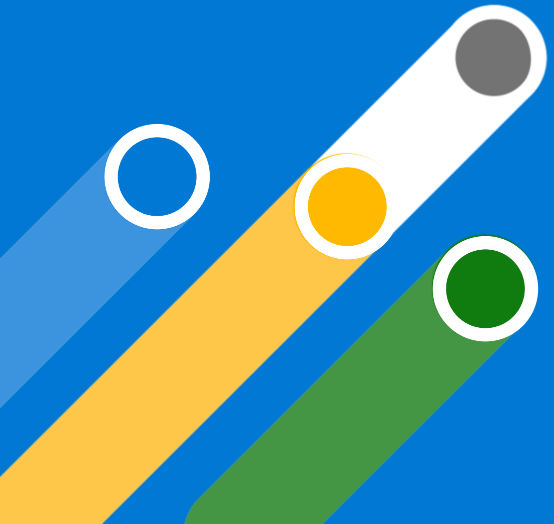
Microsoft Security

Microsoft Security adoption guide

Strengthen security while maximizing your investment

The increasingly complex state of cybersecurity, with its rapidly accelerating and expanding attack surfaces and rising risk mitigation and remediation costs, requires a comprehensive, end-to-end approach that's AI-powered and best in breed.



In the changing global dynamics and economic conditions, with the scarcity of cyber professionals and inflation pushing wages higher, everyone involved with security now needs to do more with less, balancing costs and requirements against reduced resources.

We're here to help you get the most out of your Microsoft Security investment.

By selecting Microsoft Security, powered by Microsoft Defender and Microsoft Sentinel, as your core security foundation, you're on the path to safeguarding your people, data, and infrastructure across platforms and cloud environments.

Detect threats quickly, respond effectively, and fortify your security posture by relying on the comprehensive and cost-effective security solution with industry leading AI and automation.

Partnering with Microsoft to defend against threats

Stop attacks before they happen. Reduce your attack surface and protect your assets with best-in-class security.

- ✓ Reduce the likelihood of a data breach by **45%**[1]

Detect threats across all systems. Uncover sophisticated attacks like ransomware with XDR backed by global threat intelligence.

- ✓ Reduce time-to-threat mitigation by **50%**[2]

Investigate and respond faster. Reduce alert fatigue and respond quickly with ML-based detection and built-in automation.

- ✓ Reduce the amount of labor associated with advanced investigations by **80%**[3]

1. The Total Economic Impact™ of Azure Active Directory, commissioned study by Forrester Consulting, 8/2020.
2. The Total Economic Impact™ of Azure Security Center from Forrester Consulting.
3. The Total Economic Impact™ of Microsoft Azure Sentinel from Forrester Consulting.

The path to a more secure organization

You have the peace of mind that comes with a comprehensive security solution from Microsoft. Now it's time to support you in your security adoption journey.

The Microsoft Security adoption guide leads you through three key focus areas to help realize the full value of integrated Microsoft Security solutions, enabling you to innovate, create, and grow your business.

1 Getting started

2 Operationalizing security

3 Empowering end users

Microsoft Security

Getting started

Overview of the Microsoft Security portfolio

We're in an era of heightened economic uncertainty. Organizations of all types have seen the need to accelerate digital transformation to ensure worker productivity and respond to rapidly shifting customer expectations. Data and information are the lifeblood of the transformation but also increasingly attract cybercriminal activity.

To secure your environments, you must develop new digital capabilities and break down data silos across multiple clouds, a broad portfolio of apps, and every type of device.

We believe delivering anything less than comprehensive security against digital threats is no longer acceptable. We're committed to an integrated, end-to-end security approach.

Microsoft Security technology

Identity and access management

Secure access for a connected world

Threat protection

Stop threats across your entire organization

Cloud security

Comprehensive protection for multicloud resources, apps, and data

Information protection and governance

Safeguard sensitive data across clouds, apps, and endpoints

Risk management

Identify and remediate critical data risks within your organization

Compliance management

Assess compliance and respond to regulatory requirements

Embrace proactive security with Zero Trust

Zero Trust is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction, asserts least privilege access, assumes breaches, and relies on intelligence, advanced detection, and real-time response to threats.

Verify explicitly

Always make security decisions using all available data points, including identity, location, device health, resource, data classification, and anomalies.

Use least privilege access

Limit access with just-in-time (JIT), just-end-access (JEA), and risk-based adaptive polices.

Assume breach

Minimize blast radius with micro-segmentation, end-to-end encryption, continuous monitoring, and automated threat detection and response.

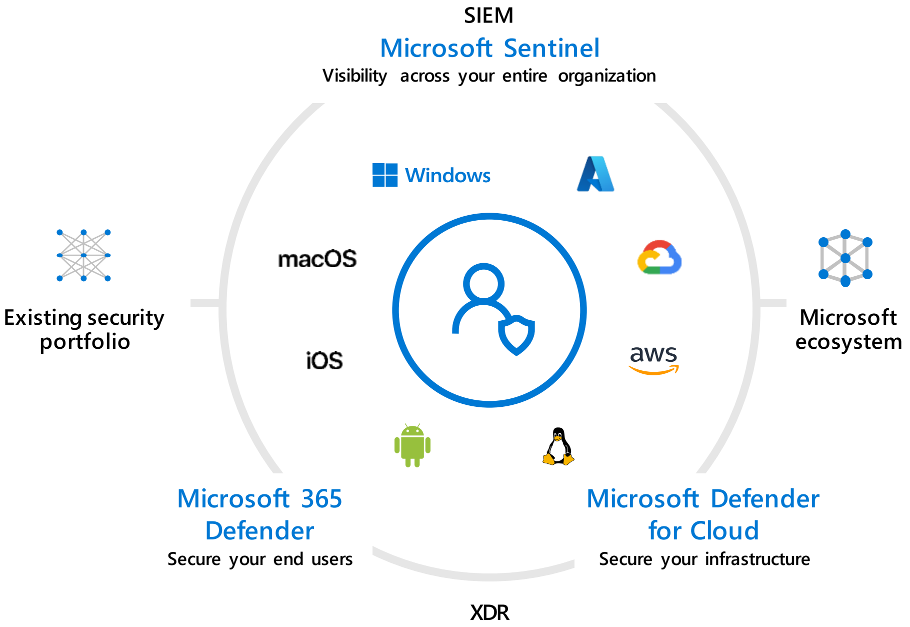
[Assess your maturity stage with our Zero Trust Maturity Assessment]().

Defend against threats with SIEM and XDR

The pervasiveness of advanced threats, combined with the desire to increase SecOps efficiencies while reducing the risk of costly data breaches, can be achieved with a foundational security strategy. A strategy built on the ability to detect, investigate, and respond to threats across your entire digital estate with speed, scale, and intelligence.

Microsoft Sentinel, our cloud-native security information event management (SIEM) tool, delivers an understanding of the breadth of your digital estate.

Microsoft Sentinel aggregates logs from all of your company's sources: OS, application, antivirus, database, and server logs. Sentinel analyzes that extensive tranche of data, searching for anomalies and signs of threats, affording you a bird's-eye view across the enterprise.


SIEM
Microsoft Sentinel
Visibility across your entire organization

Microsoft 365 Defender
Secure your end users

Microsoft Defender for Cloud
Secure your infrastructure

XDR

The depth of your security foundation is delivered through a comprehensive XDR solution: Microsoft 365 Defender and Microsoft Defender for Cloud. XDR is an emerging technology in threat protection to get ahead of today's threats. Instead of monitoring an endless list of alerts from many security point products, making it difficult for defenders to link data effectively to contain a threat, XDR delivers intelligent, automated, integrated security to close gaps in detection, response, and prevention.

Identifying opportunities to expand usage and adoption

Jump-start your Microsoft Security journey with recommended action plans and training opportunities for your SecOps teams, enabling you to reach short- and long-term milestones.

30 days

- Begin checking Microsoft Secure Score for current score and recommendations.
- Turn on audit logging for Office 365 and configure your tenant for increased security.
- Regularly review dashboards and reports in the Microsoft 365 Defender portal.

90 days

- Continue monitoring Secure Score, dashboards, and reports in Microsoft 365 Defender portal and Microsoft Sentinel.
- Review and implement software updates.
- Conduct attack simulations for spear phishing, password spray, and brute force password attacks.

Beyond

- Continue using Secure Score.
- Review dashboards and reports while maintaining implementation of software updates.
- Evaluate a holistic approach to Zero Trust across the entire digital estate.

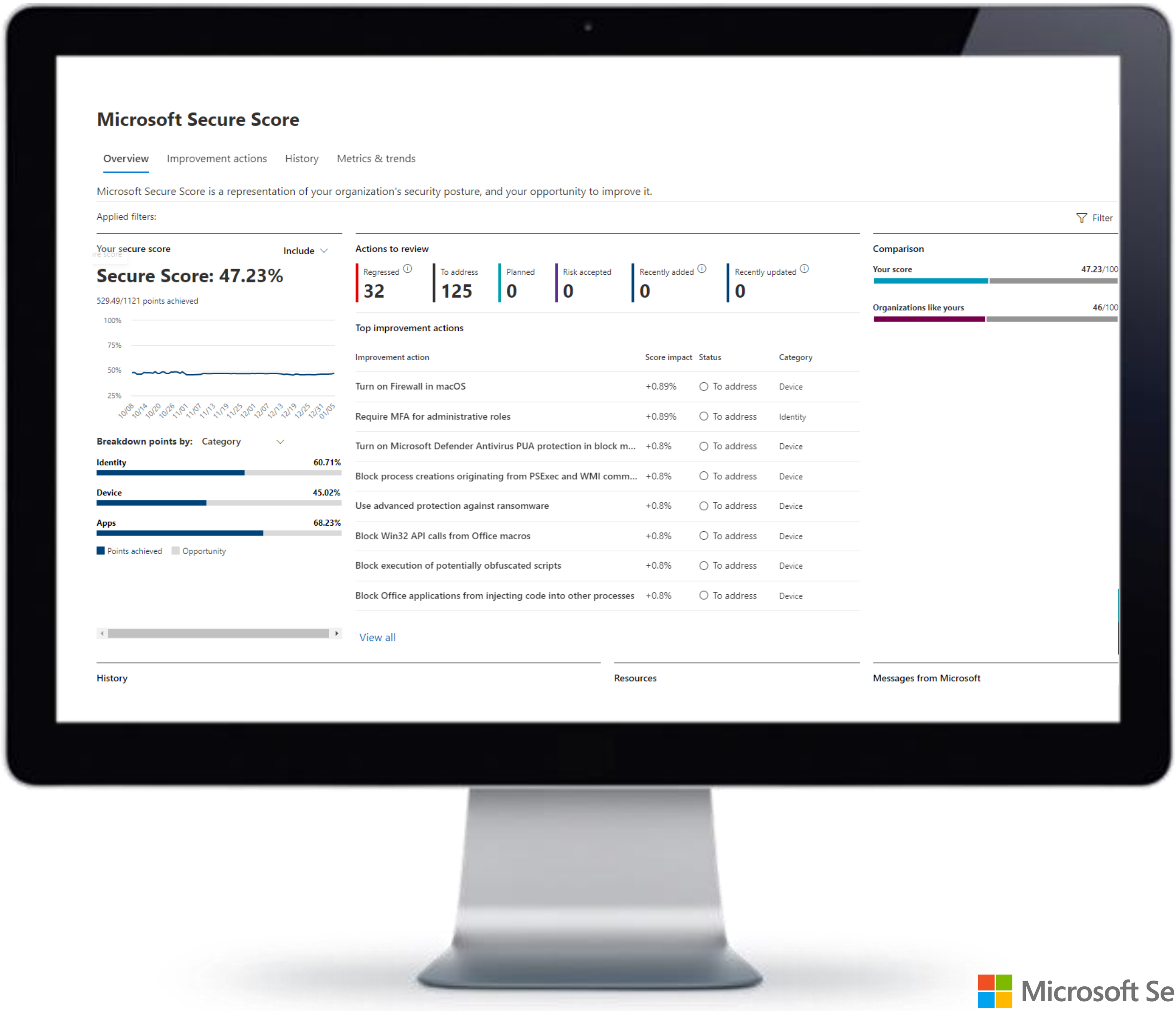
Getting started with Microsoft Secure Score

Microsoft Secure Score evaluates your organization's security posture based on your regular activities and security settings in Office 365, including Microsoft Teams.

Take advantage of Secure Score recommendations to:

- Report on the current state of the organization's security posture.
- Improve security posture by providing discoverability, visibility, guidance, and control.
- Compare against benchmarks and establish key performance indicators (KPIs).

[Learn how you can use Microsoft Secure Score](#).



Microsoft Secure Score

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Your secure score

Secure Score: 47.23%

529.49/1121 points achieved

Breakdown points by: Category

Identity	60.71%
Device	45.02%
Apps	68.23%

■ Points achieved □ Opportunity

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added	Recently updated
32	125	0	0	0	0

Top improvement actions

Improvement action	Score impact	Status	Category
Turn on Firewall in macOS	+0.89%	○ To address	Device
Require MFA for administrative roles	+0.89%	○ To address	Identity
Turn on Microsoft Defender Antivirus PUA protection in block m...	+0.8%	○ To address	Device
Block process creations originating from PSExec and WMI comm...	+0.8%	○ To address	Device
Use advanced protection against ransomware	+0.8%	○ To address	Device
Block Win32 API calls from Office macros	+0.8%	○ To address	Device
Block execution of potentially obfuscated scripts	+0.8%	○ To address	Device
Block Office applications from injecting code into other processes	+0.8%	○ To address	Device

View all

Comparison

Your score	47.23/100
Organizations like yours	46/100

History

Resources

Messages from Microsoft

Microsoft Security

Operationalizing Microsoft Security

Help your business adopt and realize the benefits of Microsoft Security capabilities

Cloud security is a journey of incremental progress and maturity.

Transforming how the business and IT teams view security requires aligning security closely to priorities, processes, and risk framework. Envision your security end state, the integrations within your organization, and across the disciplines within security.

Business alignment

Risk insights

Integrate security insights into risk management framework and digital initiative.

Security integration

Integrate security insights and practices into business and IT processes, integrate security disciplines.

Business resilience

Ensure organization can operate during attacks and rapidly regain full operational status.

Security disciplines

Access control

Establish Zero Trust access model to modern and legacy assets using identity and network controls.

Security operations

Detect, respond, and recover from attacks. Hunt for hidden threats. Share threat intelligence broadly.

Access protection

Protect sensitive data and systems. Continuously discover, classify, secure assets.

Security governance

Continuously identify, measure, and manage security posture to reduce risk and maintain compliance.

Innovation security

Integrate security into DevSecOps processes. Align security, development, and operations practices.

Key success drivers

Culture

A culture of security must be focused on safely achieving the business mission, not impeding it. At the same time, security must become a normalized part of the culture of the organization. The internet on which the business depends is open, allowing adversaries to attempt attacks at any time. The cultural shift requires improved processes, partnerships, and ongoing leadership support at all levels to communicate, model behavior, and reinforce the shift.

Risk ownership

The accountability for security risk should be assigned to the same roles that own all other risks, freeing the Security team to be a trusted advisor and subject matter expert rather than a scapegoat. They should not be held accountable for decisions they do not own. Security should provide sound, balanced advice.

Security talent

There's a chronic shortage of security talent and organizations should always be planning how to best develop and disseminate security knowledge and skills. In addition to growing security teams with technical security skill sets, mature security teams are also diversifying their strategies by focusing on:

- Growing security skill sets and knowledge within existing teams in IT and the business. It's especially important for DevOps teams to adapt a DevSecOps approach. This can take many forms, such as a security help desk, identifying and training champions within the community, or job swapping programs.
- Recruiting diverse skill sets to security teams to bring fresh perspectives and frameworks to problems (e.g., business, psychology, economics) and build better relationships within the organization. To a hammer, all problems look like nails. You'll benefit from more and broader points of view.

Implement security across the enterprise environment.

Maintain security assurances while minimizing friction with business processes.

Security operations team training opportunities

Deepen your knowledge with curated resources to put you on the path to detecting and preventing attacks across your workloads.

- **Beginner Security Skilling Path** Explore today
- **Intermediate Security Skilling Path** Explore today
- **Advanced Security Skilling Path** Explore today

Succeed against common security challenges

Explore the Microsoft Security training guide to gain the necessary skills to unblock common security challenges:

- Protect endpoints from ransomware
- Secure collaboration and prevent phishing
- Optimize the SOC

Access today

Microsoft Security

Empowering your end users

End users can be the most significant security threat

if your organization doesn't invest in ensuring the proper cybersecurity processes, tools, and training are in place. Everyone has a role in preventing threats from shutting down business operations, theft of sensitive data, or ransom demands.

Take advantage of these recommendations and protect your organization.

Train your employees to increase their awareness and reduce susceptibility to breaches.

- Offer attack simulation training in Microsoft Defender for Office 365. Explore
- Protect against phishing. Discover

Go passwordless and use multifactor authentication to confirm identities and access to applications and data.

- Plan an Azure Active Directory multifactor authentication (MFA) deployment. Explore
- Understanding multifactor authentication. Discover

Simplify user application access with My Apps, a web-based portal, to manage and launch applications in Azure Active Directory (Azure AD).

- Enhance end-user experiences with secure applications access. Explore

Make your future more secure

while ensuring usage and delivery of the maximum value for your security investment.

FastTrack for Microsoft 365

- Enable hybrid work with expert guidance delivered remotely by Microsoft engineers and approved FastTrack-ready Partners at no additional cost for the life of your eligible subscription.
  Sign in today
- Learn about how to use the service, program access eligibility, and scenarios supported by FastTrack.
  Explore today

Microsoft 365 overview guidance

- Understand how services are provisioned and deployed, and how your users benefit.
  Explore today

Customer success stories

Georgia Banking Company turbocharges growth with cloud adoption and Microsoft Security.

Learn more

Frasers Group fearlessly scales with a modernized Microsoft Security solution.

Learn more

Heineken creates the flexibility it needs to "Brew a better world" with agile, scalable Microsoft Security solutions.

Learn more

Microsoft Security