Microsoft 365 + the NIST cybersecurity framework

Microsoft

Assessing Microsoft 365 Security Solutions using the NIST Cybersecurity Framework

Introduction

Keeping your employees and organization secure without compromising productivity is a challenge. Microsoft 365 security solutions are designed to help you adhere to industry and government standards and frameworks that have been developed to simplify security for organizations and provide insight and guidance for IT pros.

In this document, we have mapped Microsoft 365 security solutions to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The NIST CSF is a guide for organizations to manage and reduce cybersecurity risk. Developed through a collaboration among industry leaders, academics, and government stakeholders, it is a thorough cybersecurity implementation guide for the United States government, and used by enterprises worldwide. The most current version of the NIST CSF is the NIST CSF Version 1.1, updated in April 2018.

The CSF is founded on two core NIST documents: the NIST SP 800-53 Rev 4 and the Risk Management Framework (RMF), which also references the NIST SP 800-53, among others. Each of these documents—the NIST CSF, the NIST SP 800-53, and the RMF—informs the review process for the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services, and is now considered the primary certification process for cloud-based solutions. Mapping your security solutions to the NIST CSF can help you achieve FedRAMP certification and provide a framework for a holistic security strategy. Although Microsoft isn't endorsing this framework—there are other standards for cybersecurity protection—we find it helpful as a baseline against commonly used scenarios.

Below, we offer guidance to help you best use Microsoft 365 security solutions to address each category within four NIST CSF core actions: Identify, Protect, Detect, and Respond. Regardless of the size of your business, this framework will guide you in deploying security solutions that are right for your organization.

This guide will help you get started with your Microsoft 365 security solutions, explain how these products work together in the greater enterprise environment, and provide insight into the most effective security scenarios you can enable for your organization.

Microsoft 365 Security Solutions

Microsoft 365 security solutions are designed to help you empower your users to do their best work—securely—from anywhere and with the tools they love. Our security philosophy is built on four pillars: identity and access management, threat protection, information protection, and security management. Microsoft 365 E5 includes products for each pillar that work together to keep your organization safe.

Identity & access management

Protect users' identities & control access to valuable resources based on user risk level

Azure Active Directory

Conditional Access

Windows Hello

Windows Credential Gaurd

Information protection

Ensure documents and emails are seen only by authorized people

Azure Information Protection

Office 365 Data Loss Prevention

Windows Information Protection

Microsoft Cloud App Security

Office 365 Advanced Security Management

Microsoft Intune

Threat protection

Protect against advanced threats and recover quickly when attacked

Advanced Threat Analytics

Windows Defender Advanced Threat Protection

Office 365 Advanced Threat Protection

Office 365 Threat Intelligence

Security management

Gain visibility and control over security tools

Azure Security Center

Office 365 Security Center

Windows Defender Security Center

The NIST Cybersecurity Framework Core

The Framework Core consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. When considered together, these functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. Below, we have aligned the security capabilities in Microsoft 365 to four of these core functions.

FUNCTIONS	 Identify	 Protect	 Detect	 Respond
CATEGORIES	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management	Identity Management and Access Control Awareness and Training Data Security Protective Technology Information Protection Processes and Procedures Maintenance	Anomalies and Events Security Continuous Monitoring Detection Processes	Response Planning Communications Analysis Mitigation Improvements

Note: Although Microsoft offers customers some guidance and tools to help with certain Recover functions (data backup, account recovery), Microsoft 365 doesn't specifically address this function.

Identify

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities

Asset Management

"The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed, consistent with their relative importance to business objectives and the organization's risk strategy."

Microsoft 365 security solutions help identify and manage key assets such as user identity, company data, PCs and mobile devices, and cloud apps used by company employees.

First, provisioning user identities in Microsoft Azure Active Directory (AD) provides you fundamental asset and user identity management that includes application access, single sign-on, and device management.

We recognize that many enterprises will be using an on-premises identity directory. Through Azure AD Connect (see Figure 1), you can integrate your on-premises directories with Azure Active Directory. This capability allows you to provide a common secure identity for your users for Microsoft Office 365, Azure, and thousands of other Software as a Service (SaaS) applications pre-integrated with Azure AD.

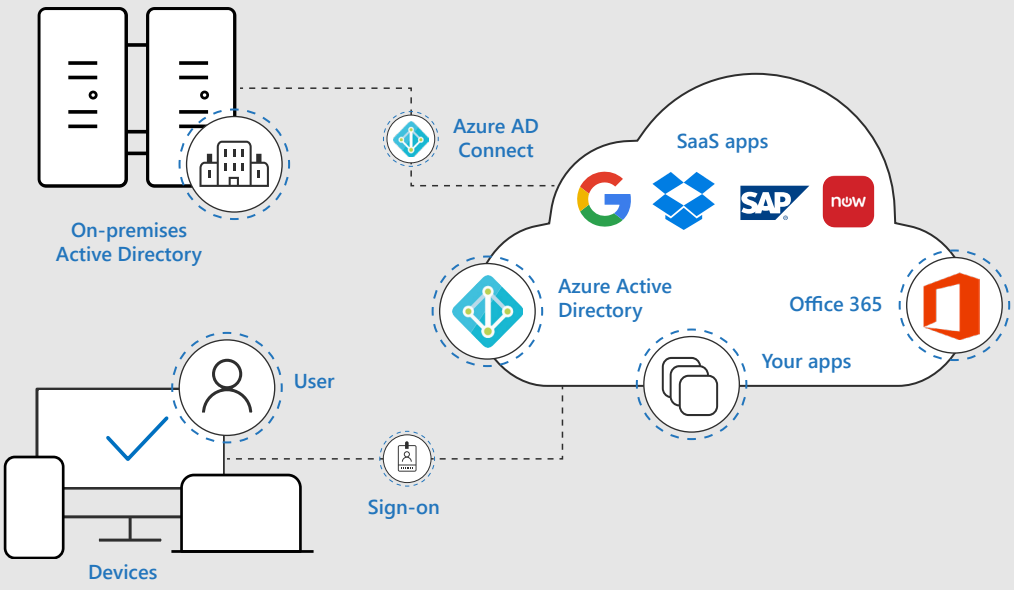

Figure 1. Through Azure AD Connect, you can integrate your on-premises directories with Azure Active Directory

For data protection and management, Azure Information Protection is a technology that uses encryption, identity, and authorization policies to assign classifications and labels to emails and documents, and other files that travel wherever they go. Data classification in Azure Information Protection helps you improve organizational understanding of risk.

Microsoft Intune provides device inventory information for all PCs or mobile devices enrolled. Microsoft System Center Configuration Manager (ConfigMgr) offers robust reporting for device inventory. Both Intune and ConfigMgr can provide a variety of information, including the status of security protection, apps installed, and operating system version. For further information on PCs, Windows Analytics offers you insights into the health of devices, computers, applications, and drivers at your organization.

For more visibility into cloud-based apps (SaaS apps) that are being accessed from your network, you can enable Cloud App Discovery through Microsoft Cloud App Security. This will help you identify Shadow IT and include third-party apps in your management and protection policies.

Start by managing identities in the cloud with Azure AD

Provision employee identities through Azure AD to implement single sign-on for all your employees to improve their experience. Azure AD Connect will help you integrate your on-premises directories with Azure Active Directory. This tool allows you to reduce the risk for Shadow IT, and allows you to begin the fundamental task of applying policies and access to each individual employee and groups of employees.

Business Environment

"The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions."

Every business environment is different. Your users and your organizational structure, mission, and leadership are unique. You know best how to manage security technology within your business environment.

Governance

"The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk."

Microsoft 365 security solutions include tools and resources to help you manage risk and meet regulatory, privacy, and operational (e.g., incident response) requirements.

For regulatory requirements, Microsoft has specific capabilities to help you along your path to compliance with whichever industry or governmental standard you need to achieve. Also, with data governance in Office 365, you can manage the full content lifecycle, from importing and storing data at the beginning to creating policies that retain and then permanently delete content at the end.

Microsoft 365 is built on a comprehensive framework of controls aimed at managing security and privacy risk. Compliance Manager, in the Microsoft Service Trust Portal, provides a rich set of capabilities to manage your compliance activities from one place, surfacing guidance about the controls in Office 365 that you must implement and test to meet the requirements of privacy standards.

For operational requirements, Microsoft 365 offers Windows Defender Advanced Threat Protection to help with endpoint threat detection and response. You can set up automated response actions on machines and files to quickly respond to detected attacks so that you can contain, reduce, and prevent further damage caused by malicious attackers in your organization.

Microsoft 365 also offers Office 365 Advanced Threat Protection to help protect your mailboxes, files, online storage, and applications against new, sophisticated attacks in real time.

In addition, Azure Advanced Threat Protection (ATP) monitors user, device, and resource behaviors; detects anomalies right away; and integrates with Windows Defender ATP and Office 365 ATP to provide you with the tools you need to manage and monitor your cybersecurity risk.

Risk Assessment

"The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals."

Capabilities in Microsoft 365 can help your organization understand cybersecurity risk related to your users, devices, apps, cloud services, and data through a variety of built-in tools and guidance.

Microsoft is committed to ensuring that our customers have visibility into the risk assessments for our cloud services and provides guidance on a number of risk assessments of Microsoft cloud services.

Microsoft 365 Secure Score provides you with better visibility and ways to improve your security posture through one single score. As you begin to understand and assess your risk position, we recommend reviewing your organization's specific score. Your score will show you how aligned you are with best security practices, allowing you to decide what action, if any, to take to improve your score. Microsoft 365 Secure Score provides risk assessment to understand your organization's top threats by showing you, through a Score Analyzer, which Microsoft 365 security features are enabled, how your score averages across other customers, and your score's history over time.

To assess risk within user identities, Azure Active Directory Identity Protection identifies weaknesses in your environment that can be exploited by an attacker. For example, Azure AD Identity Protection will alert you if multifactor identification is not configured for your organization, or if you have unmanaged cloud apps in your organization. Azure AD Identity Protection also lets you discover and resolve alerts about privileged identities in your organization.

Microsoft offers tips and tricks from leading IT pros for Active Directory risk assessment.

For risk visibility within devices, Windows Defender Advanced Threat Protection provides analysis on Windows device risk.

For operational requirements, you can perform a risk assessment to assess the compliance of Microsoft cloud services, including Azure, Microsoft Cloud App Security, Microsoft Dynamics 365, Intune, Office 365, and Microsoft Power BI. You can also review and assess the risk and compliance of third-party cloud apps in your environment by leveraging the risk score evaluation within the Discovered apps section of Microsoft Cloud App Security.

Risk Management Strategy

"The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions."

Using Microsoft 365 risk assessment capabilities will help you and your organization establish a risk management strategy.

Microsoft can help you execute this strategy as it pertains to your priorities, constraints, risk tolerances, and assumptions. Because security is an ongoing endeavor, Microsoft can help you decide on the fundamental steps that will have the most powerful and lasting effect.

Assess risk within user identities through Azure Active Directory Identity Protection

Azure Active Directory Identity Protection helps you assess potential vulnerabilities affecting your organization's identities, configure automated responses, and act on suspicious activities.

Start your risk management strategy planning with Microsoft 365 Secure Score

Secure Score looks at what Microsoft 365 security solutions you're using, analyzes your settings and activities, and compares them to a baseline established by Microsoft. You'll get a score based on how aligned your security measures are with security best practices so you can decide what action, if any, to take to improve your score.

Supply Chain Risk Management

"The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks."

A key example of supply chain risk management is Azure Active Directory business-to-business (B2B) collaboration, which enables any organization using Azure AD to work securely with users from any other organization, whether or not they use Azure AD.

Protect

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services

Identity Management and Access Control

"Access to assets and associated facilities is limited to authorized users, processes, and devices, and to authorized activities and transactions."

Your first safeguard against threats or attackers is to maintain strict, reliable, and appropriate access control. Your employees need to be able to reach the devices, apps, and data they need to be productive, balanced with the right level of access control. Too many permissions can expose vulnerabilities to attacks, and restrictions that are too cumbersome could compel your employees to circumvent your security.

Microsoft 365 security solutions include products that allow you to control access across devices, apps, and data.

Azure Active Directory conditional access (see Figure 2) is the identity security policy hub that offers you several ways to manage access control. Conditional access evaluates a set of configurable conditions, such as user, device, application, and risk.

User: conditional access can determine what groups the users are in and what location they are signing in from.

Device: conditional access evaluates the status of the device. For example, conditional access will determine whether the device is known to Azure AD, is running the latest operating system, has been jailbroken, or is running the latest antivirus software.

Applications: conditional access will evaluate apps to determine whether they contain sensitive data.

Risk: conditional access determines risk though the Microsoft Intelligent Security Graph, which uses machine learning across billions of authentications every day and analysis by cybersecurity experts to create a real-time risk score for each user and sign-in.

Based on these conditions, you can then set a variety of controls.

Route users directly into their applications without interruption (in low-risk scenarios).

Elevate permissions with multifactor authentication.

Require additional policies on devices by requiring devices to be enrolled in Intune before gaining access to data.

Block access to devices from unauthorized users (in severe situations).

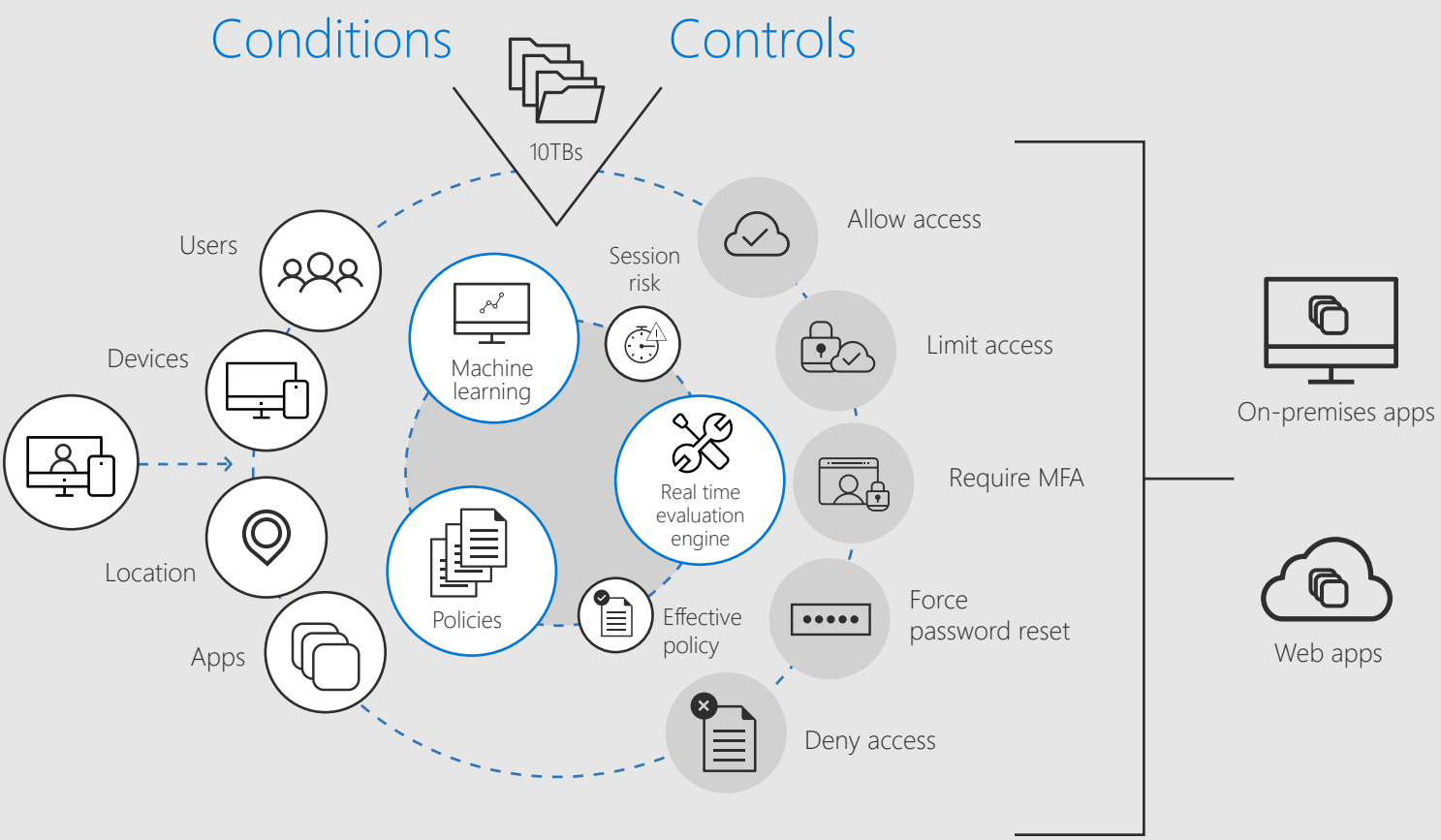

Figure 2. Azure Active Directory conditional access is the identity security policy hub

For access control on your networks, Windows Defender Firewall with Advanced Security blocks unauthorized network traffic from flowing into your local devices.

Maintain control by building conditional access policies

Conditional access is your organization's fundamental layer of protection. Through conditional access, you can apply conditions that grant access depending on a range of factors, such as location, device compliance, and employee need. In addition, conditional access is necessary to enabling multifactor authentication.

Awareness and Training

"The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities, consistent with related policies, procedures, and agreements."

Any security strategy is only as good as your user's ability to execute it. Microsoft 365 offers online resources to get your users up to speed quickly.

Since 2006, Microsoft has published a biannual global cybersecurity intelligence report known as the Microsoft Security Intelligence Report. The report offers up-to-date information about the latest cyberthreat trends and risks, plus practical recommendations on how to manage threats in your security environment. You can download the latest report and every volume prior at no cost.

Get the report: download the current volume of the Microsoft Security Intelligence Report.

Data Security

"*Information and records (data) are managed, consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.*"

Microsoft 365 security solutions can help enable data protection in accordance with your organization's risk strategy. Through Microsoft 365 security solutions, data is controlled and protected in the cloud, at rest, in storage locations, on devices, in use, and in transit.

Microsoft Information Protection capabilities (see Figure 3) use unique intelligence and an interoperating platform to help you identify, classify, protect, and monitor your data—regardless of where the data is stored or shared. Windows Information Protection helps protect business data on users' Windows 10 devices. Office 365 Information Protection, including Office 365 Data Loss Protection (DLP) and Advanced Data Governance, helps protect sensitive information across your Office 365 environment. Azure Information Protection extends beyond Office 365 to help protect sensitive information across on-premises, hybrid, and cloud services.

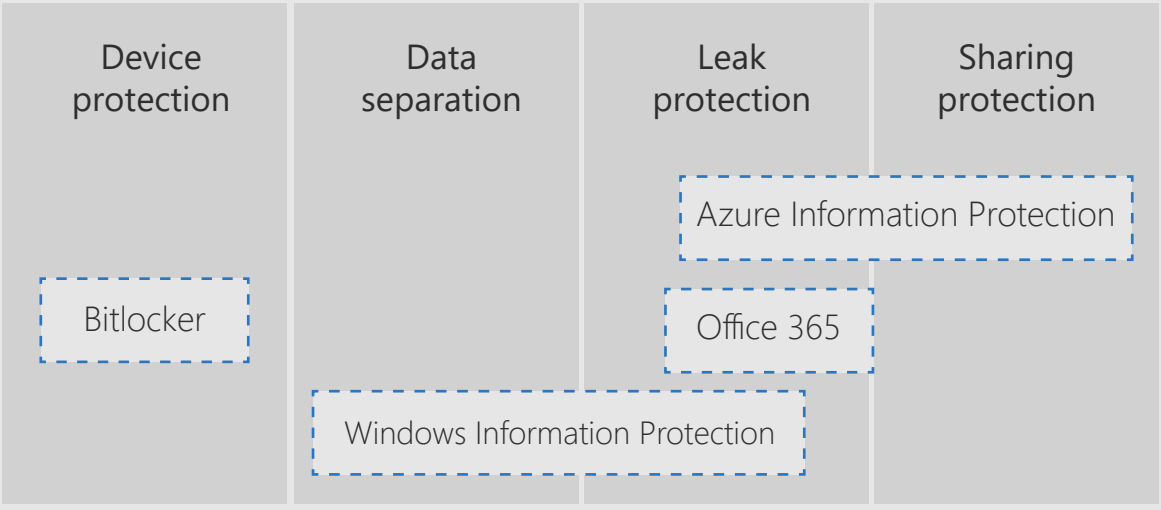

Figure 3. Microsoft Information Protection is an integrated platform that includes Windows Information Protection, Office 365 Information Protection, Azure Information Protection, and Bitlocker.

For data protection in cloud storage, enable Azure Storage Service Encryption for Data at Rest. When stored in Azure, your data can be automatically encrypted and then decrypted when you need it. The Azure Backup also provides data security.

Vulnerabilities identified and reported by Azure Active Directory Identity Protection include multifactor authentication registration not configured, unmanaged cloud apps, and security alerts from privileged identity management. We recommend that you address these vulnerabilities to improve the security posture of your organization and to prevent attackers from exploiting them. Azure AD Identity Protection will flag these issues and recommend mitigation strategies.

Microsoft Enterprise Cloud Red Teaming simulates real-world breaches, conducts continuous security monitoring, and practices security incident response to validate and improve the security of Microsoft Azure and Office 365.

Securing business partners that perform maintenance is key. Azure Active Directory B2B collaboration capabilities (see Figure 4) enable any organization using Azure Active Directory to work safely and securely with users from any other organization while maintaining complete control over their own corporate data.

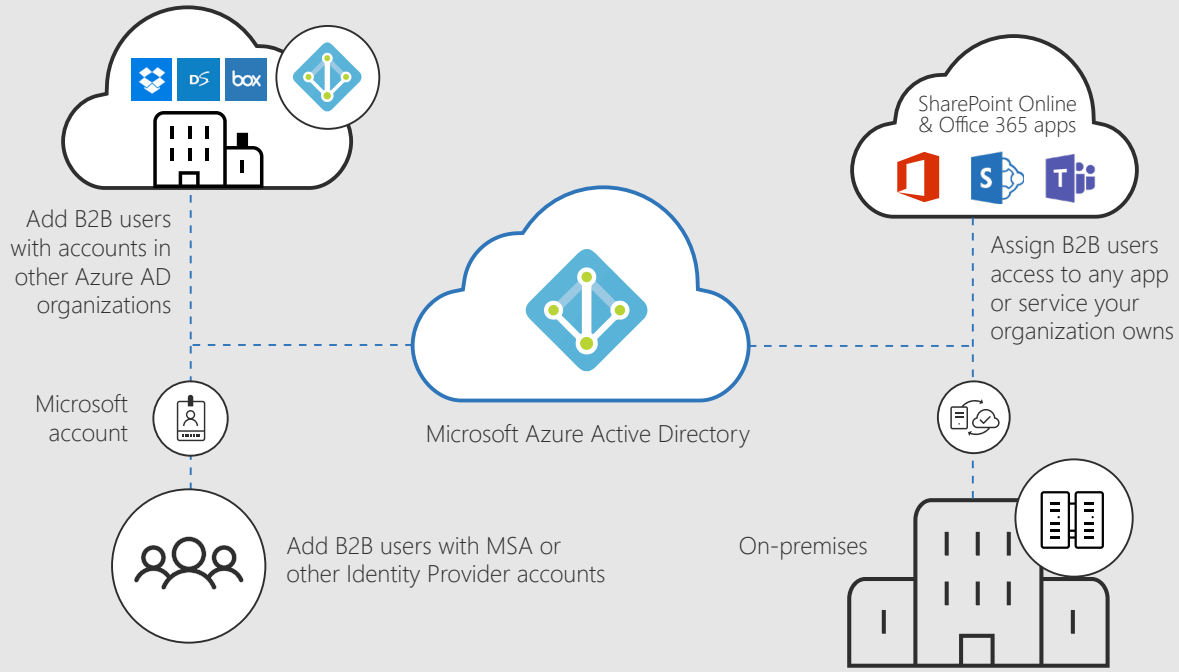

Figure 4. Azure AD B2B collaboration enables organizations using Azure AD to work securely with users from other organizations while maintaining control over their own corporate data.

Protective Technology

"Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements."

Microsoft Information Protection enables you to build an integrated security environment.

This effort can start by protecting business data at the device level. In Windows 10, you can better protect data against unauthorized access when a device is lost or stolen via Microsoft BitLocker and also protect against accidental data leaks between business and nonbusiness applications running on the device using Windows Information Protection. This protection is designed to work on both company-owned and personal devices that employees use for work, without requiring changes to your environment or other apps. Through Windows Information Protection, you can determine which apps can access business versus nonbusiness information and control what your employees can do with corporate data.

For non–Windows 10 devices, Intune App Protection extends the same level of protection to iOS and Android devices. For example, all copy-and-paste functions can be restricted from unknown sources, and remote wipe of sensitive data can be performed on devices to help prevent unauthorized mingling of personal and business data.

Beyond the device, Microsoft cloud services provide baseline protection in the form of encryption of data at rest and in transit. Microsoft Information Protection capabilities provide additional levels of protection. For example, you can easily apply extra protection for data that is stored or in transit, such as when an email attachment is sent from Outlook and is enabled with rights managements and permissions.

Through Azure Information Protection, data can be encrypted with permissions for rightful recipients and visual markings, such as watermarks can be added to remind users that the document contains sensitive information. Azure Information Protection enables you to log every request to it, including when users protect and consume documents and email. You can use these logs to analyze for business insights, monitor for abuse, and perform forensic analysis.

Protective technology at the identity and access management layer includes Azure Active Directory, which helps protect and control access to applications according to conditions of the user, device, or app.

Conditional access powered by the Microsoft Intelligent Security Graph (ISG) (see Figure 5) leverages machine learning against the billions of authentications Microsoft provides every day. The ISG provides: 1) vast threat intelligence gathered through millions of threat reports aggregated from systems around the world; 2) advanced analytics culled through machine learning and artificial intelligence from millions of signals; and 3) insights shared from customers and partners with a security API. The ISG also detects and remediates phishing attempts and identifies and blocks malicious content from entering your system. The ISG is constantly evolving to provide the most current protection and actionable insights, and serves as the backbone of your protective technology.

Another way to better protect your data in the cloud is through Microsoft Cloud App Security. You can investigate existing data in your cloud apps and take corrective action, for example, by labeling files as confidential or removing external sharing. Additionally, you can leverage Conditional Access App Control for real-time monitoring and control of users' actions across your cloud apps.

Use the tools in Microsoft Cloud App Security to gain a deeper understanding of what's happening in your cloud environment across Microsoft native and third-party cloud apps. Then, based on your environment, you can identify requirements for protecting your organization using consolidated dashboards that provide an overview of users, files, activities, required actions, app

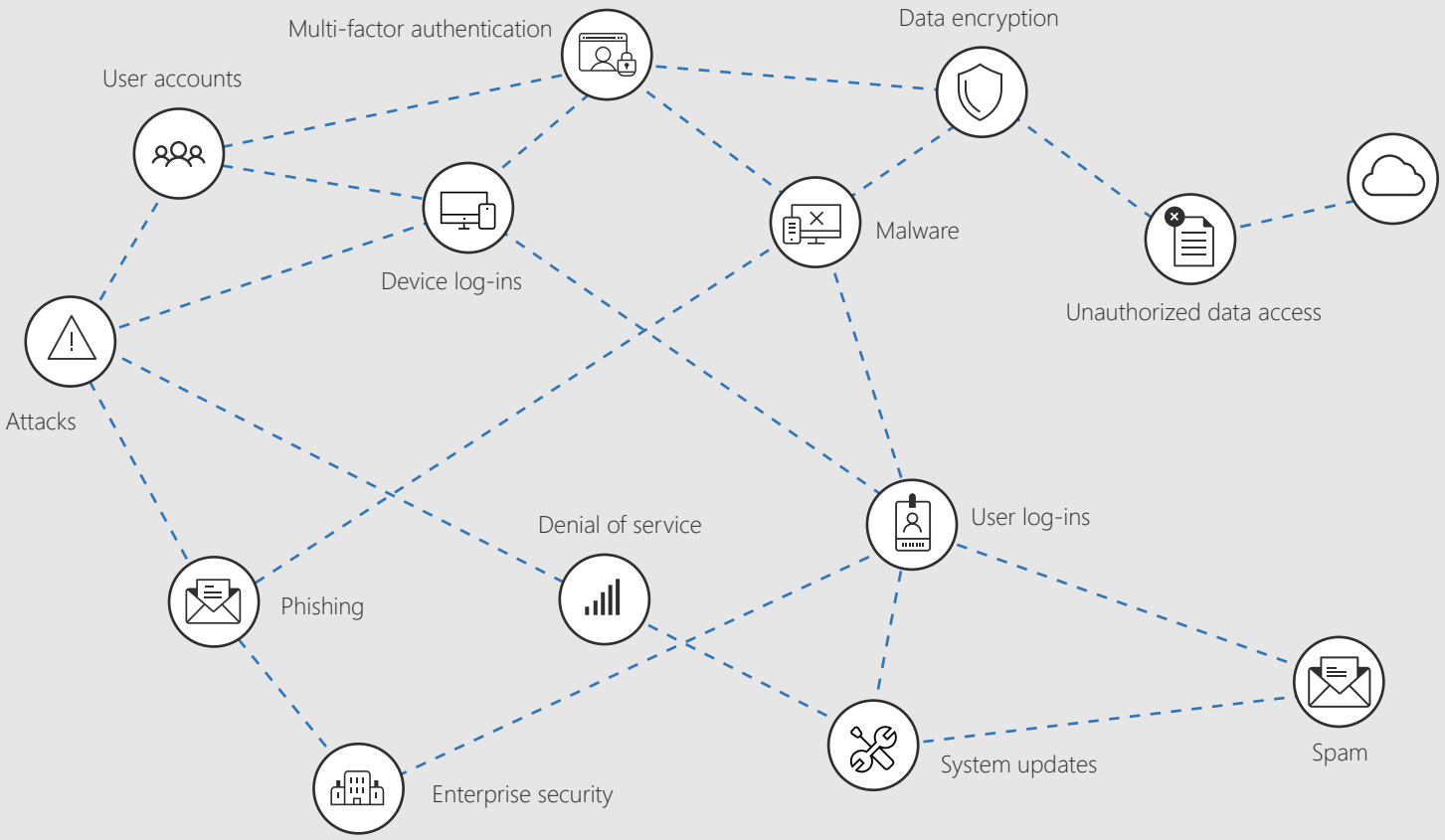

Figure 5. Microsoft Intelligent Security Graph leverages machine learning against the billions of authentications Microsoft provides every day.

Discover cloud apps with Microsoft Cloud App Security and protect shared information

Enable Cloud App Discovery to map and identify your cloud environment and the cloud apps that your organization is using. Find out what Shadow IT your employees are using in your system that may leave your company vulnerable. Derive valuable insights into what security you need and how to engender collaboration and productivity from the workloads you can discover in Cloud App Discovery.

In Office 365, you can use data governance and DLP capabilities to identify personally identifiable information (PII), financial, health, and other sensitive data across Microsoft SharePoint Online, OneDrive for Business, and Exchange Online, and in the Office client applications like Word, PowerPoint, Excel, and Outlook.

Beyond Office 365, you can use Azure Information Protection to gain visibility into sensitive data that lives in other SaaS applications, on-premises file servers, and network shares. Azure Information Protection offers you the flexibility to choose how your encryption keys are managed, including Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) options.

For data protection on devices, Windows Information Protection includes the functionality necessary to identify personal and business information, determine which apps have access to it, and provide the basic controls necessary to determine what users are able to do with business data (e.g., copy-and-paste restrictions).

Data protection on mobile devices (like iOS and Android) comes from Microsoft Intune, which can encrypt data on mobile devices and better protect data while being used within the Office 365 mobile apps and any other app integrated to its software development kit (SDK). Through Intune App Protection (see Figure 6), you can set policies to separate business data from personal data. For example, a policy can be configured to label all files downloaded from the organization's SharePoint site as "Business."

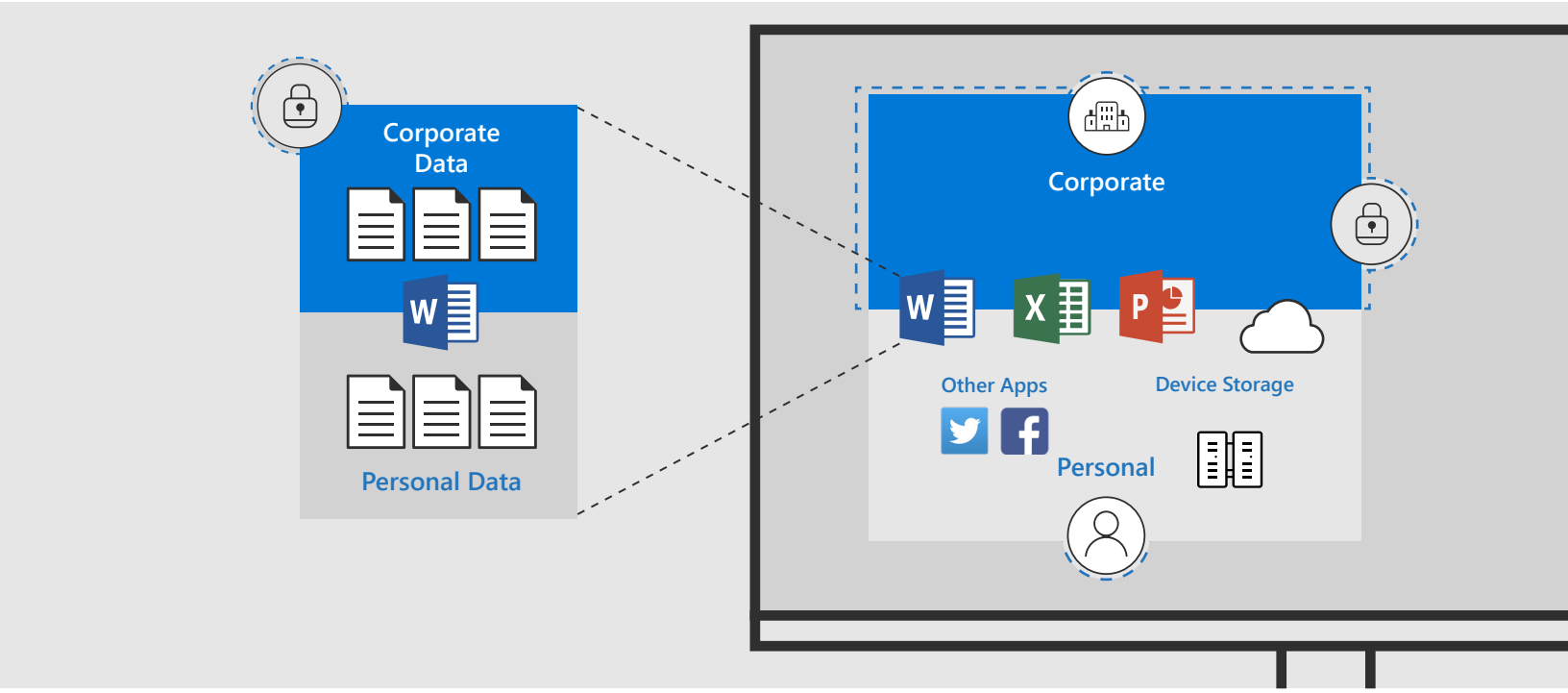

Figure 6. Intune App Protection allows you to set policies to separate business data from personal data.

In addition to separating personal data from business data on the device, you can further identify data as it is issued in different apps, such as Office mobile apps like Word, PowerPoint, Excel, and Outlook. This enables more granular identification beyond business versus personal.

Through a conditional access policy, Intune can revoke access to data for devices that don't meet compliance standards. Additionally, Office 365 can apply encryption to files and email as they are used within the Office mobile apps.

Deploy Intune App Protection to protect corporate data on devices and apps

Whether your employees use company-owned devices or bring their own, Intune can help you keep your employees mobile, compliant, and secure.

Protect your information with Windows Information Protection and Azure Information Protection

Improve information protection through access control, classification, and protection that extends to shared documents and external stakeholders with Windows Information Protection and Azure Information Protection.

Information Protection Processes and Procedures

"Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets."

Defining the security policies, processes, and procedures is an important step you will need to take to maintain the security management of your organization.

Maintenance

"Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures."

To better protect your organization from threats and data breaches, you must pay attention to the vulnerabilities that may not be visible during maintenance and repairs of industrial control and information system components, such as devices and servers. Performing these maintenance and repairs securely and consistent with policies and procedures will protect organizational users, devices, apps, and data. Microsoft 365 can help you mitigate the potential threats.

Detect

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event

Anomalies and Events

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Many common types of threats target three key attack vectors: devices, email, and identity credentials. Microsoft 365 has capabilities to detect attacks across these three attack areas.

Microsoft 365 security solutions offer advanced threat protection, security and audit log management, and application whitelisting to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Microsoft helps to secure at several layers: identity and access management, information protection, and protection from advanced threats.

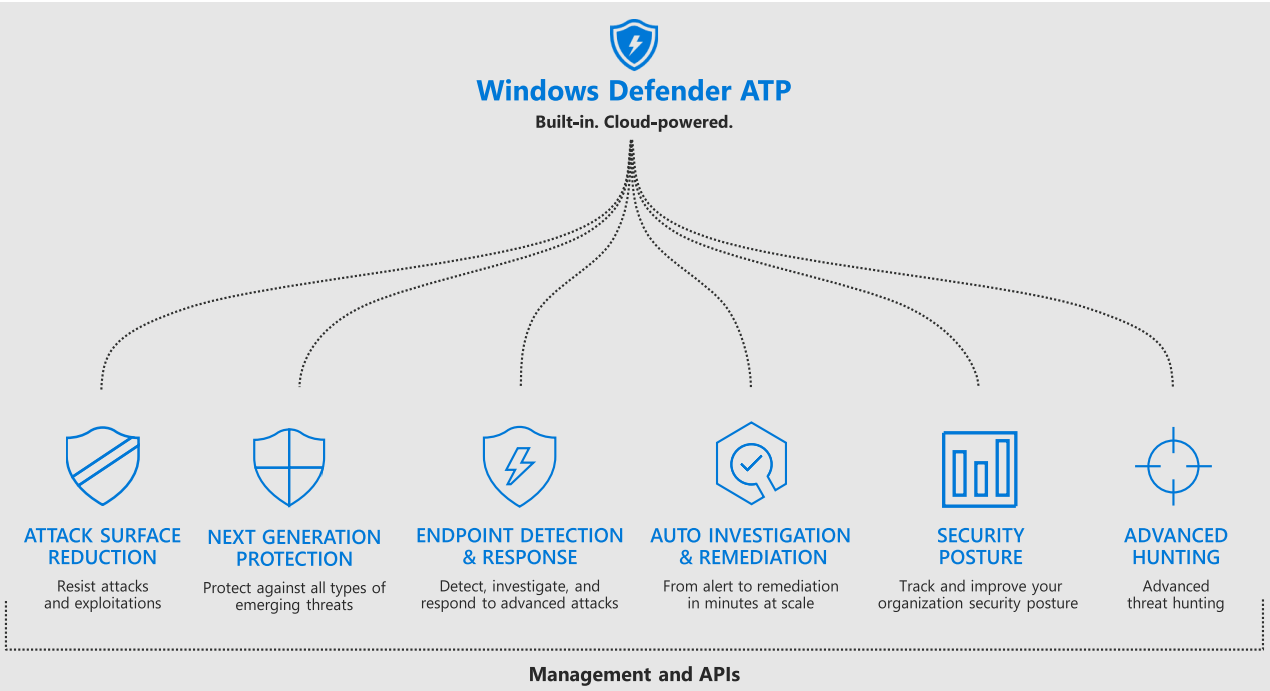

Figure 7. Windows Defender Advanced Threat Protection provides near-instant detection and blocking of new and emerging threats.

For device-based attacks, Windows Defender Advanced Threat Protection (see Figure 7) provides near-instant detection and blocking of new and emerging threats using advanced file and process behavior monitoring and other heuristics (also known as real-time protection). These endpoint behavioral sensors collect and process behavioral signals from the operating system, which are then translated into insights, detections, and recommended responses to advanced threats. Windows Defender ATP offers dedicated protection updates based on machine-learning, human and automated big-data analysis, and in-depth threat resistance research to identify attacker tools, techniques, and procedures and to generate alerts when these are observed in collected sensor data.

For email-based attacks, Office 365 ATP helps protect your emails, attachments, online storage, files, and environment through a variety of technology, including Safe Attachments, Exchange Online Protection, and rich reporting and tracking insights.

For identity credential attacks, Azure Active Directory detects six different risk events, detecting users with leaked credentials and sign-ins from anonymous IP addresses, impossible travel to atypical locations, infected devices, IP addresses with suspicious activity, and unfamiliar locations. You can also configure Azure Active Directory's Privileged Identity Management (PIM) to generate alerts when there is suspicious or unsafe activity in your environment, such as roles being assigned outside of PIM or activated too frequently.

Azure ATP detects multiple suspicious activities, focusing on several phases of the cyberattack kill chain. It can detect reconnaissance work, during which attackers gather information on how the environment is built, what the different assets are, and which entities exist. ATP also detects lateral movement cycles, during which attackers invest time and effort in spreading their attack surface inside your network. In addition, Azure ATP detects domain dominance (persistence), during which attackers capture the information—allowing them to resume their campaign using various sets of entry points, credentials, and techniques.

These services that protect specific parts of the attack surface can also share signals to alert services protecting other surfaces of the enterprise.

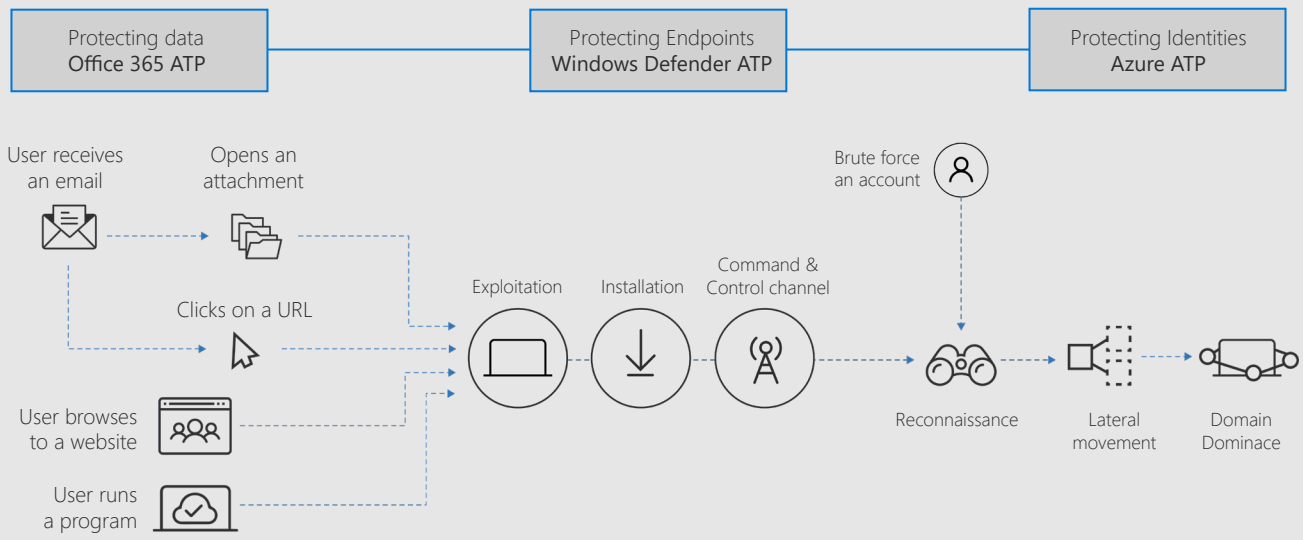

Figure 8. Threat detection integrated across Microsoft 365

For protection from advanced threats, Device Guard can help you protect business-critical machines against malware and other unwanted software. It includes a new app and software whitelisting technology that, along with Microsoft AppLocker, will give you greater control of what can run in your environment. Thanks to Managed Installer, complex, difficult-to-maintain software catalogs are much simpler to maintain.

Detect suspicious and unsafe activity through Advanced Threat Protection

Office 365 ATP, Windows Defender ATP, and Azure ATP offer holistic and ongoing protection continuously across your business apps, devices, and operating systems (see Figure 8).

Security Continuous Monitoring

"The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures."

Microsoft 365 security solutions offer continuous monitoring, threat detection, vulnerability assessment, and event logging. We make sure you have the right information to find problems and verify that you have your policies in place, whether through a front door, advanced persistent threats, or tracking.

Microsoft Cloud App Security anomaly detection policies provide out-of-the-box user and entity behavioral analytics and machine learning so that you can detect threats by identifying anomalous behavior across your environment of cloud apps. In addition, Microsoft Cloud App Security monitors user behavior across apps by allowing you to detect and take corrective action. For example, if an employee's Azure AD account has been deprovisioned, but that employee continues to access other corporate resources that weren't connected to Azure AD, an alert is triggered in the MCAS console. Another option is to configure automatic governance actions in the policy.

Office 365 ATP offers holistic and ongoing protection contiguously across your business apps in Microsoft Teams, Word, Excel, PowerPoint, Visio, SharePoint Online, and OneDrive for Business. Attack Simulator, a component of Office 365 Security and Compliance, lets you run realistic attack scenarios in your organization so you can identify vulnerable users before a real attack occurs. Attack Simulator lets you run display name spear-phishing attacks, password-spray attacks, and brute-force password attacks. Find out how your users would behave in an attack, and update policies to ensure that the right security tools are in place to protect your organization from threats—before they happen.

Windows Defender ATP offers greater visibility and management of alerts. The Alerts queue shows a list of alerts that are flagged from machines in your network. Alerts are displayed in queues according to their current status. Sort and filter alerts according to their severity so you never miss a significant threat but are not bogged down by constant alarms.

Azure ATP continuously monitors networks and users' behavior for suspicious activities while scanning and logging attack methods for forensic analysis.

Intune device monitoring helps you to maintain compliance on all your organization's enrolled devices at all times. From the Intune dashboard, you can see the overall compliance state of devices, the compliance state for an individual setting, and the compliance state for an individual policy. You can even drill down into individual devices to view specific settings and policies that affect the device.

Azure AD Privileged Identity Management lets you monitor access to resources within your organization so you can minimize and manage the number of people who have access to secure information or resources. Continually monitoring these high-access points limits vulnerabilities at a top level.

Detection Processes

"Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events."

Although the detection process is something you will be in charge of for your organization, Microsoft takes actions that help secure you.

To help combat emerging threats, Microsoft employs an innovative Assume Breach strategy and leverages highly specialized groups of security experts, known as the Red Team, to strengthen threat detection, response, and defense for its enterprise cloud services.

Microsoft Cloud App Security includes several predefined anomaly detection policies (out of the box) that include user and entity behavioral analytics and machine learning.

Respond

Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events

Response Planning

"Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events."

Microsoft 365 security solutions can help you plan your response to a threat, event, or security incident based on a variety of visibility reports and insights. Microsoft works continuously to provide highly secure, enterprise-grade services for Office 365 customers. Microsoft's goals when responding to security incidents are to protect customer data and the Office 365 services.

Use Azure AD Access and Usage reports to view and assess the integrity and security of your organization's implementation of Azure AD. With this information, you can better determine where possible security risks may lie and adequately plan to mitigate those risks.

Communications

"Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies."

Educate your employees on security

Whatever security tools you deploy to protect your company won't be effective if your employees don't use them properly or regularly, or if they work around them. Make sure all employees in your organization are aware of security threats and their role in protecting company assets.

Analysis

"Analysis is conducted to ensure adequate response and support recovery activities."

Microsoft offers guidance and education on Windows security and forensics to give organizations the ability to investigate cybercriminal activity and more effectively respond and recover from malware incidents.

Azure Advanced Threat Protection is designed to reduce the noise from alerts and provides only relevant and important suspicious activities with a simple, real-time view of the attack timeline. This tool allows you to focus on what matters, leveraging the intelligence provided by our analytics. Azure ATP integrates detection and exploration with Windows Defender ATP to provide additional layers of security at the device level.

Mitigation

"Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident."

Microsoft 365 security solutions provide tools to help with incident response as part of an organization's risk mitigation strategy, including in-depth guides to respond to security IT incidents, whitepapers on how Microsoft responds to security incidents in Office 365, and built-in reports.

For example, Azure AD offers built-in reports that can be used during incident response and mitigation, including anomaly reports, integrated application reports, error reports, user-specific reports, and activity logs that contain a record of all audited events within the last 24 hours, last 7 days, or last 30 days.

With Windows Defender ATP, you can take response actions on machines and files to quickly respond to detected attacks so that you can contain or reduce and prevent further damage caused by malicious attackers in your organization.

Assemble your Core Computer Security Incident Response Team (CSIRT)

Define a team of people who are responsible for dealing with a security incident. Team members should have clearly defined duties and roles, and should be prepared on critical security tools. Learn more about CSIRT.

Improvements

"Organizational response activities are improved by incorporating lessons learned from current and previous detection and response activities."

Using Microsoft 365 extensive reporting, logging, and insights, you'll be responsible for determining and implementing any improvements to your security endeavors. Remember that security is an ongoing and constantly changing process, and that your efforts are only as effective as your employees will allow it to be.

Get Started Securing Your Organization with Microsoft 365

Microsoft engineers who have worked with countless companies around the world know that securing your organization is not necessarily sequential. Your security efforts should look more like a cycle, and each cycle should be maximized for the best value. The first rotation is your fundamental action. The next rotation builds from that first, fundamental action, layering, connecting, and strengthening your actions as you cycle through subsequent rotations.

Throughout this document we've called out some fundamental actions to get you started securing your organization through Microsoft 365. Each organization is different and will need different security efforts, and you'll have to determine where your company will start. You may have more vulnerabilities in one area than the others. That said, each of the core functions of the NIST CSF includes layers of security, from the fundamental to the complex, and so should your organization.

For more information and resources about Microsoft 365 security solutions, visit the Microsoft Secure blog and check out the Top 10 Security Deployment Actions with Microsoft 365 infographic.

Plan for Success with FastTrack

Whether you're planning your initial rollout, need to onboard your product, or want to drive end-user adoption, FastTrack is your benefit service and is ready to assist you. Get started at FastTrack for Microsoft 365.

To learn more about FastTrack, please read our FastTrack white paper, which describes, in detail, the process and benefits of Microsoft FastTrack for your business. To find out if you are eligible for FastTrack, visit aka.ms/fasttrackeligiblility.

Top 10 Security Deployment Actions with Microsoft 365

Microsoft