Microsoft

# Discover threats quickly, remediate immediately, and mitigate the impact of malware and breaches

## Introduction

No matter how hard you work to educate your employees about the constant and evolving threats to your company, even the most conscientious employee may unknowingly open infected files or click on malicious web links. Security breaches are inevitable. The best strategy includes securing across all attack vectors and putting policies into place for reviews and change management within your organization. Microsoft 365 offers security solutions that address these attack vectors and will enable you to discover, analyze, and neutralize threats before they cause harm.

Many common types of threats target these key attack vectors: devices, email, network, and user credentials. Microsoft 365 integrates threat detection across these attack vectors by ensuring that the security and resilience of systems and assets are aligned with related policies, procedures, and agreements (see Figure 1).

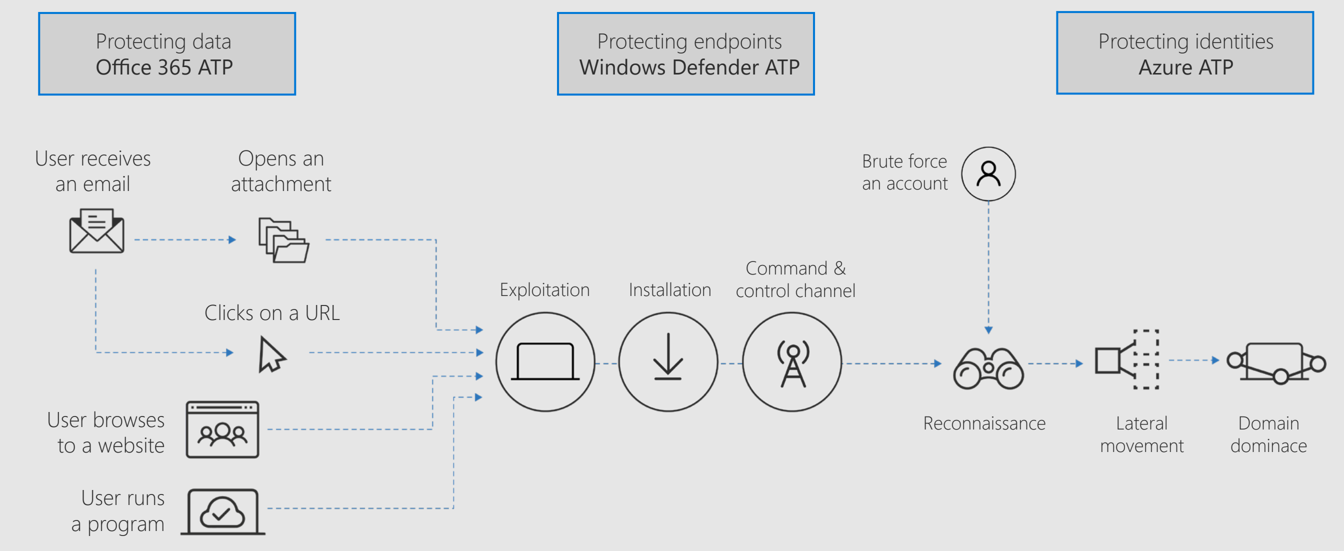

*Figure 1. Threat detection integrated across Microsoft 365.*

## Windows Defender Advanced Threat Protection (Windows Defender ATP)

For endpoint attacks, Windows Defender ATP provides near-instant detection and blocking of new and emerging threats using advanced file and process behavior monitoring and other heuristic solutions. These endpoint 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 analyses, 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.  Windows Defender ATP is built in to Windows 10, providing deeper optics and cloud-powered protection.

Microsoft Device Guard is a feature of Windows 10 that provides increased security against malware and zero-day attacks by blocking anything other than trusted apps. Device Guard is managed in Microsoft System Center Configuration Manager (ConfigMgr).

## Microsoft Office 365 Advanced Threat Protection (Office 365 ATP)

Threat protection for Office 365 begins with Microsoft Exchange Online Protection which provides protection against all known malicious links and malware. Office 365 ATP builds on this protection by offering holistic and ongoing protection across your Office 365 environment, including email and business apps such as Microsoft Teams, Word, Excel, PowerPoint, Visio, SharePoint Online, and OneDrive for Business. Office 365 ATP allows you to secure your user mailboxes, business-critical files, and online storage against malware campaigns in real time with its Safe Attachments and Safe Links features. Office 365 ATP Safe Attachments helps protect against unsafe attachments by preventing them from affecting your messaging environment. All suspicious content goes through real-time behavioral malware analysis that uses machine-learning techniques to evaluate the content for suspicious activity. Unsafe attachments are removed before being sent to recipients. The result is a malware-free inbox with better zero-day attack protection.

Office 365 ATP Safe Links supports protecting your environment offering by “time-of-click” protection from malicious links. If a link is unsafe, the user is warned not to visit the site or informed that the site has been blocked. Reporting and message trace in Exchange Online Protection allow you to investigate messages that have been blocked because of viruses or malware, while the URL trace capability allows you to track individual malicious links in the messages that have been clicked. Office 365 ATP and Exchange Online Protection can be configured in the Office 365 admin center.

Office 365 Threat Intelligence is a repository of threat intelligence data and systems that can spot suspicious patterns, behaviors, and activity. Office 365 Threat Intelligence gathers information from email and other sources. You can then use this data to understand and remediate threats against both your employee and your organization. Office 365 Threat Intelligence lives in the Office 365 Security and Compliance Center.  Attack Simulator, a component of Office 365 Threat Intelligence, lets you run realistic attack scenarios in your organization so you can identify and find vulnerable users before a real attack occurs. You can find out how your users would behave in an attack, and then update policies to ensure that the right security tools are in place to help protect your organization from threats before they happen.

## Azure Advanced Threat Protection (Azure ATP)

Azure ATP provides end-to-end network security by helping to protect user identities and credentials stored in Active Directory. To help prevent identity credential attacks, Azure Active Directory (Azure AD) detects risk events, such as users with leaked credentials, sign-ins from anonymous IP addresses, impossible travel to atypical locations, infected devices, and IP addresses with suspicious activity or unfamiliar locations.

Azure ATP detects suspicious activities across the network attack surface, such as:

- Reconnaissance work, during which attackers gather information on how the environment is built, what the different assets are, and which entities exist.
- Lateral movement cycles, during which attackers invest time and effort in spreading their attack deeper inside your network.
- 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 that help protect other surfaces of the enterprise.

Azure ATP detects these suspicious activities and surfaces the information, including a clear view of who, what, when and how, in the Azure ATP workspace portal which can be accessed by signing in to your Azure AD user account.

## Azure AD Identity Protection

Azure AD Identity Protection provides an overview of risk and vulnerabilities that may be affecting your organization’s identities. Azure AD Identity Protection uses existing Azure AD anomaly detection capabilities available through Azure AD anomalous activity reports. You can enable Azure AD Identity Protection through the Azure portal.  Azure AD Identity Protection helps you identify the risk level of a particular user. Through Azure AD Identity Protection, you can set up risk-based conditional access policies to automatically mitigate threats and secure corporate or organizational resources and data. Risk-based conditional access gets rich signals from the Microsoft Intelligent Security Graph and then converts them to actionable risk-based policies that you can apply to your organization.

Vulnerabilities identified and reported by Azure AD Identity Protection include non-configured multi-factor authentication registration, 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 prevent attackers from exploiting them. Azure AD Identity Protection will flag these issues and recommend mitigation strategies.

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

You can configure Azure AD PIM in the Azure portal to generate alerts when there is suspicious or unsafe activity in your environment, such as roles being assigned outside of Azure AD PIM or are activated too frequently.

## Microsoft Cloud App Security

Microsoft Cloud App Security gives you greater visibility and control over your enterprise app ecosystem, including all Microsoft applications and applications that are beyond the Microsoft ecosystem through threat detection, enhanced security and policy controls, and deeper discovery and insights.

Microsoft Cloud App Security lets you set up alerts based on anomaly detection policies so that you know about threats immediately. Anomaly detection works by scanning user activities and evaluating their risk against more than 70 different indicators such as sign-in failures, administrator activities, and inactive accounts. You can also set up customizable activity policies to track specific activities and flag you if something is out of the ordinary, like a huge download or multiple sign-on attempts.

Manage Microsoft Cloud App Security through an app dashboard that lets you see your organization's and employees' app usage, like how much data is being sent to OneDrive for Business, Box, Dropbox, and other cloud storage apps.

You can set your Cloud App Security policies in the Cloud App Security portal or through the Microsoft 365 Security and Compliance Center. On the Cloud App Security policy page, you can create activity policies and apply severity levels that can be used to filter your alerts later. You can also determine what action to take when one of your policies triggers an alert.

## Microsoft Secure Score

Microsoft Secure Score provides a quantifiable way to measure your security posture and track improvements over time. It also provides recommended actions to improve your score that include helpful links to learn more or configure the recommended feature. In addition, Microsoft Secure Score expands your visibility into the overall security posture of your organization. From the dashboard, you'll be able to quickly assess the security posture of your organization and obtain recommendations for actions to further reduce the attack surface in your organization—all in one place. From there, you can act according to the recommended configuration baselines.

# Deployment tips from our experts

## Consider the key attack vectors

Devices, email, network, and identity credentials are the most common areas for a cybersecurity attacks. To help secure these vectors:

- Protection for identities – Enable Azure AD Identity Protection through the Azure portal to identify the risk level of a particular user and to set up risk-based conditional access policies.

- Protecton for email – Configure Office 365 ATP and Exchange Online Protection in the Office 365 admin center to protect against malicious links and phishing attacks.

- Protection for endpoints – Set up the endpoints in your organization so that Windows Defender ATP, which is built-in to Windows 10, can get sensor data from them. You do this by onboarding your endpoints to the service and by configuring the individual security controls.

## Monitor shadow IT with Microsoft Cloud App Security

The chances are that your employees have used outside technology to do work. That unsanctioned technology, or shadow IT, can leave your organization vulnerable. Deploy Microsoft 365 Cloud App Security to see where your cloud vulnerabilities are and understand where your employees are circumventing your organization's sanctioned IT.

## Know your security position

Use Microsoft Secure Score to measure your security posture, learn recommended actions to improve your security position, and track improvements over time.

## Plan for success with Microsoft FastTrack

FastTrack comes with your subscription at no additional charge. Whether you're planning your initial rollout, needing to onboard your product, or driving end-user adoption, FastTrack is your benefit service that is ready to assist you.

Get started at FastTrack for Microsoft 365.

Microsoft