Microsoft

Security beyond Microsoft products

Secure a diverse digital estate
without limits on technology choices

Modern enterprises use a variety of technologies

Security solutions must work together to protect a broad range of devices, products, and services from many vendors

Today's organizations are adopting a variety of solutions from providers big and small to achieve their digital transformation goals. Increasingly, users expect to work with the apps, devices, and platforms they know and like, enhancing their daily experience and increasing productivity. At the same time, cloud technology brings new possibilities for data and connections, and many companies encourage their employees to explore new applications to work smarter and engage customers through personalized experiences. This proliferation of apps, devices, and platforms adds significant challenges for IT security teams.

Modern IT data centers are also evolving quickly as organizations work to host more applications, data, and workloads in the cloud. Many organizations run mission critical workloads on different operating systems, using multiple cloud platforms, and relying on a variety of vendors. The patchwork approach can significantly complicate efforts to secure an organization's digital estate.

In this heterogeneous world, it's important that security solutions work in harmony with the other security products enterprises already use. Achieving this harmony provides better protection and visibility across the devices, products, and services modern organizations use—regardless of which vendor provides them.

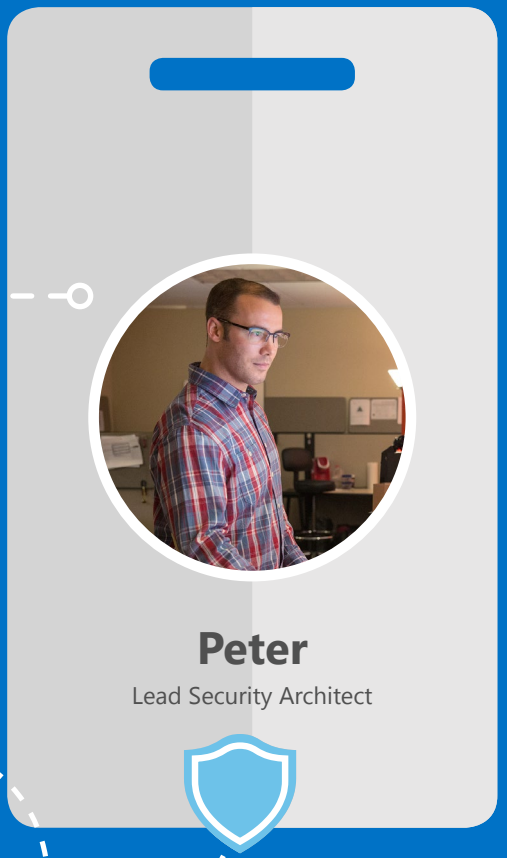
Security solutions must work in harmony to secure a diverse digital estate

Meet Peter

Peter is the lead security architect at Contoso. His job is to design and implement security solutions and he takes this responsibility seriously and is constantly on the hunt for solutions that can improve visibility and better integrate with the company's technology stack.

Over the past few years, Contoso has exceeded its sales goals and the company has doubled in size. New employees are encouraged to use their existing mobile devices and have their choice of a PC or a Mac. Peter is helping to design a major expansion of the company's cloud, supporting more than 50 new business applications and a new customer service application. He is also responsible for migrating the organization's operations to the cloud. The business uses both Azure cloud and Amazon Web Services (AWS), with about 40 percent of those Azure workloads running on Linux. Extending existing security capabilities to cover these needs has required Peter's team to purchase several security solutions, and he's become frustrated by the increased number of "security silos" and the growing cost of the integrations.

It's Peter's job to ensure that everything is secure and that the tools the SecOps team uses work in harmony across the entire digital landscape. Lately, however, the sheer quantity of technologies in play and the new security tools needed to secure them have become too much to manage.



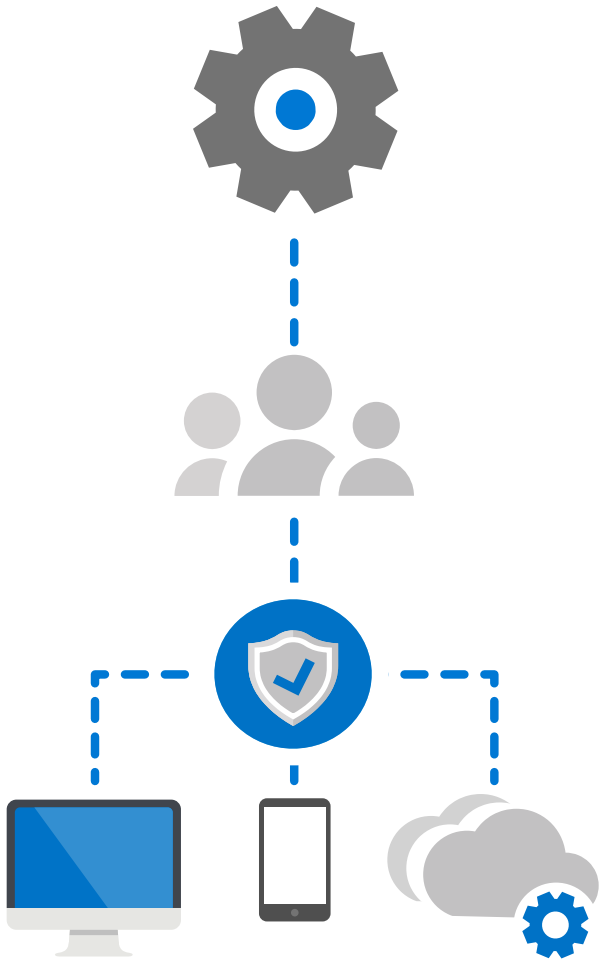
How can Peter reduce the number of security vendors he manages and better integrate with the ones he keeps?

All characters are fictitious.

Extend the reach of Microsoft 365 security to other products and services

SCENARIO

As part of the its digital transformation initiative, Contoso deployed Office 365 for productivity and team collaboration, and based on the success of that initiative, the company licensed Microsoft 365 Enterprise E5 to take advantage of the full suite of security solutions. Recently, Peter heard that Microsoft 365 Enterprise E5 and Azure Security Center can do a lot more than just secure Microsoft products, but he's skeptical. Can it handle workloads running Linux? How about AWS or Google Cloud Platform? What about mobile devices? Can Microsoft 356 Enterprise E5 protect Android Enterprise devices, and the over 600 cloud apps in use in the organization? After talking with his SecOps lead, Cathy, and doing some online research, Peter learns that Microsoft 365 Enterprise E5 can help secure much more of the company's digital estate than he thought.



Provide single sign-on to thousands of applications

Peter decides to use Azure Active Directory (Azure AD) to centralize identity and access management across the organization's cloud and on-premises environments. With Security Assertion Markup Language (SAML) single sign-on, Azure AD authenticates to cloud apps through users' Azure AD accounts. Azure AD communicates the sign-in information to applications through a connection protocol. More than 600,000 active apps integrate with Azure AD, plus thousands of popular enterprise software as a service apps with preconfigured integrations. As a result, Peter can enable employees to use one identity to sign in to Office 365, plus thousands of third-party applications and services. Users have just one password to remember, which saves them time and improves security.

Maintain data classification and protection when emails or documents travel to non-Microsoft platforms

Azure Information Protection enables Peter's team to classify and protect data by automatically applying labels to it. These labels are persistent, following the company's emails and documents (including PDFs) to any third-party platform or device—whether that's Windows, macOS, iOS, or Android. In addition, Azure Information Protection gives the IT security team visibility into and control over data that employees share. The team can track that shared data and, if necessary, revoke access to it. The protection that Azure Information Protection offers is not limited to Microsoft applications and services, either. Developers within Peter's organization, and even third-party vendors, can use Azure Information Protection's underlying technology in their own apps, whether they are on-premises or in the cloud.

Azure Information Protection can be configured to apply labels in different ways:

AUTOMATIC

Administrators define the rules and conditions for applying labels.

RECOMMENDED

Azure Information Protection recommends labels based on the rules and conditions that administrators define.

MANUAL

Users choose whether to apply a label.

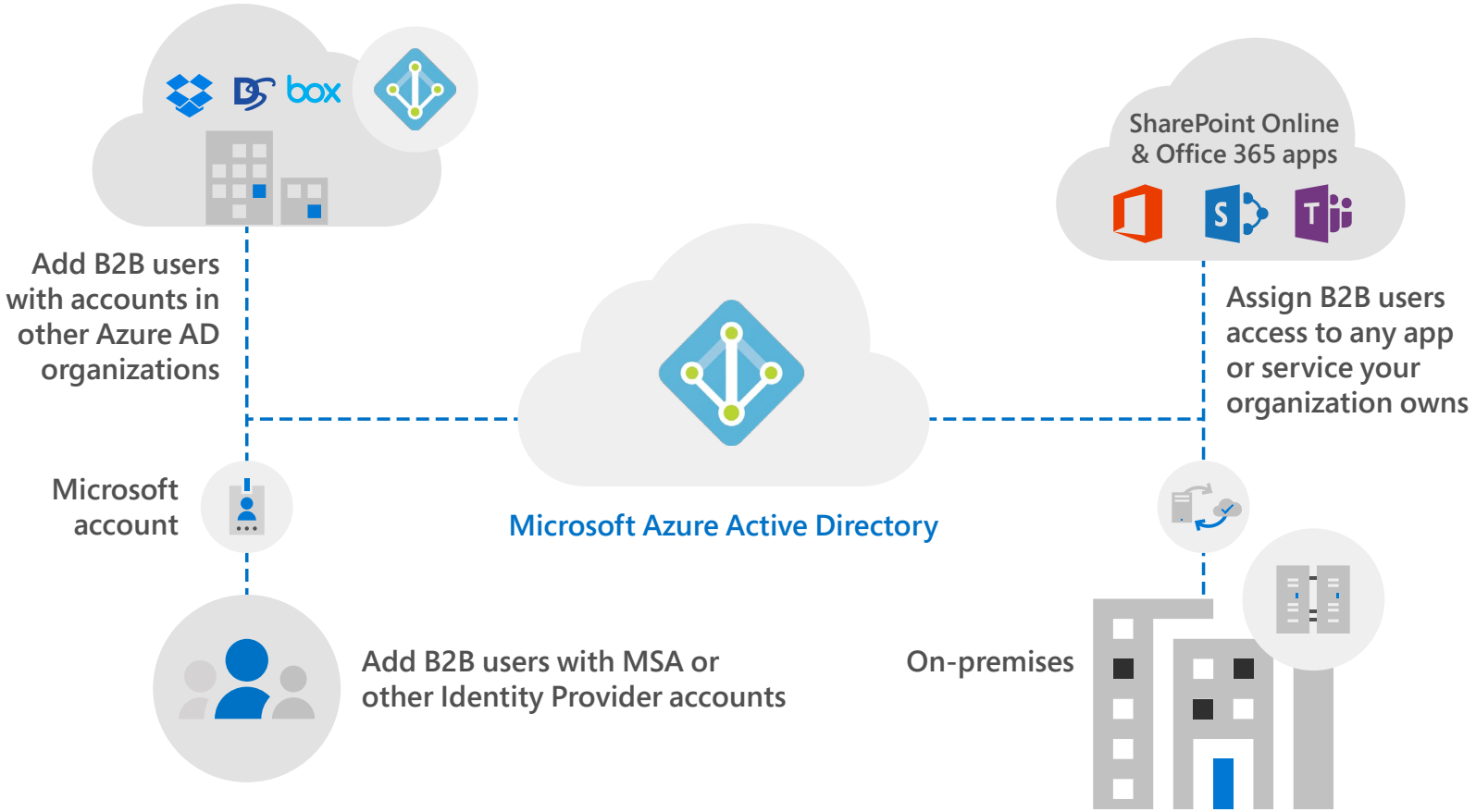
More than

600,000

active apps integrate with Azure AD

Collaborate securely with users outside your organization

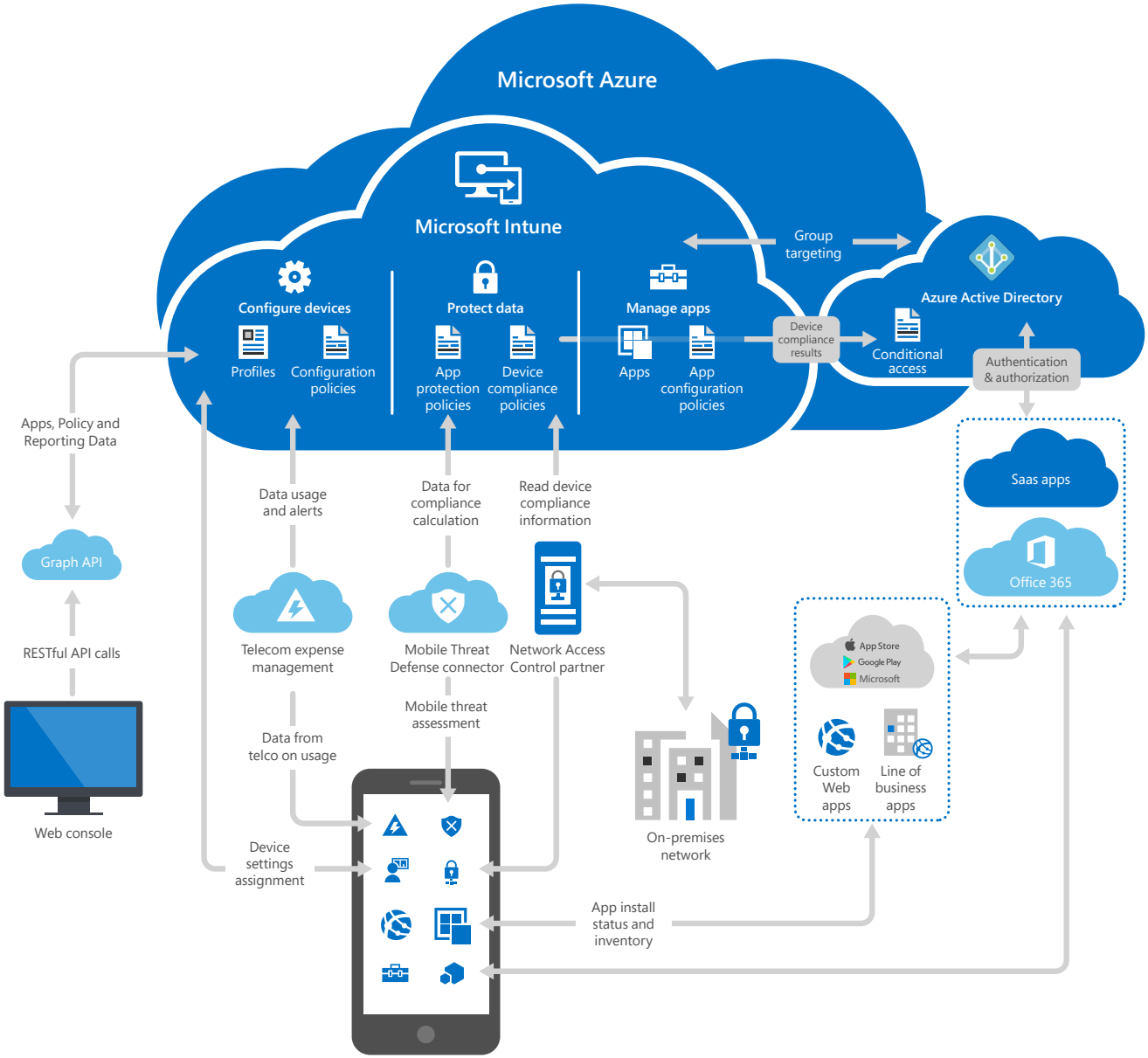
To make it easy for employees to work securely with users from other organizations, Peter enables Azure AD B2B collaboration capabilities. Now, users can grant access to documents, resources, and applications to their partners while maintaining control over corporate data. For your customers, Azure AD B2C lets Peter build identities on Windows, Android, and iOS devices or for the web, and customers' users can sign in with their existing social accounts or personal email addresses.



Protect emails and files on any device (Windows, macOS, iOS, Android, Android Enterprise)

By using Microsoft Intune, Contoso can better manage and secure the apps and data its mobile workforce uses, whether they are on Windows, macOS, iOS, or Android devices. For example, Microsoft Intune can configure device security and make compliance a condition for accessing company data. Microsoft Intune also helps improve security by preventing access to company resources by users or from devices that do not meet the security standards set for the organization by Peter and his team. It protects any corporate data that is viewed or stored on personal devices in the form of emails, calendar events, documents, and certain apps.

Peter's company uses Microsoft Intune to manage Android Enterprise devices. Microsoft Intune supports Android Work Profile, which requires users to enroll devices and provides certain device-level controls for IT administrators. For devices that do not need the device management capabilities, the company can deploy Microsoft Intune app protection policies, which manage corporate identities and protect corporate data on devices without enrollment. These device users retain control of their device settings and personal apps without putting company data at risk.



Secure hybrid cloud workloads running Windows and Linux

Azure Security Center helps secure workloads running on-premises or on any cloud platform. That's true whether those workloads are running on Windows or Linux. Peter's IT security team uses Azure Security Center to monitor the company's cloud workloads for vulnerabilities and to detect threats, including within its AWS workloads running Linux. Azure Security Center also enables the team to set security policies for those workloads so that they comply with the company's security standards, and it offers recommendations for improving the security posture of those workloads. As a result, the organization is better able to prevent, detect, and respond to attacks across on-premises and cloud platforms as well as across different operating systems.

The Azure ecosystem has expanded rapidly around Linux and Open Source solutions to support organizations of any size. Azure marketplace solutions contain Linux and Open Source offerings from the industry's most influential organizations and a broad variety of niche solutions from vendors of all sizes (more than 60 percent of Azure marketplace images are Linux-based). Because Azure is open, Peter's team can keep using Jenkins, Terraform, and Ansible and fill the gaps in their DevOps toolchain by using Visual Studio Team Services to orchestrate and supplement.

~50%

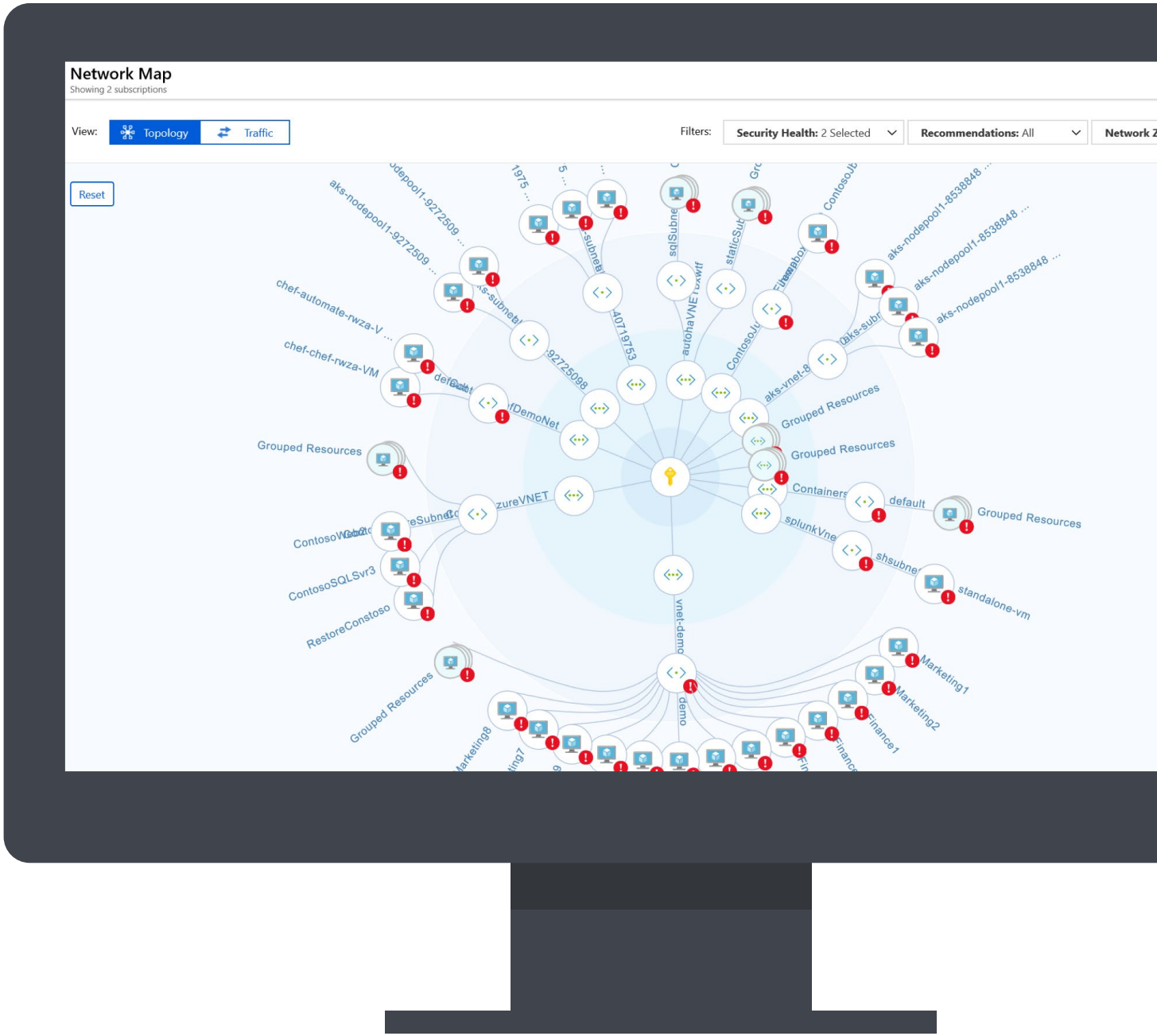
of the workloads in the Azure cloud are running Linux.[1]

In addition to Windows, Azure Security Center supports these Linux operating system flavors on any cloud platform:

- Ubuntu versions 12.04 LTS, 14.04 LTS, and 16.04 LTS
- Debian versions 6, 7, 8, and 9
- CentOS versions 5, 6, and 7
- Red Hat Enterprise Linux versions 5, 6, and 7
- SUSE Linux Enterprise Server versions 11 and 12
- Oracle Linux versions 5, 6, and 7
- Amazon Linux 2012.09 through 2017
- OpenSSL 1.1.0 (supported only on x86_64 platforms [64 bit])

[1]Microsoft, 2018

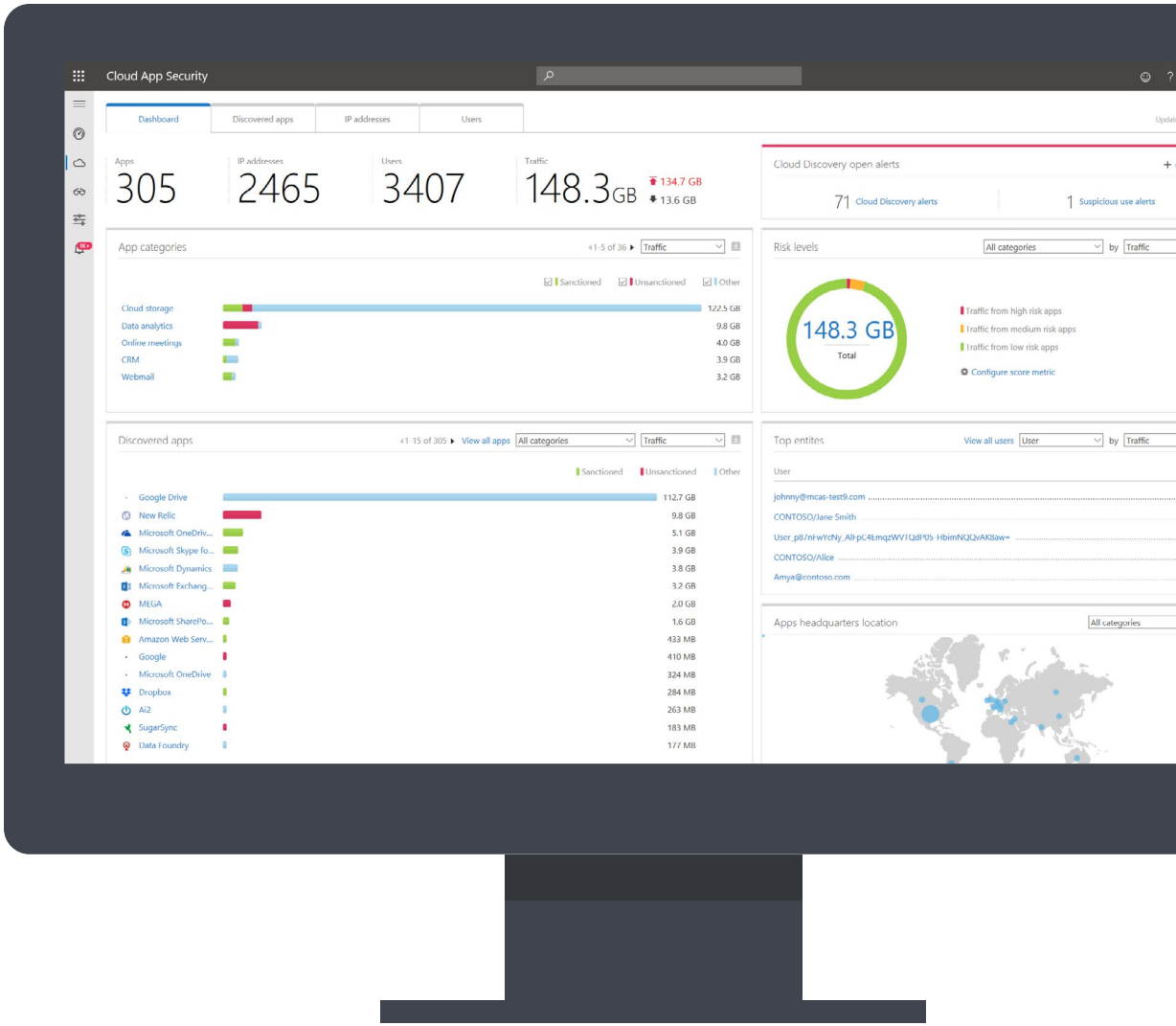
Azure Security Center provides visibility over an organization's security state across virtual networks, subnets, and nodes by generating a topology map of the layout of each infrastructure component:



Discover and protect third-party cloud apps and services

Microsoft Cloud App Security gives Peter's IT security team visibility into cloud apps and services, provides sophisticated analytics to identify and mitigate cyberthreats, and enables control over how data travels. When Microsoft Cloud App Security discovers a cloud app out of the catalog of more than 16,000 apps, Peter can assess its risks based on usage information and analysis of more than 70 risk factors, including regulatory certifications, industry standards, and best practices.

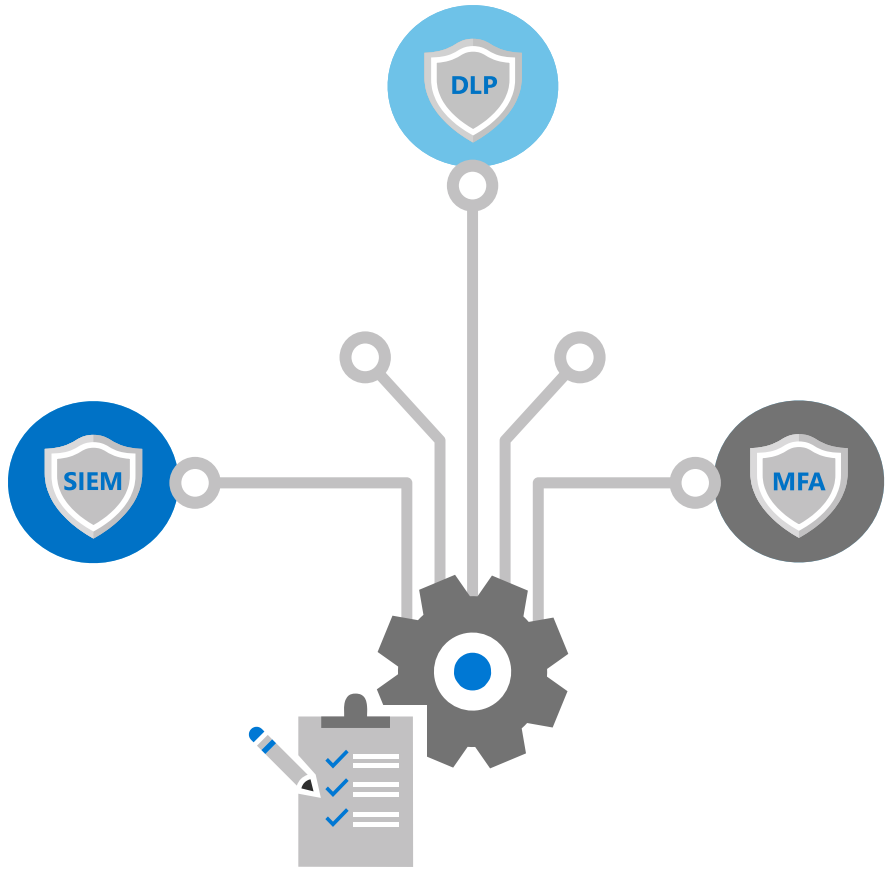
By using Microsoft Cloud App Security, Contoso can safely embrace the cloud while maintaining control of important data. Microsoft Cloud App Security integrates with Azure AD to control access to apps and help protect critical data by monitoring its storage and how people share it, using the classification labels from Azure Information Protection. Microsoft Cloud App Security can also detect suspicious user activities and anomalies (e.g., unusual user activity, ransomware) so that the security team can more quickly respond to threats. By integrating natively with Windows Defender Advanced Threat Protection (Windows Defender ATP), Microsoft Cloud App Security gives the team a more complete view of the cloud apps that employees use.



Microsoft 365 integrates with other security solutions

SCENARIO

Peter and his IT security team have already made significant investments in security that they don't want to lose in the transition to Microsoft 365 Enterprise E5. The team's multi-factor authentication (MFA), security information and event management (SIEM), and data loss prevention (DLP) systems are fully implemented, with time remaining on their contracts, and the team has invested significant effort in fine-tuning policies and training users. Building on his previous successes, Peter plans to integrate Microsoft 365 Enterprise E5 with these third-party security solutions to extend the company's investments.

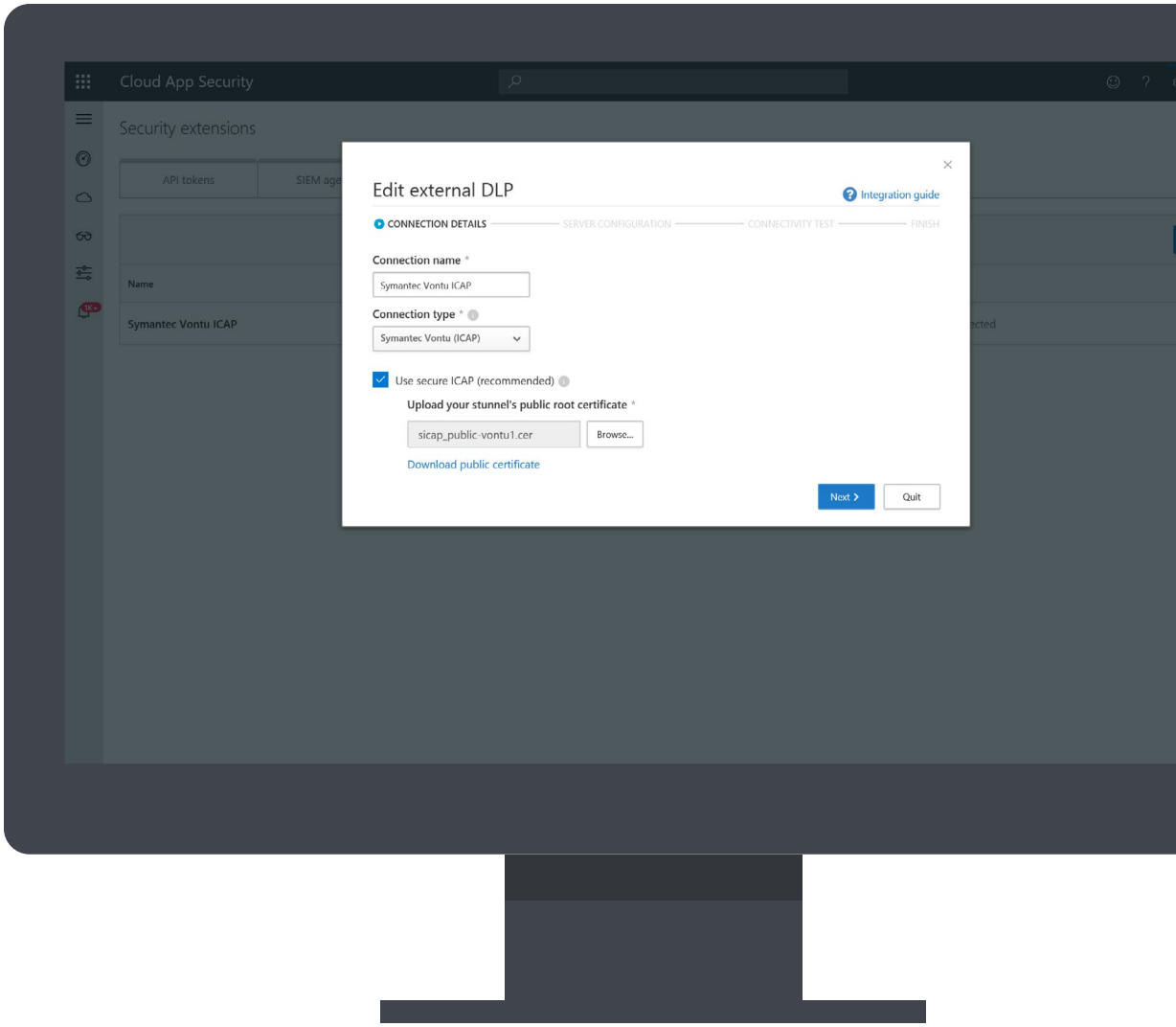


Integrate with third-party MFA

As an additional layer of security, Azure AD's MFA can prevent access if a user's identity is compromised. However, Peter has already implemented a third-party MFA solution, and Microsoft 365 Enterprise E5 works harmoniously with it. To integrate the two solutions, Peter creates a custom control in Azure AD conditional access that redirects users to the third-party MFA solution. When users sign in to Azure AD, the control redirects them to the external service to satisfy additional requirements, and then redirects the users back to Azure AD to continue the conditional access flow. Peter is able to continue using the contracted and fully deployed third-party MFA and gain the real-time access controls provided by Azure AD.

Stream security signals from Microsoft Intelligent Security Graph to a SIEM solution

Contoso's SIEM system provides a centralized hub where the security team can review event data and team members train on established playbooks. Peter uses the Microsoft Graph Security application programming interface (API) with Azure Monitor. The Microsoft Intelligent Security Graph supports high-volume streaming of alerts from all Microsoft security products (i.e., Graph Security providers) directly into their SIEM system. The rich insights these alerts give the IT security team help improve its investigations and speed up response times.



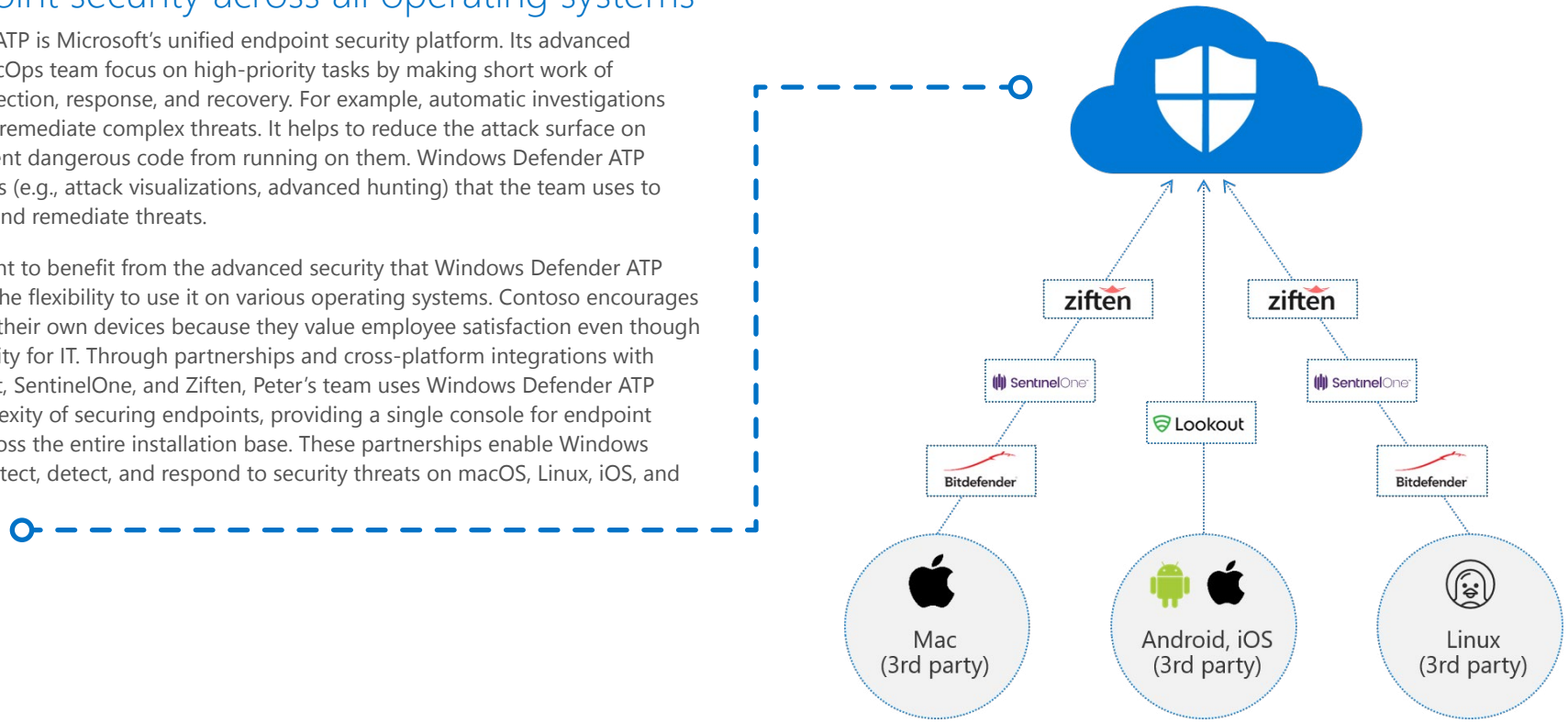
Integrate with a third-party DLP solution

Peter's team has invested significant effort in fine-tuning their existing DLP system's policies, balancing DLP against users' productivity, and training users. To not lose these investments, Peter integrates his company's DLP system through Microsoft Cloud App Security. It exposes easy-to-use interfaces, such as Representational State Transfer (REST) API and Internet Content Adaptation Protocol (ICAP) to enable integration with non-Microsoft DLP solutions. To enable this integration, Peter sets up a Secure Sockets Layer (SSL) channel between Microsoft Cloud App Security and the company's DLP solution, and then connects them. Afterward, Microsoft Cloud App Security uses a secured ICAP channel to communicate with the third-party DLP solution. This integration extends the solution's controls to the cloud, enabling Peter's team to use a consistent and unified policy for on-premises and cloud services and applications.

Unify endpoint security across all operating systems

Windows Defender ATP is Microsoft's unified endpoint security platform. Its advanced features help the SecOps team focus on high-priority tasks by making short work of mundane threat detection, response, and recovery. For example, automatic investigations can close alerts and remediate complex threats. It helps to reduce the attack surface on endpoints and prevent dangerous code from running on them. Windows Defender ATP provides robust tools (e.g., attack visualizations, advanced hunting) that the team uses to detect, investigate, and remediate threats.

Many customers want to benefit from the advanced security that Windows Defender ATP offers while having the flexibility to use it on various operating systems. Contoso encourages employees to bring their own devices because they value employee satisfaction even though it increases complexity for IT. Through partnerships and cross-platform integrations with Bitdefender, Lookout, SentinelOne, and Ziften, Peter's team uses Windows Defender ATP to reduce the complexity of securing endpoints, providing a single console for endpoint security visibility across the entire installation base. These partnerships enable Windows Defender ATP to protect, detect, and respond to security threats on macOS, Linux, iOS, and Android devices.



Secure a digital estate that includes products and services from many vendors

Your security solutions must work together to provide better protection of and visibility into the devices, products, and services in your organization. It doesn't matter which vendor provides them.

Microsoft 365 Enterprise E5 extends security capabilities to your non-Microsoft products and services. Azure AD enables your employees (and users from other trusted organizations) to use a single identity to sign in to Office 365 plus thousands of third-party applications. Azure Information Protection can protect your emails and files by automatically applying classification labels to them, and these labels persist on any third-party platform or device. Microsoft Intune protects emails and files by enforcing conditional access to company apps and data. Azure Security Center can monitor your workloads for vulnerabilities and threats on any cloud platform running Windows or Linux and Microsoft Cloud App Security can give you visibility into and control of the cloud apps in your organization.

In addition, Microsoft 365 Enterprise E5 integrates with third-party security solutions so you can use the MFA or DLP provider of your choice and you can stream security alerts from the Intelligent Security Graph to third-party SIEM solutions. Microsoft 365 Enterprise E5 also allows companies to offer their users the freedom to choose their preferred device type because Windows Defender ATP integrates with third-party products to secure macOS, Linux, iOS, and Android endpoints.

The following security products come together to protect non-Microsoft platforms, applications, and services:

- Azure Active Directory
- Azure Information Protection
- Microsoft Cloud App Security
- Microsoft Exchange Online Protection
- Office 365 Advanced Threat Protection
- Graph Security API
- Windows Defender Advanced Threat Protection
- Microsoft Intune
- Azure Security Center
- Intelligent Security Graph

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	Office 365 Data Loss Prevention	Microsoft Cloud App Security	Microsoft Cloud App Security
	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**