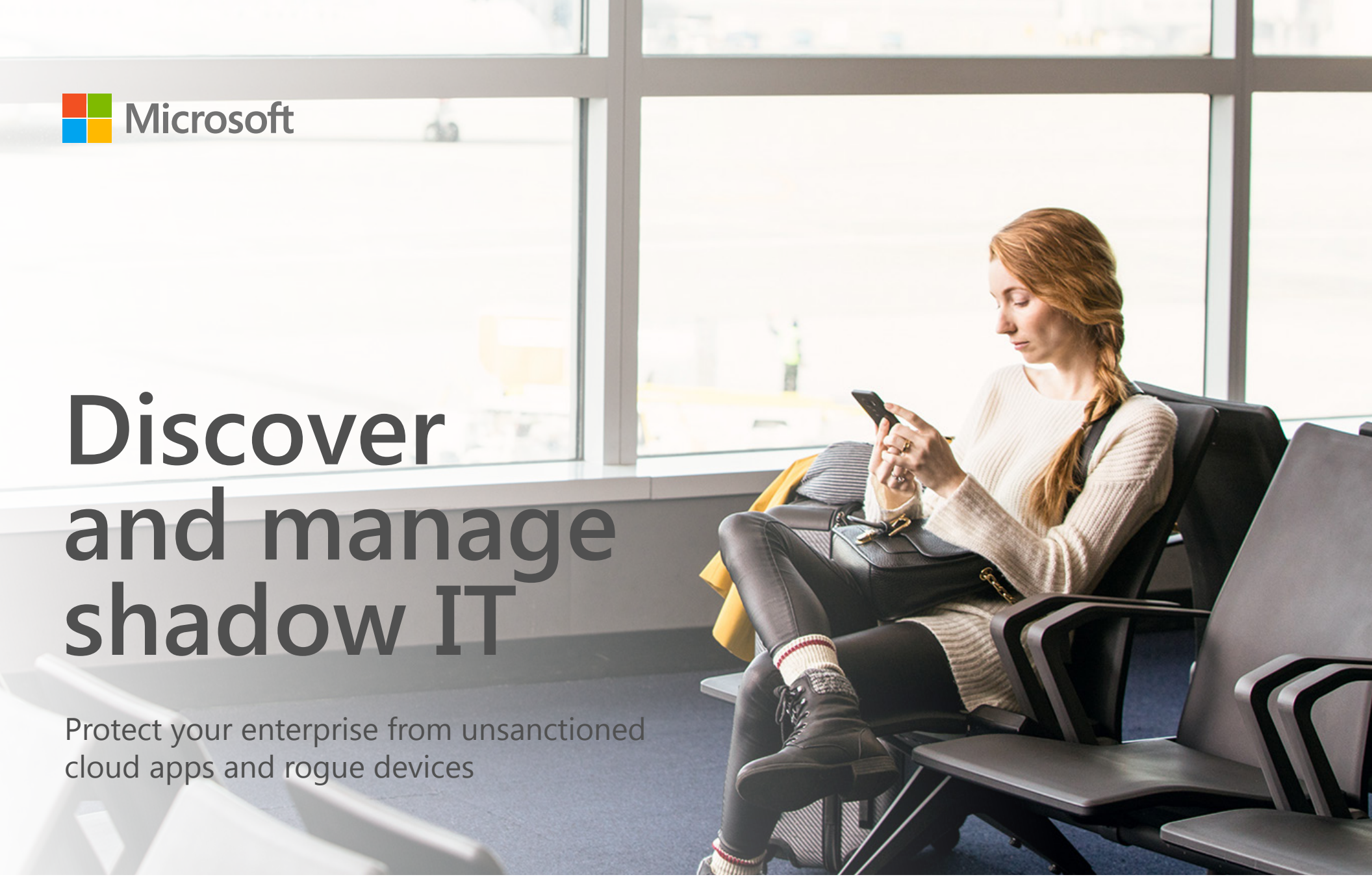
Microsoft

Discover and manage shadow IT

Protect your enterprise from unsanctioned cloud apps and rogue devices



Empower a mobile workforce without compromising security

Today's employees expect technology choices

Digital transformation has accelerated workplace productivity with cloud-based applications and mobile devices that empower users to collaborate with anyone from anywhere. These tools have become essential to the modern workplace, but they have also introduced new challenges. A growing number of devices are personal and unmanaged by IT, and the number of cloud apps used in an organization expands as the number of personal devices grows. Even businesses in the beginning of their journey to the cloud–find their employees are already there, accessing unsanctioned cloud apps with rogue devices.

On average, enterprises use 1,181 different cloud services, yet 61 percent of them go undetected by IT[1].

Mobile devices and cloud applications have increased flexibility for workers, but they have also created new opportunities for bad actors. Applications can be a good way to gain entry because their vulnerabilities are not known and managed by IT. As a result, hackers have begun to infiltrate organizations through weaknesses they discover in shadow IT and personal devices. Reducing this risk is no simple task. Restrictive policies, like locking down access to the cloud entirely or blocking personal devices, have proven to fail because they impede worker productivity. Shadow IT requires a new approach. Start with a secure authentication experience; greater visibility into the applications and devices on the network; and automatic, policy-based rules for accessing sensitive information.

75% of companies consider SaaS tools essential to their business.[2]

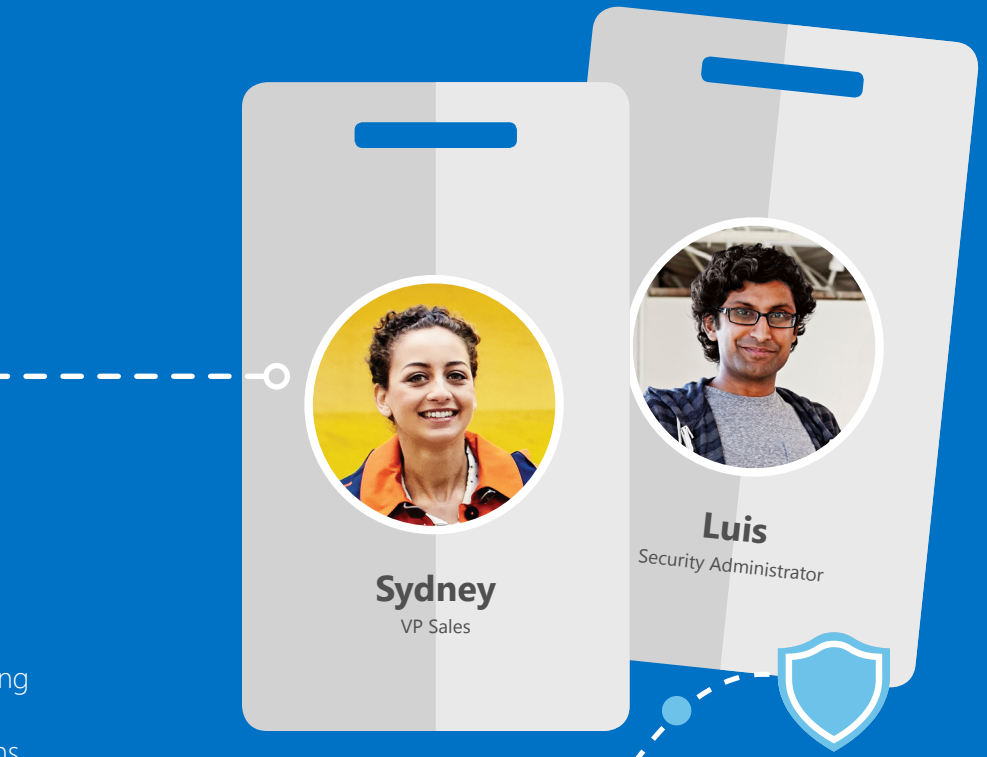
[1]Microsoft 2018 [2]"Insights on SaaS for Business." Gocardless

Regain visibility and control of shadow IT with Microsoft 365 Enterprise E5

Meet Sydney and Luis

Sydney and Luis work for Contoso, a large enterprise that has recently introduced aggressive sales goals to stay competitive. Sydney leads the sales organization and has hired staff in key markets to help meet company goals. Her team needs to be fully mobile to help them connect with customers and minimize downtime while they are on the road, and her executive team has encouraged Sydney to try new technology to help them work smarter.

Luis, who is a security administrator, understands why the company is adopting new technology to support productivity, but he is also frustrated. He was at the office until midnight the other night trying to understand unusual patterns in access to corporate data. Working long hours is becoming a trend because he can't see what devices and apps are used in the organization. He wants to support the team's use of new technology to increase their productivity, but he also needs to see what cloud apps are being used, so he can assess their risk and protect against threats.



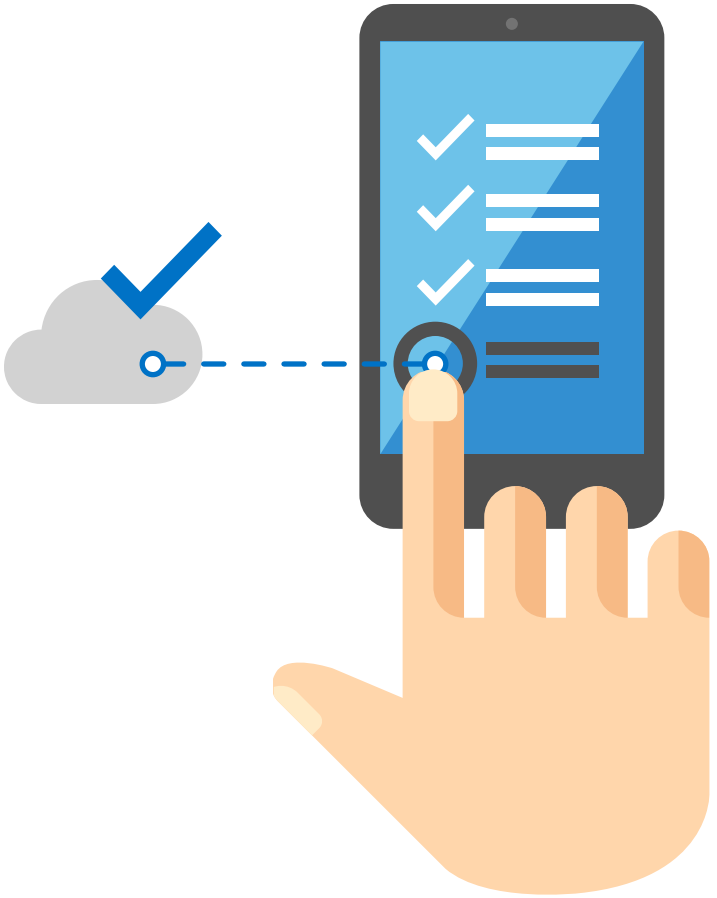
How can Luis find and manage shadow IT and rogue devices to ensure the company remains secure?

All characters are fictitious.

Discover shadow IT

SCENARIO

The biggest challenge Sydney has confronted since going mobile is keeping her team connected to each other and to good, accurate information. Sydney needs a simple way to share key materials with her team, and she wants them to know how to connect with each other for questions and coaching. Members of her team have recommended a few collaboration apps that might help. Sydney decides to test one this month. To get it started, she emails an app download link to the team. Sydney is so excited about this opportunity to help her team that she forgets to check with IT to see if the app is compliant with Contoso's security policies.



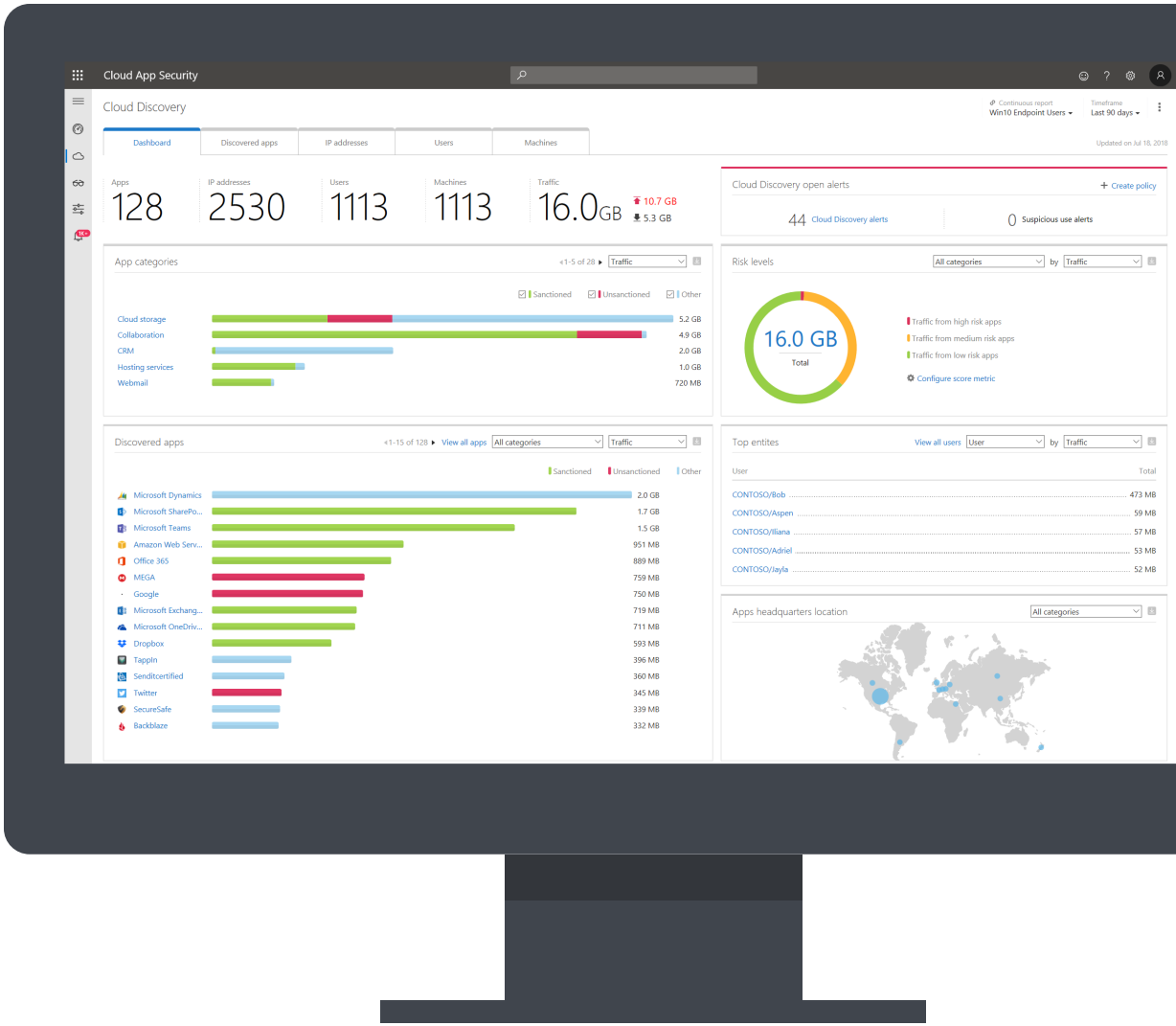
Identify cloud apps used in your organization with Microsoft Cloud App Security

A few months ago, it would have been difficult for Sydney and Luis to know if the new collaboration app meets Contoso's security policies, but last month IT invested in Microsoft 365 Enterprise E5, which has transformed Luis's job. Microsoft Cloud App Security gives him visibility into all the cloud apps and services used in the company. It provides sophisticated analytics to assess the risk and use of each app, and he can set up alerts when a new, risky application is accessed and respond quickly.

When Sydney and her team begin using the collaboration app, Luis receives an alert. He reviews the data about the app to decide how to move forward and sees that so far only Sydney and her team are using it. Microsoft Cloud App Security has given the app a high score, indicating that it is "low risk" and meets certain security and compliance standards. Luis has the option to sanction the app, tag it, or block it. This is a well-known application, and when Luis researches it further, he determines that it complies with Contoso's security policies. He officially sanctions the app and lets Sydney know that her team is good to go.

Block risky apps

Two days later Luis receives another alert. A risky cloud application was accessed via the corporate network. Luis checks his reports and sees that this application is also being tested by Sydney's team. He reviews the risk profile for the application in Microsoft Cloud App Security and finds that there are several security vulnerabilities. The app also doesn't meet Contoso's compliance requirements. He blocks the application from being accessed in the future.

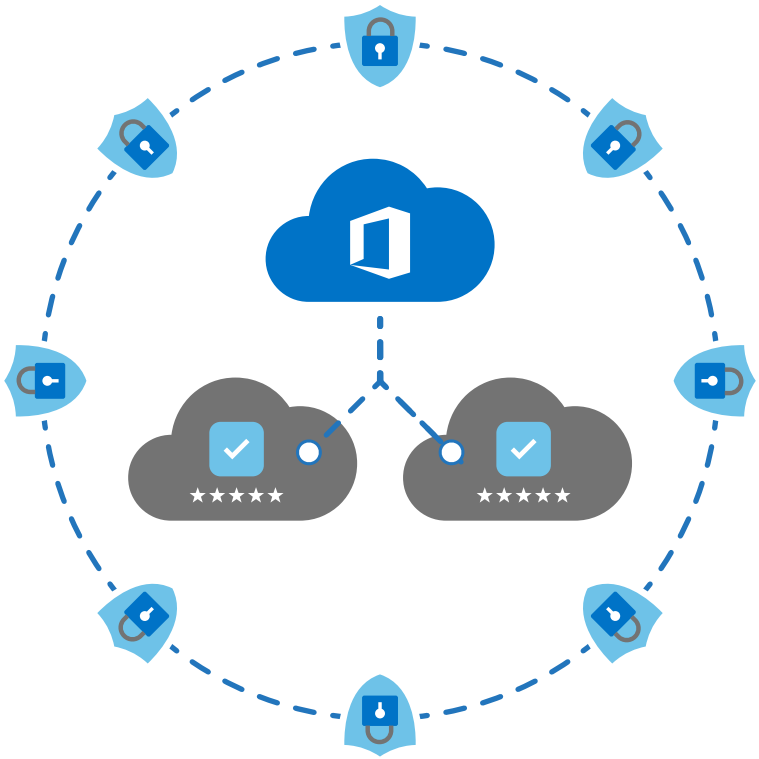


Monitor OAuth Apps

As part of his review, Luis also wants to identify the applications that have been authorized to access Office 365 data using the open authorization (OAuth) protocol. OAuth allows a user to give an app access to accounts and data without sharing credentials. Luis checks all the apps that were authorized for Office 365 and reviews their permissions levels and community use to evaluate the risk of each app. The community use rating indicates that the apps authorized to access Office 365 are commonly used in other organizations. He also sees that none of these apps have permission to access highly privileged accounts. Luis determines they represent a low risk and sanctions the apps.

Onboard new applications to Azure Active Directory

Luis sets up a meeting with Sydney to explain why he had to block one of the cloud applications and to ask how he can better support the team. They agree that the first application that Sydney tested met both the sales team's goals and the enterprise's security requirements. Luis onboards the application to Azure Active Directory (Azure AD) so that Sydney's team can access it using single sign-on (SSO) and multi-factor authentication (MFA) to provide an additional layer of security. Both teams benefit: Sydney's team members can sign in to the app with the same sign-in they use for the network, and it reduces the likelihood that an unauthorized user will access data through the app. After talking with Sydney, Luis has a better understanding of her team's needs and recommends a few secure alternative apps for Sydney to try out.



Protect sensitive data in the cloud

SCENARIO

Sydney meets with a prospective client in a coffee shop near the prospect's office. The meeting goes well, and before she heads back to the office for a meeting with her boss, Sydney wants to finalize the details of the sale. She creates a report in Salesforce that includes revenue projections for her team and decides to download the file to share with her manager. Salesforce blocks her from downloading the file because she is accessing the data from a public wireless network. Sydney is a bit annoyed that she can't finish her task in the coffee shop, but she had forgotten that she was connected to an unsecured network and is relieved that she didn't download data that could have been compromised. She drives back to the office and safely downloads the report before her meeting with her manager.

After her meeting Sydney remembers that she promised to share a file with the prospect. She finds a copy of the document on the shared OneDrive and tries to move it to Box where they share files with customers. Box will not let her upload the document because it includes sensitive information that only people in the organization can view. Sydney realizes that she accidentally tried to upload the revenue projections. That would have been a big mistake, and she is glad again for the automatic security policies. She finds the correct file and uploads it to Box.

Extend information protection to cloud apps

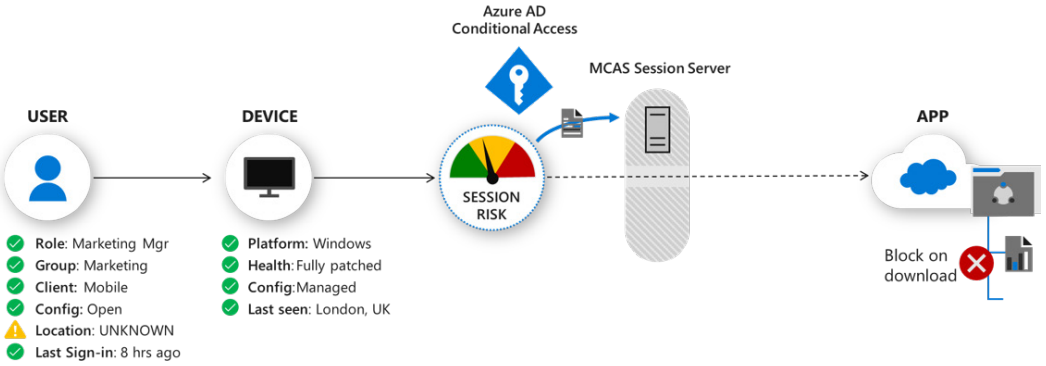
Azure Information Protection safeguards sensitive data in Contoso's documents and emails. Luis is able to configure policies to automatically classify, label, and protect data based on its sensitivity, and the protection follows the data—ensuring it remains protected regardless of where it's stored or with whom it's shared. When integrated with Microsoft Cloud App Security, Azure Information Protection extends all these capabilities to data stored in third-party cloud apps.

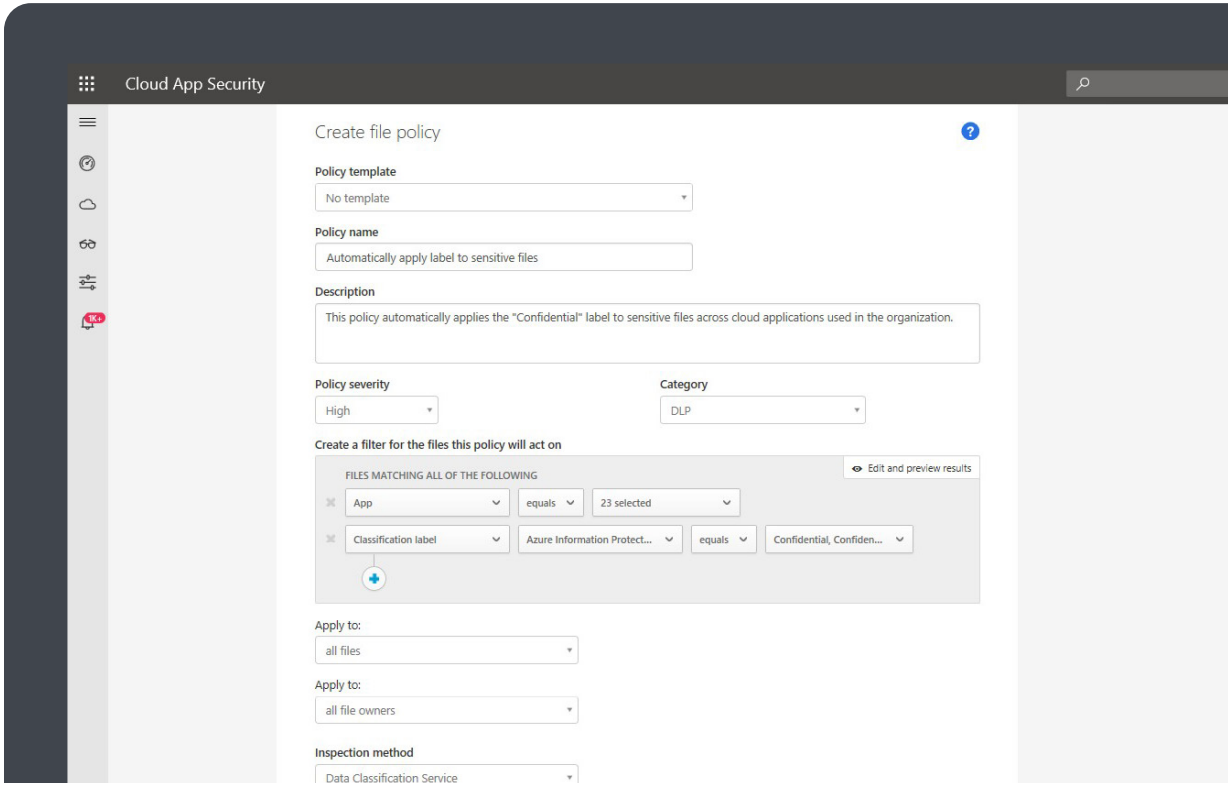
Sydney was not able to share the file outside of the organization because of the information protection policies that were applied to the revenue projection file. Because data protection is written at the meta data level, files that leave the organization remain protected, and Luis can track activities on shared data and change the policies or revoke access if necessary.

Apply conditional access rules to cloud apps

Microsoft Cloud App Security also integrates with Azure AD and Azure Information Protection to enforce conditional access rules and limit the actions a user can take while using different cloud apps. Luis is able to set up Azure AD conditional access to enforce access controls on his organization's apps based on certain conditions. The conditional access polices can be applied based on the user, the cloud app, the file sensitivity, or the location or network to determine the risk level associated with a user session.

Sydney was able to access Salesforce to create her report, but she was unable to download the revenue data because of her location, an unsecure, public network, which did not meet the requirements for downloading this category of information. Luis can also block access to certain apps entirely with flexible and granular policies that he defines.





Protect cloud apps against cyberthreats

SCENARIO

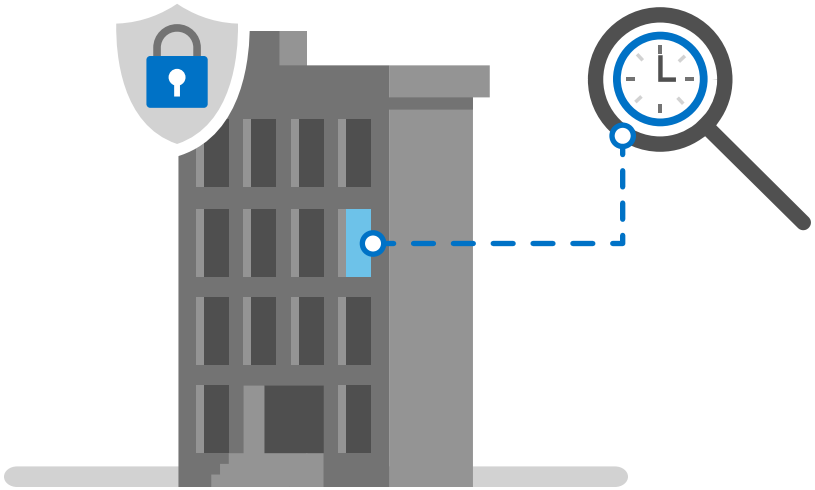
The following month, Luis is about to head home for the evening when he receives another alert. One of Sydney's sales representatives tried to download 100 documents from an Office 365 app during a time the user is typically not active. The system flagged the user as likely compromised and elevated their user risk level to "high." Luis is relieved he set access policies to automatically block compromised users from accessing Office 365 apps until they prove their identity with MFA and reset their password. He reaches out to the user to confirm that he changed the compromised credentials and starts an investigation into the data that was downloaded.

Detect anomalous behavior

Microsoft Cloud App Security uses machine learning and user and entity behavioral analytics (UEBA) to analyze each cloud app session to profile users and login patterns to develop a baseline for what's normal. Microsoft Cloud App Security looks at a number of different risk indicators, grouped into multiple categories, such as risky IP address, sign-in failures, admin activity, inactive accounts, location, impossible travel, device and user agent, and activity rate. The sales associate's behavior was deemed anomalous because the volume of downloads is not typical for him, and it took place during hours that the user is typically offline. Microsoft Cloud App Security includes several predefined anomaly detection policies, and Luis can customize policies based on Contoso's needs.

Monitor and protect Office 365 and on-premises apps, in real time

Microsoft Cloud App Security and Azure AD Conditional Access policies allow Luis to apply granular security measures to Office 365 apps, in real time. He can also use app proxy to make on-premises apps available to Sydney's remote team and apply conditional access policies to monitor and control access as soon as a risky user session is detected. If a sales rep tries to access data through an on-premises hosted line of business app using an unmanaged device, conditional access app control can limit what actions they can take. This was a key reason why Luis's team chose Microsoft 365 Enterprise E5, as no other cloud app security broker can extend real-time controls and protection to on-premises apps.



MICROSOFT CLOUD APP SECURITY LOOKS AT SEVERAL DIFFERENT RISK INDICATORS:

Threat delivery and persistence

- Malware implanted in cloud apps
- Malicious OAuth application
- Multiple failed sign-in attempts to app
- Suspicious inbox rules (delete, forward)

Indicators of a compromised session

- Activity from suspicious IP addresses
- Activity from anonymous IP addresses
- Activity from an infrequent country
- Impossible travel between sessions
- Sign-in attempt from a suspicious user agent

Malicious use of an end-user account

- Unusual file share activity
- Unusual file download
- Unusual file deletion activity
- Ransomware activity
- Data exfiltration to unsanctioned apps
- Activity by a terminated employee

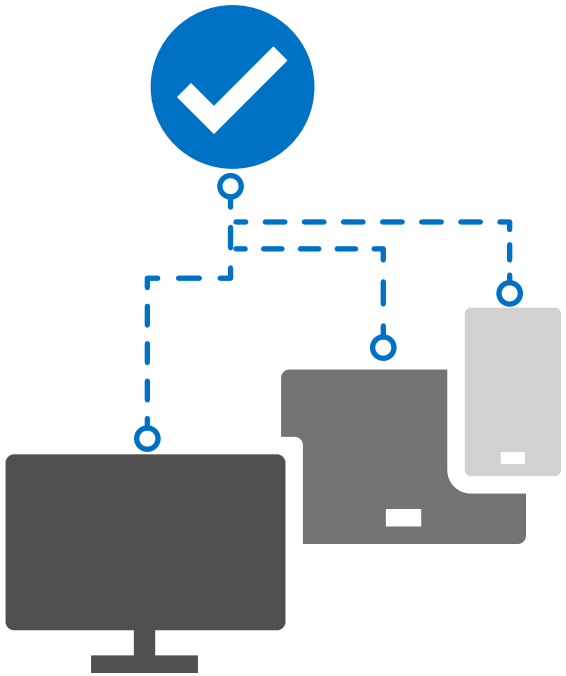
Malicious use of a privileged user

- Unusual impersonated activity
- Unusual administrative activity
- Unusual multiple delete VM activity

Automatically detect new devices

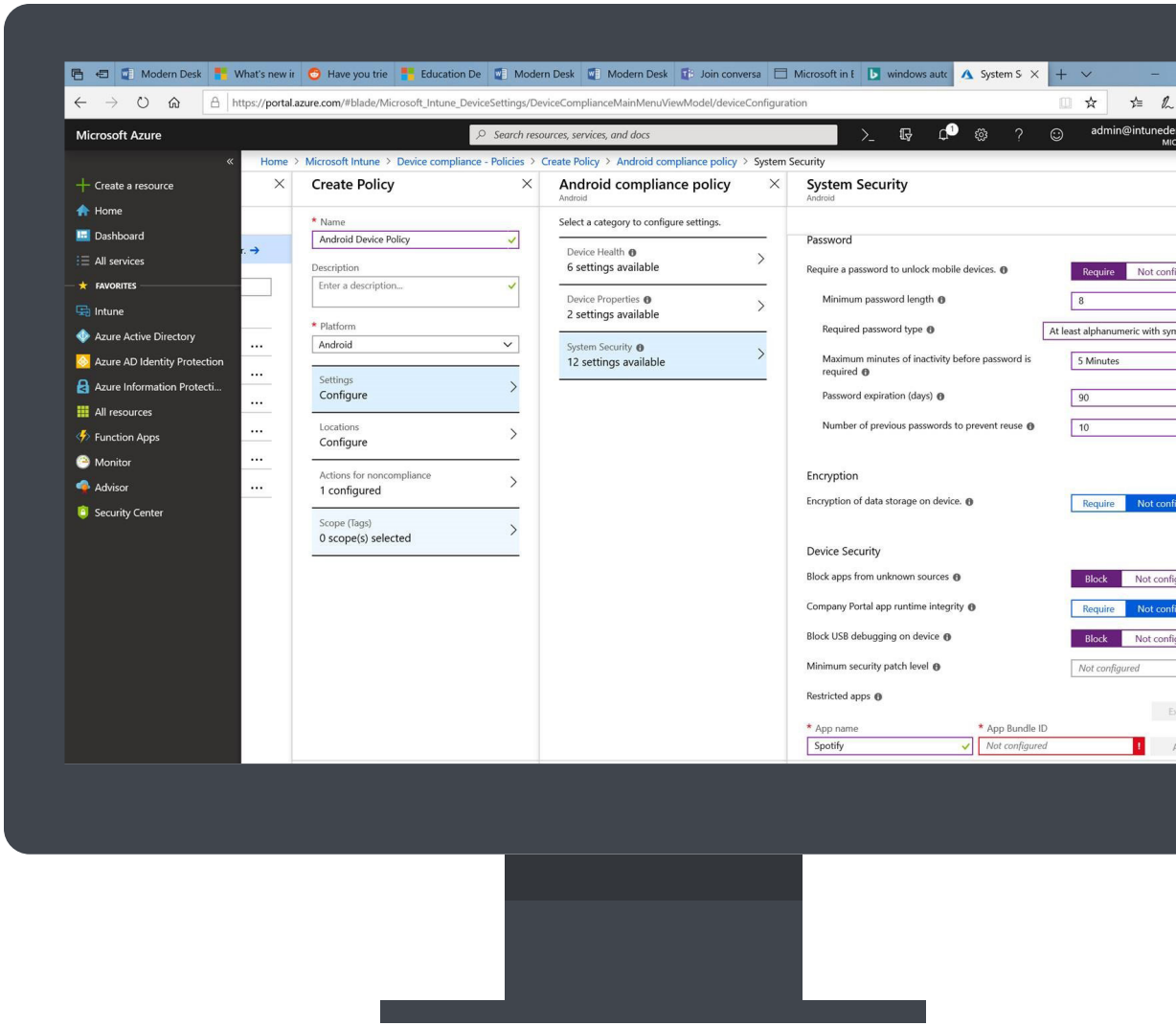
SCENARIO

Android has just released an upgrade to its phone, and Sydney decides to use a portion of her sales meeting to remind those staff members who use an Android to upgrade. The sales team uses its phones to take customer testimonial videos, which are posted to the company Instagram account, and it's important that they are high quality. "Future customers will evaluate what kind of company we are by the quality of those videos," Sydney explains. Sydney and two of her team members plan to upgrade their phones. When Sydney gets her new device, she signs in to her e-mail and is immediately prompted to register her device. Registering her device is simple. The phone automatically downloads the required line-of-business applications and all the Office 365 apps, and Sydney is prompted to download a handful of other popular Azure AD-connected apps. She chooses the apps she prefers and quickly gets back to work.



Discover rogue devices and prompt users to register

It doesn't take long for Luis to learn that upgraded Android devices have hit the network, but thanks to Microsoft Intune he doesn't have to take any action. Microsoft Intune lets Luis manage corporate and employee-owned devices through a single console. He has already set up policies based on the needs of Contoso, such as requiring users to register a new device or blocking unregistered devices from accessing sensitive information. The self-service portal makes it easy for users to enroll their devices with no assistance from IT. During the enrollment process, Microsoft Intune will prompt users to install company-mandated apps, and Luis has also required a minimum and maximum operating system so that he knows that only devices with the safest OS are accessing the network. Luis sees that Sydney has already registered her device, and he knows the other user has also received a notification. There is no additional action required of him, so he shifts to other priorities.

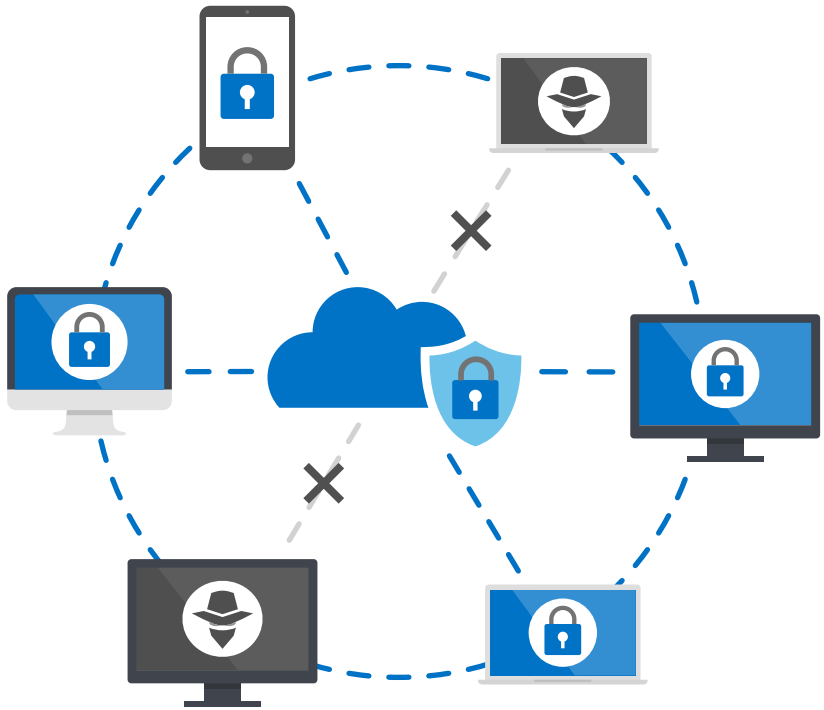


MICROSOFT CLOUD APP SECURITY

Elevate the security for all your cloud apps and services

Bring shadow IT into the light

Microsoft 365 Enterprise E5 security capabilities give you the intelligence to detect unsanctioned cloud apps and rogue devices that are attempting to access your corporate resources. You can apply policies to limit or block access depending on the rules you define. Microsoft Cloud App Security allows you to discover cloud applications that are accessed by users, evaluate their risk level, and set policies for access. Microsoft Intune lets you manage corporate and employee-owned devices, including detecting unregistered devices and prompting them to register. Microsoft Cloud App Security, Azure AD, and Azure Information Protection work together to apply information protection to your cloud apps, ensuring that sensitive data is labeled and protected no matter where it travels. Conditional access policies allow Microsoft Cloud App Security to limit actions in the cloud when a risky user session is detected, and Microsoft Cloud App Security integrates with Windows Defender Advanced Threat Protection to detect anomalous behavior across users and sessions to help you uncover bad actors and keep your enterprise safe.



These security products integrate seamlessly to help you manage shadow IT:

- Microsoft Cloud App Security
- Azure Active Directory
- Azure Information Protection
- Microsoft Intune
- 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	INFORMATION PROTECTION	THREAT PROTECTION	SECURITY MANAGEMENT
Azure Active Directory	Azure Information Protection	Azure Advanced Threat Protection	Microsoft 365 Security & Compliance Center
Microsoft Cloud App Security	Windows Information Protection	Windows Defender Advanced Threat Protection	Windows Defender Security Center
Windows Hello	Microsoft Cloud App Security	Office 365 Advanced Threat Protection	Microsoft Secure Score
Windows Defender Credential Guard	Advanced Data Governance	Microsoft Cloud App Security	Microsoft Cloud App Security
	Office 365 Data Loss Prevention		
	Microsoft Intune		
	Bitlocker		

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**