Microsoft 365: A secure solution that brings together Office 365 and EMS
Microsoft 365:
A secure solution that brings together Office 365 and EMS

Introduction
Accelerate your digital transformation

Section 1
Secure access

Section 2
Mobile management

Section 3
Advanced security

Conclusion
Build a strategy that works for your business
Introduction:

Accelerate your digital transformation
Digital transformation is creating new opportunities for nonprofits to engage with volunteers, donors, and beneficiaries. Organizations are no longer limited by geography or technology boundaries, so you can gather the best minds and resources from anywhere to scale your impact and enhance your ability to do more good for more people.

Many nonprofits are using technology to embrace this transformation so they can extend limited resources and empower employees and volunteers to work together more efficiently and securely. By enhancing collaboration and teamwork within a highly secure framework, nonprofits are benefiting from increased inspiration and dedication among the staff and reducing the risk of data breaches.

To make it easier for your organization to create such an environment, Microsoft has combined Office 365, Windows 10, and Enterprise Mobility + Security into Microsoft 365. This comprehensive, intelligent solution provides the foundation to enable your users to collaborate more securely, while allowing your IT staff to control the integrity of your data and access to it.

With the familiar tools in Microsoft 365, your staff, volunteers, and board members can work together more productively, creatively, and securely, from anywhere, to become more effective in solving the world’s greatest challenges.

It is just one example of Microsoft’s commitment to helping nonprofits address the challenges of digital transformation as you struggle with a lack of technical capacity, scarcity of resources, lack of partners, and few technology solutions tailored to meet your needs. Our goal is to help you accelerate your mission by making the latest technologies more accessible, affordable, and relevant to your organization.

$1 billion in cloud resources donated to nonprofits

To help expedite your digital transition, Microsoft launched the Tech for Social Impact initiative in late 2017. Through this initiative Microsoft Philanthropies has pledged $1 billion in donations and discounts on a variety of cloud computing resources to reach over 300,000 nonprofits by 2020.

In addition, we have built a growing ecosystem of partners who recognize the challenges that nonprofits face. These partners focus specifically on providing relevant technology and services, including Microsoft 365 solutions, to help nonprofits of all sizes to scale and drive greater impact through the cloud.

How to use this e-book

This e-book provides both an overview of Microsoft 365 and a more detailed analysis of how its components work together to provide an intelligent productivity, security, and mobility management platform. You can discover how to use built-in identity management tools to provide highly secure, seamless access to Office 365 and other applications from any device and any location.

Learn how to manage data inside mobile apps to provide a first line of defense against potential threats. And explore how to use advanced EMS analytics to detect suspicious activity and pinpoint threats across your on-premises and cloud environment to support a more seamless and secure digital transformation for your organization.
Section 1: Highly secure access
Part of the promise of digital transformation is an infrastructure that enables uncompromised productivity for your entire workforce. To that end, Office 365, provides secured, seamless access to Office Mobile apps from any device and any location. But, they won't be the only applications in your cloud app portfolio as you develop your cloud strategy and move more line-of-business apps to the cloud. As you continue to diversify your digital ecosystem, you'll need a comprehensive solution to manage and secure access for everything. Establishing a single, unified identity for each user is critical. With EMS, you can connect your current on-premises identity investments to your SaaS and on-premises workloads and establish one identity for each of your users. With one identity, you can anchor security and productivity for your workforce across your entire application portfolio.
Employees are more productive when they have just one username and password to remember. With Office 365, your users have the convenience of single sign-on to Office 365 experiences, facilitating a consistent and fluid user experience from any device. EMS extends access for employees to thousands of cloud and on-premises web apps—all through a single, secured identity. To further support productivity, EMS provides self-service capabilities to end users, such as resetting forgotten passwords or requesting access to an application, which can significantly reduce demands on your IT helpdesk.

Once you have established a single unified identity per user, managing the different privileges for your users is an important way to safeguard against potential vulnerabilities. With EMS, you gain oversight and control over all levels of user privilege. You can discover permanent administrators within your organization and use those permissions as-is, or you can enforce on-demand, just-in-time administrative access so that increased privileges are only available to certain users when needed. The EMS Security Wizard simplifies converting permanent administrators to eligible administrators to make on-demand privileges easier to manage and enforce. Audit reports and access reviews make it possible to determine who still needs administrative rights and EMS will alert you to idle roles so that you can reduce or eliminate unused privileges.
Office 365 includes conditional access based on device state, so that you can block users from accessing Office 365 resources from vulnerable or compromised devices. EMS expands your conditional access capabilities to provide more comprehensive control across multiple levels: identity, device, application, and file. With EMS, you can define conditions for access that include:

Add risk-based conditional access informed by an expanded set of conditions.
Assign multiple conditions (based on location, application, device, and risk levels) to all users or to multiple security groups. You can also specifically exclude groups from being affected by conditional access policies.

Define a set of trusted IP addresses to allow access only from them. If a user attempts to access corporate assets from an unknown network, set specific controls that either challenge the user with multi-factor authentication (MFA) or block access entirely. You can also apply policies to user groups.

Set policy that defines the conditions of access to an app based on the sensitivity you specify. For example, you can block access to an app from unknown locations, or require MFA. You can require MFA every time an app is accessed or base its requirement on the location from which access is being attempted. These policies can be applied to any cloud (SaaS) or on-premises app protected by Azure Active Directory, including any related rich, mobile, or browser-based clients.

Assess risk in real time. Machine learning in the Microsoft Intelligent Security Graph leverages billions of signals daily, detects suspicious behavior, and applies risk-based conditional access that protects your applications and critical company data in real time. As conditions change, controls are triggered that allow, block, or challenge users with MFA, device enrollment, or password updates.
Section 2: Mobile management
Once you’ve enabled secure and managed access, the next step is to protect your data. Applications, such as your Office Mobile apps, are the most likely point of access to your corporate resources, acting as a sort of “front door” to your environment and its data. This makes application management a critical part of your security strategy—especially given the complexity of different user devices, apps, preferences, and behaviors. With EMS, you can manage data inside Office Mobile apps as well as your line-of-business and third-party apps. Flexible solutions for mobile management give you the control to decide exactly what happens to your data once it’s been accessed.

“With EMS, you can manage data inside Office Mobile apps”
Protect apps with and without device enrollment

In addition to a complex workforce, your circle of collaboration extends beyond your own organization to include other business partners and contractors. The nuances of your mobile ecosystem may require flexibility when it comes to device and app management, and EMS gives you choices.

You can have full management of corporate-owned or user-owned devices through enrollment in mobile device management (MDM) with EMS. Once a device is enrolled, you can define and enforce compliance with security policies, automatically deliver apps, set cut/copy/paste/save-as restrictions, jailbreak detection, PIN requirements, as well as remote-wipe protected data from any of your EMS-managed apps or devices.

In some situations, it’s necessary to provide users with access to corporate resources from devices that aren’t feasible or desirable to enroll in MDM. Managing application policies without MDM enrollment gives you—and your users—the flexibility to deploy Office Mobile apps on iOS, Android, and Windows devices without requiring enrollment through EMS. You may also be using a non-Microsoft MDM solution. In that case, you may choose to use your current MDM solution or forego MDM altogether and still protect access to Office 365 and your company data.

EMS application protection policies protect your data at the app level without requiring device enrollment. The security capabilities include app encryption at rest, app access control requiring a PIN or credentials, secured web browsing, and secured viewing of PDFs, images, and videos. Even without device enrollment, you can still define cut/copy/paste/save-as restrictions and apply app-level selective wipe when needed.

You’ll have visibility and control over your line-of-business apps and an ever-growing collection of third-party apps that your users access from a variety of devices. EMS adds granular application management so that you can deliver a perfect balance between productivity and protection to pave the way for more secure collaboration.
Extend Office 365 rights management for collaboration

Your users can apply persistent rights management protections to Office files through Office 365 so that data is protected when shared. EMS extends persistent data protection to any file type so that your users can collaborate safely within and outside of your organization. To capture the greatest advantages of file-level protection, EMS includes automatic data classification based on sensitivity, preventing data vulnerabilities from inconsistencies in classification. You can define policies that automatically classify and label data at the time of creation or modification, based on source, context, and content itself.

Manage collaboration with file tracking and revocation

For even more visibility and control over internal and external collaboration, you can monitor shared files and respond to potential leaks through EMS. IT and users can track shared files to monitor activity by authorized collaborators, revoke access if necessary, and revise classification. You can use powerful logging and reporting on shared files to monitor, analyze, and reason over data. With persistent information protection through EMS, you can empower secured collaboration for any file, on any device, anywhere.
Section 3: Advanced security
Office 365 delivers anywhere, anytime, uncompromised productivity. Adding secured access and mobile management through EMS builds the framework to help you protect your organization both on-premises and in the cloud. EMS uses managed and protected identity as the core of advanced security that works to detect internal threats with cutting-edge behavioral analytics and anomaly detection technologies. Using EMS, you can uncover suspicious activity and pinpoint threats across your on-premises and cloud ecosystem.
Advanced Threat Analytics

Even with the advantages of the cloud, on-premises protection remains critical. Using machine learning and event logs, EMS identifies advanced persistent threats on-premises and detects known malicious attacks almost as instantly as they occur. With clear and relevant information provided through a concise attack timeline, you can quickly focus on critical response actions.
Extend Office 365 Advanced Security Management with Cloud App Security

Office 365 gives you a great foundation for securing your Office Mobile apps against cloud-based threats. To build comprehensive cloud application security that safeguards all your apps, EMS includes powerful visibility, threat detection, attack prevention, and deep discovery of shadow IT. You can monitor user behavior and data flow characteristics for detailed insight on how your users are working with cloud apps. With real-time monitoring and control over your cloud applications you can limit and control the activities performed within the user sessions in SaaS apps based on conditions such as user identity, location, device and detected sign-in risk level. For example, you can allow access to SaaS apps from an unfamiliar location or unmanaged device while blocking the download of the sensitive documents.

EMS cloud application security capabilities also interface with your existing response mechanisms so that you can continue building on your current investments. Monitor, assess, and make decisions based on real-time risk estimates.

The combined capabilities of Office 365 and EMS can help you take a more informed, agile, and comprehensive security posture with respect to the complex and ever-changing identity security landscape. Even the most sophisticated attacks leave behind traces that form detectable patterns. Every month Microsoft processes a tremendous volume of these signals.

In addition, we update more than 1 billion devices, process more than 450 billion authentications, and scan 400 billion emails for malware and phishing.

Microsoft threat intelligence systems observe nearly every kind of attack and push the collected data directly into our Microsoft Intelligent Security Graph. The Intelligent Security Graph pulls together telemetry and signals from the hundreds of cloud services that Microsoft operates, extensive and ongoing research that identifies emerging attack vectors and malware, as well as data from partnerships with industry leaders and law enforcement organizations. We apply machine learning and data analytics to identify anomalous and suspicious activities that characterize advanced and persistent attacks. The graph makes it possible for Microsoft to deliver recommendations and automated actions to help prevent attacks and to counter them. We calculate and assign a risk level (low, medium, or high), based on the gathered data, to every sign-in activity and user account. We also assign a risk score to possible configuration vulnerabilities, such as administrators with weak authentication options, or the absence of an initial MFA configuration for end users.

Through Microsoft 365, the Microsoft Intelligent Security Graph is part of your advanced security strategy.
Conclusion: Build a strategy that works for your business
As you pursue your digital transformation through Microsoft 365, deploying Office 365 may be one of the first steps your organization takes. Build on top of your security and management capabilities with EMS to progress on this journey with enhanced confidence. As you roll out Office 365 across your organization, you can give your users more freedom and autonomy in how they work and collaborate, while building an intelligent management and security strategy. Deploy EMS for secured access, mobile management, and advanced security to help you manage and secure your digital transformation.
Nonprofit Sales Desk

To learn more about nonprofit offers and to get help finding the right products for your organization, contact nonprofit sales via email or phone (Monday–Friday, 7 AM–7 PM Central Time).

Email us

Call us: (800) 258-6149

© 2019 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.