
Microsoft
Secure access to your enterprise
Enforce risk-based conditional access in real time

The intelligent cloud has created an opportunity to do security better

Traditional security perimeters no longer apply. Identity is the new control plane.

Cloud computing has fueled an intelligence revolution that connects us to our data, devices, and each other like never before. We access work applications from the coffee shop and social media at the office—often using the very same device. The blurring of lines between work and personal has made life more convenient, but it has also reduced privacy and created new security risks. Each of our digital touchpoints, whether it's a personal account or a business tool introduced through a company's digital transformation initiative, requires a unique sign-in. The result: users need to remember a lot of passwords, and smart hackers know how to exploit this as a new vulnerability.

As a mobile workforce accesses sensitive corporate data through mobile devices and cloud apps, the opportunities for bad actors to use compromised identities to do real damage to your business have exploded. Protecting the enterprise requires that you shift your focus from guarding traditional security perimeters to protecting identities. It requires a layered approach that starts with a great user authentication experience with automatic, policy-based rules for accessing sensitive information, regardless of location or device type.

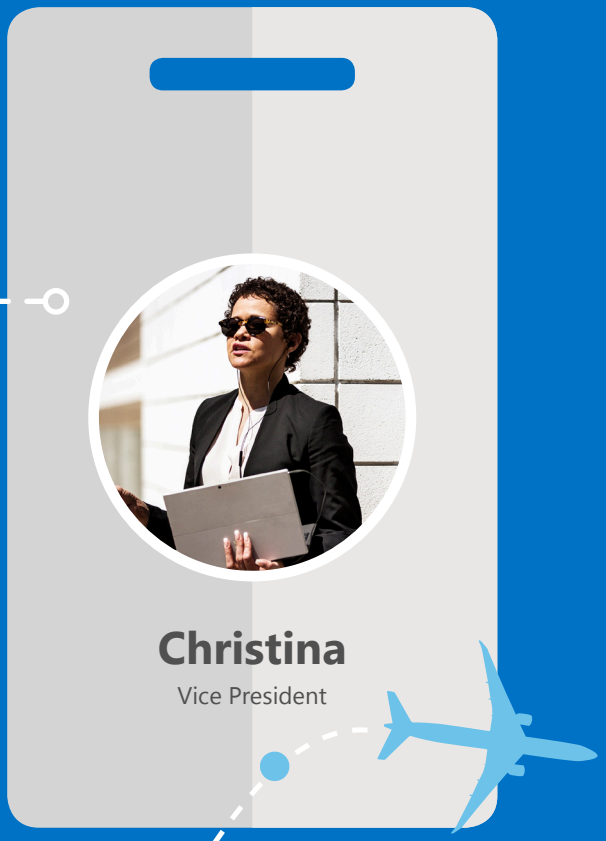
81% of hacking breaches leverage stolen and/or weak passwords[1]

[1] 2017 Verizon Data Breach Investigations

Detect and secure the enterprise against compromised identities, devices, and apps

Meet Christina

Christina is a division VP at Contoso and travels frequently to visit the five offices that she manages across the US, China, and Canada. She has access to highly sensitive information, so it's important to her and the company that her user identity is protected. Because she travels overseas so frequently and connects to corporate assets from unknown wireless networks, it's more challenging to protect her identity and device. Her company needs security that understands what is normal for her and detects when her user or device risk is elevated.



If Christina's user credentials or device become compromised, how can IT automatically enforce additional layers of authentication to keep the organization safe?

All characters are fictitious.

Simplify and protect access to devices and apps

SCENARIO

On a daily basis, Christina signs in to her personal laptop, an iPhone, her Surface, Office 365 apps, Salesforce, and a handful of custom on-premises apps and databases required for her job. She also uses Spotify, WhatsApp, and Netflix when she is on the road. She knows it's not safe to use the same password for each of them, but she can't keep track of a dozen, highly secure passwords, so she often reuses the same password.

Increase productivity and security with single sign-on

Azure Active Directory (Azure AD) centralizes identity and access management across cloud and on-premises environments, allowing users like Christina to use a single user identity to sign in to Office 365 and thousands of on-premises and cloud apps. With Azure AD single sign-on (SSO) enabled, she only needs to remember one user name and password, saving her time and increasing her security. If she does forget her password or gets prompted to change it, she can quickly reset it herself using Azure Self-Service Password Reset. Christina can get back to work quickly, and the IT department saves significant time and money.

73%

of passwords are duplicates[2]

[2] Enreprenuer.com "Password Statistics: the Bad the Worse and the Ugly." June 3, 2015.

Safeguard user credentials with MFA

Azure multi-factor authentication (MFA) is an additional layer of access protection that doesn't excessively burden users. Azure MFA requires at least two forms of authentication, such as a six-digit PIN plus a known mobile device. This significantly increases the odds of verifying the identity of the person signing in. If Christina travels to Tokyo instead of one of her five typical offices, or if she uses an unknown device, Azure AD can be configured to automatically require MFA as an added precaution.

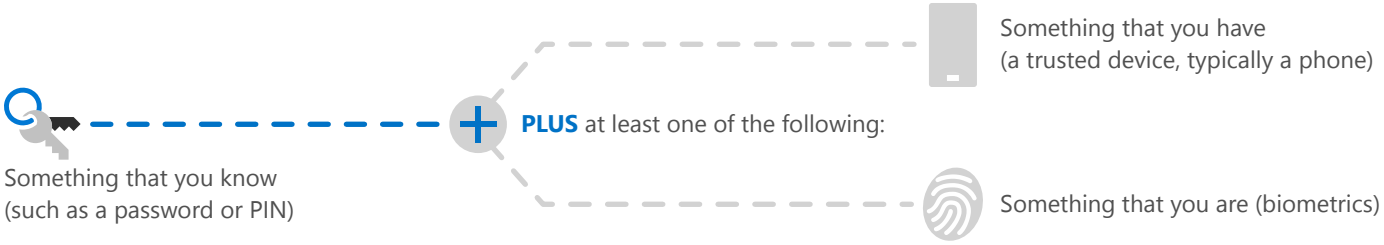
Go password-less by using more secure forms

It would be even easier for Christina, and safer for the company, if she didn't have to remember a password at all. Windows Hello provides more secure authentication options, like facial recognition, fingerprint scanning, and/or six-digit PINs to identify users at sign-in. And, Christina won't need a password to sign in to any Azure AD-synced account on her mobile devices while using the Microsoft Authenticator app. Password less sign-in means there are no weak passwords to guess or steal, and it is significantly more challenging for hackers to obtain both the device and the biometric information, making spoofing unlikely.

Guide users towards more secure passwords

When Christina creates a new password, Azure AD password protection will automatically prevent her from picking one of 500 commonly used passwords. IT can augment this banned password list with additional passwords or rules that they want to enforce. This will make it easier for Christina to comply with her company's security best practices when she resets her password.

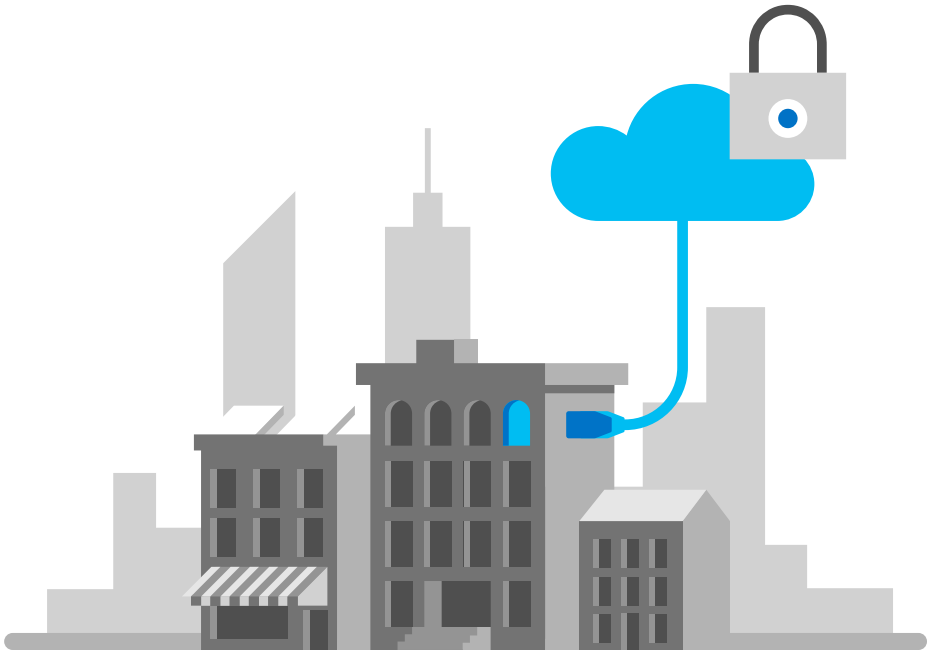
MFA USES AT LEAST TWO FORMS OF AUTHENTICATION:



Automatically enforce risk-based conditional access

SCENARIO

Like all users, Christina's sign-in behavior is different from anybody else at her organization. When she is in the US or Canada, she is an early morning person, likely to sign in before many others get to work, but when she travels to China, her sign-in times change dramatically. She will have meetings with colleagues during local Chinese business hours as well meetings with her team back in North America, which is several hours behind. No matter where she is, Christina frequently checks emails or downloads documents from her iPhone. She is very busy and doesn't want security to get in the way of her productivity, but if Christina's behavior is unusual, IT needs to quickly validate that it's really her and let her get back to work. IT needs a security solution that knows what's normal for Christina, so they can determine when behavior is atypical and automatically enforce access policies to re-authenticate the user and/or restrict access.



Extend conditional access to third-party cloud apps

Azure AD works with Microsoft Cloud App Security and Azure Information Protection to protect both corporate data and access to it through cloud applications. Via the Microsoft Intelligent Security Graph, Microsoft Cloud App Security extends conditional access to cloud applications and can restrict actions within cloud apps, even blocking access to certain apps and data based on flexible and granular policies that IT defines. Microsoft Cloud App Security also helps IT discover what apps are being used in the organization and works with threat protection to help detect anomalous user behavior.

Assess user and device risk at every sign-in near-real time

Conditional access uses a combination of user, location, device, app, and other risk conditions to ensure only the right users have access to apps and data. Azure AD works with Windows Defender Advanced Threat Protection, Microsoft Cloud App Security, Microsoft Intune, and Azure Information Protection to evaluate Christina's risk level at the moment she signs in to make sure that it's safe for her to access corporate apps and data. If user or device risk is elevated, or other conditions are not met, Azure AD will automatically enforce her company's security policies which may:

- Require MFA to prove her identity
- Change the actions she can take in cloud apps (e.g. limit download or sharing functionality)
- Restrict access to sensitive data
- Block access
- Require a password reset

Work doesn't have to stop when a user is not on the corporate network.
Secure access to corporate cloud and on-premises apps and maintain control with conditional access.

FACTORS THAT CONTRIBUTE TO ASSESSING AND SCORING RISK:

USER RISK:

Is the user login behavior consistent with known behavior?

Is this a privileged user?

Have the credentials been found in public?

DEVICE-BASED RISK:

Is the device healthy?

Is the device currently managed through Microsoft Intune?

Does the user typically use this device?

Is malware detected?

LOCATION-BASED RISK:

Is the IP address or geo-location on the safe list?

Has the user signed in from this location before?

Is this impossible travel?

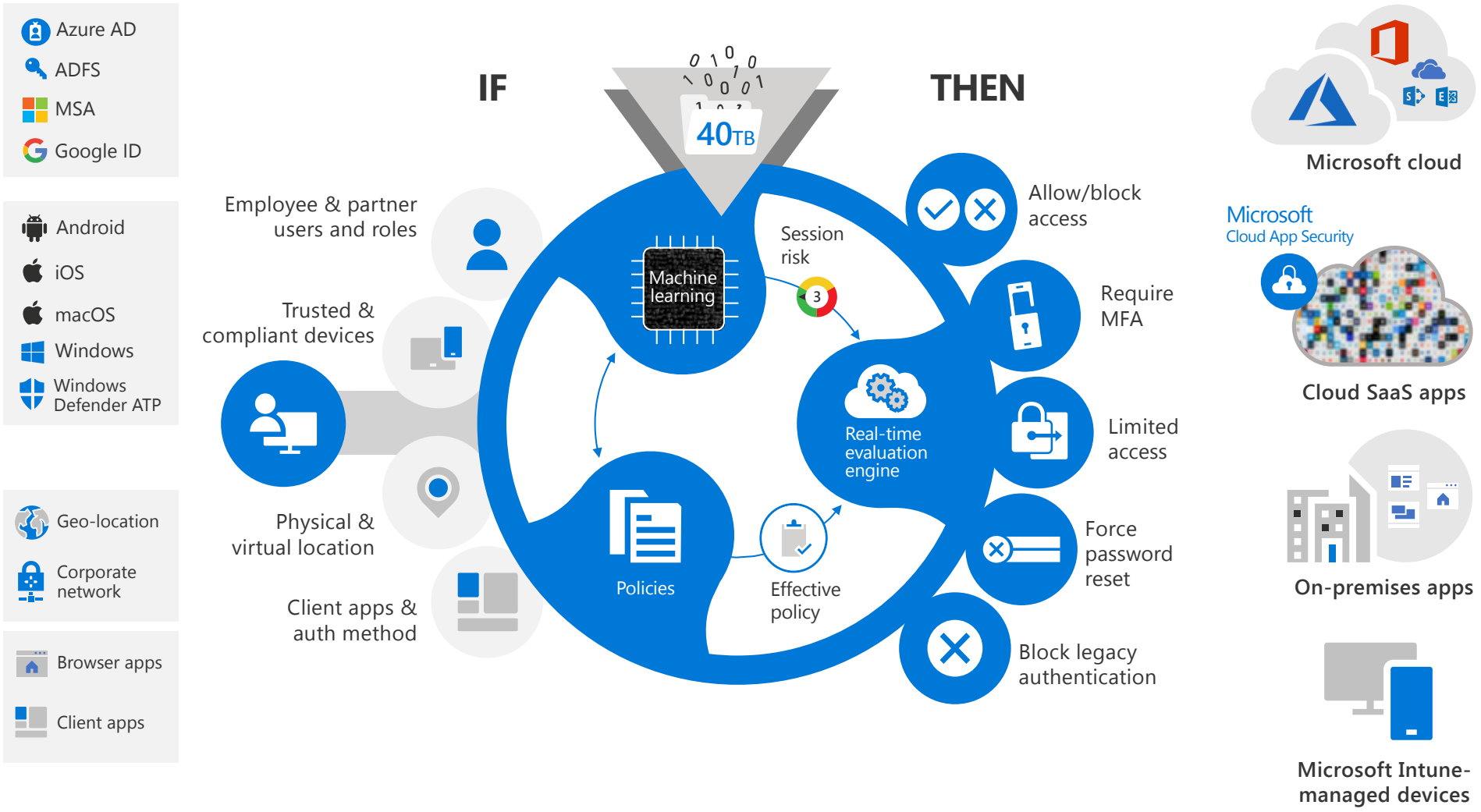
APPLICATION-BASED RISK:

Does the user typically access this application?

Does the application contain sensitive data?

Does the application require administrator access?

Conditional Access



Take back control when user credentials are compromised

SCENARIO

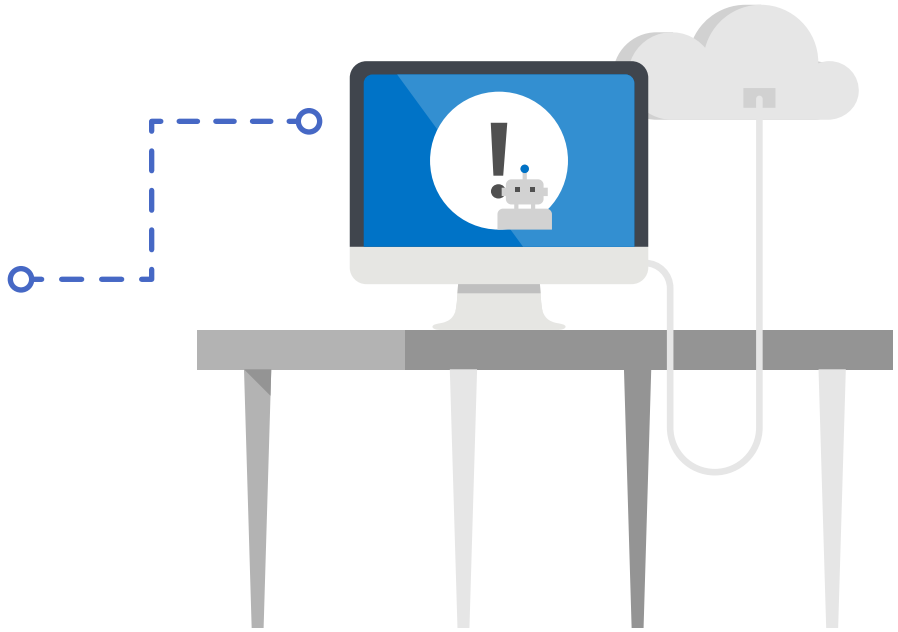
Attackers have become very sophisticated in using low-privilege user accounts to get into an organization. Once in, they move laterally to higher-value users who have access to sensitive company information that they can then sell on the dark web, along with the stolen identities used in the attack. If Christina signs in from Hong Kong and then later that same day she is unable to come up with a second form of authentication during an attempt to sign in from Tokyo using a different device, there is a strong likelihood that she has been hacked. Her company needs a security solution that alerts IT and takes immediate action.

Reclaim compromised user credentials

Azure AD will alert security administrators if it's likely that Christina's identity has been stolen. The next time she attempts to sign in, if she can validate her identity with MFA, Azure AD will automatically trigger a password reset so that future attempts to use the stolen credentials will be unsuccessful.

Discover user credentials on the dark web

Azure AD Identity Protection proactively finds and alerts security administrators if Christina's username and password are found for sale on the dark web.



Protect your privileged account identities

SCENARIO

Christina is a senior leader and therefore she has full administrator privileges. There are times when she needs to access the HR database to get salary and promotion information for her direct reports, but she doesn't need that access every day. If her credentials are stolen, all of that data is at risk, so it is critical to add additional security measures to privileged accounts like hers.

Enable on-demand, just-in time administrative access

Azure AD Privilege Identity Management (PIM) gives security administrators the ability to reduce the corporate attack surface by providing as-needed access to privileged data and set a time limit on that access. Christina can request elevated access when she needs it. Each time she makes a request, she will have to prove her identity by using MFA. Once privilege is granted, it will expire after a set amount of time. If hackers do steal her credentials, PIM acts as a roadblock when they attempt to get to sensitive data.

Defend against hackers with intelligent identity and access management

Microsoft 365 Enterprise E5 identity and access management solutions give you the intelligence to detect risky sign-in behavior and the capabilities to apply policies to limit or block access depending on the rules you apply. Azure AD and password-less sign-in make it easier for users to adhere to security policies without decreasing their productivity. And, in circumstances when a user needs access to privileged data, you can enforce on-demand, just-in-time administrative access using PIM. The Microsoft Intelligent Security Graph powers Azure AD, Microsoft Intune, and Microsoft Cloud App Security to uncover atypical behavior, assign a risk level, and automatically apply rules that you define. You can monitor risk across users, devices, data, and apps; set and enforce granular policies based on different risk factors; and, when a breach does happen, use Azure AD to quickly take back control of identities that have been compromised.

These security products integrate seamlessly to help protect user identities and manage access from any device or location:

- Azure Active Directory
- Windows Hello
- Microsoft Intune
- Microsoft Cloud App Security
- Azure Information Protection
- Windows Defender Advanced Threat Protection

THE INTELLIGENT CLOUD OFFERS AN OPPORTUNITY TO DO SECURITY BETTER

For enterprise customers that embrace the Microsoft productivity suite, there are significant gains to be realized in security. Microsoft 365 Enterprise E5 includes built-in security solutions that integrate easily and share insights from the 6.5 trillion security signals per day seen on the Intelligent Security Graph across the global Microsoft ecosystem. It allows customers to reduce the number of security vendors they manage by unifying security and productivity tools into a single suite that safeguards users, data, devices, and applications—without sacrificing the user experience.

IDENTITY & ACCESS MANAGEMENT

- Azure Active Directory
- Microsoft Cloud App Security
- Windows Hello
- Windows Defender Credential Guard

INFORMATION PROTECTION

- Azure Information Protection
- Windows Information Protection
- Microsoft Cloud App Security
- Advanced Data Governance
- Office 365 Data Loss Prevention
- Microsoft Intune
- Bitlocker

THREAT PROTECTION

- Azure Advanced Threat Protection
- Windows Defender Advanced Threat Protection
- Office 365 Advanced Threat Protection
- Microsoft Cloud App Security

SECURITY MANAGEMENT

- Microsoft 365 Security & Compliance Center
- Windows Defender Security Center
- Microsoft Secure Score
- Microsoft Cloud App Security

Microsoft

GET COMPLETE, INTELLIGENT ENTERPRISE SECURITY

Test it yourself with a free trial, get serious with a proof of concept, or learn more at **aka.ms//M365E5/Security**

© 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. Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.