrading the user experience.



### Cloud App Security — Provide security for your cloud apps

Bring security capabilities to SaaS cloud applications to gain better visibility and enhanced protection against cloud security issues.



### Azure Information Protection — Better secure sensitive information, anytime, anywhere

Nonprofit organizations need to be able to control the access to information, no matter where it's stored or who it's shared with.



### Microsoft Intune — Meet your data protection needs while delivering the best user experience

Flexible mobile device and app management controls let staff and volunteers work with the devices and apps they choose while protecting the organization's information.



### Data Loss Prevention — Create policies to identify, monitor, and protect sensitive data

To comply with privacy and security standards and best practices, organizations need to protect and prevent the disclosure of sensitive information such as financial data, credit card numbers, social security numbers, and health records.



### Advanced compliance — Meet compliance obligations, establish policies and simplify access

As digital content multiplies, organizations need tools to help meet compliance obligations, manage complex corporate data, and respond to security incidents.

# Threat protection

**Gain visibility into existing security position , create policies and enable controls, leverage in-built security tools.**

Protect information in documents and emails with encryption that travels as they move inside and outside your organization.

- Shadow IT Detection: Discovering Apps and Risk Scoring
- Intelligent Classification and Tagging of content
- Document encryption, tracking, revocation
- Monitoring shared files and responding to potential leaks
- Data segregation at a device/app level



Microsoft 365 products and services can help you develop solutions for a security practice focused on threat protection.



**Office 365 Advanced Threat Protection — Provide protection against threats**

As hackers launch increasingly sophisticated attacks, organizations seek tools that provide stronger protection against specific types of advanced threats.



**Azure Advanced Threat Protection — Better secure sensitive information, anytime, anywhere**

Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.



**Cloud App Security — Provide security for your cloud apps**

Bring security capabilities to SaaS cloud applications to gain better visibility and enhanced protection against cloud security issues.



**Windows Defender Advanced Threat Protection — protection, detection, investigation, and response**

Protect endpoints from cyber threats, detect advanced attacks and data breaches, automate security incidents, and improve security posture.



**Advanced eDiscovery — Better understand your Office 365 data and reduce your eDiscovery costs**

Analyze unstructured data within Office 365, perform more efficient document review, and make decisions to reduce data for eDiscovery.





# Security management

**Detect and remediate breaches, correlate across attack vectors, protect the digital estate.**

Use security management tools to gain end-to-end visibility of your organization and manage policy centrally.

- Shadow IT Detection: Discovering Apps and Risk Scoring
- Conditional Access
- Device and App access level controls: PIN
- Device and App encryption at rest
- Save-As, Copy, Paste restrictions
- Device and App level data wipe

Microsoft 365 products and services can help you locate and classify information across devices and apps in the cloud and on premises.



### Microsoft security and compliance center — simplify IT with a unified experience

Provides security and compliance specialists with integrated management capabilities across Office 365, Windows, and EMS, as well as Microsoft 365 Device Management, and device management capabilities across Intune, Office, and Windows.



### Windows Defender security center

Flexible mobile device and app management controls let employees and volunteers work with the devices and apps they choose while protecting organization information.



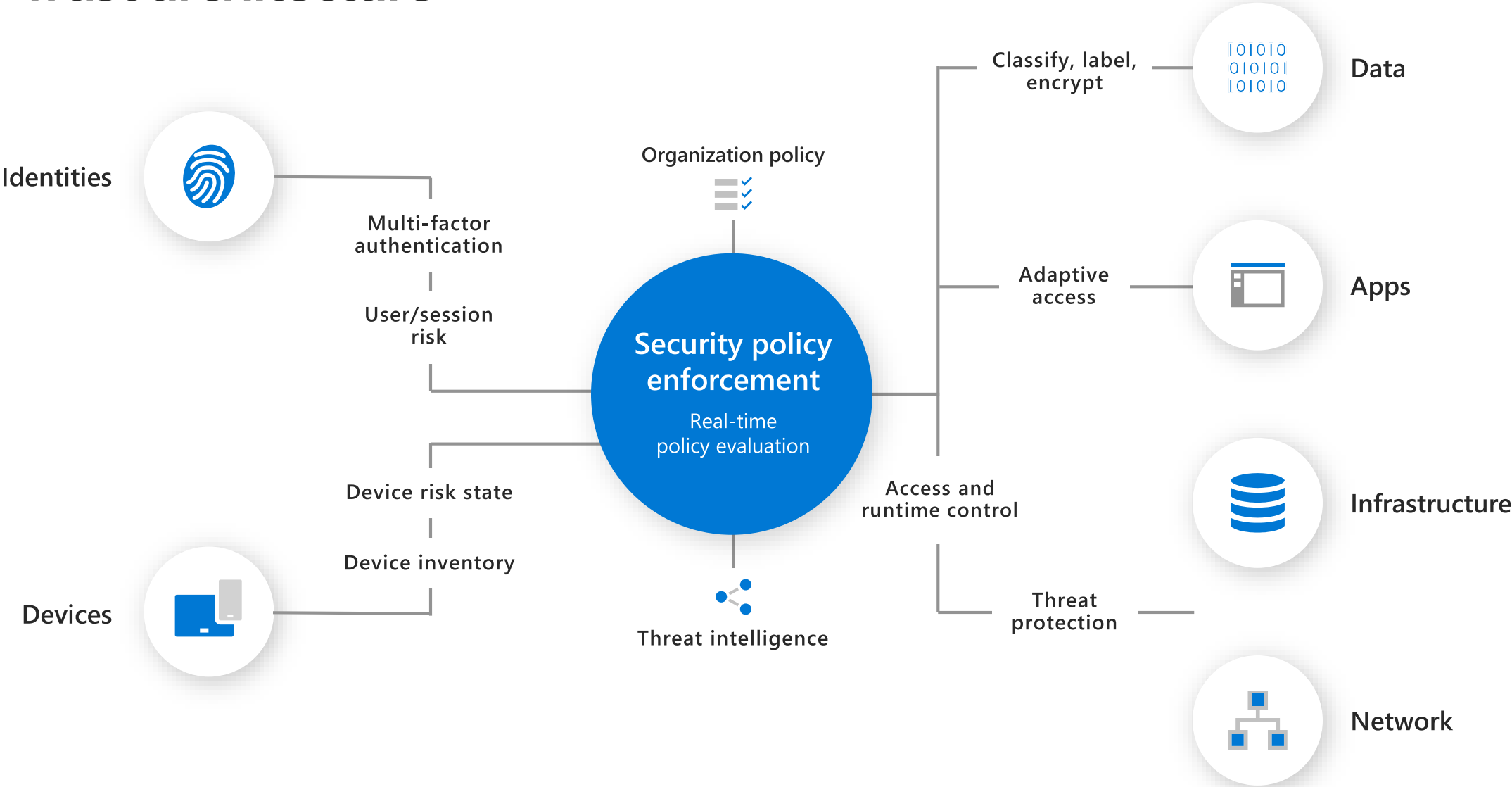
A man with a beard, wearing a dark suit jacket over a light blue patterned shirt, stands in a modern office hallway with large glass windows. He is looking off-camera to the left while holding a smartphone in his hands. In the background, other office workers are visible, including a woman in a blue top and black blazer carrying a laptop.

# Principles of Zero Trust

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



# Zero Trust architecture



# Strengthen your security posture

Visibility and guidance to help you take full advantage of your security platform

Assess your posture

Take advantage of prioritized recommendations

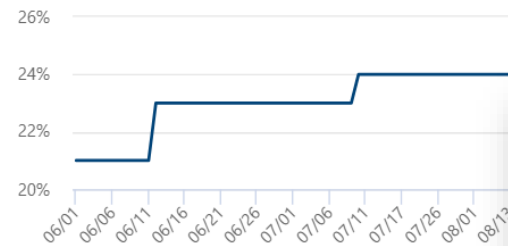
Determine risks and impact

Your secure score

Include

Secure Score: 24%

27/111 points



Breakdown points by: Category

Identity

Data

Device

Apps

Infrastructure

points Opportunity

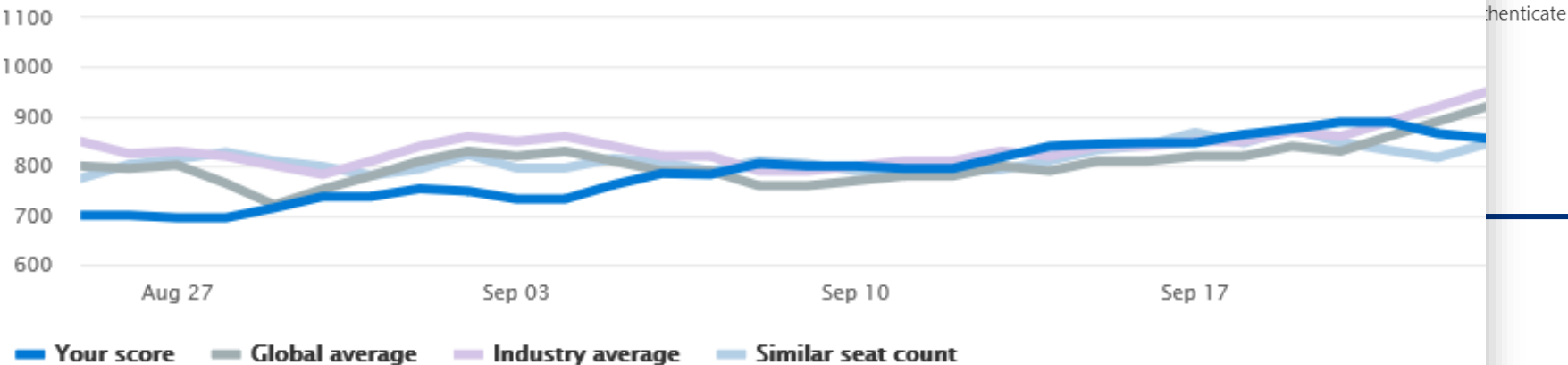
Track your score

Improvement actions > **Require MFA for Azure AD privileged roles**

Requiring multi-factor authentication (MFA) for all Azure Active Directory accounts with privileged roles makes it harder for attackers to access accounts. Privileged roles have higher permissions than typical users, and include all admin roles such as global admin, SharePoint admin, or Exchange admin. If any of those accounts are compromised, critical devices and data will be open to attacks.

Score over time

Total score



# Next Steps

- Download  
<Partner Managed Services deliverable>
- Take a [guided tour](#) of Microsoft 365 Business
- Find more [Microsoft 365 Business](#) resources





# Our expertise + Microsoft 365

## We're experts at...

Supporting point #1

Supporting point #2

Supporting point #3

## We can help you...

Supporting point #1

Supporting point #2

Supporting point #3

## We can manage your...

Supporting point #1

Supporting point #2

Supporting point #3



Turn to <<Microsoft Partner>> for the expertise you need to help you safeguard your business data. We know IT security and we know Microsoft 365. We can help you control and manage access to sensitive information, protect company data across devices, and guard against unsafe attachments, suspicious links, and other cyber threats.

You can expect guidance, recommendations, and best practices to keep your business data safe from both internal and external threats with a simple, cost-effective solution.

Our [Offer name for Microsoft 365 Secure Deployment] will:

- Assess your current security state to help us understand how secure your organization really is
- Remediate high priority security concerns and identify security objectives based on strengths, distinctions and uniqueness of your organization
- Deploy Microsoft 365
- Configure advanced security features based on
- Identify and protect sensitive data
- Provide ongoing services based on an actionable security roadmap

Partner  
Logo

<<Microsoft Partner>>

<<Microsoft Partner Contact Information>>





**Thank you**

