



“Digital transformation  
is about the mobility of  
the human experience.”

-Satya Nadella



Secure access



Mobile management



Advanced security

## Accelerate your digital transformation

Office 365 is a powerful platform and a critical step in your organization's digital transformation. You can derive great business value from uncompromised productivity with cloud-powered tools that give your users the freedom to work from anywhere, using any device. The fundamental **management and security capabilities** built into Office 365 are designed to give you control without disrupting the end user experience. As you deploy Office 365, you must

extend these robust management and security capabilities to your broader digital ecosystem for a comprehensive and holistic security strategy.

With **Microsoft Enterprise Mobility + Security (EMS)**, you can use your Office 365 deployment to accelerate your organization's specific priorities at every stage of your digital transformation. EMS provides additional security for Office 365 and extends your capabilities to **securely deliver your**

**broader portfolio of cloud-based or cloud-aware apps** to any device and safeguard your critical corporate assets everywhere. Additionally, EMS **protects your overall app portfolio** and end-user computing infrastructure against threats both **on-premises and in the cloud**.

EMS provides strategic capabilities to help you realize digital transformation: secure access, mobile management, and advanced security.

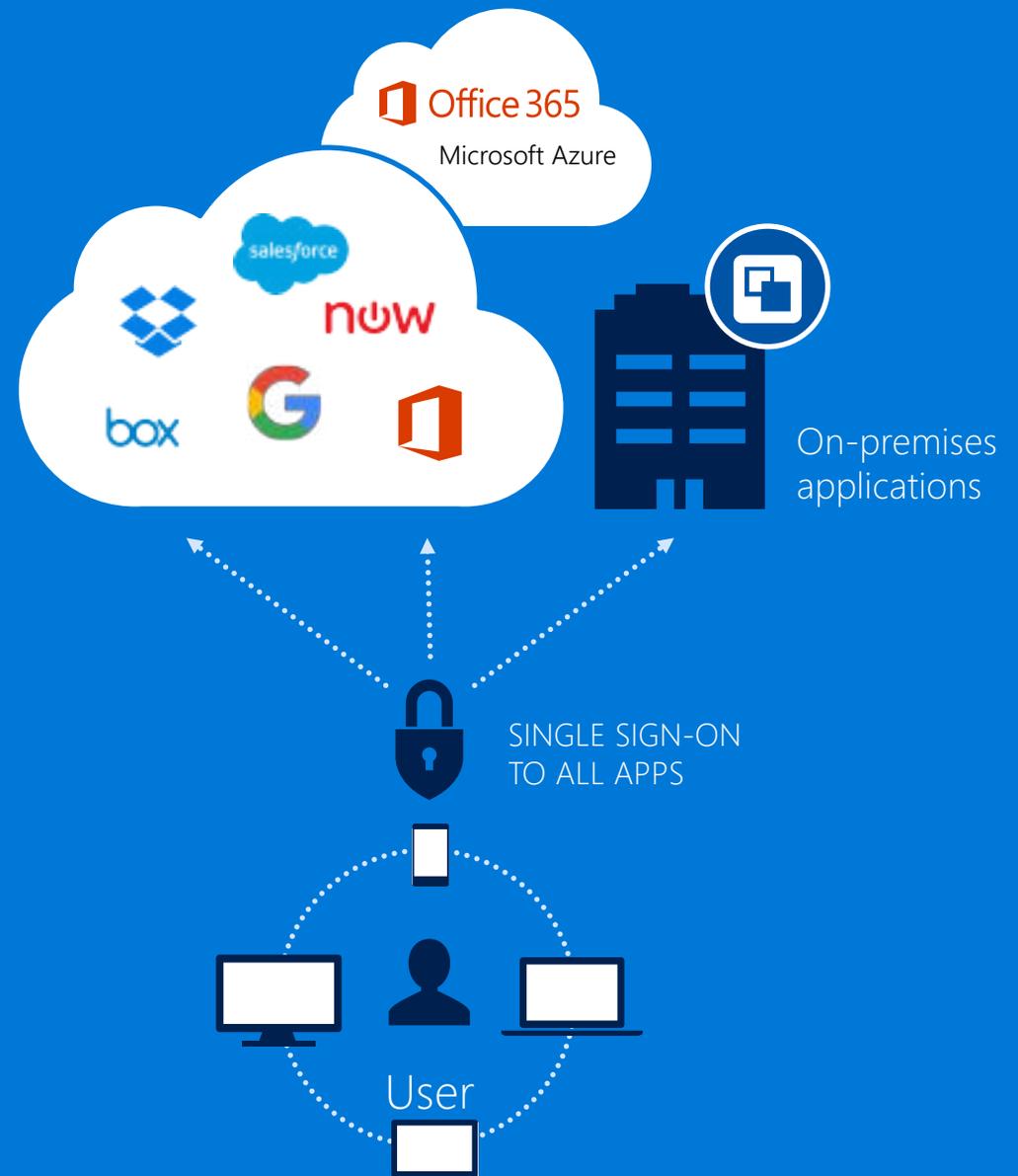
# Secure access

Part of the promise of digital transformation is an infrastructure that enables uncompromised productivity for your entire workforce. To that end, Office 365 provides secure, seamless access to its apps from any device and any location. But, Office Mobile apps 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. **A single, unified identity for each user is critical.** Use EMS to **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 entire application portfolio.



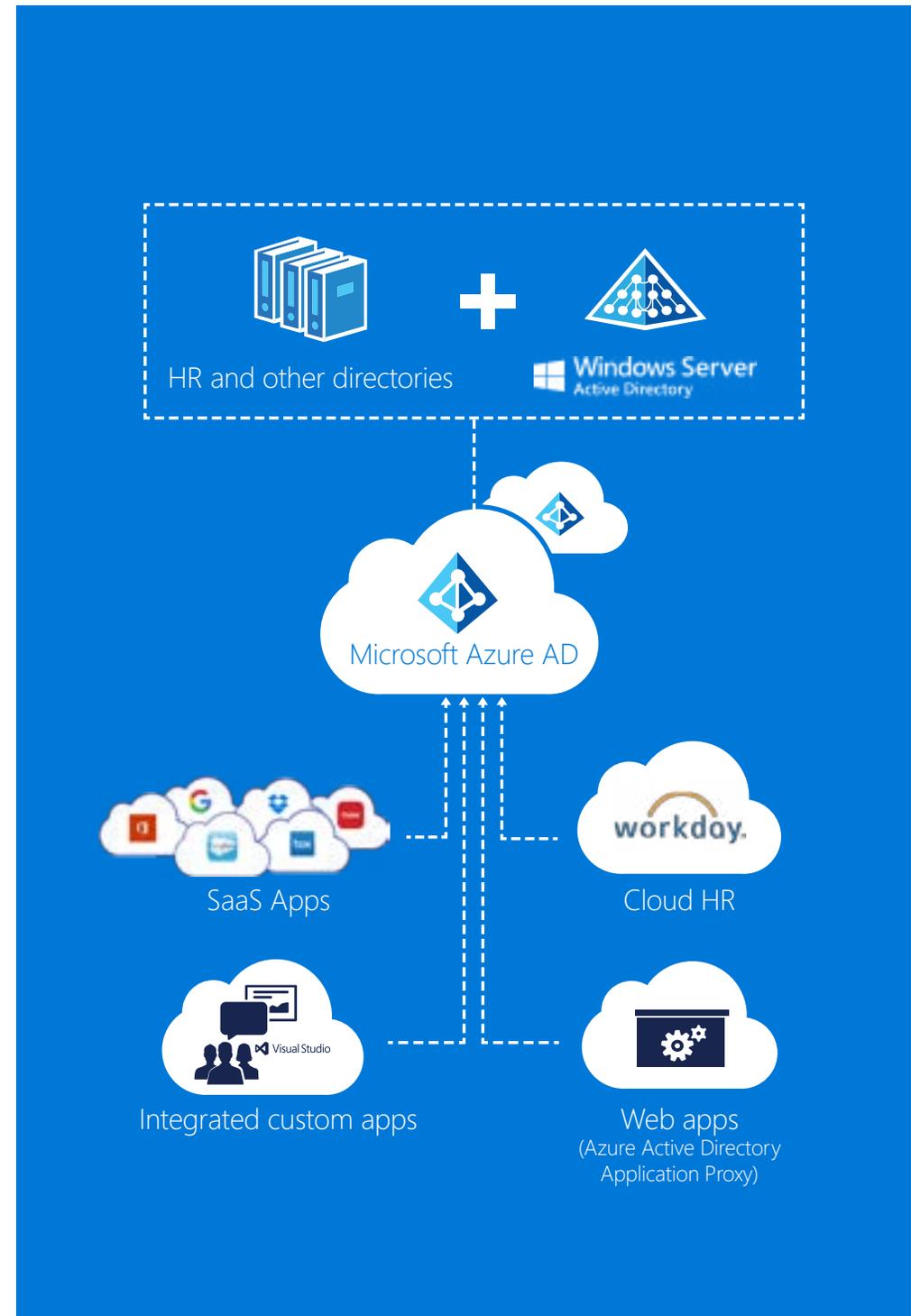
## Start with single sign-on to Office 365 and all of your apps

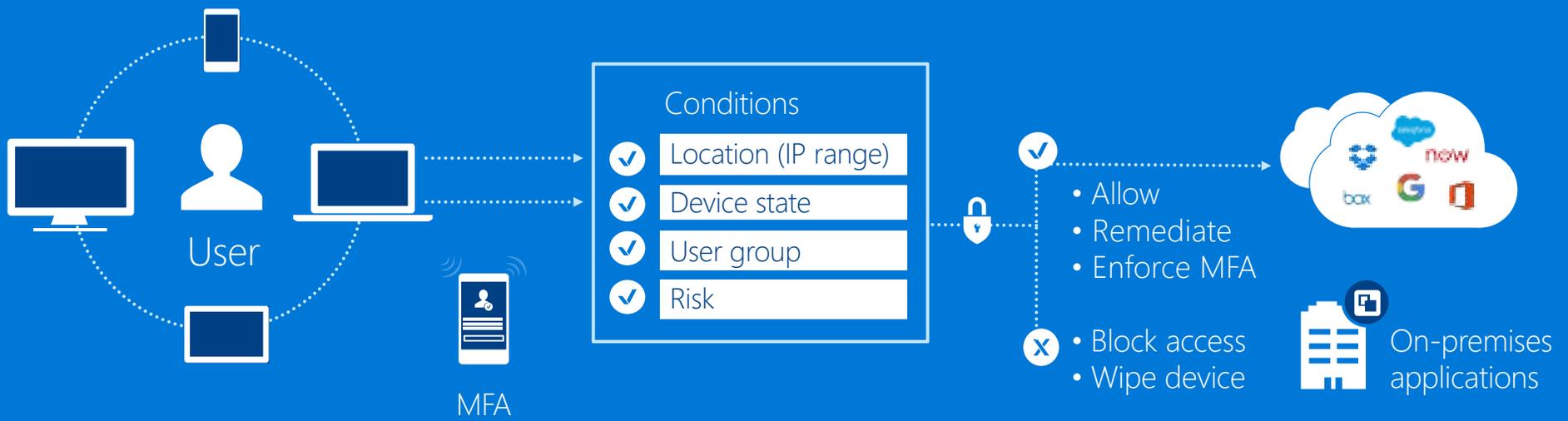
Employees are more productive when they have just one username and password to remember. With Office 365, your users have the convenience of single sign-on to Office 365 experiences, facilitating a consistent and fluid user experience from any device. **EMS extends this capability to thousands of cloud and on-premises web apps**—all through a single, secure 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.



## Ensure you protect and manage privileged identities

Once you have established one, 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 as-is, or 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.





## Add risk-based conditional access informed by an expanded set of conditions

Office 365 includes conditional access based on device state, so that you can block users from accessing Office 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:

### User

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.

### Location

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.

### Application

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, which you can require every time an app is accessed or base requirement on the location from which it's being

accessed. These policies can be applied to any cloud (SaaS) or on-premises app protected by Azure Active Directory, including their rich, mobile, or browser-based clients.

### Risk

**Assess risk in real time.** Machine learning in the Microsoft Intelligent Security Graph leverages billions of signals daily, can **detect 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 multi-factor authentication, device enrollment, or password change.

# 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.



## Protect apps with and without device enrollment

In addition to the complexity of your workforce, your circle of collaboration is extending 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, IT can define and enforce compliance with security policies, automatically deliver apps, set cut/copy/paste/save-as restrictions, jailbreak detection, PIN requirements, and 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.

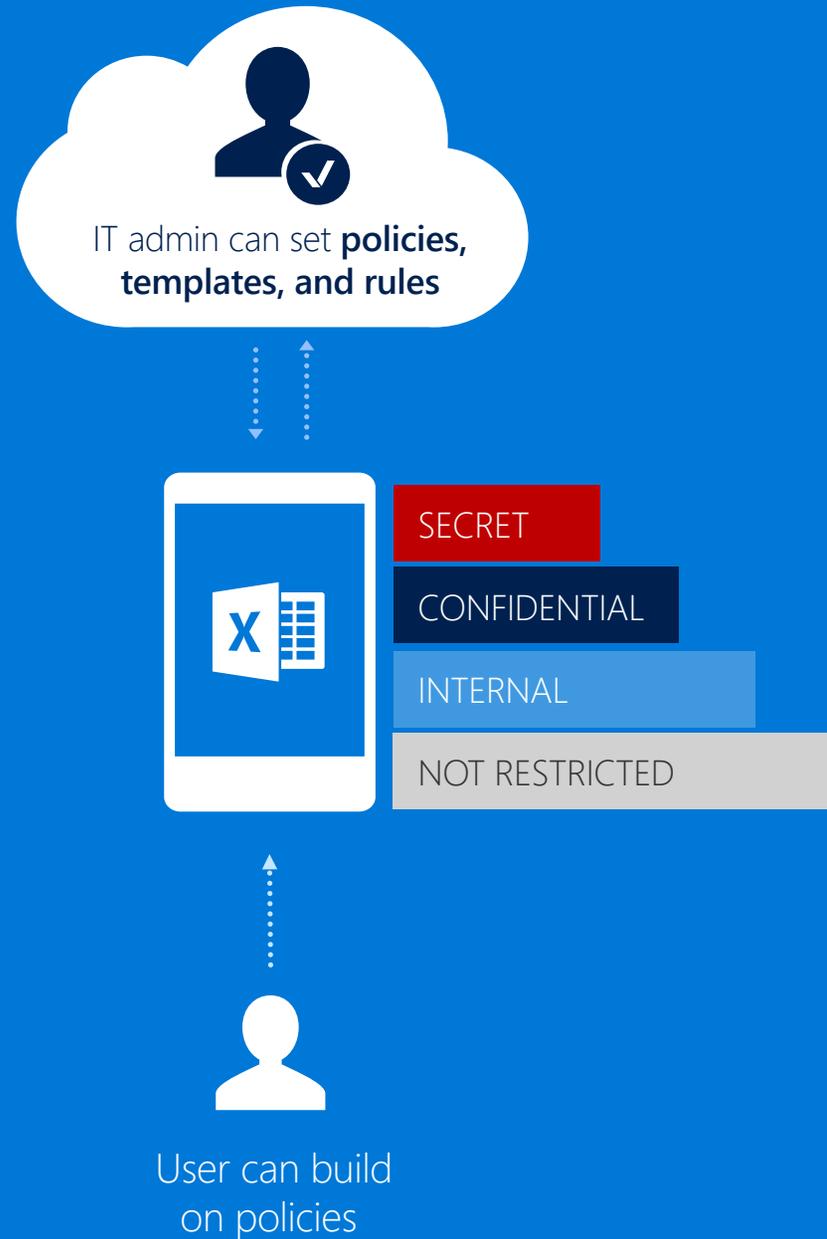
EMS application protection policies protect your data at the app level without requiring device enrollment. The security capabilities include app encryption at rest, app access control requiring a PIN or credentials, secure web browsing, and secure viewing of PDFs, images, and videos. Even without device 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 IT can deliver a perfect balance between productivity and protection to pave the way for 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. Your IT team 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 secure collaboration for any file, on any device, anywhere.



Track file and revoke access if needed

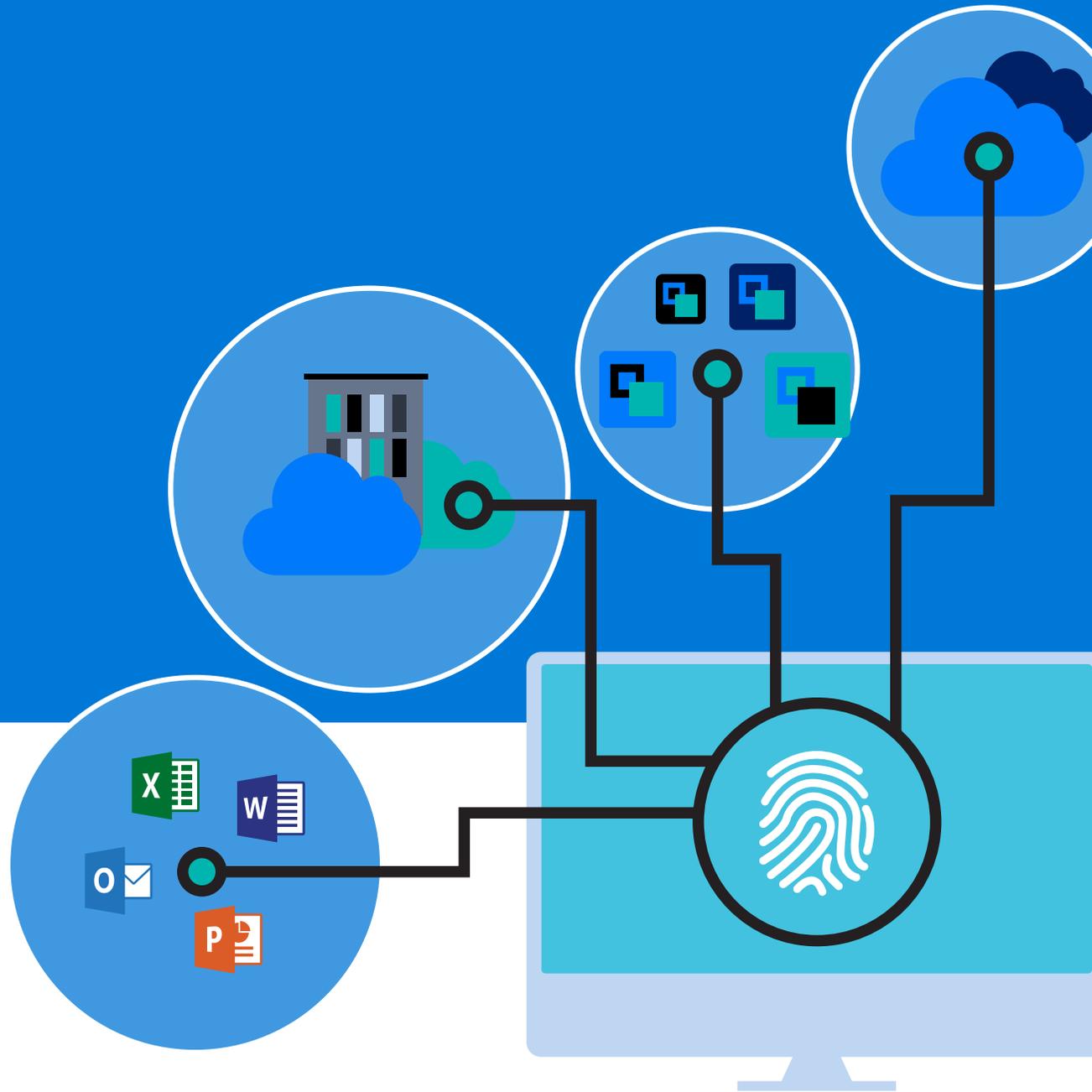
Monitor who accessed the data, when, and where



-  Bob accessed from South America
-  Jane accessed from India
-  Joe blocked in North America
-  Jane blocked in Africa

# Advanced security

Office 365 delivers anywhere, anytime, uncompromised productivity. Adding secure 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.



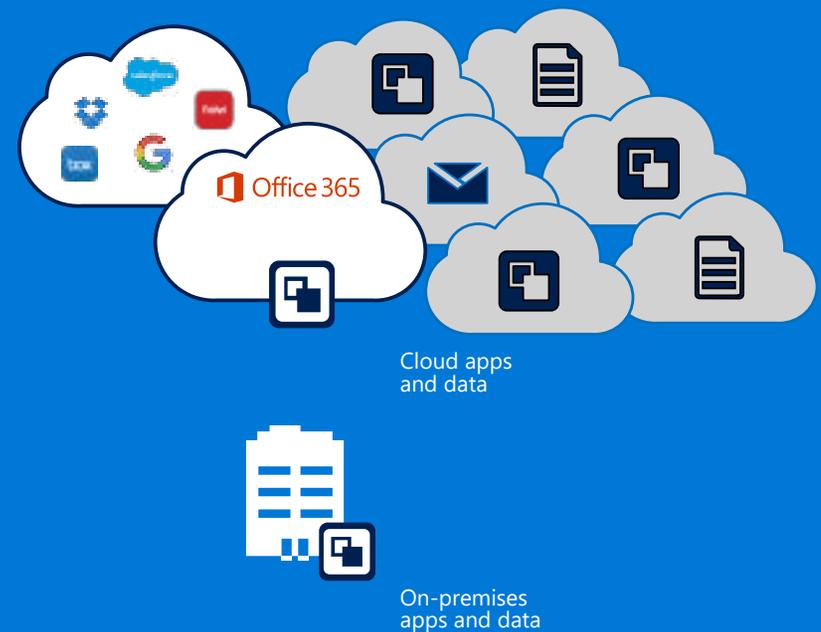
Powerful visibility,  
threat detection, attack  
prevention, and deep  
discovery of shadow IT

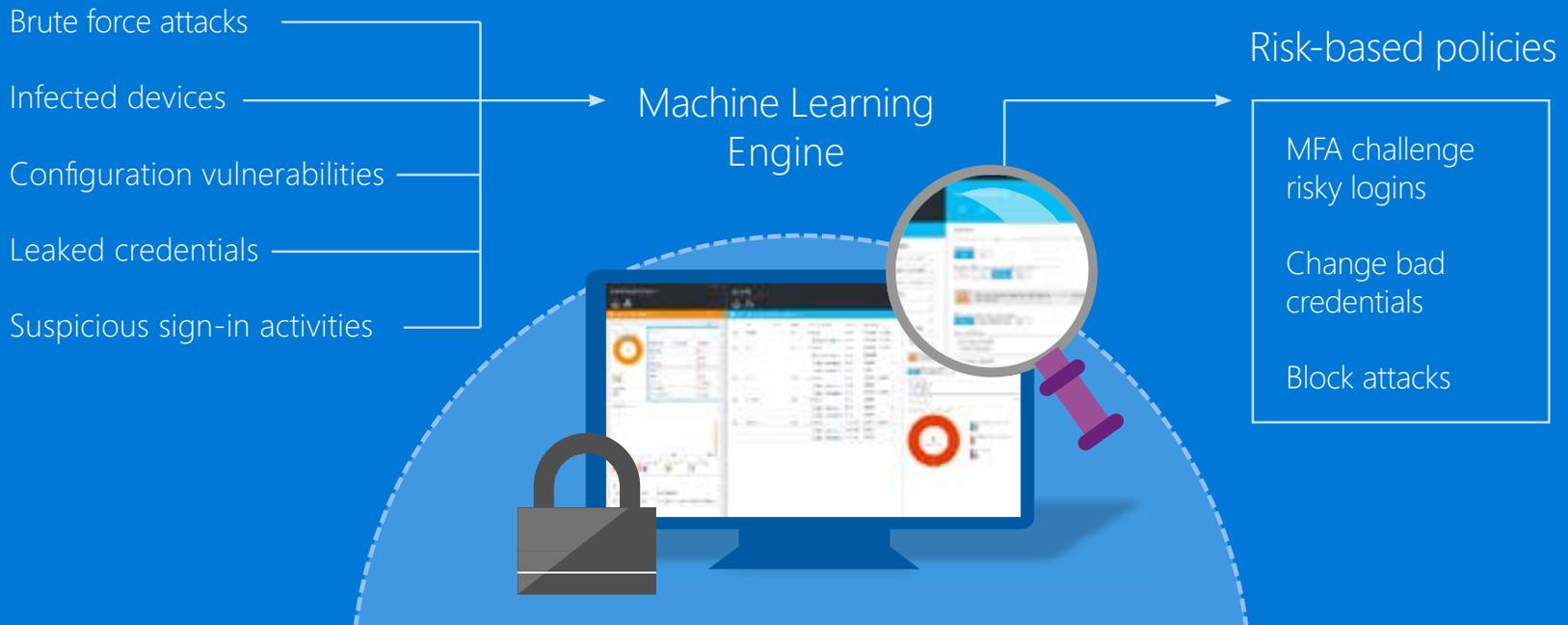
## Advanced Threat Analytics

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

Your Office 365 investment 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. **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

With Office 365 and EMS, you can 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 PCs, service more than 450 billion authentications, and analyze more than 200 billion emails for malware and malicious websites.

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 Office 365 and EMS, the Microsoft Intelligent Security Graph is part of your advanced security strategy.

# Build a strategy that works for your business

Your digital transformation is underway. Deploying Office 365 may be one of the first steps your organization takes toward its transformation. Build on top of your Office 365 security and management capabilities to progress on this journey with enhanced confidence. As you roll out your Office 365 and Enterprise Mobility + Security deployment across your organization, start to consider an expanded SaaS app portfolio while growing your circle of collaboration within, and outside, your organization.



## Assess your mobility strategy

Evaluate your mobility landscape with the [EMS assessment](#) to identify strengths and uncover hidden gaps in your enterprise mobility strategy.

**Assessment Tool** 

## Try EMS with your Office 365 deployment for free today

Learn more about [Enterprise Mobility + Security](#) solutions and the ways your organization can build on your Office 365 investment.

Explore Microsoft solutions to [manage mobile productivity](#).

Safeguard corporate resources at the front door with [identity-driven security](#).

Start your [free trial](#) and take advantage of in-depth [deployment guidance](#).

## Start today!

Enable [conditional access](#) and keep corporate data secure while enabling employees to be productive on any device.

Maximize employee productivity with access to corporate resources on their favorite Office 365 mobile apps. Set [app protection policy](#) from within your Office 365 Management console.

Protect your on-premises web applications with [secure remote access](#).

# EMS benefits for Office 365 customers

<p>Enterprise Mobility + Security</p> 	<p>Identity and access management </p>	<p>Identity-driven security </p>	<p>Managed mobile productivity </p>	<p>Information protection </p>
	<p><b>Azure Active Directory</b></p> <ul style="list-style-type: none"> <li>• Risk-based conditional access</li> <li>• Advanced security reports</li> <li>• Single sign-on for all apps</li> <li>• Advanced MFA</li> <li>• Dynamic Groups, group-based licensing assignment</li> <li>• Privileged identity management</li> </ul>	<p><b>Cloud App Security</b></p> <ul style="list-style-type: none"> <li>• Visibility and control for all cloud apps</li> </ul> <p><b>Advanced Threat Analytics</b></p> <ul style="list-style-type: none"> <li>• Identify advanced threats in on-premises identities</li> </ul>	<p><b>Intune</b></p> <ul style="list-style-type: none"> <li>• Mobile app management</li> <li>• Users self-service management</li> <li>• Certificate provisioning</li> <li>• PC management</li> </ul>	<p><b>Azure Information Protection</b></p> <ul style="list-style-type: none"> <li>• Automated intelligent classification and labeling of data</li> <li>• Tracking and notifications for shared documents</li> <li>• Protection for on-premises Windows Server file shares</li> </ul>
<p><b>Basic identity management via Azure Active Directory for Office 365:</b></p> <ul style="list-style-type: none"> <li>• Single sign-on for Office 365</li> <li>• Basic MFA for Office 365</li> </ul>	<p><b>Advanced Security Management</b></p> <ul style="list-style-type: none"> <li>• Insight into suspicious activity in Office 365</li> </ul>	<p><b>Basic mobile device management via MDM for Office 365</b></p> <ul style="list-style-type: none"> <li>• Device settings management</li> <li>• Selective wipe</li> <li>• Built into Office 365 management console</li> </ul>	<p><b>RMS protection via RMS for Office 365</b></p> <ul style="list-style-type: none"> <li>• Protection for content stored in Office (on-premises or Office 365)</li> <li>• Access to RMS SDK</li> <li>• Bring your own key</li> </ul>	