

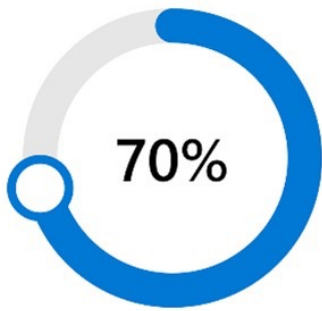
# A GUIDE TO MICROSOFT SECURITY TECHNOLOGIES

# TABLE OF CONTENTS

<b>Product Families</b>	Page 5
<b>Microsoft Defender</b>	
• Microsoft Defender	Page 6
• Defender for Cloud	Page 7
• Defender for Business	Page 8
• Defender for individuals	Page 9
<b>Microsoft Entra</b>	Page 10
• Active Directory	Page 10
• Microsoft Entra Permissions Management	Page 12
• Microsoft Entra Verified ID	Page 13
• Microsoft Entra Workload Identities	Page 14
• Microsoft Entra Identity Governance	Page 15
<b>Microsoft Intune</b>	Page 16
<b>Microsoft Priva</b>	Page 18
• Microsoft Priva Privacy Risk Management	Page 18
<b>Microsoft Purview</b>	Page 19
• Microsoft Sentinel	Page 20
<b>Additional information (quick views of portals):</b>	Page 21
• Microsoft 365 Defender	Page 21
• Microsoft Sentinel	Page 21
• Microsoft Defender for Cloud	Page 21

## MICROSOFT SECURITY

Increased security concerns with the changing SMB landscape.



Over 70% of SMBs think cyber threats are becoming more of a business risk.



With nearly one in four SMBs stating that they had a security breach in the last year, they have reason to be concerned.



Less than half of the SMBs surveyed have a dedicated IT security person in-house.

To better understand the evolving SMB security demands, Microsoft conducted a survey of more than 150 small and medium-sized organisations in April 2022.

More than 70% of SMBs responded that the risk posed by cyberthreats to their businesses is rising. They have cause for fear because almost one in four SMBs report having had a security compromise in the previous year. In reality, ransomware assaults have increased by more than 300 percent, and more than half of them targeted small enterprises.

Even while SMBs face comparable risks to businesses, they frequently lack access to the necessary tools and resources. Many SMBs still rely on conventional antivirus programs to protect themselves. Even while 80 percent of SMBs claim to have some sort of antivirus protection, 93 percent still worry about the growing and changing nature of cyberattacks, with phishing, ransomware, and data security topping their list of worries.

SMBs are particularly vulnerable since they sometimes have limited resources and no trained security personnel. Fewer than half of the SMBs polled, claimed to have an internal IT security specialist, and SMBs rank a shortage of qualified security personnel as their top security risk issue. Sophisticated enterprise security solutions are frequently too expensive, too complex, or both.

### Delivering on security for all to help protect SMBs

Microsoft shared their belief in security for all and agreed that small and medium-sized businesses should be able to afford the same degree of security as large corporations. With the release of the standalone edition of Microsoft Defender for Business, they're thrilled to move that objective one step closer today. Defender for Business offers SMBs endpoint detection and response (EDR) features of enterprise-grade endpoint protection at prices and with the ease of use that small business clients and their partners expect.

Microsoft 365 Business Premium, an all-inclusive security and productivity solution for companies with up to 300 employees, already comes with Microsoft Defender for Business. Defender for Business is now available for purchase as a stand-alone product.



5

#### reasons to choose

Microsoft Defender for Business



Enterprise-grade endpoint security



Easy to use



Cost-effective



Top-rated security vendor<sup>1</sup>



Flexible licensing

## Enterprise-grade security to protect against ransomware and other cyberthreats

SMBs require enhanced security to guard against the number and sophistication of cyberattacks like ransomware. Many SMBs continue to use outdated antivirus software, which offers only a single layer of security by matching signatures to guard against known threats. In order to protect and remediate against known and unknown threats, Defender for Business offers multi-layered protection, detection, and response that spans the five phases of the National Institute of Standards and Technology (NIST) cybersecurity framework—identify, protect, detect, respond, and recover. Let's take a closer look at the capabilities:

### Identify

Threat and vulnerability management enables you to prioritize and concentrate on the flaws that threaten your company's operations. You can proactively provide the groundwork for a safe environment by identifying, prioritizing, and addressing software vulnerabilities and configuration errors.

### Protect

Attack surface reduction options help to minimize your attack surface (like the places that your company is vulnerable to cyberattacks across your devices and applications), leaving bad actors with fewer ways to perform attacks.

Next-generation protection helps to prevent and protect against threats at your front door with antimalware and antivirus protection—on your devices and in the cloud.

### Detect and respond

Endpoint detection and response provides behavioral-based detection and response alerts so you can identify persistent threats and remove them from your environment.

### Recover

Auto-investigation and remediation help to scale your security operations by examining alerts and taking immediate action to resolve attacks for you. By reducing alert volume and remediating threats, Defender for Business allows you to prioritize tasks and focus on more sophisticated threats.

## Built for SMBs, easy to use, and cost-effective

Defender for Business was created with SMBs' needs in mind.

Microsoft aimed to offer a solution that was simple to set up and could automatically detect and remediate threats because IT administrators for SMB customers and partners frequently juggle multiple jobs at once. This gives you more time to concentrate on operating your business. Defender for Business has pre-installed policies to help you get going quickly. For Windows devices, we've also added a streamlined wizard-based onboarding process. It is planned to further simplify macOS, Android, and iOS.

By continuously detecting and automatically removing the majority of risks, automated investigation and remediation performs the kind of work often done by a professional Security Operations (SecOps) team.

## Benefits for partners

SMBs frequently, and correctly, rely on partners to secure their IT systems. We are aware that helping partners effectively secure their clients often requires giving them tools to do so.

Partners now have more opportunities thanks to Defender for Business and Microsoft 365 Business Premium to help secure customers at scale with value-added managed services. For Microsoft Cloud Solution Provider (CSP) partners to view security incidents across tenants in a centralized interface, both solutions integrate with Microsoft 365 Lighthouse, which was commercially accessible on March 1, 2022.



## PRODUCT FAMILIES

The Microsoft Security Product Families are as per below:

### What is Microsoft Defender

Microsoft Defender for Cloud is a security posture management and workload protection solution that helps you improve the overall security posture of your environment and finds vulnerabilities throughout your cloud configuration. It also offers threat protection for workloads across multi-cloud and hybrid environments.

### What is Microsoft Entra

The new product line, Microsoft Entra, includes all of Microsoft's identity and access features. Microsoft Azure Active Directory (Azure AD) and two new product categories, decentralized identity and cloud infrastructure entitlement management (CIEM), are all part of the Entra family. The Entra family of products, which offer identity and access management, cloud infrastructure entitlement management, and identity verification, will contribute to ensuring that everyone has secure access to everything.

### What Is Microsoft Intune

Microsoft Intune is a cloud-based endpoint management solution. It controls user access and makes managing apps and devices across all of your different endpoints—including mobile phones, desktop PCs, and virtual endpoints—simpler. On devices controlled by the organization and those owned by the users, access and data can be protected.

### What is Microsoft Priva

Microsoft Defender for Cloud is a security posture management and workload protection solution that helps you improve the overall security posture of your environment and finds vulnerabilities throughout your cloud configuration. It also offers threat protection for workloads across multi-cloud and hybrid environments.

### What is Microsoft Defender

Priva gives you the tools you need to: Identify and guard against privacy threats including data hoarding, improper data transfers, and data oversharing in advance. Obtain insight into the handling and transfer of personal data. Encourage staff to handle data in a wise manner.

### What is Microsoft Purview

Your on-premises, multicloud, and software as a service (SaaS) data can be managed and governed with the help of Microsoft Purview, a unified data governance solution. With automated data discovery, sensitive data classification, and end-to-end data lineage, you can quickly generate a comprehensive, up-to-date map of your data environment.



## Microsoft Defender:

Integrated threat protection, detection, and response across endpoints, email, identities, applications, and data can help secure your users as attacks become more sophisticated.



### Endpoints

Discover and secure endpoint and network devices across your multiplatform enterprise.



### Cloud apps

Get visibility, control data, and detect threats across cloud services and apps.



### Identities

Manage and secure hybrid identities and simplify employee, partner, and customer access.



### Email and documents

Protect your email and collaboration tools from advanced threats, such as phishing and business email compromise.

## Microsoft Defender capabilities:

### Prevent cross-domain attacks and persistence

Automatically prevent threats from breaching your organization and stop attacks before they happen. Understand attacks and context across domains to eliminate lie-in-wait and persistent threats and protect against current and future breaches.

### Reduce signal noise

View prioritised incidents in a single dashboard to reduce confusion, clutter, and alert fatigue. Use automated investigation capabilities to spend less time on threat detection and focus on triaging critical alerts and responding to threats.

### Auto-heal affected assets

Handle routine and complex remediation with automatic threat detection, investigation, and response across asset types. Then return affected resources to a safe state and automatically remediate isolated attacks.

### Hunt threats across domains

Search across all your Microsoft 365 data with custom queries to proactively hunt for threats. Use your organisational expertise and knowledge of internal behaviors to investigate and uncover the most sophisticated breaches, root causes, and vulnerabilities.

Microsoft Defender is an approach that organisations use to safeguard the data and workflows associated with the individual devices that connect to a business network.

Microsoft defender is endpoint security that is best suited for organisations that are looking for an easy way to protect sensitive data and information.

Microsoft Defender empowers organisations of all sizes to rapidly stop attacks, scale your security resources, and evolve your defenses by delivering best-in-class endpoint security across Windows, macOS, Linux, Android, iOS, and network devices. This is best suited for organisations looking to secure their endpoint machines.

## Defender for cloud:

Bolster security posture, safeguard workloads against contemporary threats, and support the creation of secure apps. Protect your resources in hybrid and multicloud scenarios. Learn more about the synergistic interactions between Microsoft Defender for Cloud, Microsoft Entra Permissions Management, Azure Network Security, GitHub Advanced Security, and Microsoft Defender External Attack Surface Management to deliver complete cloud security.



### Reduce risk with contextual security posture management

Assess multicloud and hybrid cloud security in real time and improve posture by prioritising the most critical risk with context-aware cloud security.



### Help prevent, detect, and respond quickly to modern threats

Help prevent, detect, and respond quickly to modern threats. Strengthen protection against evolving attacks with a comprehensive solution across multicloud and hybrid workloads.



### Unify security management for DevOps

Empower security teams with unified DevOps security management across multicloud and multiple-pipeline environments to help keep software secure from the start.

## Defender for cloud capabilities:

### Visualise and improve security posture proactively

Get free continuous assessment, built-in benchmarks, and recommendations to improve your cloud security posture in Azure, AWS, and Google Cloud.

### Prioritise critical risks with contextual threat analysis

Discover high-priority risks with attack path analysis. Get contextual threat data from cloud security graph queries to help prioritise remediation.

### Help protect workloads comprehensively

Gain broad coverage to secure workloads with insights from industry-leading security intelligence across virtual machines, containers, databases, and storage.

### Efficiently scan with agentless or agent-based approach

Get agentless and agent-based vulnerability scanning for agility and comprehensive workload protection.

### Unify visibility for DevOps security posture

Gain visibility into DevOps inventory and the security posture of application code and configurations across multicloud and multiple-pipeline environments.

### Accelerate remediation of critical issues in code

Prioritise and provide remediation guidance natively in the developer tools based on comprehensive contextual insights from development to runtime.

### Secure configurations throughout the development lifecycle

Enable security of infrastructure-as-code templates and container images to minimise cloud misconfigurations reaching production environments.

### Get cloud-security benchmark mapped to industry frameworks

Follow best practices for multicloud security compliance with controls mapped to major regulatory industry benchmarks by default.

Microsoft Defender for Cloud is best suited for organisations looking for security and visibility across all of the Azure, on-premises and multicloud (Amazon AWS and Google GCP) workloads. Defender for cloud fills 3 vital security needs as they manage their workloads both in the cloud and on-premises.

1. Knowing the security posture of the organisation by identifying and tracking vulnerabilities
2. Harden workload resources and services with the best security standards
3. Detect and resolve threats to your resources and services

Defender for Cloud is best suited for organisations looking for Cloud Workload Protection Platform (CWPP) and Cloud Security Posture Management (CSPM) Solutions.

## Microsoft Defender for Business:



### Elevate your security

Defender for Business delivers a comprehensive security solution to help you secure your business, allowing you to focus on what matters.



### Enterprise-grade endpoint protection

Deploy security across your devices, and use automated built-in intelligence to rapidly protect, detect, and respond to threats.



### Simple setup, easy to use

Take advantage of streamlined onboarding and management experiences that provide actionable insights for fast and easy use.



### Cost-effective protection

Deliver comprehensive security value at a price point that works for your business.



### Defender for Business capabilities

Defender for Business is optimized to meet the needs of small and medium-sized businesses of up to 300 users.



### Simplified client configuration

Configure devices in a few simple steps with recommended security policies activated right out of the box.



### Threat and vulnerability dashboard

Identify and manage software vulnerabilities and misconfigurations in real time.



### Next-generation protection

Reinforce and verify the security perimeter for your network.



### Endpoint detection and response

Detect and respond to attacks using behavioral-based detection, plus manual and live response capabilities.

## Additional capabilities:

### Automated investigation and remediation

Automatically investigate alerts to help address complex threats.

### Cross-platform functionality

Extend protection across devices for Windows, macOS, iOS, and Android.

### Threat intelligence from our security experts

Proactively guard against threats using human and AI analysis of trillions of signals.

### Network protection and web blocking

Guard against dangerous domains that host malicious content and help protect your devices from web threats.

Microsoft Defender for Business is a suite of security technologies that help customers protect their networks, this is a wholistic endpoint security solution that helps SMB businesses with upto 300 users protect themselves against cyber threats, including Malware and Ransomware in an easy-to-use cost effective package.

Microsoft Defender comprises of many additional features and many product sets within the stack.



## Microsoft Defender for individuals:

An easy-to-use security app for individuals and families that helps protect identities, data, and devices from online threats.

### Online security, simplified



#### All-in-one security app

Get one centralised view to easily manage and monitor the security status of your and your family's personal information, computers, and phones.



#### Safeguard your identity and devices

Get trusted antivirus and identity theft monitoring for you and your family.



#### Stay ahead of hackers and scammers

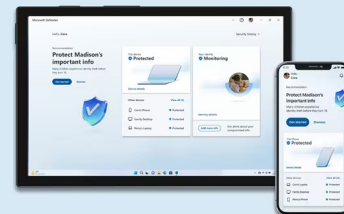
Get real-time alerts with recommended actions plus security tips about how to stay safer online.

### Manage your security in one place



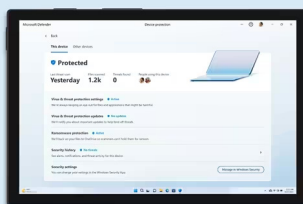
- Access a simple dashboard to easily check your protections and take actions to stay safer online.
- Quickly check the security status of your and your family's protected devices.
- Review alerts and take recommended actions.
- View the status of other antivirus protections you and your family may be using.

### Improve the security of your identity with Experian®



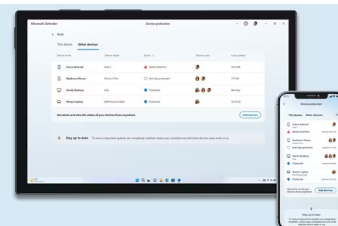
- Help protect your and your family's identity with continuous web monitoring of your personal data.
- Receive alerts if your or a family member's information is compromised or at risk.
- Use expert guidance to take steps to protect your and your family's identity.
- Call an identity theft restoration expert anytime, day or night.
- Get identity theft insurance<sup>4</sup>, up to USD 1 million, to help cover fees associated with restoration.

### Get reliable device protection



- Protect your and your family's devices against malware, spyware, and ransomware with continuous antivirus and anti-phishing scans.
- Get alerted if any malicious apps are detected.
- Specify files and apps that you use regularly and don't want Microsoft Defender to scan.

### Stay informed and stay safer



- Review security tips in your dashboard to help keep you and your family safer online.
- Stay ahead of threats with daily automatic updates to your protections.

## Microsoft Entra:

Microsoft Entra is the new name for the family of identity and access technologies now brought into one place under one portal. Entra goes beyond the traditional identity and Access Management – it's Microsoft's Vision for the future of Identity and access.

### Identity and access for a connected world

Confidently enable smarter, real-time access decisions for all identities across hybrid, multicloud, and beyond.



#### Protect access to any app or resource

Safeguard your organisation by protecting access to every app and every resource for every user.



#### Secure and verify every identity

Effectively secure every identity including employees, customers, partners, apps, devices, and workloads across every environment.



#### Provide only the access necessary

Discover and right-size permissions, manage access lifecycles, and ensure least privilege access for any identity.



#### Simplify the experience

Keep your users productive with simple sign-in experiences, intelligent security, and unified administration.

## Azure Active Directory:

Safeguard your organisation with a cloud identity and access management solution that connects employees, customers and partners to their apps, devices, and data.



### Protect your users, apps, workloads, and devices

Learn how Azure Active Directory (Azure AD) can help with your identity and access management business challenges.



#### Secure adaptive access

Protect access to resources and data using strong authentication and risk-based adaptive access policies without compromising user experience.



#### Seamless user experiences

Provide an easy, fast sign-in experience across your multicloud environment to keep your users productive, reduce time managing passwords, and increase productivity.



#### Unified identity management

Manage all your identities and access to all your applications in a central location, whether they're in the cloud or on-premises, to improve visibility and control.

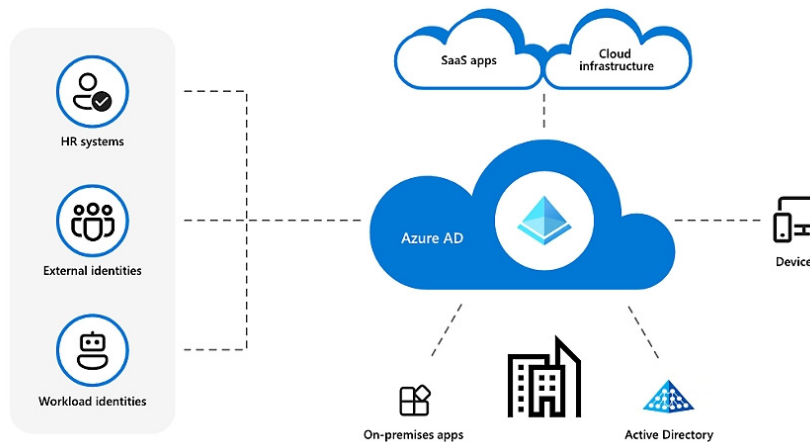


#### Simplified identity governance

Control access to apps and data for all users and admins efficiently with automated identity governance to ensure only authorized users have access.

## Multicloud identity and access management

Azure AD is an integrated cloud identity and access solution, and a leader in the market for managing directories, enabling access to applications, and protecting identities.



### Comprehensive capabilities:

Azure AD helps protect your users from 99.9 percent of cybersecurity attacks.

#### Single sign-on

Connect your workforce to all your apps, from any location, using any device.

#### Multifactor authentication

Help safeguard access to data and apps and keep it simple for users.

#### Conditional access

Apply the right access controls to keep your organisation more secure.

#### External identities

Share resources or apps with users outside your organisation.

#### Identity governance

Help protect, monitor, and audit access to critical assets.

#### Passwordless

Provide ease of use without the inherent risk of passwords.

#### Lifecycle management

Automate and simplify the access lifecycle.

#### Identity protection

Automate detection and remediation of identity-based risks.

#### Privileged identity management

Strengthen the security of your privileged accounts.

#### App integrations

Simplify app access from anywhere with single sign-on.

### Azure AD comes in four editions:

Azure AD Free - The free edition of Azure AD is included with a subscription of a commercial online service such as Azure, Dynamics 365, Intune, Power Platform, and others.

- **Office 365** - Additional Azure AD features are included with Office 365 E1, E3, E5, F1, and F3 subscriptions.<sup>4</sup>
- **Azure AD Premium P1** - Azure AD Premium P1, included with Microsoft 365 E3, offers a free 30-day trial. Azure and Office 365 subscribers can buy Azure AD Premium P1 online.
- **Azure AD Premium P2** - Azure AD Premium P2, included with Microsoft 365 E5, offers a free 30-day trial. Azure and Office 365 subscribers can buy Azure Active Directory Premium P2 online.

Microsoft Active Directory is developed for customers who have Microsoft and Windows Domain networks and require visibility of their network identities and centralised domain management.

## Microsoft Entra Permissions Management:

One unified solution to manage the permissions of any identity across multicloud infrastructure.

### Discover, remediate, and monitor permission risks for any identity or resource

Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) product that provides comprehensive visibility and control over permissions for any identity and any resource in Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP).



#### Get full visibility

Discover what resources every identity is accessing across your cloud platforms.



#### Automate the principle of least privilege

Use usage analytics to ensure identities have the right permissions at the right time.



#### Unify cloud access policies

Implement consistent security policies across your cloud infrastructure.

### Discover all cloud permissions

Get comprehensive and multidimensional visibility into actions performed by any identity on any resource across your cloud infrastructures.

### Evaluate your permission risks

Assess permission risks by evaluating the gap between permissions granted and permissions used.

### Manage permissions and access

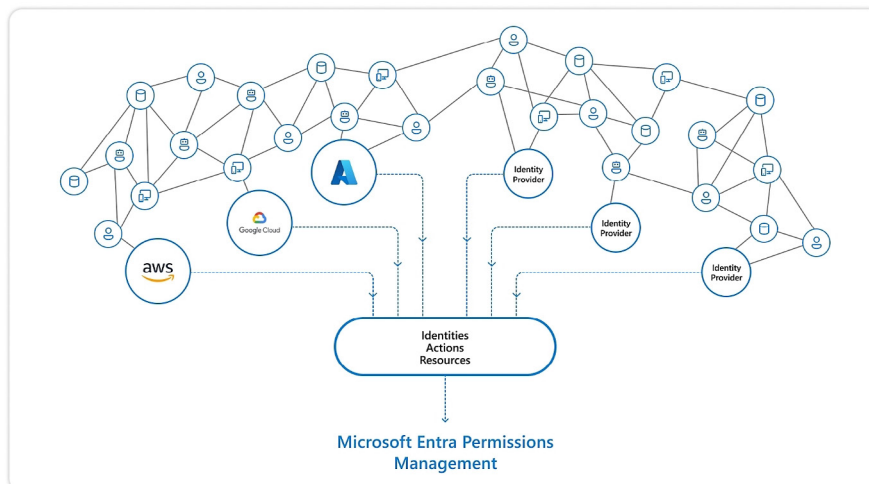
Right-size permissions, grant permissions on demand, and automate just-in-time access.

### Monitor permissions continuously

Detect anomalous activities with machine learning-powered alerts and generate detailed forensic reports.

## Navigate multicloud with an integrated CIEM solution

Discover how Microsoft Entra Permissions Management helps you improve your security posture by ensuring the principle of least privilege across identities and resources in your IaaS infrastructure.



Microsoft Entra Permissions Management is a solution best suited for organisation's that are looking for comprehensive visibility into permissions assigned to all identities – users and workloads – actions, and all resources across cloud infrastructure and identity providers. Microsoft Entra Permissions Management is a Cloud Infrastructure Entitlement Management (CIEM) solution.

## Microsoft Entra Verified ID:

Microsoft Entra Verified ID is an Issuance and Verification Service, the enable identity owners within the service to generate, present, and verify claims. This essentially forms the basis of Trust between the users of the system.

### Start your decentralised identity journey

Enable more secure interactions with Verified ID, the industry-leading global platform from Microsoft.



#### Quickly onboard employees, partners, and customers

Digitally validate identity information to ensure trustworthy self-service enrollment and faster onboarding.



#### Provide self-service account recovery

Replace support calls and security questions with a streamlined self-service process to verify identities.



#### Access high-value apps and resources

Quickly verify an individual's credentials and status to grant least-privilege access with confidence.



#### Work with a Microsoft Partner

Ensure a smooth and secure verifiable credential experience, made possible by Microsoft partnerships with leading identity verification providers.

## Verified ID capabilities

Confidently issue and verify workplace credentials, education status, certifications, or any unique identity attributes with Verified ID.

### Easily set up and deploy

Start issuing and accepting verifiable credentials in minutes by configuring Verified ID in your Microsoft Entra administrator portal.

### Create and issue credentials

Customise and configure verifiable credentials for individuals using a prebuilt template or your own rules and design files

### Verify credentials

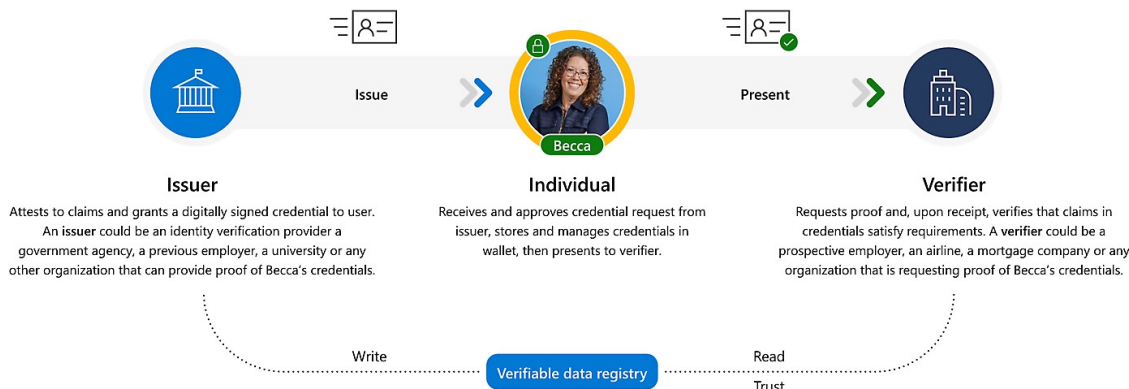
Enable interactions that respect the individual's privacy. Validate a Verified ID credential with their approval through their digital wallet.

### Suspend or invalidate credentials

Revoke or suspend active verified status of an individual's credential, while allowing the invalidated credential to remain in their possession.

## Help people control their digital identity

Based on open standards, Verified ID automates verification of identity credentials and enables privacy-protected interactions between organisations and users.



Microsoft Entra Verified ID is best suited for organisations looking to efficiently verify and issue workplace credentials, education status, Certifications, or any unique identity attributes, it also helps organisations empower their users to own and control their Digital Identity for improved business security.



## Microsoft Entra Workload Identities:

Microsoft Entra Workload Identities lets organisations set Conditional Access policies, such as blocking compromised apps or services and access attempts from nontrusted locations. There's also an Identity Protection capability for things like "compromised credentials, anomalous sign-ins, and suspicious changes to accounts.

### Manage and secure access by apps and services to cloud resources



#### Create more secure access policies

Assign conditional access policies to your apps or services based on location and risk level, all in one place.



#### Detect compromised identities

Help reduce risk exposure by intelligently detecting and responding to compromised workload identities.

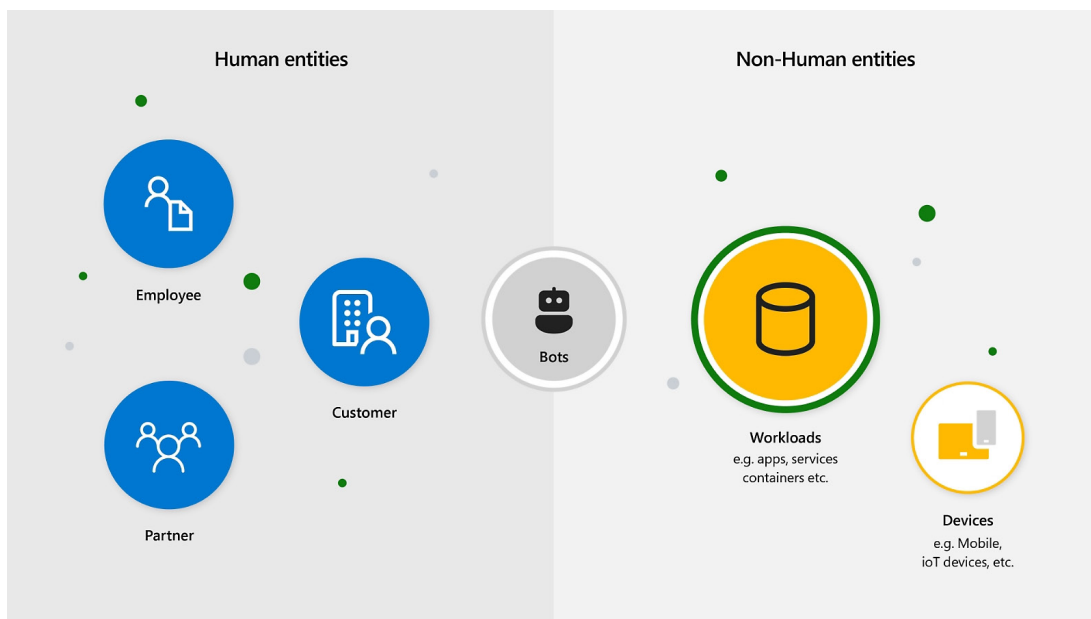


#### Simplify lifecycle management

Manage lifecycles more easily with insight into access activities and status of workload identities.

## What are workload identities?

Workload identities are identities granted to apps or services that need to access and communicate with other services.



## Enhance security with conditional access

Create security policies for each workload identity using conditional access.

#### Contain threats and reduce risk

Intelligently detect and respond to compromised workload identities using cloud-based AI.

#### Get more insight into workload identities

See new and unused workload identities and receive actionable recommendations to address security issues.

#### Review usage and implement least privilege

See new and unused workload identities, then review their privileged access regular.

Microsoft Entra Workload identities is best suited for organisations looking to create more secure access policies, detect compromised identities and simplify lifecycle management for their business users and environments

## Microsoft Entra Identity Governance:

Microsoft Entra Identity Governance allows organisations to balance the organisation's need for security and employee productivity with the right processes and visibility for existing business critical third party on-premises and cloud based applications.

### Enhance productivity and security

Identity governance increases employee productivity and helps meet compliance and regulatory requirements.



#### Improve productivity

Automate employee, supplier, and business partner access to apps and services—in the cloud and on-premises—at enterprise scale. Help ensure that people have access when they require it—without the burden of manual approvals.



#### Strengthen security

Reduce risk arising from access abuse and make smart access decisions based on machine learning. Set up requirements for recurring reviews to ensure that there is a continuing need for users, group memberships, and access.



#### Simply powerful. Powerfully simple

Cloud-based, for straightforward deployment and operation.  
Flexible, to support both cloud and on-premises apps and resources. Integrated, for unparalleled support of Microsoft resources. Open, to support hundreds of non-Microsoft apps.  
Robust, to meet the needs of all types of organisations.

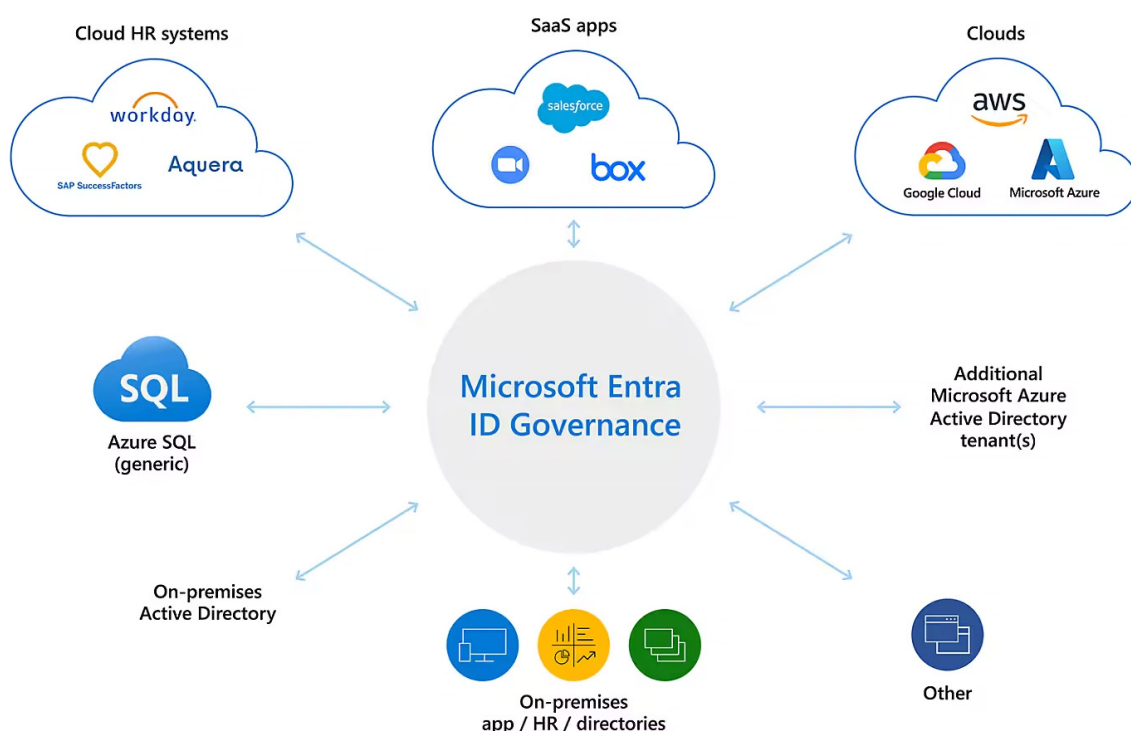


#### Automate routine tasks

Delegate day-to-day resource access requests to relevant business groups and automate the approval process for customary resource access to help you focus on AI-provided insights and exceptions

### Control identities and access

Automatically create user identities and roles in the apps users need to access and maintain and remove user identities as status or roles change.



## Microsoft Entra ID Governance capabilities

Get robust identity governance and simple deployment with Microsoft Entra ID Governance.

### Entitlement management

Manage the identity and resource access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.

### Lifecycle workflows

Design workflows to ensure new employees and those with role changes are productive immediately—and that accesses are removed when employees leave.

### Access reviews

Ensure that users or guests have appropriate access and still need it, based on automated insight. Enable self-assessment or assign reviewers.

### Privileged identity management

Automatically mitigate excessive, unnecessary, or misused access to important resources in your organisation with time and approval-based role activation.

Microsoft Entra Identity Governance is best suited for organisations that have an integration requirement for their heterogeneous platforms across the Datacentre, including HR on-premises HR systems, business directories and databases. Microsoft Entra Identity Governance augments Azure AD cloud-hosted services by enabling organisations to have the right user access for their business applications.

## Microsoft Intune:

Previously a component of Microsoft Endpoint Manager, Microsoft Intune is now a family of endpoint management tools. In that family, Configuration Manager is still a crucial member.



## See, manage, and help secure all endpoints in one place

Manage and protect endpoints for better hybrid work experiences and lower total cost of ownership with Intune



### Simplify endpoint management

Cut costs and complexity by managing any device with a single, unified tool already built into Microsoft 365. Gain full visibility into the health, compliance, and security status of your cloud and on-premises endpoints.



### Help protect a hybrid workforce

Fortify your Zero Trust security architecture with a management solution that builds resiliency and centralises endpoint security and identity-based device compliance. Help protect data on company-owned and bring-your-own devices.



### Power better user experiences

Empower IT to deliver the best possible endpoint experience through zero-touch deployment, flexible, non-intrusive mobile application management, and proactive recommendations based on Microsoft Cloud data.

## Be more efficient

Save up to 60 percent by using comprehensive Microsoft Security rather than multiple point solutions.

### Reduce your security and compliance costs with Microsoft Security



1. Savings based on publicly available estimated pricing for other vendor solutions and web direct/base price shown for Microsoft offerings. Price is not guaranteed and subject to change.

## Microsoft Intune capabilities

### Cross-platform endpoint management

Manage on-premises, cloud, mobile, desktop, and virtualised endpoints across platforms including Windows, mac, iOS, Android, and Linux operating systems.

### Built-in endpoint security

Reduce risk of endpoint vulnerabilities with automatic threat detection and remediation.

### Mobile application management

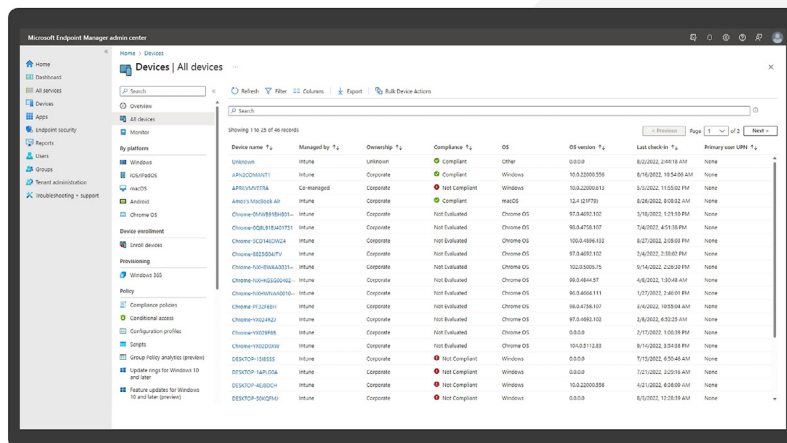
Help protect data without requiring mobile device enrollment while giving workers flexible, non-intrusive experiences.

### Endpoint analytics

Improve user experiences every day with app and device health scores. Limit slowdowns that impact productivity with data-driven recommendations.

### Specialty and shared devices for frontline workers

Support the diverse technology needs of frontline workers with capabilities like shared device mode, maintenance windows, and endpoint management for specialty devices.



Microsoft Intune is best suited for organisation who are looking for a cloud-based enterprise mobility management tool that aims to help organisations manage the mobile devices employees use to access corporate data and applications, such as email for example.

## Microsoft Priva:

Protect personal data, automate risk mitigation, and manage subject rights requests at scale.

### Streamline Privacy Management

Store, process, and dispose of personal information in compliance with local and global regulations.

Microsoft Priva Helps organisations to discover personal data automatically and provide key analytics and insights to Administrators, to help them understand the privacy issues and associated risks with the organisation.



#### Identify and resolve privacy risks

Assess your organisation's privacy posture and proactively find and resolve privacy risks like data hoarding, data transfers, and data oversharing.



#### Automate subjects rights requests

Process data subject requests and subject rights requests at scale with automated data discovery, conflict detection, in-place review, and secure collaboration.



#### Empower employees to make smart data handling decisions

Increase awareness of privacy requirements and risks with privacy training and automated reminders to review and delete obsolete items.

## Microsoft Priva Privacy Risk Management:

Microsoft Priva Privacy Risk Management helps organisations automatically discover where and how data is stored in Microsoft 365 data by means of leveraging data classification and user mapping intelligence.

### Build a privacy-resilient workplace

Identify personal data and critical privacy risks, automate risk mitigation, and empower employees to make smart data handling decisions.



#### Identify critical privacy risks and conflicts

Gain visibility into your personal data and associated data privacy risks arising from overexposure, hoarding, and transfers with automated data discovery and correlated risk signals.



#### Automate risk mitigation and prevent privacy incidents

Effectively mitigate privacy risks and prevent privacy incidents with automated policies and recommended user actions.



#### Empower employees to make smart data handling decisions

Foster a proactive privacy culture by increasing awareness of and accountability toward privacy incidents and risks without hindering employee productivity.

## Enhance security with conditional access

Create security policies for each workload identity using conditional access.

#### Actionable privacy insights

Assess your organisation's privacy posture—how much personal data exists in the environment, where it's located, how it moves, and the privacy risks detected.

#### Data transfer

Help detect personal data movements between customisable boundaries, such as geography or departments, and block risky transfers in near real time.

#### Data minimisation

Help detect unused personal data, send users email digests to review and delete obsolete items, and provide privacy training to reduce data hoarding.

#### Data overexposure

Help detect personal data overshare, inform file owners to review and adjust access, and provide privacy training to reduce overexposure incidents.

Microsoft Priva Privacy Risk management is ideally suited for organisations that require actionable insights around data privacy, data minimisation, data transfer and data over exposure within the organisations network.



## Microsoft Purview:

Governance, protection, and compliance solutions for your organisation's data.

Microsoft Purview is a Unified data Governance Solution that helps organisations manage and govern their on-premises, multicloud, and software as a service (SaaS) data.

## Microsoft Purview secures your most important asset: your data

You can't innovate without knowing where your data is. Get visibility, manage data securely, and go beyond compliance with Microsoft Purview. Safeguard all your data across platforms, apps, and clouds with comprehensive solutions for information protection, data governance, risk management, and compliance.



### Understand and govern data

It's never been harder to understand and govern an organisation's sensitive information. Get visibility into all your data and manage assets across your environment.



### Safeguard data, wherever it lives

Protect sensitive data across apps, clouds, and devices—even if it's not stored on Microsoft platforms.



### Improve risk and compliance posture

Identify data risks and manage regulatory requirements so your organisation can stay in compliance.

## Discover the Microsoft Purview product family

Help keep your organisation's data safe with a range of solutions for unified data governance, information protection, risk management, and compliance.

### Communication Compliance

Foster a safe and compliant workplace by detecting sensitive or inappropriate content shared across your organisation's communication channels.

### Compliance Manager

Reduce risk by translating complex regulatory requirements into specific improvement actions that help you raise your score and track progress.

### Data Lifecycle Management

Classify and govern data at scale to meet your legal, business, privacy, and regulatory content obligations.

### Data Loss Prevention

Automatically protect sensitive information from risky and unauthorised access across apps, services, endpoints, and on-premises files.

### Data Map and Data Catalog

Maximise the business value of data for your consumers by creating a unified map to automate and manage metadata from hybrid sources. Make data easily discoverable and understand the origin of your data with interactive data lineage visualisation.

### eDiscovery

Discover and manage your data in-place with end-to-end workflows for internal or legal investigations.

### Information Protection

Discover, identify, classify, and protect sensitive data that is business critical, then manage and protect it across your environment.

### Insider Risk Management

Detect, investigate, and act on critical risks in your organisation, including data theft, data leaks, and security policy violations.

Microsoft Purview is suited for customers who are looking or require data discovery, Purview helps organisations understand their data discovery problems and enhance the understanding for IT security teams.

Ultimately, the better an organisation can understand their data, the more effectively they can secure and use the data across their environment.

## Microsoft Sentinel:

See and stop Threats across your entire enterprise with intelligent security analytics.

Microsoft Sentinel is a cloud-native security information and event manager (SIEM) platform that makes use of Artificial Intelligence to help analyse large volumes of data across the organisation quickly.



### Build next-generation security operations

Uncover sophisticated threats and respond decisively with an easy and powerful security information and event management (SIEM) solution, powered by the cloud and AI.



#### Get unlimited cloud speed and scale

Eliminate security infrastructure setup and maintenance, and elastically scale to meet your security needs—while reducing costs as much as 48 percent compared to legacy SIEM solutions.



#### Empower your SOC with Microsoft intelligence

Optimise your SecOps with advanced AI, world-class security expertise, and comprehensive threat intelligence.



#### Detect, investigate, and respond effectively

Stay ahead of evolving threats with a unified set of tools to monitor, manage, and respond to incidents.



#### Lower your total cost of ownership

Get started faster while reducing infrastructure and maintenance with a cloud-native SaaS solution.

## Microsoft Sentinel capabilities

### Collect data at cloud scale

Easily connect your logs with Microsoft Sentinel using built-in data connectors—across all users, devices, apps, and infrastructure—on-premises and in multiple clouds.

### Stay ahead of threats

Gain more contextual and behavioral information for threat hunting, investigation, and response using built-in entity behavioral analytics and machine learning.

### Accelerate response and save time by automating common tasks

Triage incidents rapidly with automation rules and automate workflows with built-in playbooks increasing security operations centre (SOC) efficiency.

### Streamline investigation with incident insights

Visualise full scope of an attack, investigate related alerts, and search historical data.

## Integrated threat protection with SIEM and XDR

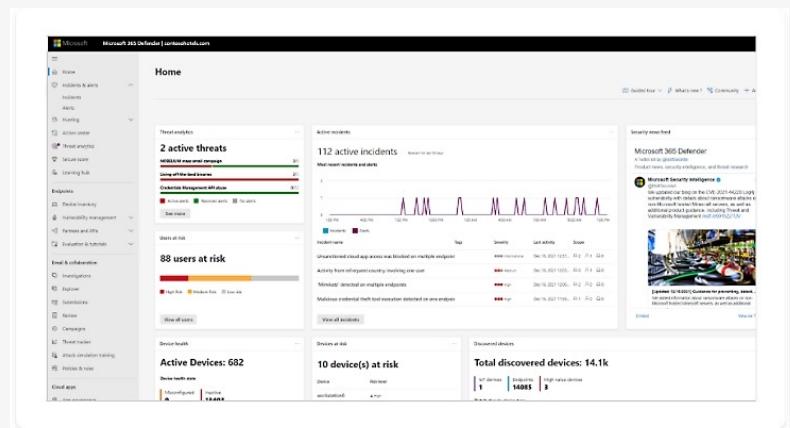
Microsoft empowers your organisation's defenders by putting the right tools and intelligence in the hands of the right people. Combine security information and event management (SIEM) and extended detection and response (XDR) to increase efficiency and effectiveness while securing your digital estate.

Microsoft Sentinel provides organisation with the much needed tools to perform an analysis of threats, proactive hunting and threat response.

It is best suited for organisations who have a need or focus on data collection, threat detection, incident investigation and incident response capabilities.

### Microsoft 365 Defender

Prevent and detect attacks across your Microsoft 365 workloads with built-in XDR capabilities.

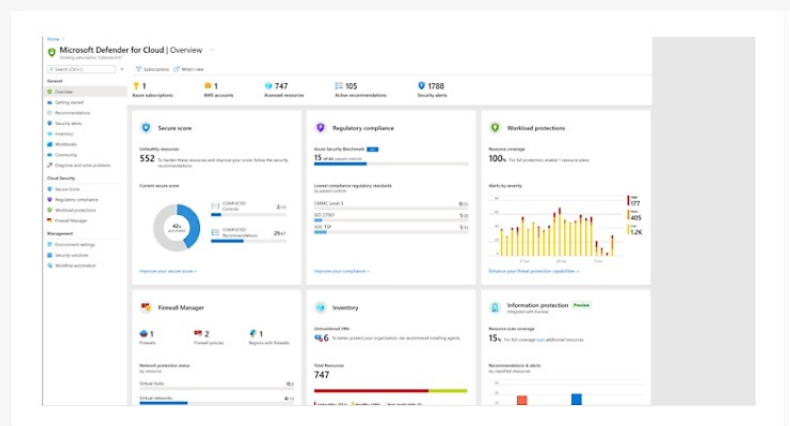


### Microsoft Sentinel

Aggregate security data and correlate alerts from virtually any source with cloud native SIEM from Microsoft.


### Microsoft Defender for Cloud

Help protect your multicloud and hybrid cloud workloads with built-in XDR capabilities.



## CONTACT US

 [microsoft.firstdistribution.com](https://microsoft.firstdistribution.com)

 +27 (0) 11 540 2640

 [microsoft.leads@firstdistribution.com](mailto:microsoft.leads@firstdistribution.com)