Microsoft Security

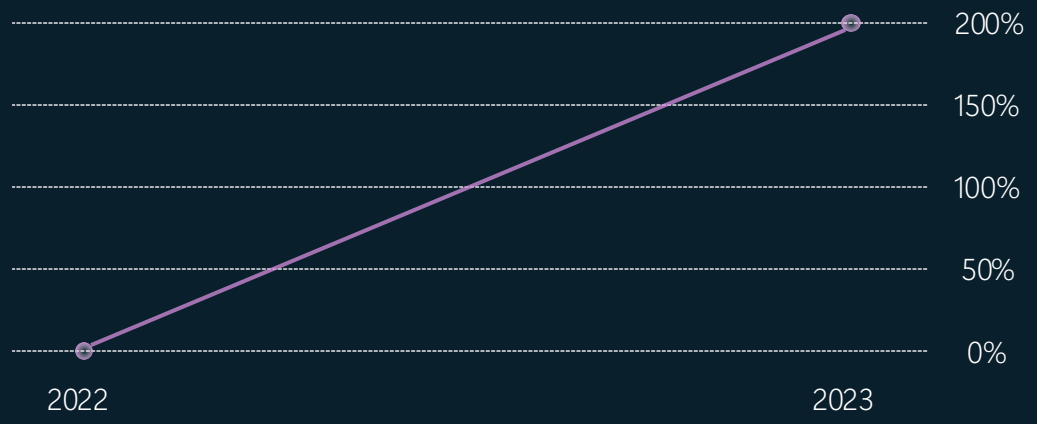
Security Success Kit

Contents

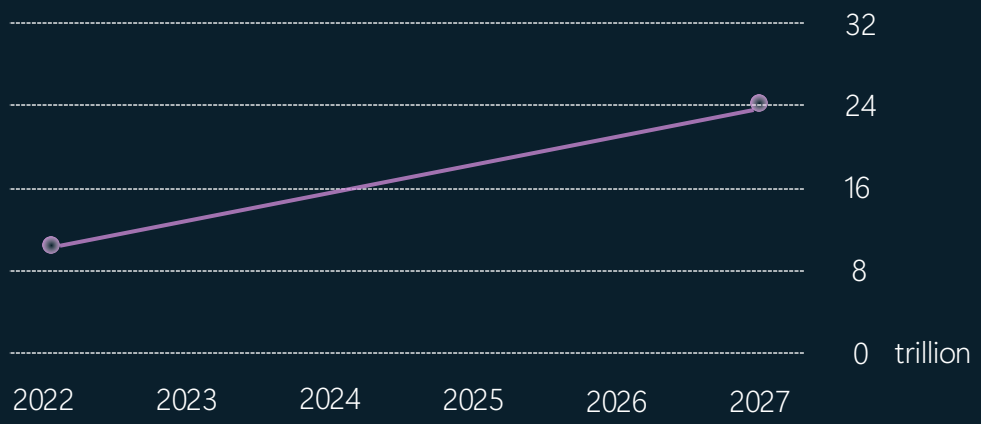
Explore how Microsoft Security can safeguard your digital estate

Microsoft's response to evolving cybersecurity threats

With a **200%** increase in human-operated ransomware attacks from 2022 to 2023[1] and an estimated **7,000** password attacks per second, the odds are against security defenders.[2]



Additionally, research indicates the cost of cyberattacks will reach **$24 trillion** by 2027, up from $8.5 trillion in 2022.[3]



1. Microsoft Digital Defense Report (MDDR) 2023.
2. Microsoft Diigtal Defense Report (MDDR) 2024.
3 Statistica

Microsoft Security helps you do more with less with a unified approach to security

Simplify vendor management

Eliminate redundant capabilities and reduce license and consumption costs by **25%** by consolidating with Microsoft Security.[1]

Reduce threats with AI and automation

Detect and respond faster and more accurately to attacks and insider risks and protect and govern data.

Improve operational efficiency

Increase productivity with automation and process improvements with improved security management.

Efficient security management resulted in **50%** increased efficiency and optimized headcount.[1]

[1] Forrester Consulting, "The Total Economic Impact™ of Microsoft Security", February 2023, commissioned by Microsoft

Save costs with Microsoft´s integrated, comprehensive cybersecurity solutions

Lack of visibility into cyber threats across endpoints, cloud workloads, apps, and services allow attackers to go undetected, making it harder for SecOps teams to get ahead of risks and prevent repeat attacks, detect in-progress attacks, and respond.

With **78 trillion** threat signals synthesized per day in 2024, Microsoft proves to be a leader in security, staying ahead of threats.[1]

By simplifying your security operations with seamlessly integrated end-to-end protections, you gain cost savings, improved productivity, and increased value of your security investment.

60%

potential cost savings by consolidating licenses with Microsoft 365 E5 Security and Microsoft 365 E5 Compliance.[2]

75%

reduction in password requests after introducing Self-service Single-Sign-On (SSO) with Azure Active Directory.[3]

$479,000

human capital freed up by redeploying IT time with Microsoft Endpoint Manager.[4]

231%

ROI when investing in Microsoft Security.[5]

1 Microsoft Digital Defense Report (MDDR) 2024.

2 Savings based on publicly available estimated pricing for other vendor solutions and Web Direct/Base Price shown for Microsoft offerings

3 Forrester Consulting, "The Total Economic Impact™ Of Zero Trust Solutions From Microsoft", December 2021, commissioned by Microsotf

4 Forrester Consulting, "The Total Economic Impact™ Of Microsoft Endpoint Manager," April 2021, commissioned by Microsoft

5 Forrester Consulting, "The Total Economic Impact ™ Of Microsoft Security", February 2023, commissioned by Microsoft

“

With the help of Microsoft Unified support, we installed advanced safeguards on tens of thousands of endpoints in a matter of a week or two.”

- Will Luker, Chief Information Security Officer, Department of the Premier and Cabinet , Government of South Australia

Government of South Australia

Government of South Australia enhances security, drives resiliency with Microsoft Unified Support

34  agencies implemented Microsoft 365 E5 Security and E3, improving security and compliance

Quick response time from Unified Support on **430+** support requests

1,900 on-demand courses available for public sector employees

Learn more →

Defender Experts for XDR gave us so much more visibility beyond what our security team used to have and feed our team up to focus on threats that actually demand our attention."

- Chris Rowtcliff, Head of IT, Westminster School

Westminster School improves security and gets peace of mind with Microsoft Defender Experts for XDR

2,000+ students and staff protected

Almost **100%** action items remediated for each incident

Enhanced collaboration and cybersecurity

Learn more →

We sleep much more soundly knowing that Microsoft and Tanium are closely partnered to provide us with assurance on both the depth and quality of our security controls across our technology estate."

- Joe Silva, Chief Information Security Officer, Jones Lang LaSalle

JLL

Jones Lang LaSalle cuts cybersecurity spending by 20 percent by consolidating vendors and using Tanium and Microsoft Defender for Endpoint

$5 million saved annually with Microsoft 365 E5 cyber innovation

decrease in security spending

90,000 endpoints protected

Learn more →

“

The main advantage is that all products are centralized, allowing staff to access everything from one platform. They can easily switch between applications, such as moving from their mailbox to Microsoft Forms, all within a single sign-on session.”

- Maitha Mohamed Al Teneji, Director of infrastructure and Technical Equipment Department, MOHRE

UNITED ARAB EMIRATES
MINISTRY OF HUMAN RESOURCES
& EMIRATISATION

MOHRE boost productivity by 20% with Microsoft 365 E5

increase in employee productivity

5x more mailbox size

Improved collaboration among more than 1,000 employees

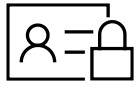
Learn more →

Zero Trust framework

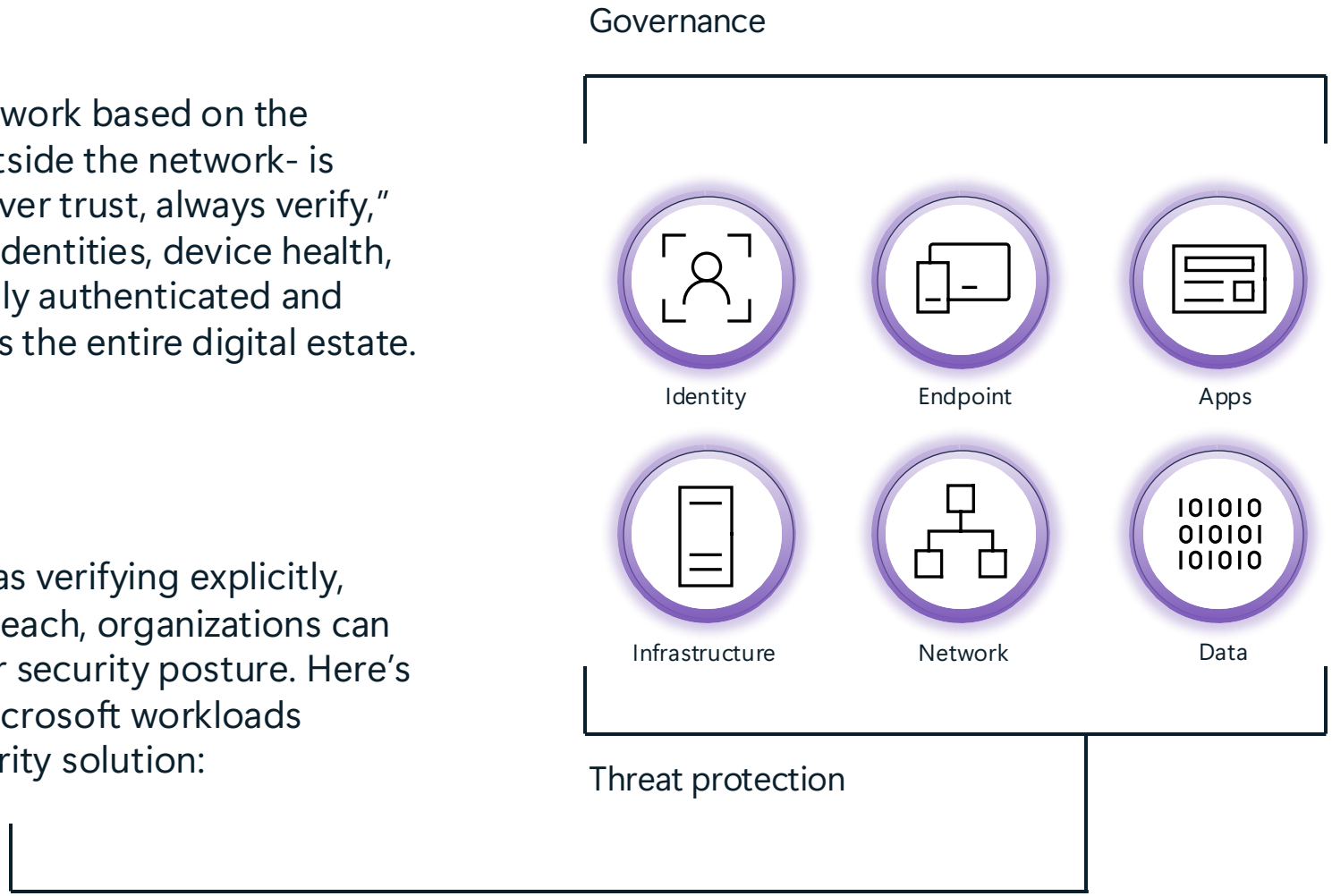
Zero Trust framework

Discover how our products integrate to protect your digital estate

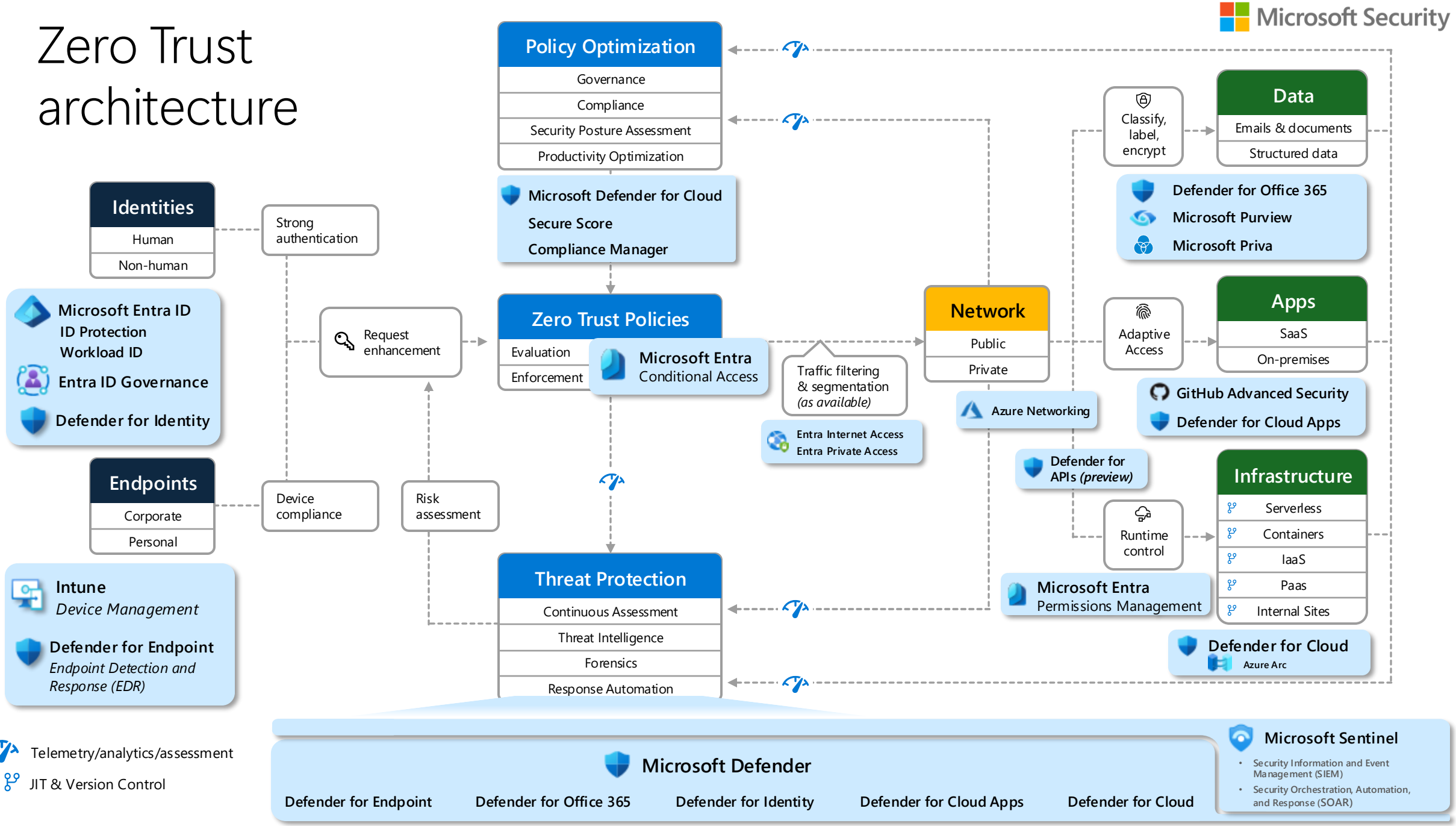
Zero Trust is a comprehensive security framework based on the principle that no entity-whether inside or outside the network- is inherently trustworthy. Its approach is to “never trust, always verify,” emphasizing continuous verification of user identities, device health, and access permissions. This ensures that only authenticated and authorized users can access resources across the entire digital estate.



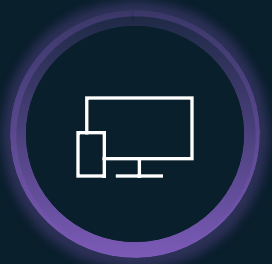
By implementing Zero Trust principles, such as verifying explicitly, using least privilege access, and assuming breach, organizations can significantly minimize risks and enhance their security posture. Here’s a sample Zero Trust architecture where all Microsoft workloads seamlessly integrate to deliver a robust security solution:



Zero Trust architecture



Workload adoption pathways



Advanced Identity & Device Management

Threat Protection

Data Security

Modern Security Operations

Cloud Security

Identity and Device Management

Enhanced solutions

Adoption pathway

My organization requires modern identity and device management capabilities

My team needs guidance on understanding Microsoft Security workloads that can help drive my organization's secure identity and device management strategy

Entra → Intune →

My team needs to learn how to get started with deploying the products to enhance security for accessing our applications

Entra → Intune →

I want to become highly proficient and skilled in using Microsoft Entra and Intune →

I want to learn more about advanced deployment, integrate workloads, or develop an architecture of my own →

Stay abreast on latest updates and tech →

Threat Protection

For MDO, MDI, MDE, MDCA

Enhanced solutions

Adoption pathway

My organization requires modern threat protection capabilities

My team needs an understanding of the Defender family's capabilities for threat detection, suspicious activity remediation, and incident response →

My team needs to learn how to get started with deploying the products under the Defender family →

I want to become highly proficient and skilled in using the Defender family of products →

I want to learn more about advanced deployment, integrate workloads, or develop an architecture of my own →

Stay abreast on latest updates and tech →

Data Protection

For Purview workloads and Priva

Enhanced solutions

Adoption pathway

My organization requires data security capabilities

My team seeks guidance on which products and workloads to leverage for securing my organization's data estate

Purview → Priva →

I want to learn how to deploy, operate, and troubleshoot Microsoft Purview and Microsoft Priva workloads →

I want to set up a framework to achieve my organization's security requirements and determination of all the appropriate data security solutions →

I want to become highly proficient and skilled in using the Purview and Priva workloads →

Stay abreast on latest updates and tech →

Sentinel

Enhanced solutions

Adoption pathway

My organization requires modernization of its security operations

My team needs guidance for modernizing SecOps strategy, processes, architecture, technology, and SIEM capabilities →

I want to learn how to deploy, operate, and troubleshoot Microsoft Sentinel →

I want Microsoft assistance to design a solution architecture to support my Sentinel deployment →

I want to become highly proficient and skilled in using Sentinel →

Stay abreast on latest updates and tech →

Defender for Cloud

Enhanced solutions

Adoption pathway

My organization requires help protecting cloud resources across multi and hybrid cloud environments

My team needs guidance on understanding Microsoft Defender for Cloud and how it can help protect my cloud resources →

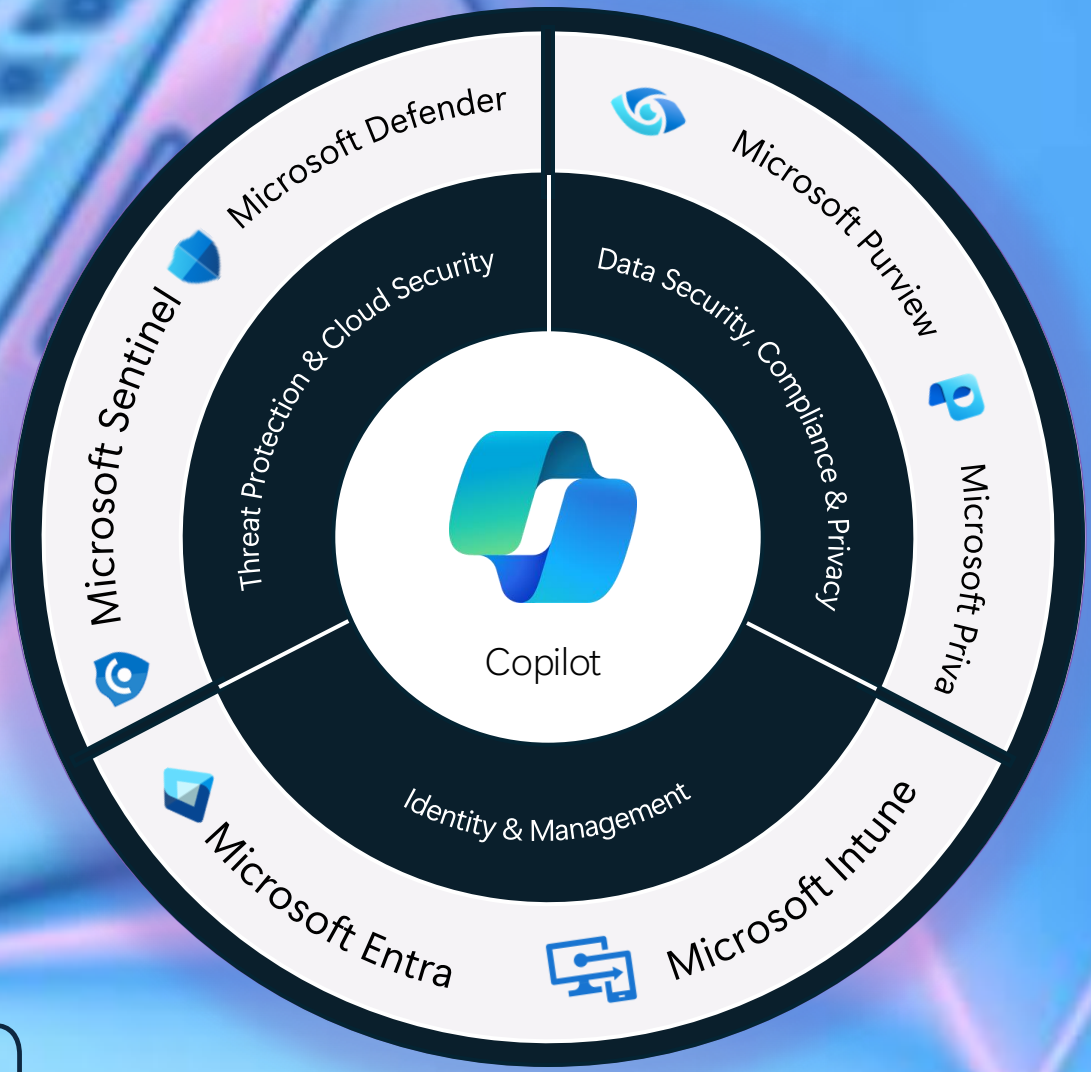
I want to learn how to set up and deploy Microsoft Defender for Cloud →

I want to learn more about advanced deployment, integrate workloads, or develop an architecture of my own →

I want to become highly proficient and skilled in using Defender for Cloud →

Stay abreast on latest updates and tech →

Product information



Microsoft Defender

Microsoft Defender offers integrated security solutions that deliver comprehensive threat prevention, detection, and response capabilities for all users.

Key capabilities:

Proactive prevention, detection, and mitigation to attacks across devices, workloads, clouds, and more

Enterprise–grade endpoint protection

Safeguard all data from potential malicious threats

Microsoft 365 Defender subproducts

Defender for Office 365: Secure email and Microsoft Teams with advanced protection against phishing, ransomware, and other cyberthreats.

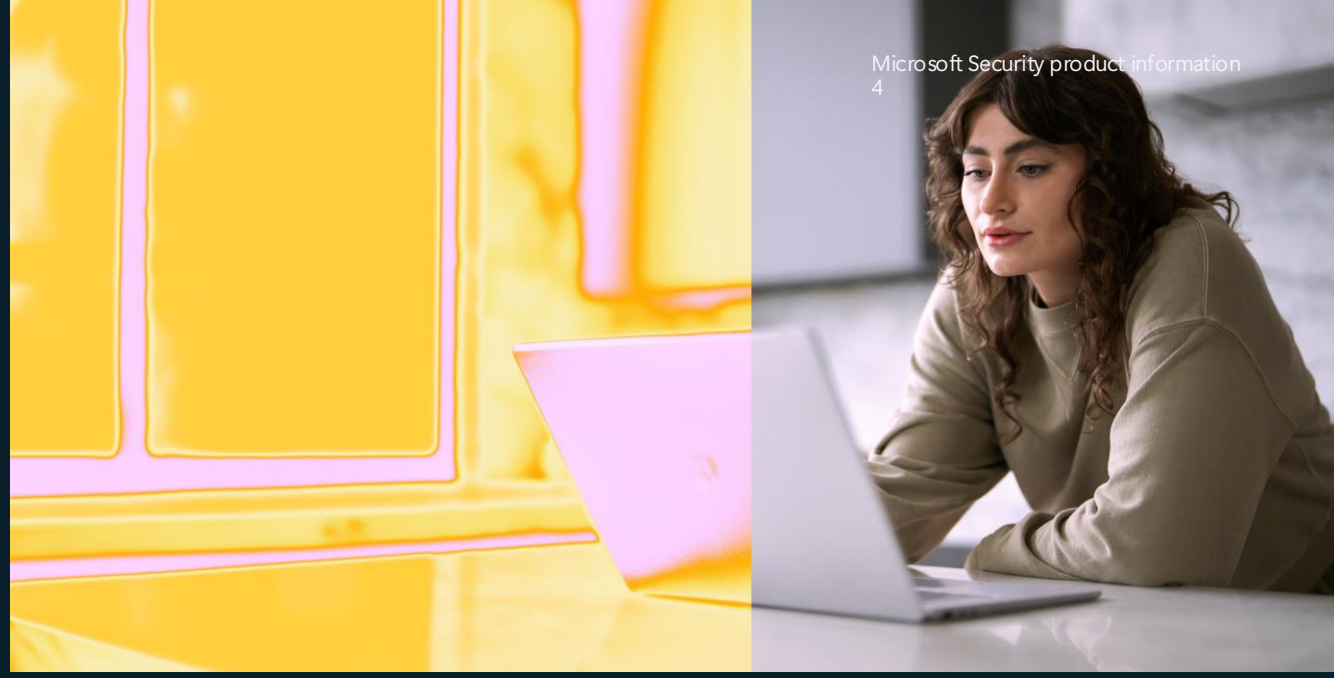
Defender for Endpoint: Safeguard against malicious threats posed by email, links (URLs), and collaboration tools.

Defender for Identity: Detect and investigate advanced threats, compromised identities, and malicious insider actions.

Defender for Cloud Apps: Secure apps, protect data, and elevate app posture with software as a service (SaaS) security.

Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native security information and event management (SIEM) that provides cyberthreat detection, investigation, response, and proactive hunting, with a bird's-eye view across your enterprise.



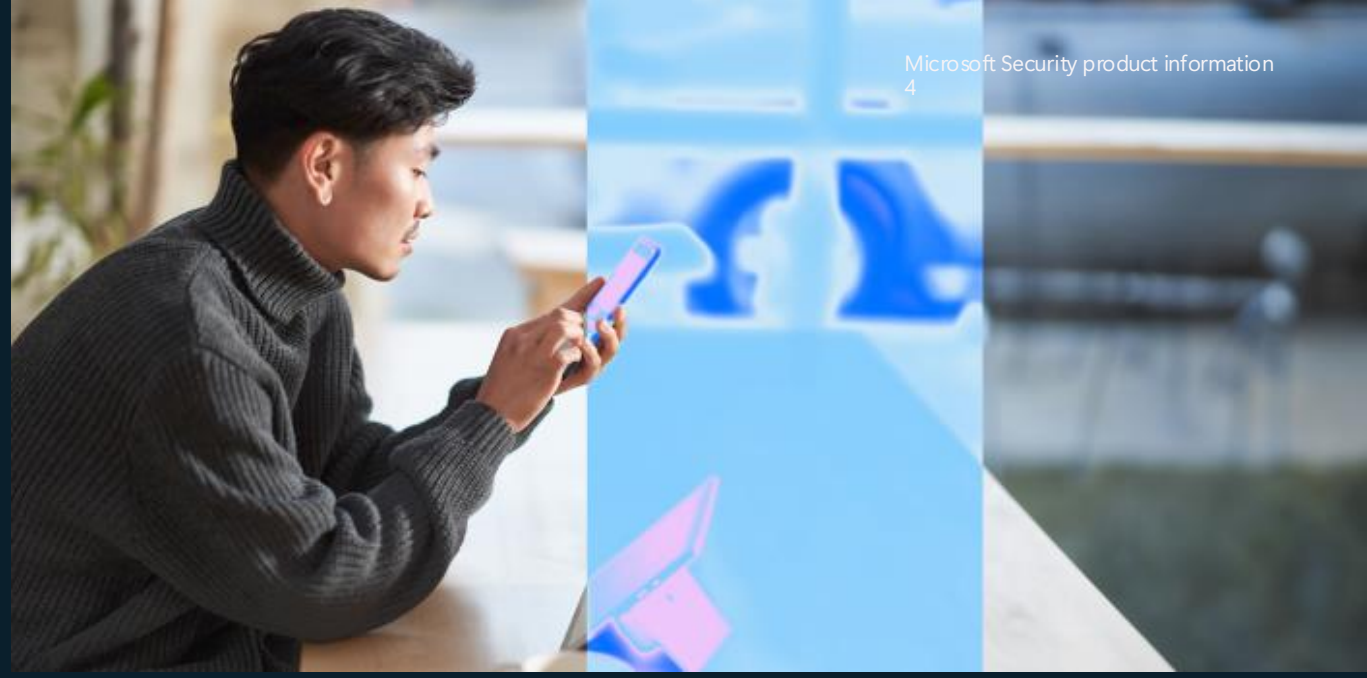
Key capabilities:

- Collect data across all users, devices, applications, and infrastructure
- Utilize AI to investigate threats and hunt for suspicious activity at scale
- Detect previously undetected threats
- Enable scalable automation as new technologies and threats emerge

Sentinel

Microsoft Endpoint Manager (Intune)

Microsoft Intune provides simplified endpoint management to protect and manage your endpoints in one place.



Key capabilities:

- Cross-platform endpoint management
- Endpoint analytics
- Mobile application management and Microsoft Configuration Manager

Intune

Cloud Security

Microsoft Defender for Cloud is a cloud-native application protection platform that is designed to protect cloud-based applications from cyber threats.

Key capabilities:

- Cloud security posture management (CSPM)
- Unifies security management at the code level across multicloud environment
- Multicloud visibility

Microsoft Entra

Microsoft Entra is a single place to secure identities and access to any resource

Key capabilities:

- Single sign-on (SSO) to all apps
- Conditional Access, Evaluation, and Risk-Based Policies
- Multifactor and passwordless authentication
- Identity lifecycle and governance

Entra

Microsoft Purview

Microsoft Purview helps govern, protect, and manage data across Microsoft and non-Microsoft assets with a unified, comprehensive approach.

Key capabilities:

Data governance: Manage visibility and governance of data assets across your environment

Data protection: Protect sensitive data across clouds, apps, and devices

Risk and compliance: management: Identify data risks and manage regulatory compliance requirements

Microsoft Purview subproducts

Purview Insider Risk Management: Secure email and Microsoft Teams with advanced protection against phishing, ransomware, and other cyberthreats.

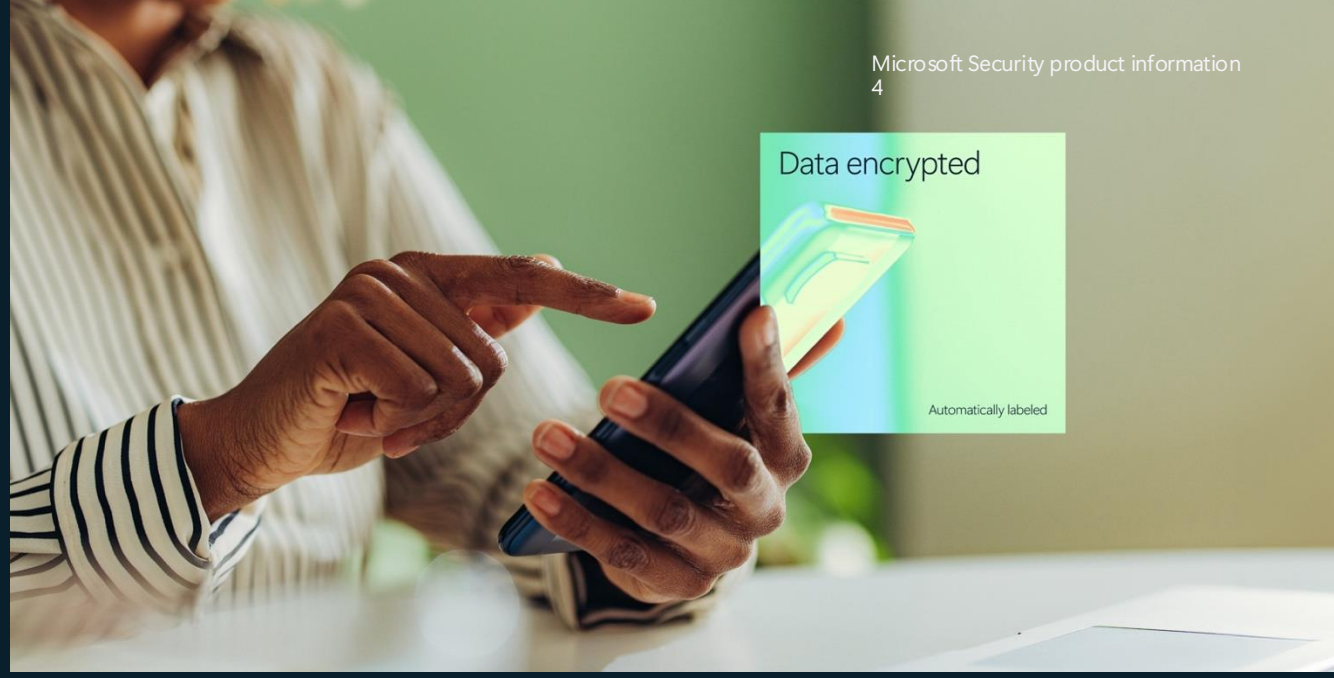
Purview Information Protection: Manage and protect your business data by implementing data classification, sensitivity labels, and advanced encryption.

Purview Data Lifecycle Management: Retain the content you need and delete the content you don´t with built-in information governance.

Purview Data Loss Prevention: Provides intelligent detection and control of sensitive data using built-in exfoliation policies for M365 apps and services.

Microsoft Priva

Microsoft Priva helps manage and build a privacy-resilient workplace by safeguarding personal data and standardizing compliance.



Key capabilities:

- Identify and remediate privacy risks
- Accelerate digital transformation and ensure customer data stays private
- Automate and consolidate data privacy operations and responses across on-premises, hybrid, and multicloud environments

Priva

Deployment guidance

Onboarding & Deployment Guidance: Microsoft Entra

Configure Microsoft Entra ID

Microsoft Entra ID is a cloud-based identity and access management service that helps your employees sign in and access apps and services. Learn how to configure initi...

Go to guide

Add or sync users to Microsoft Entra ID

Based on your environment and needs, you can choose to add users individually, migrate your on-premises directory with Microsoft Entra Connect cloud sync or...

Go to guide

Collaborate using B2B or multitenant organizations

This guide enables organizations to more securely share applications and services with guest users from other organizations while maintaining control over their own...

Go to guide

Plan your self-service password reset deployment

Microsoft Entra ID self-service password rest (SSPR) gives users the ability to change or reset their password, with no administrator or help desk involvement...

Go to guide

Clean up Microsoft Entra ID for education

This guide helps you maintain a healthy tenant and keep administration manageable. You'll be guided through typical year-end transition task that cove...

Go to guide

Migrate AD FS to Microsoft Entra ID

Using Microsoft Entra ID rather than AD FS as your main authentication process will reduce the risk of a security breach. Use this guide to migrate from your existing...

Go to guide

Plan your passwordless deployment

Upgrade your sign-in approach to allow users to access their devices securely without entering passwords. This guide will help you discover the best passwordless...

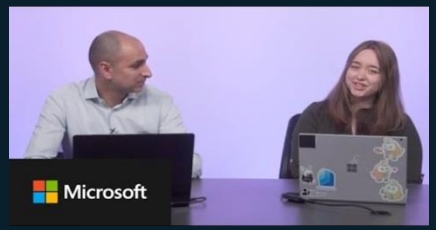
Go to guide

Prepare your environment

Before you start using Microsoft 365, turn on basic features and strengthen the security of your data in the Microsoft cloud

Go to guide

Microsoft Entra Suite deep dives



How to set up Microsoft Entra ID Protection

Microsoft Entra ID Beginner's Tutorial (Azure Active Directory)

Onboarding & Deployment Guidance: Microsoft Intune

Deploy and set up Microsoft Intune and Intune Suite

Deploy and set up Microsoft Intune to manage devices in your organization. For full control of corporate devices, use Intune's...

Go to guide

New Microsoft Intune Suite with Privilege Management, Advanced Analytics, Remote Help & App VPN

Onboarding & Deployment Guidance: Microsoft Purview & Priva

Protect data with Microsoft Purview Information Protection

Implement Microsoft Purview Information Protection to help you discover, classify, and protect sensitive information wherever it lives or travels. Microsoft Purview...

Go to guide

Configure Microsoft Purview Audit

Microsoft auditing solutions provide an integrated solution to help organizations effectively respond to security events, forensic investigations, and compliance...

Go to guide

Set up Microsoft Purview Data Lifecycle and Records management

Data Lifecycle Management is needed to classify your organization's data and how long it's retained. Get guidance...

Go to guide

Set up Microsoft Purview Data Loss Prevention (DLP) policy

Protect sensitive data comprehensively with the Microsoft Purview DLP policies. These policies extend to email...

Go to guide

Endpoint Data Loss Prevention (DLP) | What it is and how to set it up in Microsoft 365

Data Loss Prevention across endpoints, apps, & services | Microsoft Purview

Microsoft Purview Compliance Manager setup guide

Microsoft Purview Compliance Manager helps you manage your organization's compliance requirements with ease and convenience. Learn how Compliance...

Go to guide

Configure eDiscovery solutions in Microsoft 365

Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases. You can use...

Go to guide

Set up Microsoft Purview Communication Compliance and Insider Risk Management

Insider risks are a top concern for security and compliance professionals. These risks can result in workplace harassment, the loss of intellectual property, and more...

Go to guide

Set up Microsoft Priva

Microsoft Priva helps manage and build a privacy-resilient workplace by safeguarding personal data and standardizing compliance.

Go to guide

Microsoft Purview Insider Risk Management Admin Set-up Tutorial

Microsoft Priva | AI-based privacy management for Microsoft 365

Go to the next slide for more resources

Onboarding & Deployment Guidance: Microsoft Defender Family

Set up your Zero Trust security model

Zero Trust is a security model that more effectively adapts to the complexity of the modern environment, embraces the hybrid workplace, and helps protect people...

Go to guide

Set up Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a cloud access security broker (CASB) with features that let you take control of the cloud apps in your environment. It...

Go to guide

Deploy and configure Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a unified platform for preventive protection, post-breach detection, automated investigation, and respond...

Go to guide

Deploy Microsoft Defender for Office 365

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links, and collaboration tools.

Go to guide

Deploy Microsoft Defender for Identity

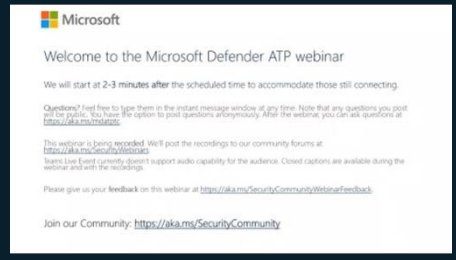
Microsoft Defender for Identity, formerly Azure Advanced Threat Protection, is a cloud-based security solution. It used your on-premises Active Directory signals to...

Go to guide

Analyze your security posture with Security analyzer

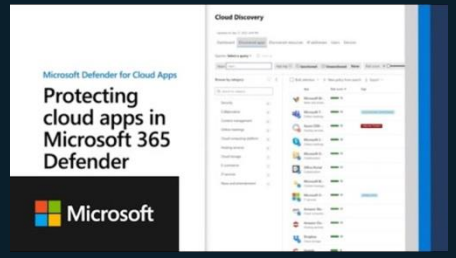
The Microsoft security suite offers an integrated ecosystem to help protect your organization. The Microsoft secure score is a measurement of an organization's...

Go to guide



Microsoft Defender for Endpoint webinar: Gain end-to-end security for your endpoints

Microsoft Defender for Identity webinar: Deployment and configuration



Protecting cloud apps in Microsoft 365 Defender

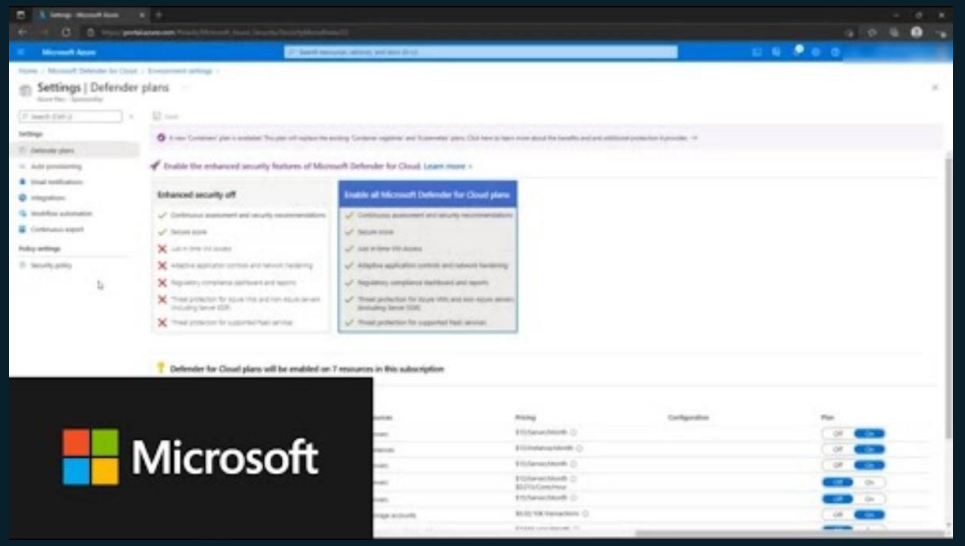
Microsoft Defender for Office 365

Onboarding & Deployment Guidance: Microsoft Defender for Cloud

Microsoft Defender for Cloud

Microsoft Defender for Cloud is a cloud-native application protection platform that is designed to protect cloud-based applications from cyber threats.

Go to guide



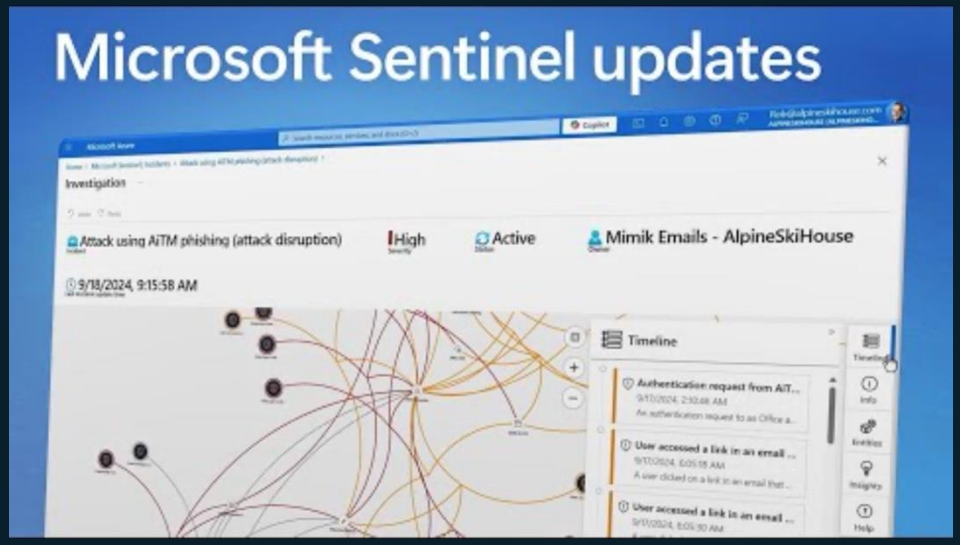
Getting Started with Microsoft Defender for Cloud

Onboarding & Deployment Guidance: Microsoft Sentinel

Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native security information and event management (SIEM) that provides cyberthreat detection, investigation, response, and proactive hunting.

Go to guide



Microsoft Sentinel AI, Process Automation & SIEM Migration

Deployment assistance

Deployment Assistance: FastTrack for Microsoft 365

FastTrack is a Microsoft delivered benefit designed to help you deploy Microsoft Security products.

If your subscription is eligible for the FastTrack benefit, Microsoft specialist are available to provide deployment assistance at no added cost. A request for Assistance (RFA) can be raised to receive support. The ability to submit a new RFA is available for administrators of primary Microsoft 365 services, security, and compliance.

Request FastTrack assistance →

Eligible customers can access FastTrack and related user enablement resources. Explore the technical documentation below for self-guided deployment guides.

- Microsoft Intune →
- Microsoft Purview Information Protection →
- Microsoft Purview Insider Risk Management →
- Microsoft Entra ID (Azure AD Premium) →
- Defender for Endpoint →

Training, certifications, and skilling

Training, certifications, and skilling

Microsoft provides comprehensive technical guidance and resources to support the planning and implementation of modern cybersecurity strategies, architectures, processes, and technologies. Whether you're an aspiring, new, or experienced cybersecurity professional, you can access a wealth of tools and training to build both foundational and advanced skills. Additionally, Microsoft offers opportunities to earn credentials that showcase your expertise. Through Microsoft Learn, you'll find practical insights to address security challenges and prepare for the evolving demands of the cybersecurity landscape.

Defend Against cyber threats with Microsoft Defender XDR

"Validate your technical skills and open doors to new opportunities by proving your ability to detect and respond to cyberthreats."

Earn your credential

Implement Microsoft Purview Insider Risk Management

"Learn to effectively detect, investigate, and respond to internal risks while protecting data, ensuring compliance, and maintaining employee trust."

Start the learning path

Defender for Cloud in the field

"Turn possibility into reality with simplified cloud security posture management and workload protection with Microsoft Defender for Cloud."

Watch now

Microsoft Sentinel & Defender XDR Virtual Ninja Training

"This training, based on the Ninja blogs bring you up-to-date quickly on all things Microsoft Defender XDR."

Watch now

See below certifications and applied learning for each one

Certifications and applied learning

Course certification for each workload

Explore role-based and workload-centric certifications for our Microsoft Security product families

- Threat Protection
- SecOps
- Identity
- Microsoft cybersecurity architect exam
- Data Security
- Multicloud security
- Data governance

Applied skilling

Hands-on, scenario-based training focused on real use cases

- Sentinel
- Cloud Security
- Data Security (information protection and data loss prevention)
- Microsoft Defender
- Data Security (retention, eDiscovery, and Communication Compliance in Microsoft Purview

Microsoft Learn Security Hub


Stay connected

Get in touch with Microsoft

Connect with the community →

Join the conversation in the Security Compliance, and Identity community, with cybersecurity discussions and posts that explore key security topics.

Find a Microsoft Training Services Partner →

Discover Training Services Partners around the world that offer security training solutions in formats and styles to help you meet your leaning goals.

Check out Microsoft Security Virtual Training Days →

Learn to protect your data and organization with Microsoft Security solutions, including identity and access management and compliance.

Boost your team's skills →

Take advantage of the security training resources and opportunities for team skill-building on Microsoft Learn for Organizations.

Meet the Microsoft AI Red Team →

Gain practical insights on how to safeguard your organization's AI with guidance and best practices from the industry-leading Microsoft AI Red Team.

Follow Microsoft cybersecurity news →

Read the latest Microsoft cybersecurity news, from recent work by Microsoft to strengthen protection, to helping keep used data safe around the world.

Get the latest on Security Copilot →

Stay up to date with the most recent Security Copilot developments, along with current releases, known issues, and plans for updates.