
Microsoft
Defend your digital landscape
Respond to security breaches before they cause major damage

A security breach is inevitable

Combine prevention with strong incident response capabilities

A security breach is inevitable and often starts with a successful phish attempt against an unsuspecting employee. Once the attackers gain access to that employee's credentials, they can remain hidden in an organization's infrastructure for weeks, maybe months—watching, waiting, and learning. Then, they move laterally until they compromise a privileged account, establish domain dominance, and exfiltrate sensitive data from the organization's apps, devices, and cloud storage.

Modern digital estates are vast and highly variant: a dream for attackers. The attack surface is huge, and the number of attack vectors continues to grow. Prevention is ideal, but modern security frameworks encourage a layered defense-in-depth strategy that operates under an assumption of compromise. In the past, securing the perimeter was enough to secure the network. Bring your own device (BYOD) adoption and the explosion of mobile devices and virtual private networks (VPN) have made the perimeter a thin veil that can't always keep intruders out of the network. By assuming that attackers could have compromised the network, security operations (SecOps) teams can focus on strategies and tools to expose them quickly, while limiting their ability to steal data or cause harm. Detection relies on alerts, but, without context, each alert is just one of thousands that SecOps receives every day. To know which alerts to prioritize, SecOps needs threat protection tools that can combine related alerts into an incident that the team can address.

Enterprises need security that detects, responds to, and recovers from these threats—fast—to prevent attacks from damaging their business. Microsoft 365 Enterprise E5 threat protection products work well as standalone products, but they were purpose-built to work together to ease the burden on SecOps teams. The Microsoft 365 Enterprise E5 threat protection products share security signals and correlate alerts across all products into an attack timeline and automate many aspects of the investigation and remediation processes. As a result, teams are free to focus on more complex and interesting security challenges.

76% of breaches were financially motivated.[1]

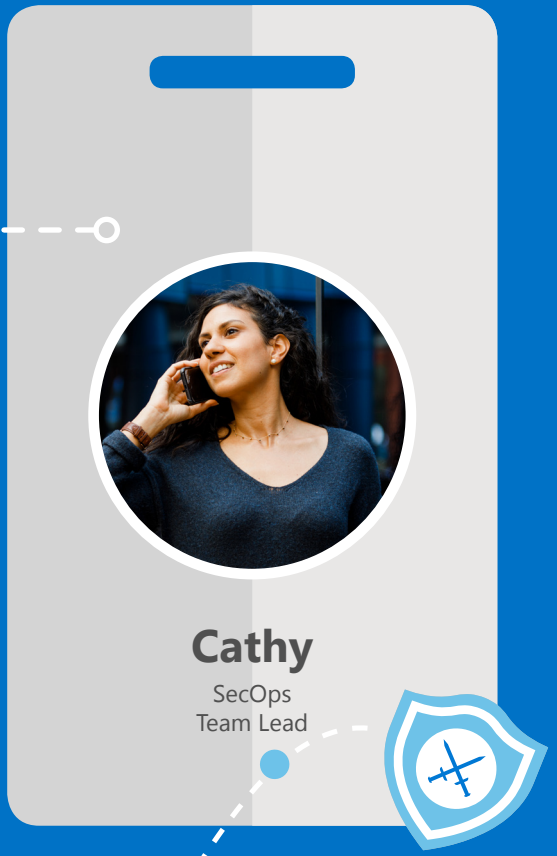
20% of attacks were motivated by espionage.[1]

[1] 2018 Verizon Data Breach Report

Quickly detect, respond to, and recover from a breach

Meet Cathy

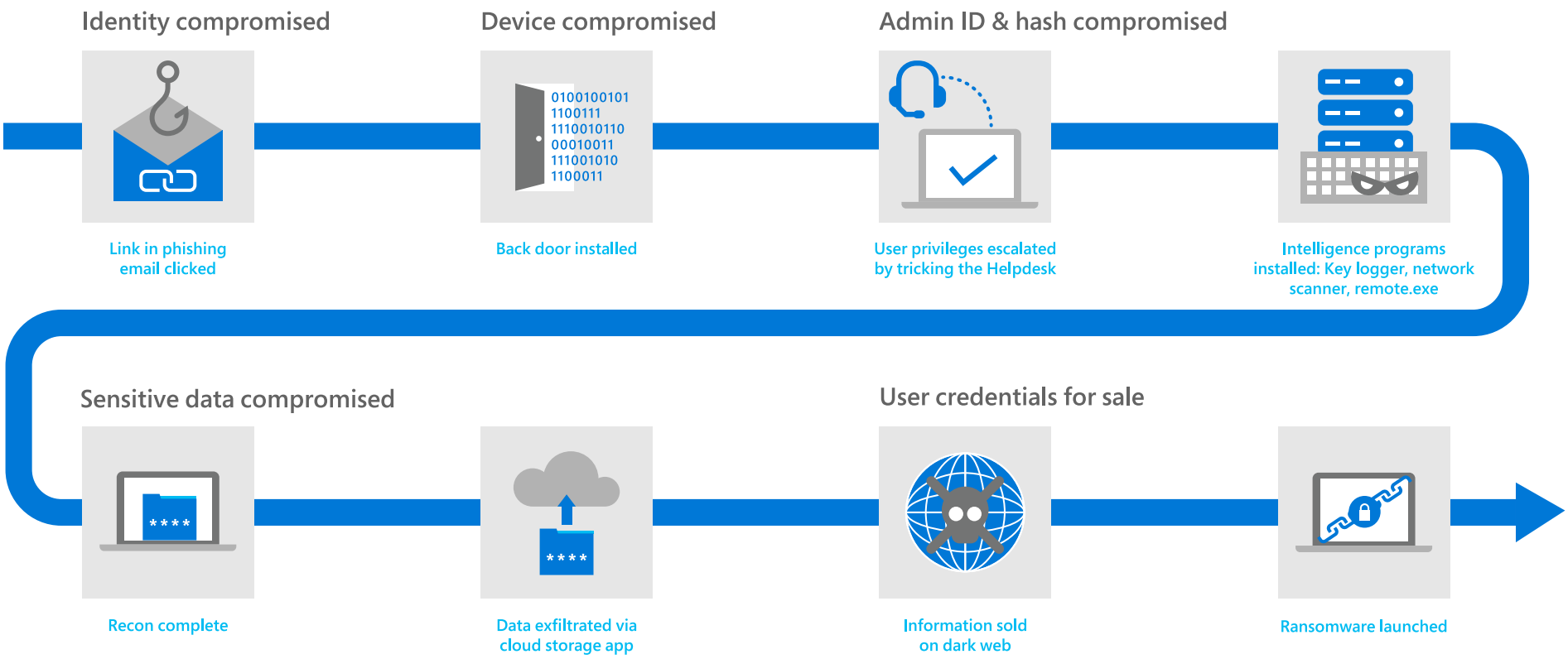
Cathy is the lead on Contoso's SecOps team. The help desk sent Enzo, one of the company's top sales reps, to Cathy because he discovered ransomware on his computer. Cathy has tried to get rid of the malware, but the company ultimately paid the ransom to get the sensitive files back. The team's investigation revealed that the attack started with a phishing email sent to Enzo, and the attackers then lingered in the network for 52 days. Cathy's team needs to figure out what was compromised, who was affected, how to recover from the attack, and how to prevent a similar attack in the future.



A breach is inevitable. How can Microsoft help Cathy detect it and respond fast to limit the damage?

All characters are fictitious.

ATTACK TIMELINE

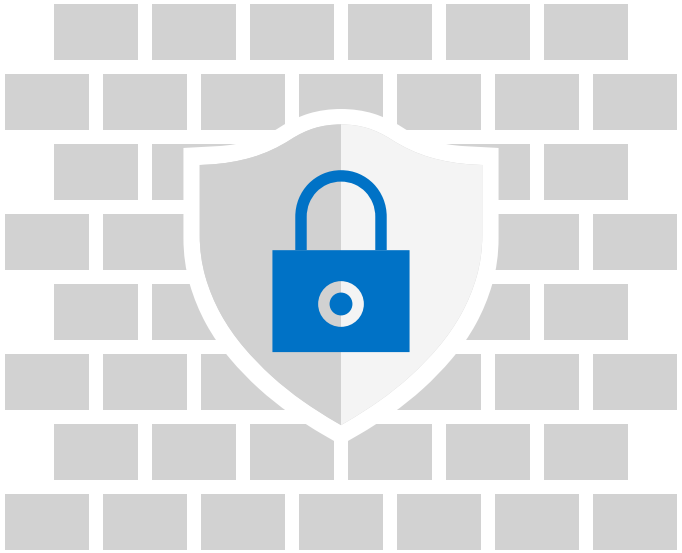


The attacker remained undetected for 52 days before executing the ransomware.

Prevent security threats from breaching your defenses

SCENARIO

The attack on Enzo's computer was the reminder Cathy's team needed to make proactive defense a top priority. The SecOps team needs safeguards that block or contain potential security threats, like Enzo's phishing email, and to make the company more resilient against security threats. Contoso recently purchased Microsoft 365 Enterprise E5, so Cathy launches an initiative to understand how the platform's security capabilities can help prevent incidents like this in the future.



Protect against phishing attacks and zero-day malware across emails and files

Office 365 Advanced Threat Protection (Office 365 ATP) has a cloud-based email filtering service that protects Contoso's email and builds on the security features of Exchange Online Protection to provide better zero-day protection and sophisticated anti-phishing capabilities. Exchange Online Protection provides real-time protection for messages from most known threats. Office 365 ATP extends those capabilities by providing real-time detonation capabilities to find and block unknown threats, including malicious links and attachments. In addition, it protects files in Microsoft Teams, Word, Excel, PowerPoint, Visio, SharePoint Online, and OneDrive for Business.

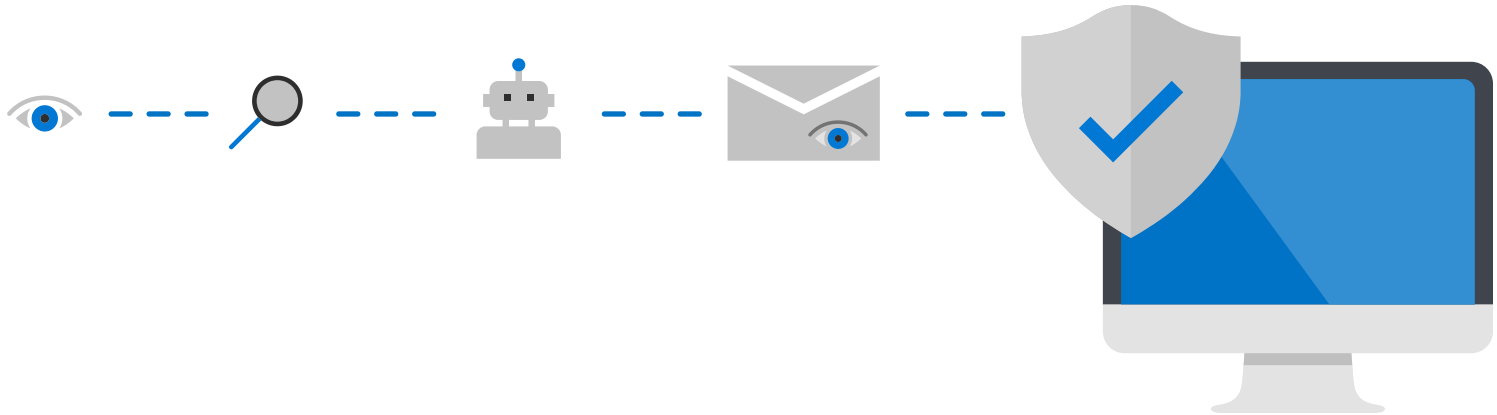
- **Office 365 ATP anti-phish capabilities** configure policies to protect against spoofing, user impersonation, domain impersonation, and brand impersonation.
- **Office 365 ATP Safe Attachments** uses real-time behavioral malware analysis (machine learning) to evaluate files for potential threats. If it detects malware, it removes the attachment and generates an alert. As a result, it prevents malicious attachments from affecting an organization's messaging environment—even unknown threats.
- **Office 365 ATP Safe Links** protects users like Enzo from URLs in messages and attachments that link to malicious websites. This feature checks links continuously, even if it initially determines that the link was safe, because attackers sometimes wait to get past email filtering before adding their malware.
- **Office 365 content analysis and detonation** flags suspicious content and protects users from malicious links and attachments.

Block ransomware and automatically detonate files

Office 365 ATP extends the email and file protection capabilities it uses for phishing to protect Enzo against ransomware threats in real time by using robust file sandboxing, heuristics, and machine learning. Sandboxing inspects a file's behavior in a controlled environment and processes thousands of signals. Office 365 ATP uses machine learning to sort that information and deliver a verdict for each file it analyzes. If the verdict is negative, Office 365 ATP blocks the file, and Enzo won't be able to open it.

Next-generation antivirus capabilities in Windows Defender Advanced Threat Protection (Windows Defender ATP) protect Enzo's device in real time against known and unknown threats. Capabilities like hardware-based isolation protect against ransomware Enzo may download from malicious websites. In addition, Cathy can configure controlled folder access to protect valuable data in specific folders against ransomware. If Windows Defender ATP determines that a program file is malicious or suspicious, controlled folder access does not allow the file to make changes to any protected folder, including Enzo's important documents.

Threat detection policies in Microsoft Cloud App Security help control network cloud traffic. One of these policies updates SecOps when it detects suspicious activities indicative of ransomware, and it offers automated actions that can prevent users from saving ransomware to the cloud. Using Microsoft's security research expertise to identify behavioral patterns that reflect ransomware activity, Microsoft Cloud App Security gives admins robust protection.



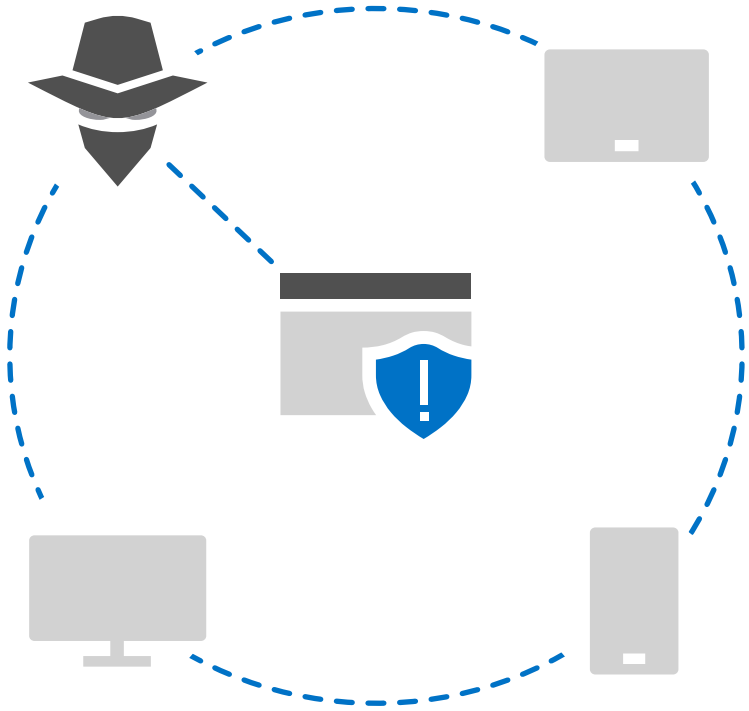
Detect anomalies and suspicious behavior without having to create and fine-tune rules

Enzo prides himself on the ability to execute simultaneously across many fronts, and he leverages a broad range of technology to achieve his sales goals. He knows it's important to keep the company secure, but he just wants to focus on his job and expects the applications he uses to be secure and to inform him if anything suspicious is noticed.

Azure Advanced Threat Protection (Azure ATP) uses user behavior analytics and machine learning to detect risky and suspicious incidents that could indicate compromised identities and sign-ins. When it detects an incident, Azure ATP alerts Cathy's SecOps team so that it can investigate further and remediate, if necessary. Embedded machine learning determines what constitutes normal activity for employees like Enzo. SecOps teams can remediate a security incident with custom policies and rules they defined in Azure Active Directory (Azure AD) Identity Protection. Finally, Microsoft Cloud App Security monitors normal cloud app usage patterns out of the box by using user and entity behavioral analytics and machine learning to provide advanced threat direction across Contoso's cloud environment. Extreme changes in those behaviors trigger security alerts. These protections are enabled by default to provide immediate protection for the company's cloud infrastructure.

Automatically enforce conditional access policies

Someone using Enzo's credentials tries to sign in to his mailbox. Azure AD detects that the person is using an anonymous IP address and generates a risk event. Based on that and related events, Azure AD raises Enzo's risk level from 'low' to 'medium'. Because Cathy had previously configured a sign-in risk policy that blocks access for risk levels "medium" or higher, Azure AD triggers an automatic response. The next time Enzo signs in to his account, Azure AD will prompt him to change his password after using multi-factor authentication (MFA) to verify his identity.



Block access for accounts that may be compromised, even if the credentials entered were accurate

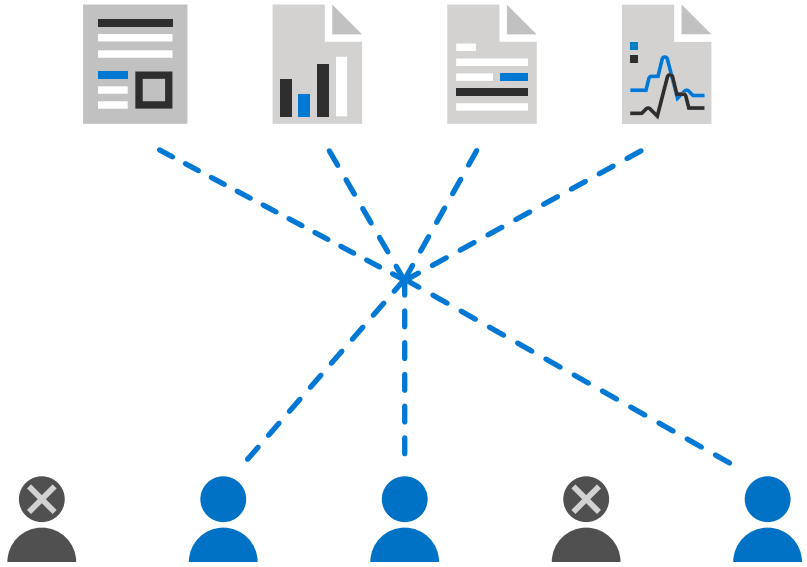
Cathy knows that most security breaches take place when an attacker gains access by stealing a user's identity, just like in Enzo's case, but her team is struggling to detect compromised identities. As Cathy learns more about the adaptive machine learning algorithms and heuristics in Azure AD to detect risk events, she gets excited about the possibilities.

Identity Protection in Azure AD monitors sign-ins and identifies accounts that may be compromised, even when correct credentials have been used. Azure AD Identity Protection can detect six types of suspicious sign-in activities:

Sign-in activity	Risk level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses associated with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

Just-in-time, just-enough access for privileged accounts

Now that Cathy has completed her research into the breach, she has a chance to think more strategically about how Microsoft 365 Enterprise E5 can reduce Contoso's attack surface area. She's concerned about the number of admin accounts in her environment, so she uses Azure AD Privileged Identity Management first to discover the admin accounts in her environment. Then, she can enable or disable access based on who absolutely needs it, reducing the company's attack surface area. She uses the just-in-time/just-enough access capabilities to add an approval workflow for better visibility into and control over who gets admin access and to ensure that future admin access is granted only for a scheduled period.



Automatically block unusual data downloads from approved apps

On the one hand, Cathy wants to enable employees like Enzo to be productive, which means allowing them to access apps so they can work at any time, from any device. On the other hand, it's her job to protect the company's assets, and that includes proprietary and privileged information.

By applying machine learning algorithms, Microsoft Cloud App Security enables Cathy to detect behavior that could indicate that a user is misusing data. She can configure policies to monitor specific actions, such as unexpectedly high rates of a certain activity. For example, Cathy can set a policy so that she receives an alert when there has been an uncharacteristic number of downloads.

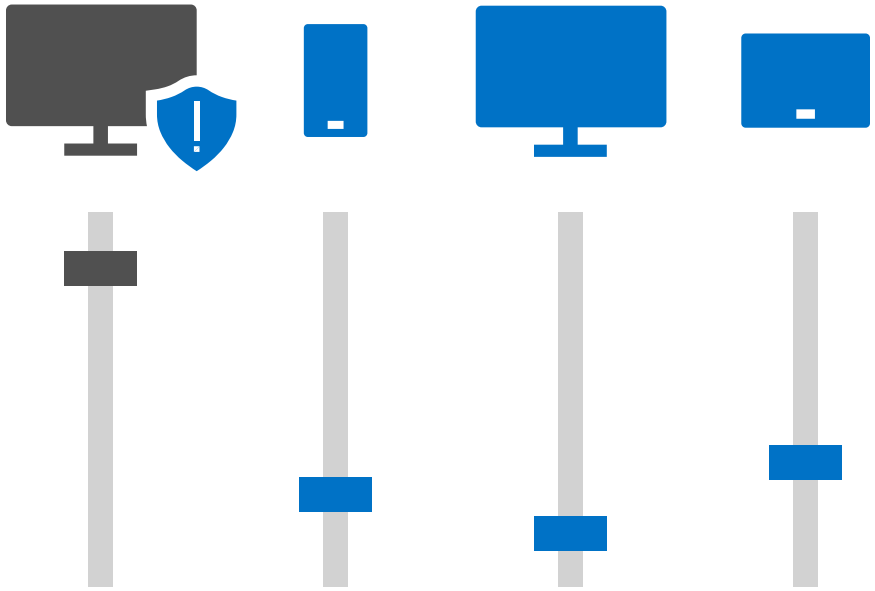
Cathy can configure several automated actions for connected apps. Granular actions can be enforced by app, but specific actions vary depending on app terminology.

Automatically block endpoint with active threats

A user at Cathy's company opens a document that contains malware and enables its macro content, giving the attacker access to the user's device. The attacker's end goal is to move laterally until they achieve domain dominance.

To block attacks like this, Cathy uses the native integration capabilities in Microsoft 365. She uses Windows Defender ATP and Microsoft Intune to define an acceptable level of risk and to block connections from anything that exceeds that level. To do that, she creates a compliance policy that sets 'medium' as the maximum machine risk level, and then creates an Azure AD conditional access policy that grants access only to compliant devices.

Windows Defender ATP detects this attack, records a detailed alert, and automatically sets the machine risk level to "high". As a result, the victim is no longer able to access the corporate resources. Windows Defender ATP automatically investigates and remediates the threat, and then removes the risk level from the machine, which allows the user to access corporate resources again.

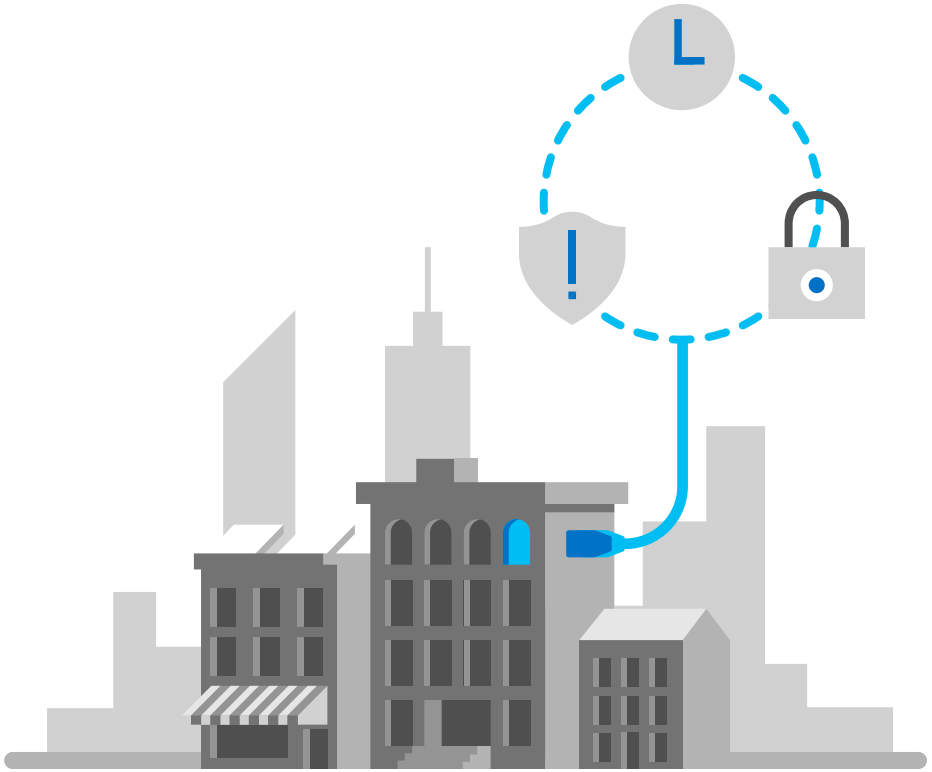


Faster incident response

SCENARIO

Cathy learned a lot from Enzo's ransomware attack and wants to improve Contoso's incident response playbooks. Her SecOps team needs security tools that make incident response easier and help the team quickly piece together individual data points into an attack timeline so they can assess damage and recover. Investigating Enzo's computer took eight full days of Cathy's and her colleague's time. Meanwhile, her leadership team was demanding answers that Cathy couldn't give them. Working backwards to trace the attacker's activity across users, devices, applications, and data accessed was painstaking, with the process made slower by the number of different security tools Cathy used to investigate each facet of the attack. Which devices were compromised? Who was affected? What files were taken? Does the attacker still have access?

Since the ransomware attack, Cathy's security department has fully deployed the security solutions within Microsoft 365 Enterprise E5, and Cathy is looking forward to improving the department's incident response times.



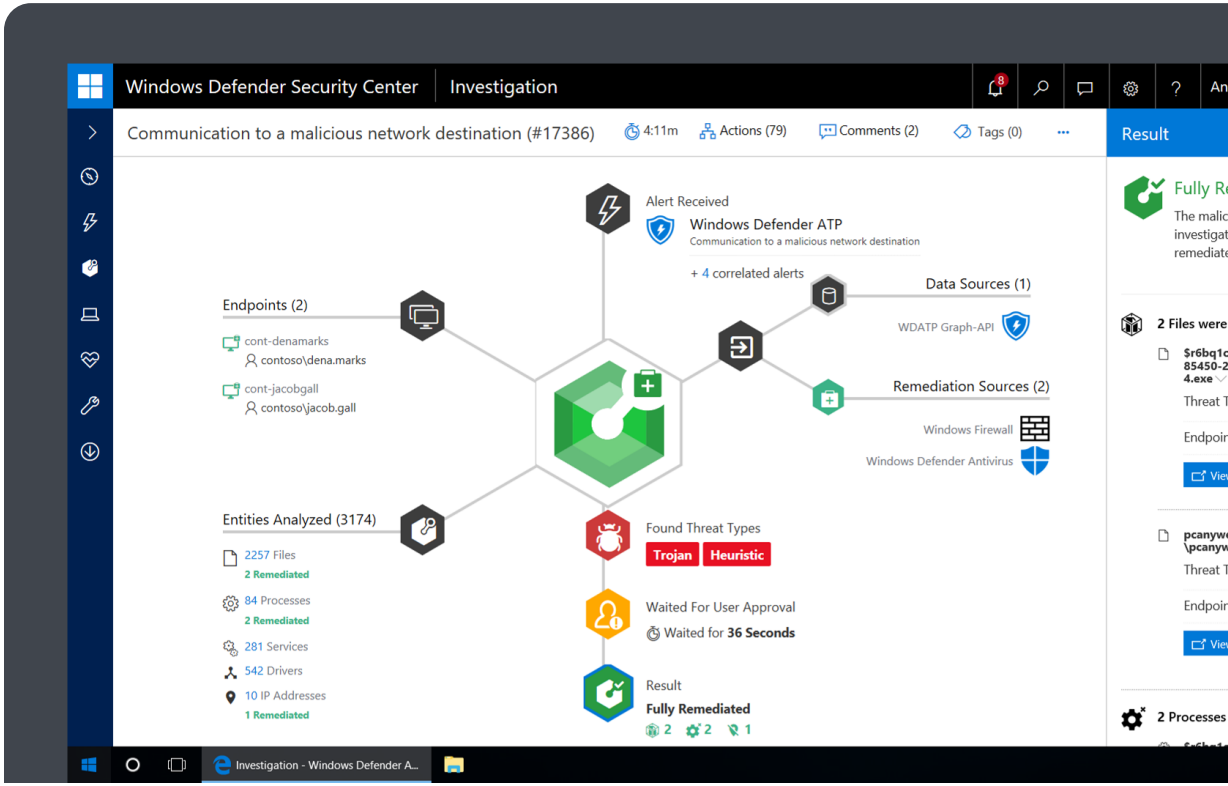
Automatically investigate and remediate endpoint threats

SecOps teams like Cathy's, that have many endpoints to manage, can quickly become overwhelmed by the quantity of alerts they must triage. Cathy is looking forward to using the recently deployed Windows Defender ATP because its automated investigation and remediation capabilities significantly reduce the number of alerts the team needs to resolve manually. Artificial intelligence–based technology mimics the work of a security analyst, using hundreds of playbooks to automatically contain or block attacks in progress, investigate alerts, determine whether machines are compromised, and take remediation actions to bring the machine back to a healthy state.

AUTOMATION LEVELS THAT WINDOWS DEFENDER ATP SUPPORTS:

- **Not protected:** No automated investigations will run on machines.
- **Semi—require approval for any remediation:** Approval is required for any remediation action.
- **Semi—require approval for non-temp folders remediation:** Approval is required on files or executables that are not in temporary folders. Files or executables in temporary folders, such as the user's download folder or the user's temp folder, will automatically be remediated, if needed.
- **Semi—require approval for core folders remediation:** Approval is required on files or executables that are in the operating system directories, such as the Windows folder and the Program files folder. Files or executables in all other folders will automatically be remediated, if needed.
- **Full—remediate threats automatically:** All remediation actions occur automatically.

Windows Defender ATP is built into the Windows 10 operating system for deeper insights even into kernel and memory-level attacks—no agent to deploy, no additional overhead or conflicts with other products on the endpoint. Windows Defender ATP extends to macOS, iOS, and Linux through integration with leading cross-platform security companies. These third-party solutions forward all events and alerts to the Windows Defender Security Center, making it the centralized console for most security administrators' day-to-day work. Configuration of the third-party solution client is still handled in its product, but that is typically a one-time task. Cathy can deploy these clients by using Microsoft Intune, Microsoft System Center Configuration Manager, or a third-party solution.

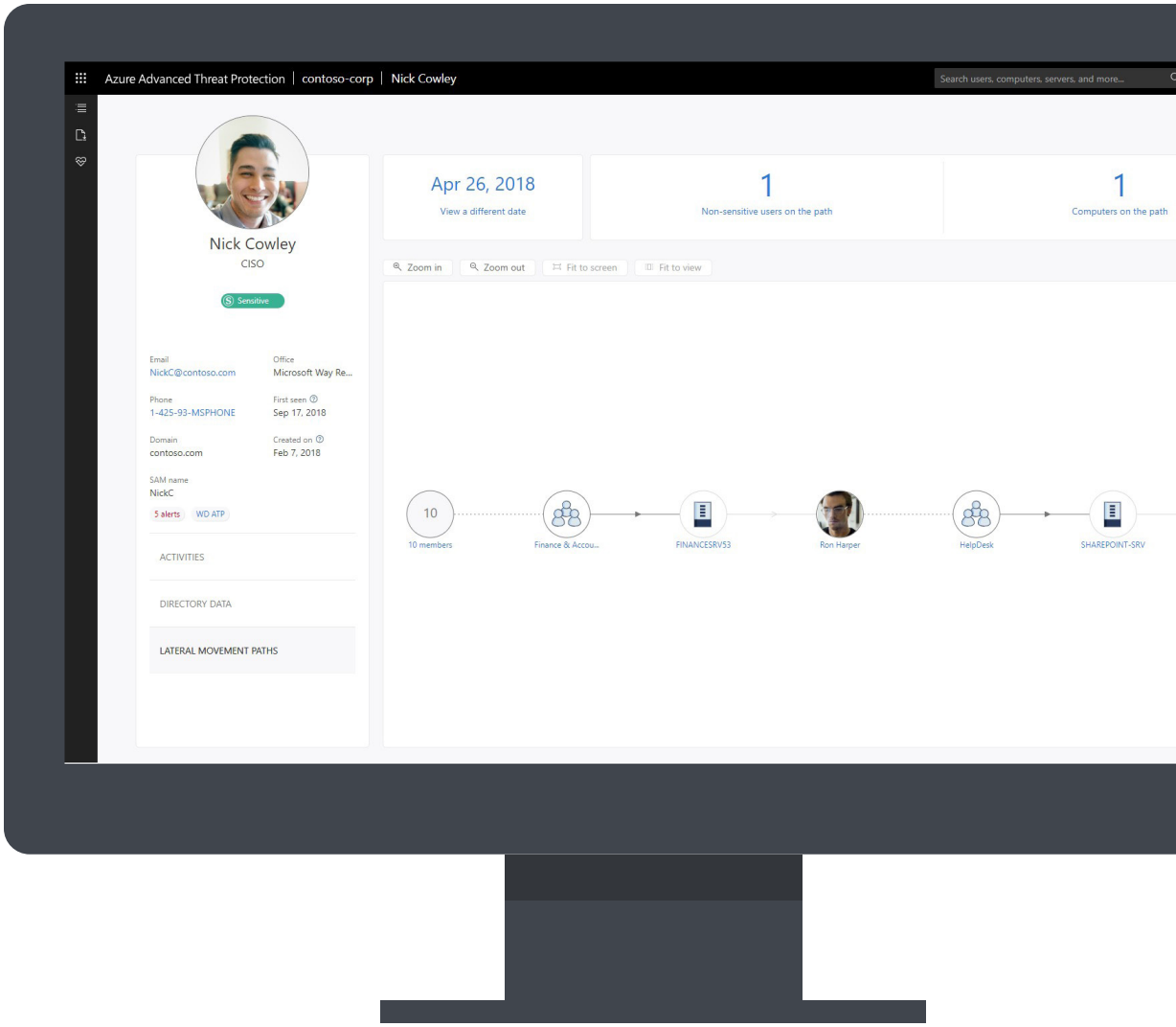


Drill into alert details through a visual attack timeline

Azure Advanced Threat Protection (Azure ATP) correlates alerts across users, devices, email accounts, and applications to create a single attack timeline. It reduces the time spent investigating alerts by showing only relevant suspicious activity in a functional, clear, and convenient timeline. When Cathy investigates a potential breach, she can drill into additional details with a single click.

Visualize a hacker's lateral movement

To help investigate lateral movements, Cathy's SecOps team uses Lateral Movement Paths (LMPs) in Azure ATP. Using these easy-to-interpret visual guides, the team can quickly understand how attackers move within the company's network and which people and devices are affected. By viewing LMPs in Azure ATP, the team can rapidly mitigate the breach by eliminating attacker's access before they cause major damage or achieve domain dominance.



Pivot from device analysis to user profiles or emails without losing context

Now that Cathy's company has deployed Microsoft 365 Enterprise E5, Cathy is working to reduce her department's incident response times. Investigating a recent incident in Windows Defender ATP, Cathy drills into an alert that shows a user downloading malware from a malicious email attachment. Office 365 ATP integrates with Windows Defender ATP, so the email details are available in Windows Defender Security Center. As a result, the team does not have to waste time looking for them. To identify other users who may have received this email, Cathy pivots to Office 365 ATP without losing context. There, she discovers three other users who received the same attachment, but Office 365 ATP blocked it after the first detection.

Curious to see if the attacker moved laterally within the network, Cathy quickly pivots to Azure ATP to see each user's profile and check the LMPs. She discovers that the attacker moved from the first and only compromised machine to other machines, including a domain controller, but she is able to shut down the attack just minutes after it happened instead of the hours it used to take. The ability to pivot easily among Windows Defender ATP, Office 365 ATP, and Azure AD significantly reduces the time required to investigate and remediate this threat.

During another recent investigation, Cathy is alerted to high-volume download activity in one of the company's cloud apps. After identifying the machine generating all the traffic, she is able to pivot from Microsoft Cloud App Security to Windows Defender ATP to continue her investigation into that machine.

An average of

44%

of security alerts are not investigated. Of those, **34%** are legit and of those, **51%** are remediated and **49%** are not remediated.[2]

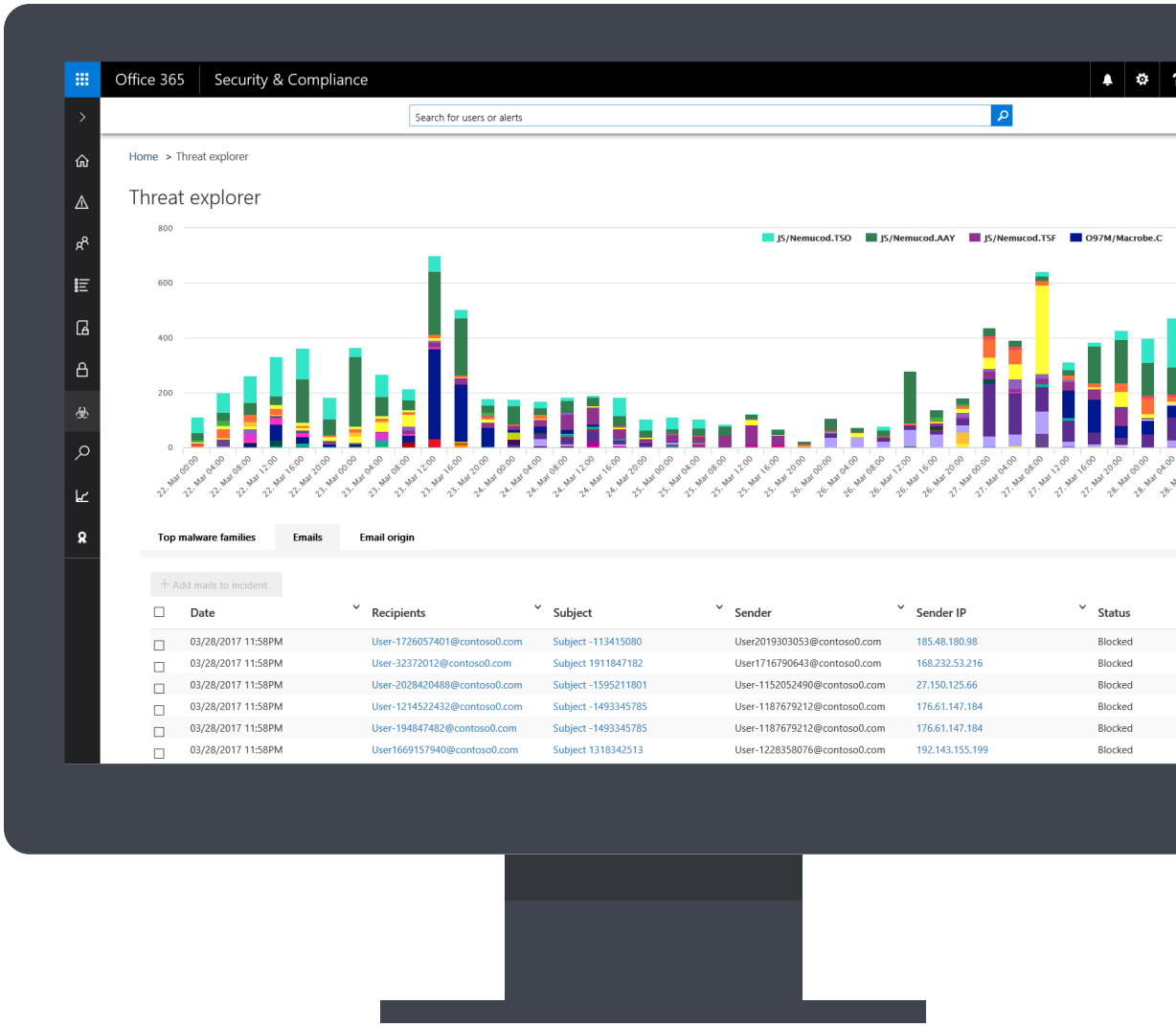
[2] Cisco 2018 Annual Cybersecurity Report

Recommend what to investigate and remediate

Alerts are the SecOps team's entry point to the security landscape. Windows Defender ATP, Office ATP, and Azure AD provide metadata about each alert, plus extra information that helps Cathy make better decisions. For example, in addition to a description, alerts often recommend step-by-step instructions for investigating them. Moreover, many alerts include remediation steps or links to detailed remediation guidance. Cathy's SecOps team uses this information to eliminate the guesswork and remediate threats more quickly.

Investigate across company-wide email

Office 365 ATP monitors signals from sources like user activity, authentication, email, endpoints, and security incidents. Explorer in Office 365 Threat Intelligence is Cathy's window into some of that information. Her team uses Explorer to find and investigate suspicious email delivered to employees across the entire company. For example, while investigating a recent phishing email, Cathy uses Explorer to find and remove that same phishing email from every mailbox.



Run advanced hunting queries against endpoint data for proactive forensic investigation

Cathy just heard about a new zero-day exploit in a security report she monitors, so she uses Advanced Hunting in Windows Defender ATP to see if any of the company's endpoints were exposed to it. Sure enough, she finds the malware installed on an endpoint and is able to remediate it. Then, Cathy creates a custom detection rule based on her hunting queries to reveal alerts in Windows Defender Security Center.

Advanced Hunting is a powerful search and query tool for hunting threats across company endpoints. Now that Cathy has reduced the number of alerts she has to resolve, she has time to go on the offensive and proactively hunt for threats that have not yet shown indicators of compromise.

Remove ransomware and recover files from OneDrive for Business

After the company paid the ransom to get back Enzo's files, Cathy is determined to give her SecOps team better tools to recover from security breaches. The team needs security that removes ransomware, helps recover lost files, and automatically remediates threats on endpoints. The team also needs intelligent recommendations for eradicating other attacks as they occur.

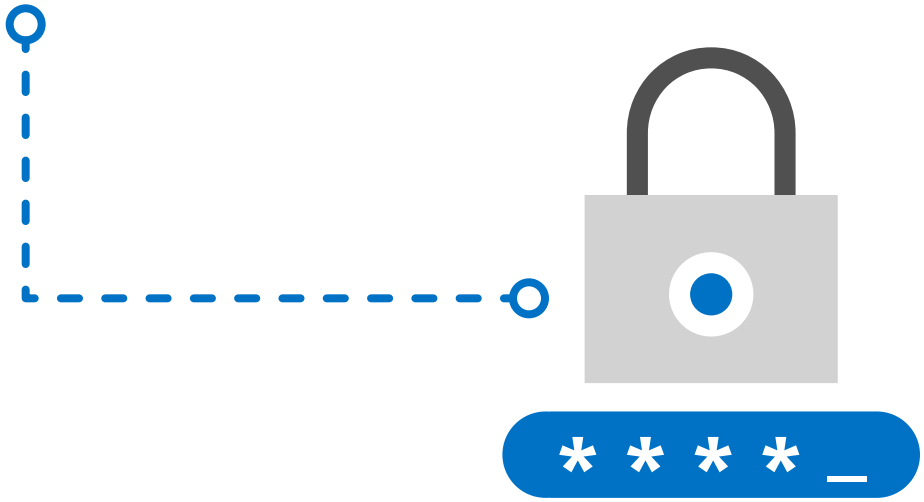
After Enzo's ransomware attack, Cathy put the pieces in place to help the SecOps team recover more easily from future attacks that get through the company's defenses. Not long after, the team finds a reason to use these tools. An attacker has installed ransomware on an employee's computer by using a brute force Remote Desktop Protocol attack. The SecOps team uses Windows Defender ATP to remove the ransomware from the target computer. After that, the team uses the Files Restore feature in OneDrive for Business to restore all the victim's files to a point just prior to the attack. The combination of Windows Defender ATP and OneDrive enables the SecOps team to recover from ransomware attacks without paying the ransom.

Teach users to guard against email phishing by simulating an attack

To identify vulnerable users in her company, Cathy uses the Attack Simulator in Office 365 ATP to run a realistic phishing attack. She creates a phishing email with a sender's display name that recipients will trust and click through to the phishing sign-in server. The simulator includes email templates that Cathy can use, but she is also free to create her own. After creating the phishing email, she sends it to everyone in the organization. Attack Simulator tracks users' clicks, so Cathy can identify who requires additional training.

Automatically trigger a password reset for compromised identities

Each time a user signs in to Azure AD, it analyzes the event to detect suspicious activity. For example, Cathy is alerted to someone using an employee's credentials to sign in to their mailbox; however, the attacker cannot complete MFA. The attacker clearly knows the user's password, so Azure AD generates a risk event that raises that user's risk level to "high." Based on the sign-in risk policy that Cathy had previously defined, that employee must change their password after using MFA to verify their identity. The user is able to use the self-help password reset tool to keep their account secure without having to call the help desk.



Secure your organization against advanced threats and compromised identities

Microsoft 365 Enterprise E5 includes products that companies can use to prevent security threats from breaching their defenses. Office 365 ATP is a cloud-based filtering service that helps protect company email and files. It can detonate attachments in real time to determine whether they are malicious, preventing malware from landing in employee mailboxes. Windows Defender ATP protects users' files on endpoints. In concert with Microsoft Intune, Windows Defender ATP contains attacks by preventing at-risk devices from accessing the network. The protected folders feature blocks suspicious program files from changing protected files, like users' documents. Microsoft Cloud App Security and Azure AD detect suspicious behaviors and can prevent users from uploading ransomware to the cloud. Microsoft Cloud App Security can alert the SecOps team when it detects unusual download activity, like a big change in the amount or sensitivity of data downloaded. Azure AD monitors use of privileged identities and alerts the team when it detects suspicious or unsafe activity.

In the event that an attacker does compromise the company's defenses, Microsoft 365 Enterprise E5 offers faster incident response. First, to alleviate alert overload for endpoints, Windows Defender ATP offers automated investigations that can remediate obvious threats and leave the SecOps team free to focus on higher-priority investigations. The Windows Defender ATP, Azure ATP, and Office ATP consoles provide easy-to-use, visual timelines that can simplify investigations. And, because they work together well, analysts can move around freely without losing context. These tools provide guidance for investigating and remediating threats to reduce guesswork and quicken resolution. Windows Defender ATP can remove malware for endpoints, and OneDrive for Business makes recovering from ransomware without paying the ransom a snap.

These security products work seamlessly to secure organizations against advanced threats and compromised identities:

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

THE INTELLIGENT CLOUD OFFERS AN OPPORTUNITY TO DO SECURITY BETTER

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

IDENTITY & ACCESS MANAGEMENT

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

INFORMATION PROTECTION

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

THREAT PROTECTION

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

SECURITY MANAGEMENT

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

Microsoft

GET COMPLETE, INTELLIGENT ENTERPRISE SECURITY

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