Microsoft Security

Enhanced protection with Microsoft 365 E5 Security

What we'll cover:

1. The need to elevate your security
2. Why choose Microsoft 365 E5 Security suite
3. Expanding security with Microsoft 365 E5 Security suite
4. Making it real with Microsoft 365 E5 Security suite
5. Resources to get you started

Cyber threats have grown 10X

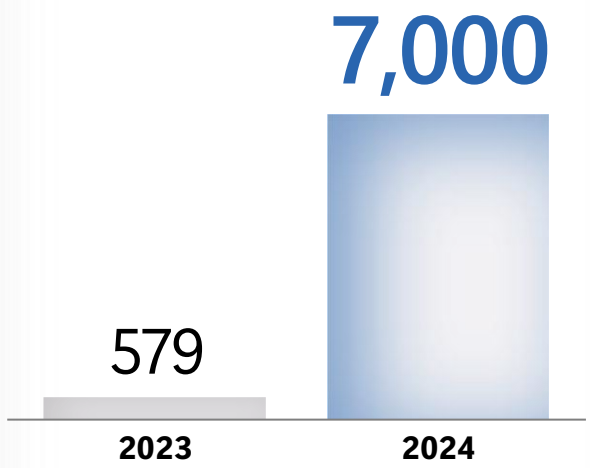
Speed

1h 12mins

median time for an attacker to access private data from phishing

Source: 2022 Microsoft Digital Defense Report

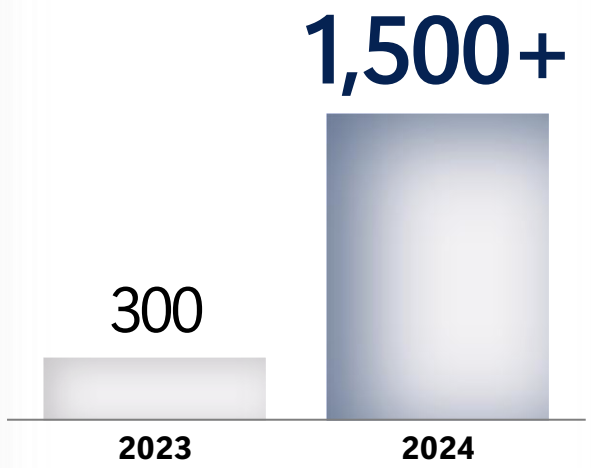
Scale



password attacks per second

Source 2024 Microsoft Digital Defense Report

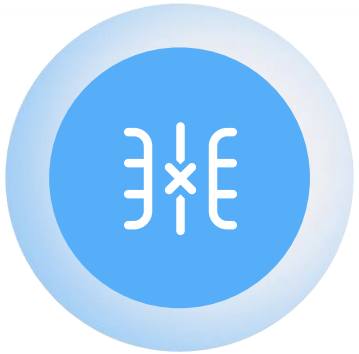
Sophistication



threat actors tracked by Microsoft

Source 2024 Microsoft Digital Defense Report

Cyber jobs feel 10X harder



A disconnected collection of fragmented tools

Source: Microsoft

4M

cybersecurity professionals needed in the world

Source: ISC2

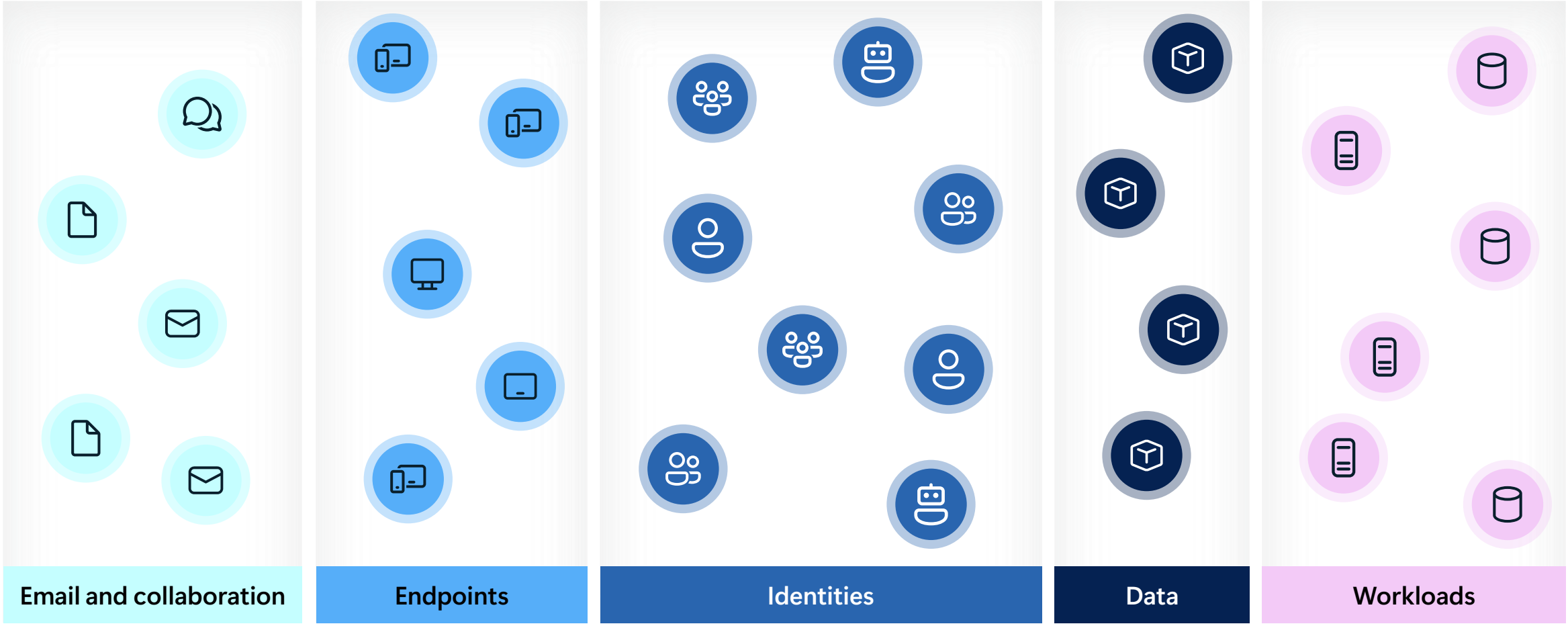
250

new regulatory updates tracked every day

Source: IDC

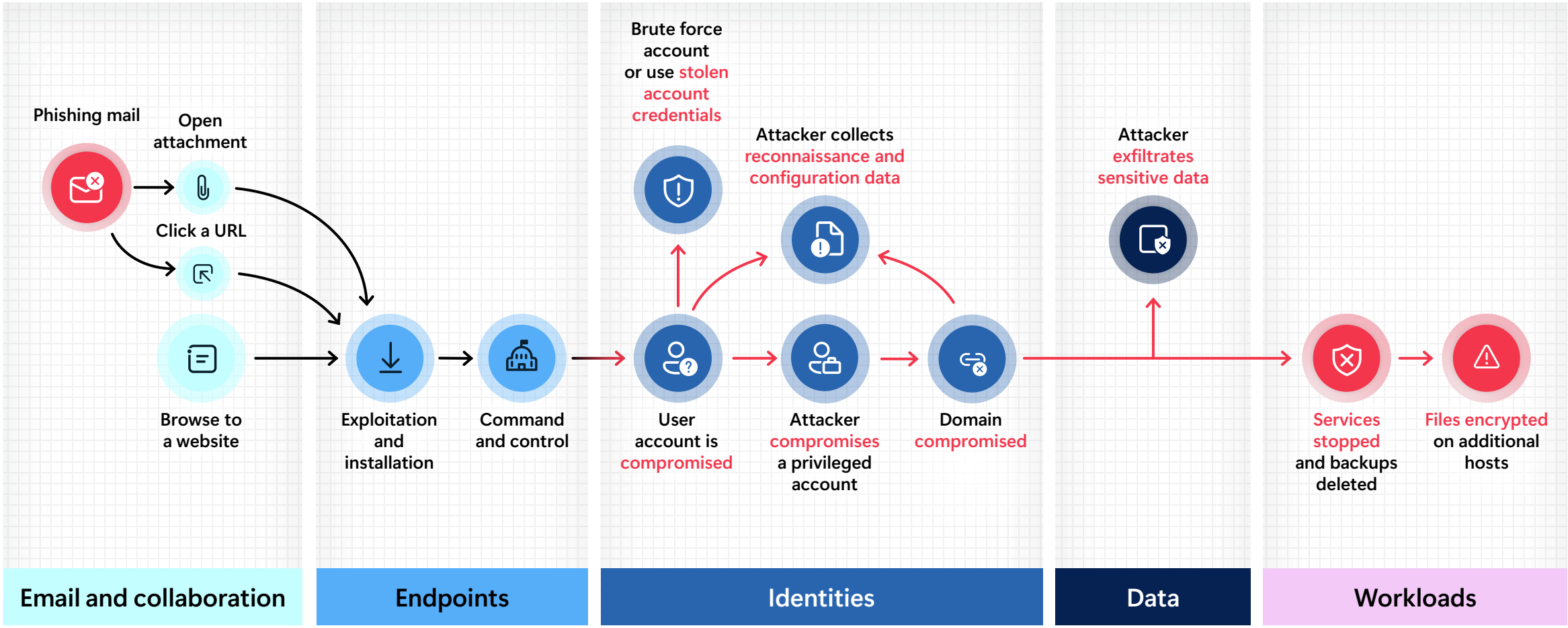
Security teams are forced to defend in silos

Organizations use an average of 80 security tools[1]



[1]Microsoft Internal Research

Attackers think in graphs



Why choose Microsoft 365 E5 Security suite?

Enhanced security

Start with strong, layered security at your pace, focusing on current needs with the option to upgrade to Microsoft 365 E5 later

Cost-effective

Save more compared to standalone licenses or a full Microsoft 365 E5 subscription

Industry recognized

Recognized as a leading security vendor for businesses by independent industry experts

Enhanced security

Microsoft 365 E5 Security

Identity and access controls

Microsoft Entra ID Plan 2

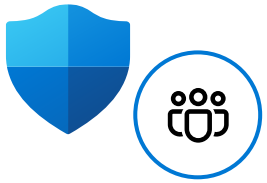
Risk-based conditional access and real-time dynamic user and sign-in assessment

Identity protection using advanced machine learning to identify risky sign-ins, compromised accounts, and insider threats

Granular control over privileged accounts with automated elevation and access reviews

Adjusts access policies in real-time based on user risk

Identity protection



Microsoft Defender for Identity

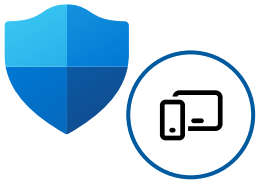
Threat and suspicious user activity detection across identities and infrastructure

Built-in response and automated playbooks for quick threat mitigation

Context-rich identity insights during incident investigations—like recent events, activities and risk scoring

Tailored configuration vulnerabilities and attack path modeling

Device security



Microsoft Defender for Endpoint Plan 2

Industry-leading antimalware, cyberattack surface reduction, and device-based conditional access

Comprehensive endpoint detection and response (EDR)

Advanced hunting with support for custom detections

Attack surface reduction capabilities powered by Secure Score

Collaboration security

Microsoft Defender for Office 365 Plan 2

Protection againstt advanced attacks like phishing and malware business email compromise and spam

Protection beyond email to Microsoft Teams, OneDrive and SharePoint

AI and automation to investigate, analyze, and respond to email threats

Cyberattack simulation training and detailed reporting

SaaS security

Microsoft Defender for Cloud Apps

Full SaaS security capabilities.

Visibility into “Shadow IT” by discovering apps in use

SaaS app security posture that uncovers configuration gaps and offers recommendations

OAuth-enabled and line of business app monitoring, governance and protection

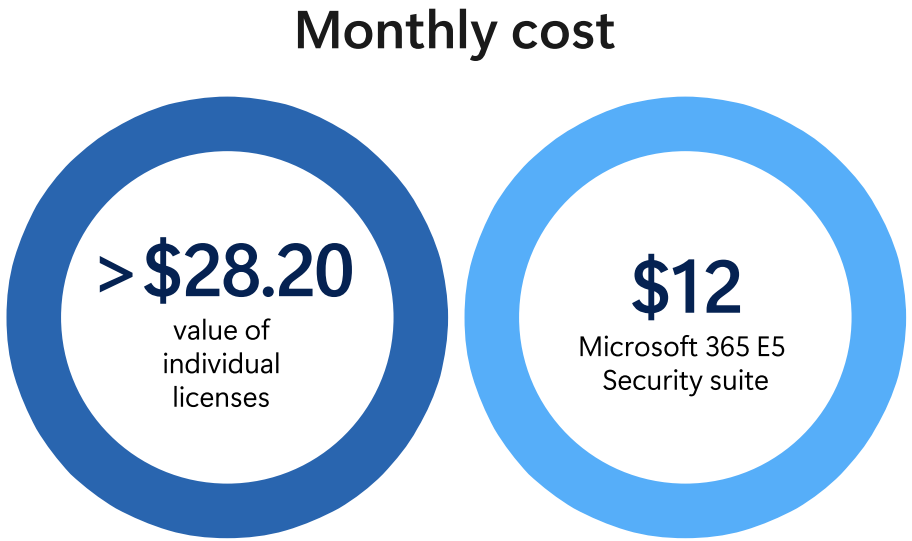
Microsoft 365 E5 Security

Microsoft Defender

Defender for Endpoint P2	**$5.20**
Defender for Office P2	**$5.00**
Defender for Identity	**$5.50**
Defender for Cloud Apps	**$3.50**

Microsoft Entra

Entra ID Plan 2	**$9.00**



Microsoft 365 E5 Security suite

- Save ~57% per license
- Enable end-to-end security

[1]Price is pupm and subject to change based on subscription term, currency and region.

Microsoft 365 E5 Security

Advanced security tools to protect digital assets and data

Microsoft 365 E5 Security ($12.00)

Microsoft Defender for Office 365 Plan 2	**$5.00**	A cloud-based email filtering service that helps protect your organization against unknown malware and viruses by providing robust zero-day protection and includes features to safeguard your organization from harmful links in real time. In addition to Plan1, Plan 2 also offers automated investigation and response, threat trackers, and an attack simulator
Microsoft Defender for Cloud Apps	**$3.50**	A multimode Cloud Access Security Broker (CASB). It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services.
Microsoft Entra ID P2	**$9.00**	Microsoft's cloud-based identity and access management service, which helps employees sign in and access resources. In addition to Free and P1 features, P2 also offers Identity Protection to help provide risk-based Conditional Access to apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.
Microsoft Defender for Identity	**$5.50**	A cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Microsoft Defender for Endpoint Plan 2	**$5.20**	A unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and response. The product offers Threat and Vulnerability Management, tools to surgically reduce the attack surface, next-generation protection to block threats and malware, Endpoint detection and response to detect advanced attacks, automated investigation and remediation of threats and Managed threat-hunting service.
Safe Documents[1]	*	Uses Microsoft Defender for Endpoint to scan documents and files that are opened in Protected View or Application Guard to automatically check Office documents (Excel, PowerPoint, Word etc.) "against known risks and threat profiles" before users open them.
Application Guard for Office 365[1]	*	Isolates untrusted documents to protect users against malicious and potentially harmful threats. at risk. When a user encounters a malicious document, it is safely isolated.
Microsoft Defender for IoT – EIoT[2]	*	Includes coverage of 5 EIoT devices for each Microsoft 365 E5 license; additional device coverage is $0.85 per device per month. Provides discovery of network devices, vulnerability management, and threat detection and response.

Prices – ERP /per user/per month
[1]Only provided via Microsoft 365 E5 or Microsoft 365 E5 Security
[2]Per device per month

A Leader in security, compliance, identity, and management

A Leader in three

Gartner® Magic Quadrant™ reports

A Leader in nine

Forrester Wave™ categories

A Leader in eight

IDC MarketScape reports

IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2024 Vendor Assessment, Doc #US50521223, January 2024
IDC MarketScape: Worldwide Modern Endpoint Security for Midsize Businesses 2024 Vendor Assessment, Doc #US50521323, February 2024
IDC MarketScape: Worldwide Modern Endpoint Security for Small Business 2024 Vendor Assessment, Doc #US50521424, March 2024
IDC MarketScape: Worldwide eDiscovery Early Case Assessment Software 2022 Vendor Assessment, Doc #US48970222, October 2022
IDC MarketScape: Worldwide Client Endpoint Management Software for Windows Devices 2024 Vendor Assessment, Doc #US51234324, April 2024

IDC MarketScape: Worldwide Unified Endpoint Management Software 2024 Vendor Assessment, Doc #US51234224, April 2024
IDC MarketScape: Worldwide Unified Endpoint Management Software for Small and Medium-Sized Businesses 2024 Vendor Assessment, Doc #US51779424, April 2024
IDC MarketScape: Worldwide Unified Endpoint Management Software for Frontline/IoT Devices 2024 Vendor Assessment, Doc #US51779324, April 2024

Value proposition

Business Premium + E5 Security

Microsoft 365 Business Premium

Productivity and Security suite

- Entra ID P1: **Conditional Access** based on predefined conditions like device compliance, location, and app sensitivity
- MDO P1: Email and collaboration security, including **anti-phishing, anti-malware**, and **safe links/attachments.**
- MDB: AI-powered, SMB optimized **endpoint security with EDR and automatic attack disruption.** Across Windows, macOS, Linux, Android, and iOS.
- Purview Information Protection: **Encrypt emails** and discover, classify, and manually label sensitive data.
- Intune P1: Manage **devices and work data** on company-owned and employee devices. Remove business data from lost or stolen devices

Microsoft 365 E5 Security

Enterprise-Grade XDR solution

- Entra ID P2**: Risk-based conditional access**, visibility into risky sign-ins and user behavior anomalies. **ID Governance** and **Privileged Identity Mgmt.**
- MDO P2: Advanced email and collaboration security with **automated investigation and response,** and **end user phishing simulation trainings**
- MDE P2: **Endpoint security and EDR with advanced threat hunting,** as well as access to threat experts for additional investigations.
- Defender for Cloud Apps: **CASB solution to automatically discover and block apps** based on risk level, unusual user activity, or data-sharing behavior to protect against sophisticated SaaS-based attacks.

Value comparison

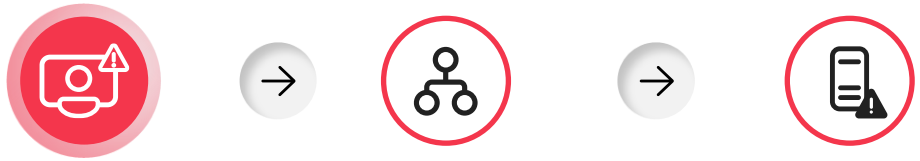
Business Premium + E5 Security

	Security capability	Business Premium	Microsoft 365 E5 Security
Identity and access controls	Basic Identity and access management (single sign on (SSO), multi-factor authentication (MFA), self-service password reset)	✓	✓
	Risk based MFA: require MFA if a user is accessing resources from an unrecognized device or unfamiliar location		✓
	Adjust authentication requirements based on risk assessment, such as asking for MFA only if login behavior is unusual		✓
	Self-service password reset with enhanced policies. Example: Only allow password reset if the user has passed security questions or an additional validation step		✓
	AI-driven risk detection analyzes user behavior to detect compromised accounts or risky sign-ins		✓
Identity security	AI-driven risk detection analyzes user behavior to detects compromised accounts and suspicious activities (e.g., impossible travel or unusual logins) that suggests an account has been compromised		✓
	Provides detailed alerts on identity-based threats		✓
	Protects on-premise Active Directory from attacks		✓
Device security	Endpoint protection with basic features like anti-virus and firewall	✓	✓
	Cloud-delivered protection, which includes near-instant detection and blocking of new and emerging threats	✓	✓
	Detects unusual system activity, flags suspicious processes, and provides attack timelines to help security teams contain the threat before data is stolen or encrypted	✓	✓
	Automated Investigation and Response (AIR) immediately correlates data across identity, email, and endpoint activity; If it detects a compromised account, it automatically revokes access, isolates the device, and generates an incident report		✓
Email and app security	Basic email protection from phishing and malware with simple filtering	✓	✓
	Automatically scans files and links in emails, Microsoft Teams, SharePoint, and OneDrive before they can be opened or shared; If a file or link is unsafe, it's blocked to prevent harm	✓	✓
	AI-driven phishing protection that detects and stops sophisticated phishing attempts, impersonation attacks, and email fraud	✓	✓
	Detailed reports on who is being targeted, which attacks were blocked, and potential weaknesses in the organization		✓
Cloud access security	Shows what apps employees use	✓	✓
	Shows what apps employees use, and evaluates how safe they are		✓
	Automatically blocks or restricts risky apps		✓
	Detects suspicious behavior in cloud apps, such as strange file access patterns or unusual downloads		✓

Challenge

XDR-level protection and response

Attacks like those launched by Octo Tempest leverage a broad variety of tactics—like brute spray, social engineering, phishing, and malware—to try and gain entry. Once they have a foothold, they work to increase their privileges and gain access to valuable data, crossing different identities, endpoints, workloads, and even cloud. These types of coordinated attacks are hard to detect without comprehensive alert correlation.

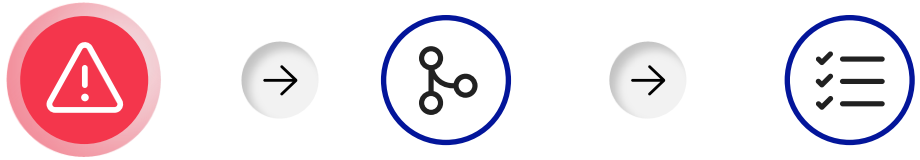


Attacker launches multiple waves targeting organizations

Once successful, they begin moving inside the organization

Eventually reaching your data and exfiltrating it

Meanwhile, your security team is trying to manually correlate alerts while the attacker is active in the environment.



Multiple alerts trigger across multiple portals

Defender has to manually correlate together across different sources

Remediation requires yet more manual steps, giving the attacker valuable time to continue their efforts

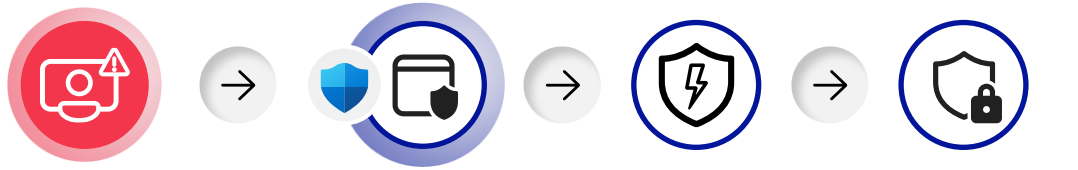
90% of successful ransomware attacks involve an unmanaged device.[1]

[1]Source: Microsoft Digital Defense Report, 2024

Solution

XDR-level protection and response

Microsoft Defender XDR delivers incident-level visibility across the entire kill chain, so your analysts can focus on fully mitigating the threat instead of uncovering what happened. Automatic attack disruption will stop lateral movement of advanced cyberattacks, such as ransomware, with AI to limit the attacker's progress early on, and give your SOC team full control to investigate and remediate cyberthreats.



Attacker launches attack waves

Defender coordinates defense across domains

Attack is disrupted

Security professionals clean up after and implement changes to reduce exposure

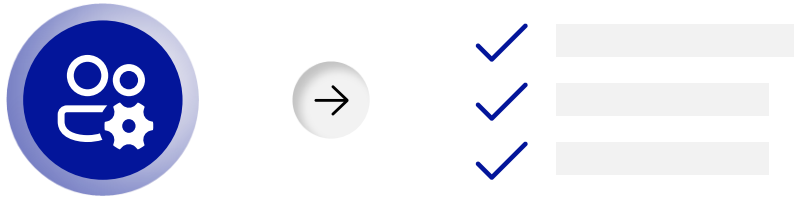
3 mins average time to disrupt a ransomware attack with Defender XDR.[2]

[2]Source: Microsoft Internal Research

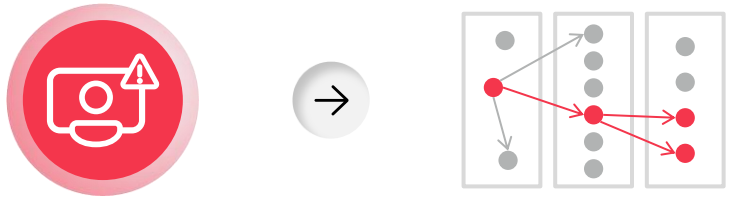
Challenge

Managing risk exposure

The average large organization has tens of thousands of exposures—prioritizing these effectively takes more than just burning-down lists of vulnerabilities of configuration problems. Attackers don't just target your biggest vulnerability—they target the group that cumulatively result in the biggest exposure.



Defenders think in lists, working across tables of alerts, vulnerabilities, and threat intelligence



Attackers are thinking in graphs, mapping vulnerabilities together

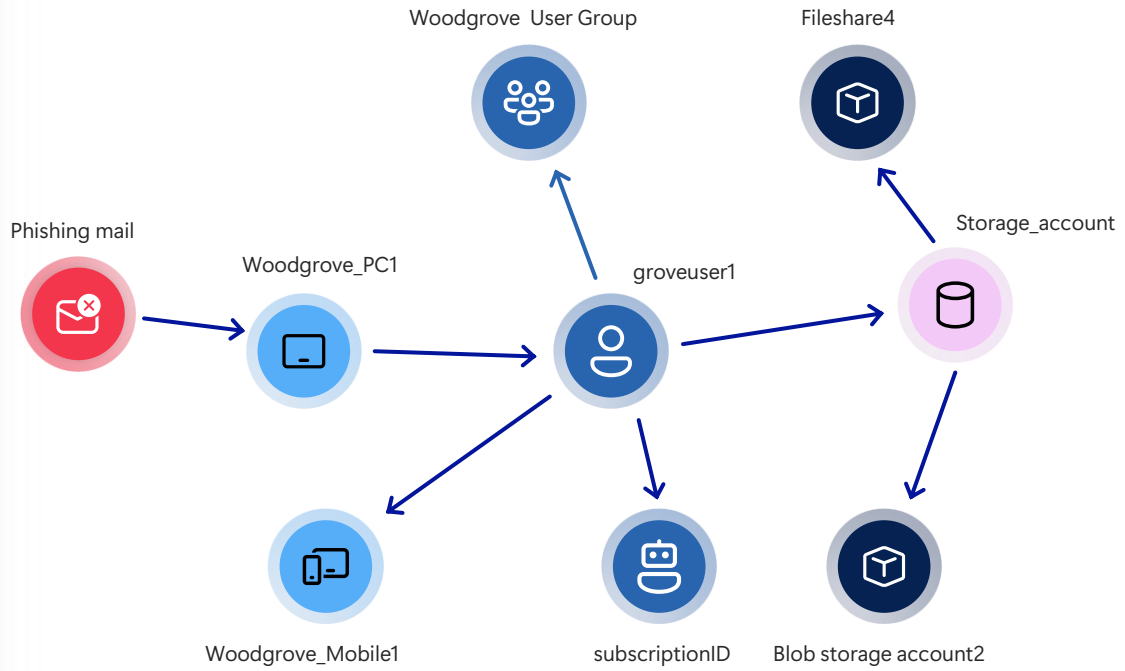
80% of organizations have attack paths that expose critical assets.[1]

[1]Source: Microsoft Digital Defense Report, 2024

Solution

Unified exposure management

Microsoft Security Exposure Management helps your team build a continuous threat exposure management program by unifying disparate data silos, providing security teams with end-to-end visibility of their organization's security posture.



Challenge

Advanced social engineering attacks

We're in a new era of social engineering. Phishing emails are being tailored to each recipient with GenAI and don't contain the well-known markers—like malicious links or attachments—making them hard to detect with traditional tools.

Contoso LLC Reply Reply all Forward

To: Rebecca Smith

Hey Rebecca,

Please be on the lookout for an invoice from Contoso LLC. We're finishing it up now and it will be sent over shortly.

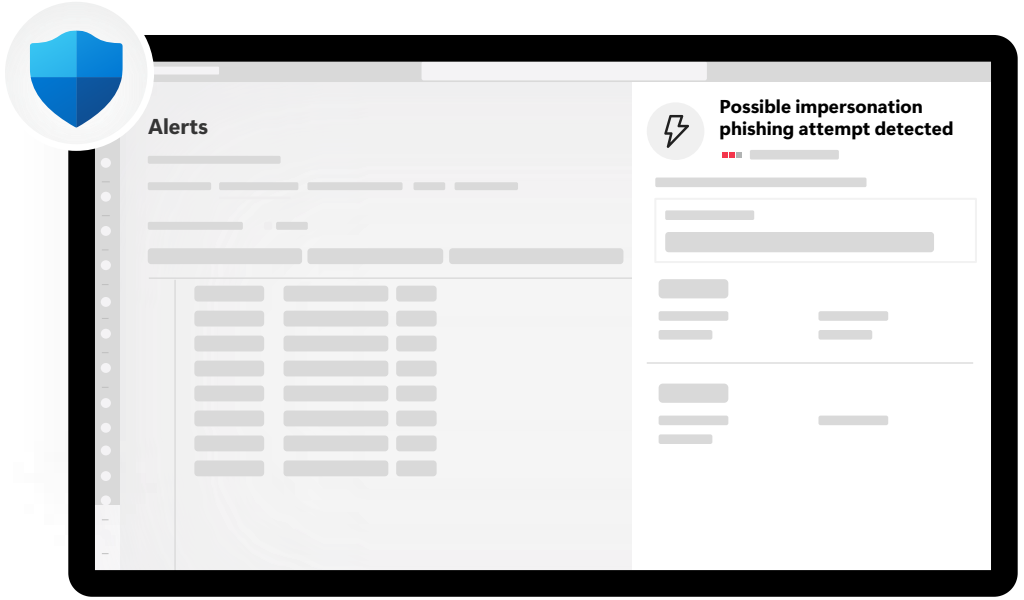
25% Business email compromise behaviors involve lateral phishing.[1]

[1]Source: Microsoft Digital Defense Report, 2024

Solution

LLM-based business email compromise detection

Microsoft Defender for Office 365 uses purpose-built large language models (LLM) at scale to provide AI-powered email and collaboration security.



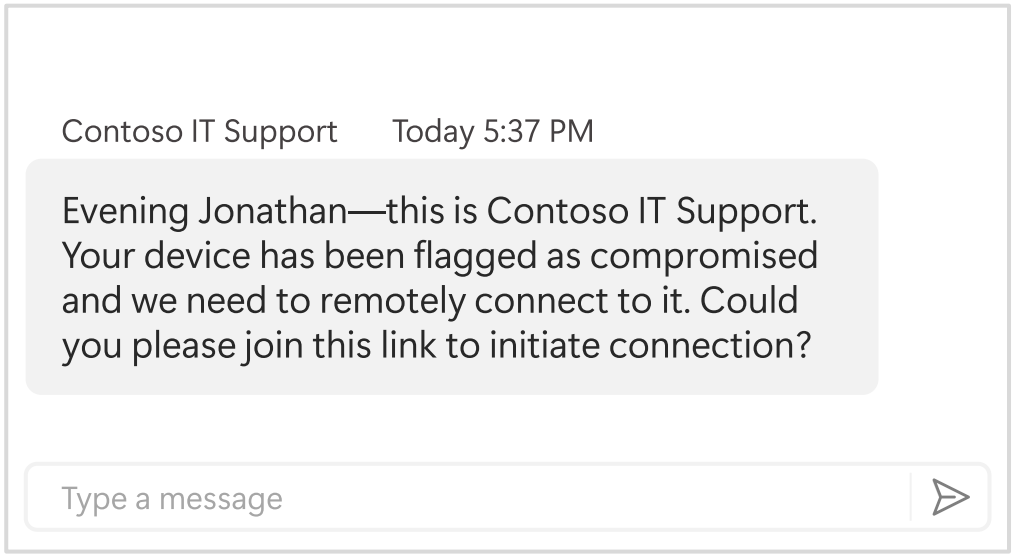
99.9% Attacker intent detection accuracy and filtering.[2]

[2]Source: Microsoft Internal Research

Challenge

Phishing targeting collaboration platforms

The last couple of years have seen a significant rise in novel social engineering techniques in collaboration platforms like Microsoft Teams. Threat actors are masquerading as legitimate help desk or tech support, providing a new channel to send their malicious payloads, request user credentials/MFA approvals, and even establish remote monitoring and management connections.



Solution

Full protection across Microsoft Teams

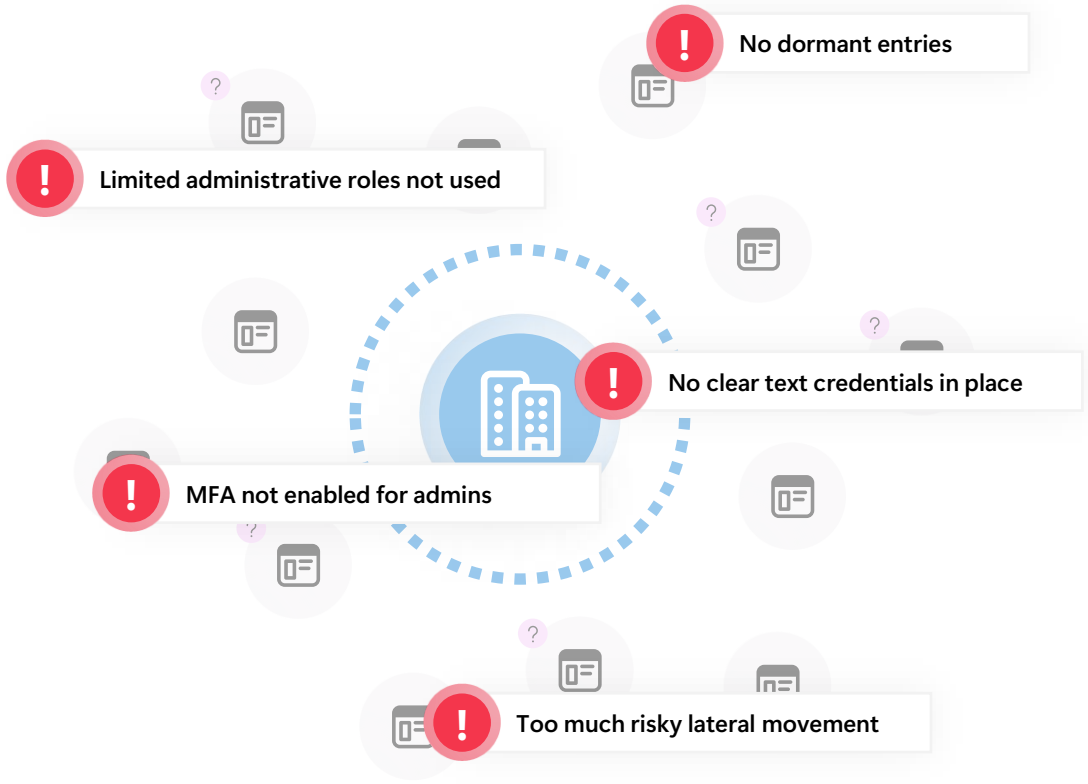
Microsoft Defender for Office 365 protects Microsoft Teams users against phishing and other social engineering threats while providing SOC teams visibility into alerts and remediation.

- Malicious message detection and quarantining
- User training and attack simulation
- User threat reporting
- Potentially malicious URL warning
- SOC alerting
- File type protection

Challenge

SaaS protection limited to shadow IT

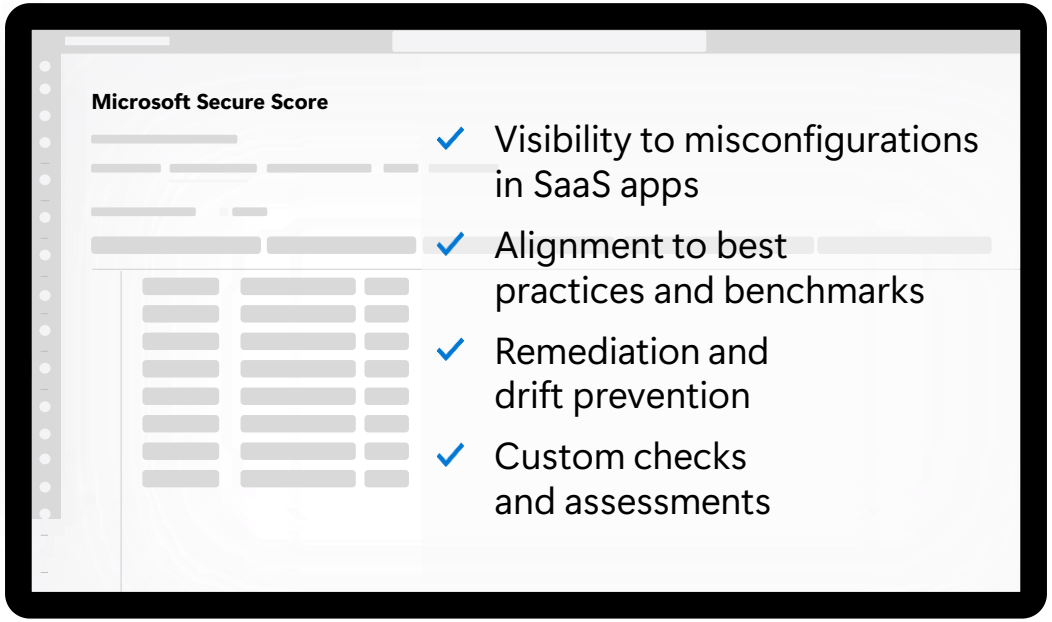
SaaS app misconfigurations can lead to a potential breach and have emerged as a common attack vector. Yet, most security teams lack the tools to uncover these mitigations, understand them in the context of their broader exposure, and easily mitigate the problems.



Solution

Monitor your SaaS security posture

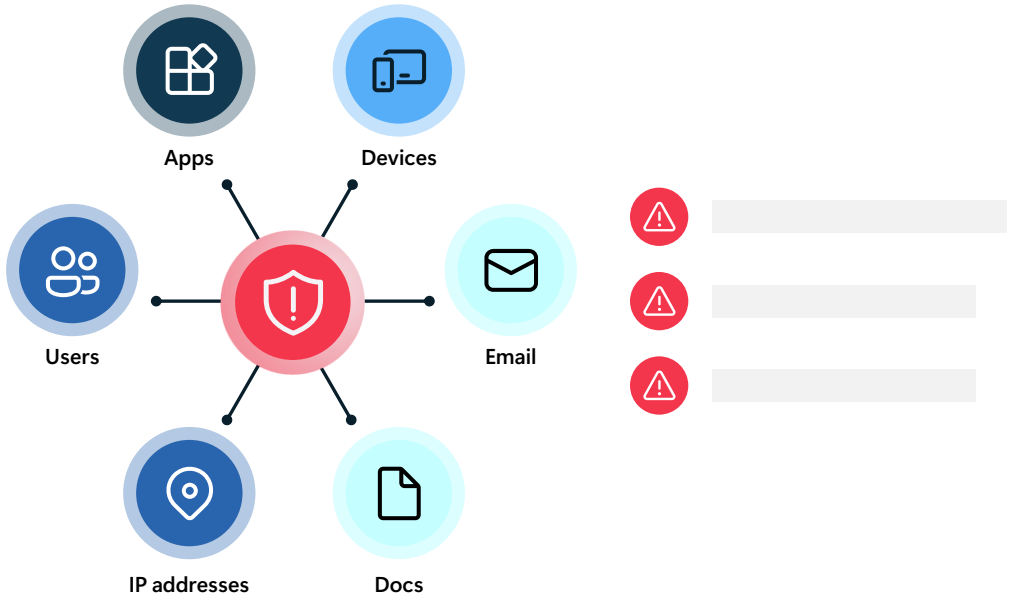
Defender for Cloud Apps enables automated and continuous monitoring of SaaS apps to reduce security vulnerabilities and increase compliance by detecting misconfigurations and providing remediation steps for risky configurations.



Challenge

Threats from AI apps

Decentralized business units are eagerly experimenting with AI and GenAI use cases without the guidance of an enterprise framework to manage AI trust, risk and security.



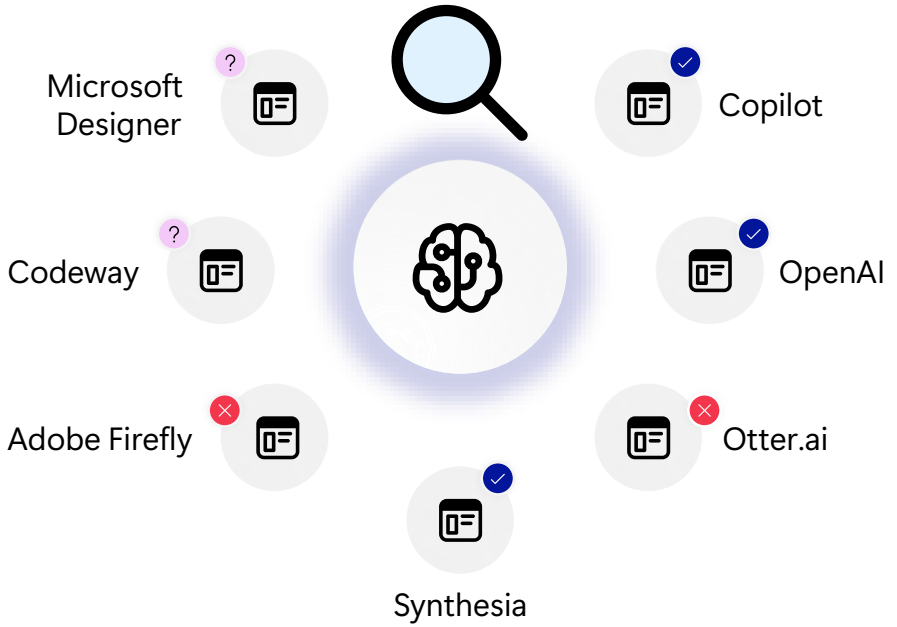
80% of enterprises will be using Generative AI apps or deploying Generative AI-enabled applications by 2026.[1]

[1]Source: Gartner Says More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI-Enabled Applications by 2026

Solution

Comprehensive protection

Proactively gain visibility into AI usage within the organization and implementing corresponding controls.



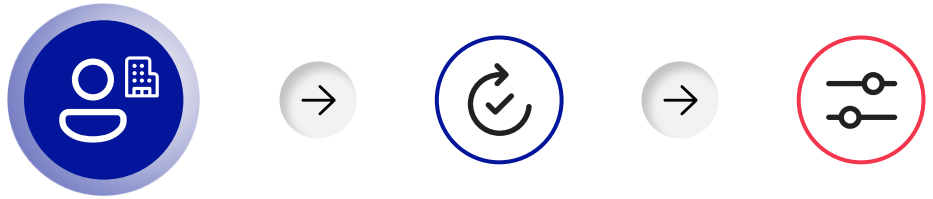
400+ GenAI apps already supported.

40+ Risk factors built into ready-to-use risk assessments to help with discovery.

Challenge

Handling rapid workforce growth

ABC Peanut Company frequently adjusts its workforce, necessitating various workflows and processes for users to access needed resources. Historically, these processes have been manual. IT administrators have depended on scripts to complete the onboarding process, making troubleshooting problems complex and time-consuming.

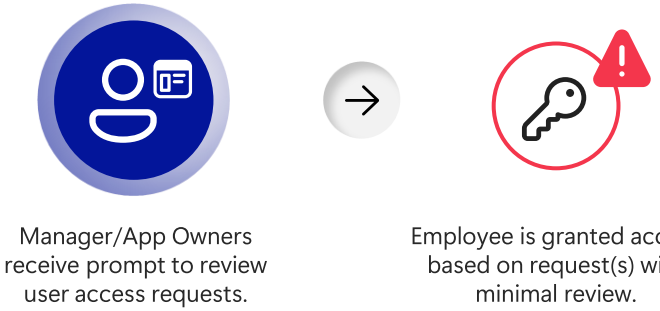


Employee

Access requests is routed to IT for system access

IT manually processes access request

Managers and app owners frequently receive prompts to review new requests for access and to maintain existing access. This frequent prompting can lead to them approving requests without thorough consideration.



Manager/App Owners receive prompt to review user access requests.

Employee is granted access based on request(s) with minimal review.

Solution

Identity governance capabilities

Microsoft 365 E5 Security includes identity governance capabilities, which integrate with HR platforms to help automate employee onboarding, streamlining the process and reducing IT workload. Admins can provision access packages, which bundle permissions for both cloud-based and on-premises resources. When employees change roles or locations, they easily receive new access permissions.

HR creates user account in their system.

Employee identity is created and automatically provisioned for access to necessary applications and systems based on access package(s).

Employee is granted access

Access certification and recertification support time-bound reviews, user self-approvals, and multi-layer approvals, as well as automated recommendations to review the access of inactive users, helping to minimize outdated access permissions and reducing attestation fatigue.

Challenge

Security breach simulation

TechTech Inc. conducts a controlled security breach simulation. The scenario involves a password spray attack targeting the company's employee accounts. Attackers attempt to gain unauthorized access by trying a small number of commonly used passwords across many different accounts.

IT team

Receives security alert(s) and initiates security protocols

Manually reviews account activities including unauthorized access and potential data breaches

The IT team is alerted and manually investigates the alert to take necessary actions to mitigate the threat.

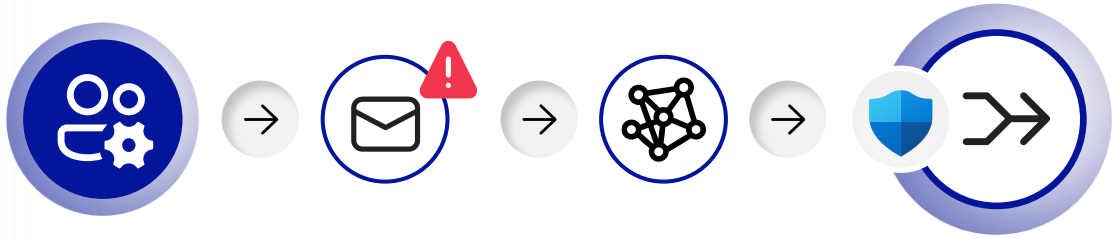
Manually locking compromised accounts, resetting passwords, and enforcing multi-factor authentication (MFA).

Completes policy reviews and implements precautionary measures for employees

Solution

ID protection

Microsoft 365 E5 Security includes Microsoft Entra ID Protection, which uses advanced machine learning and threat intelligence to block identity attacks in real time. These features incorporate behavioral analytics, and signals from user risk and sign-in risk to identify the password spray attempt with greater accuracy and speed. The IT receives an automated email notification alerting them of detected risks like compromised user accounts or suspicious sign-ins. This prompts investigation and remediation, significantly reducing the response time and minimizing human intervention.



IT team

Receives security alert(s) through ML-backed real-time and offline detections.

Reviews automated incident response reporting and leverages machine learning to identify and auto-remediate risky users

Entra ID Protection alerts are integrated with Microsoft 365 Defender and Sentinel to streamline incident response workflows.

> **Premium P2 tenants who use risk-based Conditional Access remediate user risk 140 times faster than P2 tenants who don't use risk-based Conditional Access.**

Challenge

Identities are the new security boundary

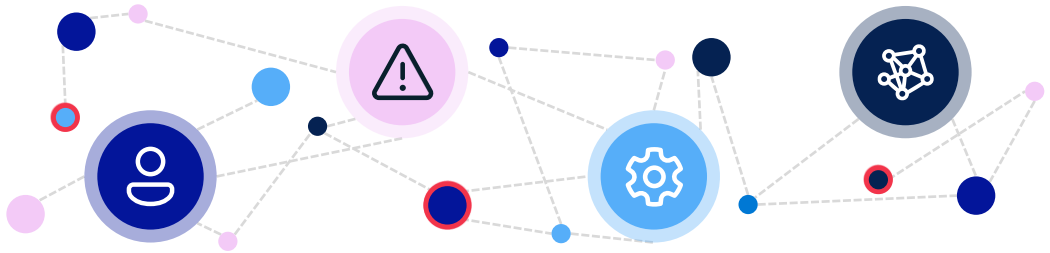
Identities are one of the most common attack vectors and the speed, sophistication and scale of identity-based attacks have increased exponentially.

7,000
password attacks per second in 2024, up from 4,000 in 2023.

+111%
increase in token theft attacks in just 1 year.

60 seconds
The median time for attackers to access private data from phishing.

It only takes one misconfiguration or gap in protection to give attackers a valuable foothold within your organization and today's complex identity environments offer ample opportunities.



1 compromised identity comprises even the most robust security practices.

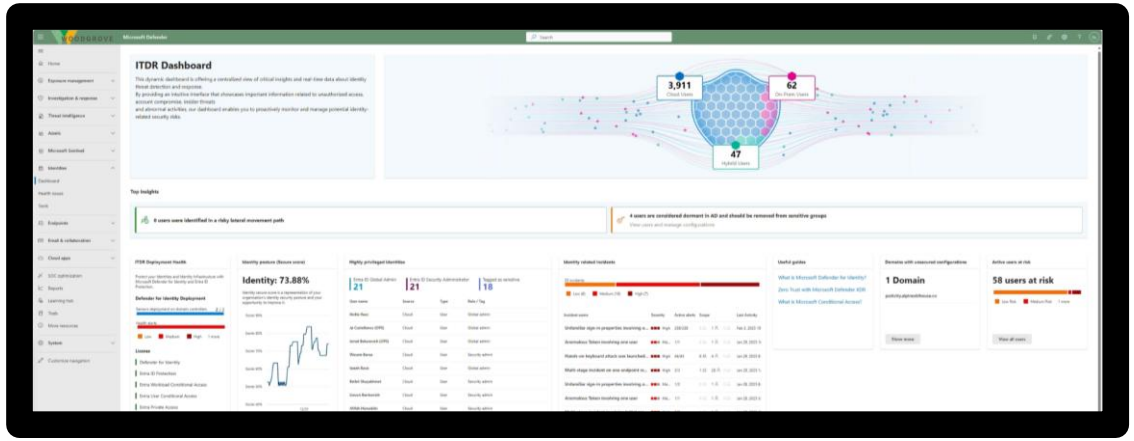
Solution

Microsoft Defender for Identity

Microsoft Defender for Identity provides identity-specific security capabilities as an integrated part of Microsoft Defender XDR.

Dedicated sensors for on-premises identity infrastructure combined with native integration for Entra ID and bi-directional connectors for other common solutions allow Defender for Identity to comprehensively protect your unique identity landscape.

Powerful identity-specific detections are automatically enriched and correlated with data from other domains offer unparalleled insights and incident level visibility.



Challenge

Ransomware

During the busiest time of the year, Northwind Trader's mission critical files became unusable. **Hackers used ransomware to encrypt Northwind's files,** demanding a payment for the encryption "key". Northwind must pay for the encryption "key" or lose their data, which could result in business closure.

275% increase in ransomware attacks from 2022 to 2024.[1]

[1]Source: Microsoft Digital Defense Report, 2024

Solution

Ransomware defenses

With Microsoft 365 E5 Security, **employee devices are protected with Microsoft Defender for Endpoint P2** which provides multi-layered ransomware protection to thwart attacks before they occur. Endpoint Detection Response with AI powered automatic attack disruption helps defend against manual and targeted attacks and stop them from moving through the network.

Microsoft Defender for Business protects company from ransomware attacks

3x threefold decrease in ransom attacks reaching encryption stage over the past two years.[1]

[1]Source: Microsoft Digital Defense Report, 2024

Resources to get started with E5 Security

Business Premium

Customer resources

- **Microsoft Security for Business:** https://aka.ms/SMBSecurity
- **Tech Community Blog:** http://aka.ms/BusinessPremiumPlusE5SecurityBlog

Partner resources

- **Business Premium Partner Playbook:** https://aka.ms/M365BPPartnerPlaybook
- **Microsoft Security for Partners:** https://aka.ms/MsftSecurityPartners

New SMB Security SKUs

Microsoft is offering three new SMB Security SKUs to provide security added value for Microsoft 365 Business Premium subscription plans for mid- market organisations (25-300 seats): Defender for BP, Purview for BP, Defender & Purview for BP

M365 Business Premium ($34.55/u/m)

- Cloud Services
- M365 Apps Desktop, Web & Mobile
- Microsoft Entra ID P1 ($9.45/u/m)
- Intune ($12.60/u/m)
- M365 Defender for Business ($4.73/u/m)
- M365 Defender for Office P1 ($3.15/u/m)

+ Defender Suite for Business Premium ($15.75/u/m)

(E5 Security)

- Microsoft Defender for Office 365 Plan 2 ($7.88/u/m) (Email Protection)
- Microsoft Defender for Cloud) Apps ($5.45/u/m) (SaaS Protection)
- Microsoft Entra ID P2 ($14.18/u/m) (Identity Protection, PAM)
- Microsoft Defender for Identity ($8.62/u/m) (Identity Monitoring)
- Microsoft Defender for Endpoint P2 ($8.19/u/m) (Endpoint Protection)
- Microsoft Defender for IoT – EIoT ($1.33* /d/m) (IoT Protection)

+ Purview Suite for Business Premium ($15.75/u/m)

(E5 Purview)

- M365 E5 eDiscovery & Audit ($10.80/u/m)
- M365 E5 Insider Risk Management ($10.80/u/m)
- M365 E5 Information Protection & Governance ($12.60/u/m)

+ Defender & Purview Suite for Business Premium ($23.52/u/m)

(E5 Security & Purview)

- Microsoft Defender for Office 365 Plan 2 ($7.88/u/m)
- Microsoft Defender for Identity ($8.62/u/m)
- M365 E5 eDiscovery & Audit ($10.80/u/m)
- Microsoft Defender for Cloud Apps ($5.45/u/m)
- Microsoft Defender for Endpoint P2 ($8.19/u/m)
- M365 E5 Insider Risk Management ($10.80/u/m)
- Microsoft Entra ID P2 ($14.18/u/m)
- Microsoft Defender for IoT – EIoT ($1.33*/d/m)
- M365 E5 Information Protection & Governance ($12.60/u/m)

*CSP List Price M/Y

Crayon