Microsoft Security

Enhance multicloud and hybrid environments protection with Microsoft Defender for Cloud

Strengthen posture, protect workloads, and secure DevOps with Microsoft Defender for Cloud.

Digital transformation enables enterprises to innovate faster, which is why so many organizations continue to move to the cloud.

57% of security decision makers estimate more than 75% of their organizations' workloads will be in the cloud in the next year.

But cloud migration comes with challenges.

Security challenges

As a result of the rise in multicloud approaches by organizations, security teams face:

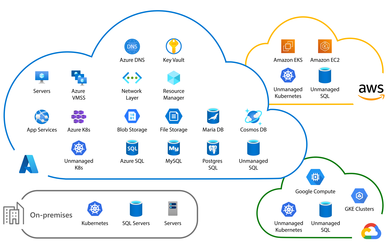
- Complex threats across ever-expanding attack surface areas
- An overload of security risks and a lack of prioritization
- No shared posture visibility between development and security teams

This results in exponentially increased security attacks, with a 1070% increase in organizational ransomware attacks between 2020 and 2021.

It's no surprise that 51% of security professionals say their company's security strategy is not keeping up with their company's multicloud environment.

Microsoft Defender for Cloud

Secure your hybrid-cloud and multicloud workloads



Defender for Cloud secures your workloads in three primary ways:

- Reduce risk with contextual security insights
- Prevent, detect, and respond to threats
- Improve communication and share visibility between development and security teams

1.Strengthen security posture

Assess workload security posture in real time and prioritize critical risks with contextual cloud security.

- Leverage Secure Score insights to assess security posture and optimize security across networks and Azure services.
- Enable comprehensive security posture visibility with in-code fixes and Defender for DevOps insights
- Use Defender for CSPM, the new cloud security graph, to analyze attack paths and prevent and remediate threats
- Meet compliance, policy, and regulatory standards, including CIS, PCI, and NIST, across all cloud workloads, with automated monitoring

2.Protect against threats

Implement an integrated, multicloud XDR solution, prevent, detect, and respond to security attacks.

- Understand and manage security posture across hybrid and multicloud workloads in one console
- Detect and block malware and threats with preventative and post-breach detection
- Reduce deployment complications with agentless and agent-based vulnerability scanning and ensure comprehensive monitoring with Defender for Servers
- Prevent administrative port attacks with Azure VMs and hardened network NSG rules

3.Unify DevOps security

Implement an integrated, multicloud XDR solution, prevent, detect, and respond to security attacks.

- Strengthen development lifecycle cloud configurations with Defender for DevOps by enabling security scanning for Infrastructure as Code templates and container images
- Find and fix security vulnerabilities and embedded secrets in code through integrated scanning
- Integrate feedback for code fixes directly into developer workflows and tools
- Unify security posture visibility across multiple CI/CD pipelines, including Azure DevOps and GitHub and multicloud environments across Azure, AWS, and Google

Strengthen your multicloud security posture and optimize your time

Microsoft Defender for Cloud reduces risk of a cloud security breach by up to 25%.[1]

Microsoft Defender for Cloud reduced time to threat mitigation by 50%.[1]

Ready to learn more?

Learn how to protect multicloud and hybrid cloud workloads, including servers, storage, databases, containers, and more with Microsoft Defender for Cloud.

- Visit the website >>
- Start a free trial >>
- Experience the interactive guide >>

[1] Forrester Total Economic Impact™ of Azure Security Center, Forrester Consulting, 2021.