

E-book Series

Get integrated protection for your multicloud resources, apps, and data



Protect your enterprise with a comprehensive cloud security strategy

 Microsoft Security





The digital transformation accelerates productivity—and introduces new challenges



Modernize security practices to meet the unique needs of the cloud



We're in an era of transformation—digital, cloud, and security—and organizations are navigating it in unique ways. Accelerated in large part by the migration of workloads and apps to the cloud, work patterns and business operations have been reshaped or completely reimaged. For example, 91% of IT decision-makers indicated that their organization uses at least two different public clouds.¹ To stay ahead of potential threats, enterprises must modernize their approach to protecting their expanding landscape of cloud resources.

Era of transformation

Digital transformation



Cloud transformation



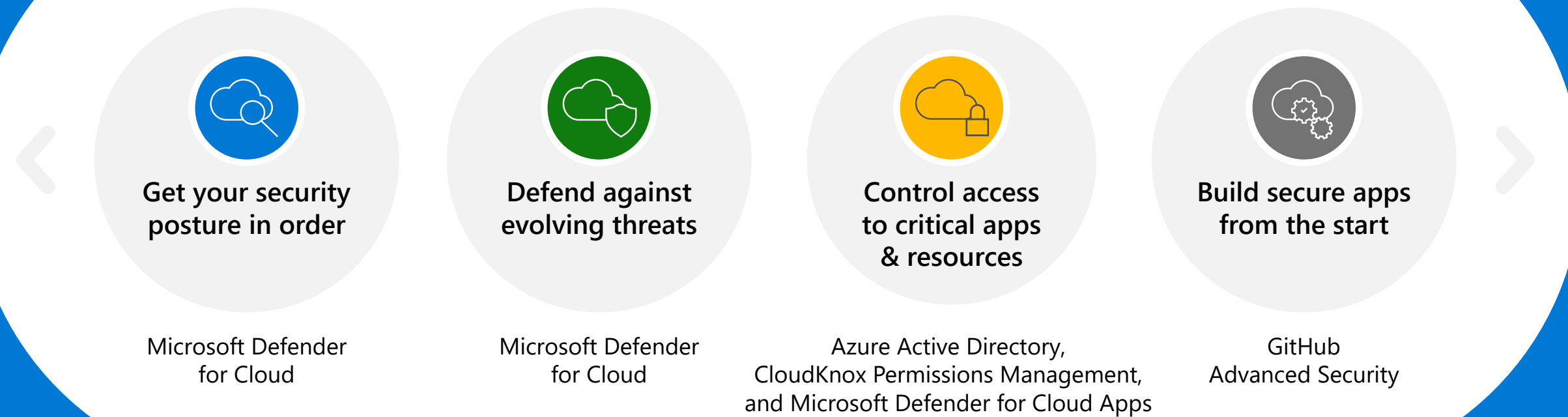
Security transformation



¹Data on file. Microsoft internal research.

Cloud Security from Microsoft

Get integrated protection for your multicloud resources, apps, and data



Threats and risks to cloud environments are different from those that affect traditional on-premises environments. The types of vulnerabilities and attacks may sound familiar, but they have elements unique to infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Misconfiguration of resources, loss of sensitive data, compromised user accounts, shadow IT, unsanctioned apps, and ransomware—these types of risks manifest in different ways in the evolving cloud landscape. As a result, cloud security is top of mind for business and IT leaders, 34% of whom cite secure configuration of cloud resources as a priority² and 52% of whom cite data security concerns as a barrier to cloud expansion.³

You need a comprehensive cloud security strategy to protect your multicloud and hybrid environments—your resources, workloads, apps, and data. Cloud Security solutions from Microsoft provide a complete set of capabilities that can help you do just that, enabling you to:

- Strengthen your cloud security posture.
- Defend against evolving threats.
- Control access to critical apps and resources.
- Secure every step of the cloud-native development lifecycle.

By taking advantage of these capability areas and using Microsoft’s integrated tools and services—such as [Microsoft Defender for Cloud](#), [Microsoft Defender for Cloud Apps](#), Microsoft Azure Active Directory (Azure AD), [CloudKnox Permissions Management](#), and GitHub—you can implement a flexible and comprehensive cloud security strategy that meets your specific needs.

²Verizon. 2018 data breach digest. Published 2018.

<https://www.verizon.com/business/resources/reports/2018-data-breach-digest.pdf>

³SecureID. 451 Research report: securing cloud transformation.

<https://www.securid.com/offers/451-research-report-securing-cloud-transformations/>



Priority area 1:
Strengthen your
cloud security posture



Get a bird's-eye view of your multicloud and hybrid security state



For many organizations, the first step in strengthening their security posture is to configure cloud resources in a secure manner that minimizes exposure to risks and reduces the overall attack surface. This step can also play an important role in meeting internal and external compliance requirements.

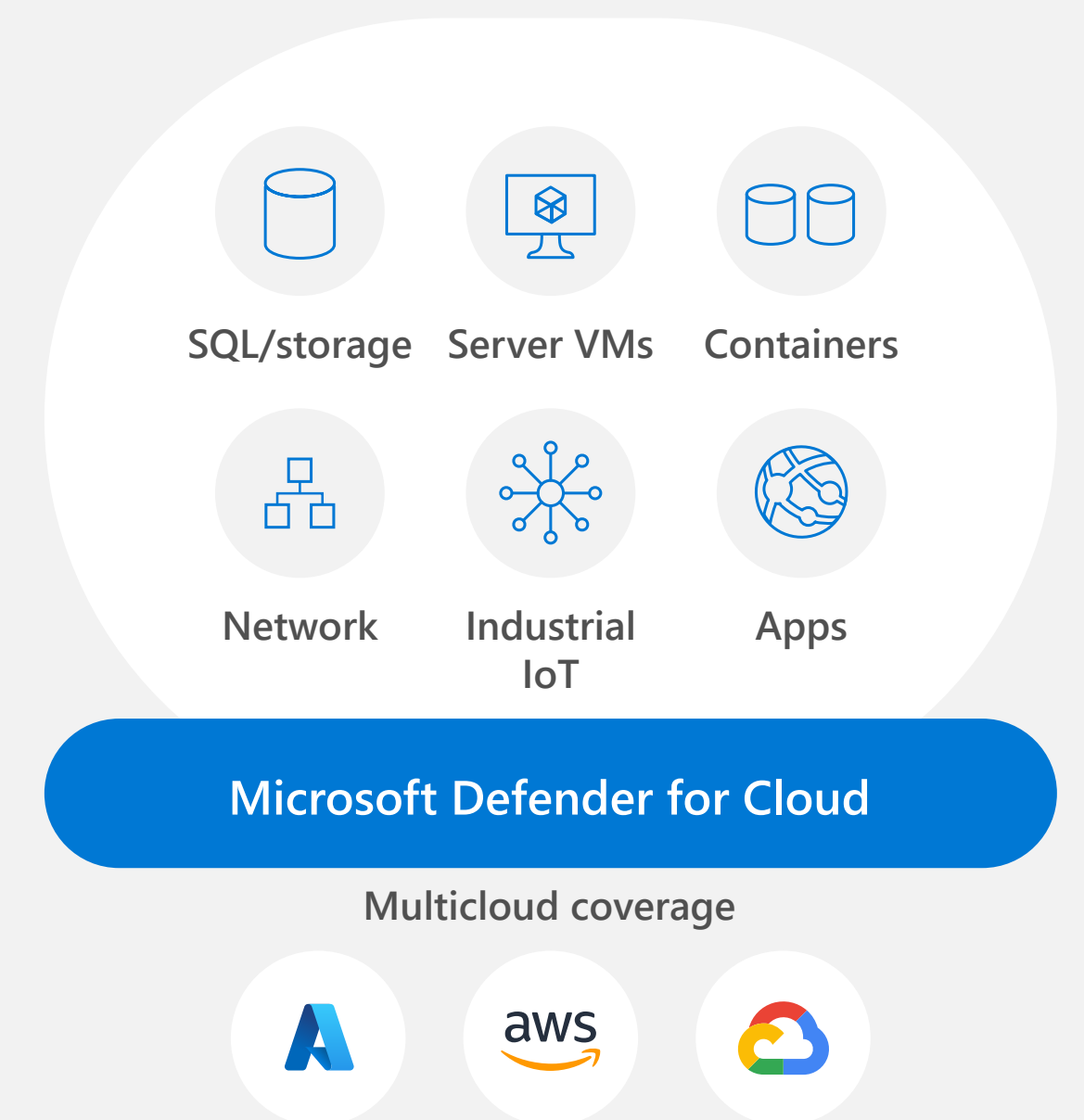
Microsoft Defender for Cloud gives you deep visibility into the security state of your cloud environments—including Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP). [Secure Score](#) gives you an assessment of your current state and provides prioritized recommendations for actions you can take to improve your overall security posture and remediate common misconfiguration issues, such as failing to enable encryption for data at rest; updates that haven't been installed; or lack of network security layers, such as firewalls, implementing role-based access control, or improving container configurations.

Microsoft Defender for Cloud continuously monitors your environment and discovers new resources and workloads. When a new resource is discovered, it is assessed against security best practices, and anomalies are flagged. Microsoft Defender for Cloud then recommends fixes to better protect your resources and services.

Strengthen your cloud security posture

Easily assess and improve the security configuration of your critical multicloud resources

- Follow best practices recommendations for Azure, AWS, and Google Cloud Platform
- Get a bird's-eye view of your security posture across clouds with Secure Score
- Continuously monitor and protect your multicloud resources
- Ensure compliance with industry and regulatory standards as well as custom requirements of your company





Ensure compliant configuration of resources across Azure, AWS, and GCP



Microsoft Defender for Cloud gives you a centralized and streamlined approach to monitoring the security posture of your evolving multicloud estate. When you connect AWS and GCP to Microsoft Defender for Cloud, you can monitor and improve the security posture of these services—all in a single place. Microsoft Defender for Cloud supports a range of top compliance standards, including Center for Internet Standards benchmarks, Payment Card Industry, [Azure Security Benchmark](#), and AWS Foundational Security Best Practices.

Native support for AWS and GCP environments makes it easy to onboard AWS and GCP accounts through an agentless design using native cloud application programming interfaces (APIs). After onboarding, you can start reviewing and acting on out-of-the-box recommendations to harden the configuration of your AWS and GCP resources.

Next steps

- Enable Microsoft Defender for Cloud in all your environments and on all your resources.
- Use Secure Score to assess and improve the configuration of your cloud resources.
- Connect your AWS and GCP services to Microsoft Defender for Cloud to strengthen your multicloud security.

A decorative graphic on the left side of the slide. It features three diagonal bands: a blue band at the top with a blue circle, a yellow band in the middle with a yellow circle, and a green band at the bottom with a green circle. A white, rounded rectangular shape overlaps the top of the yellow band, containing a red circle.

Priority area 2: Defend against evolving threats



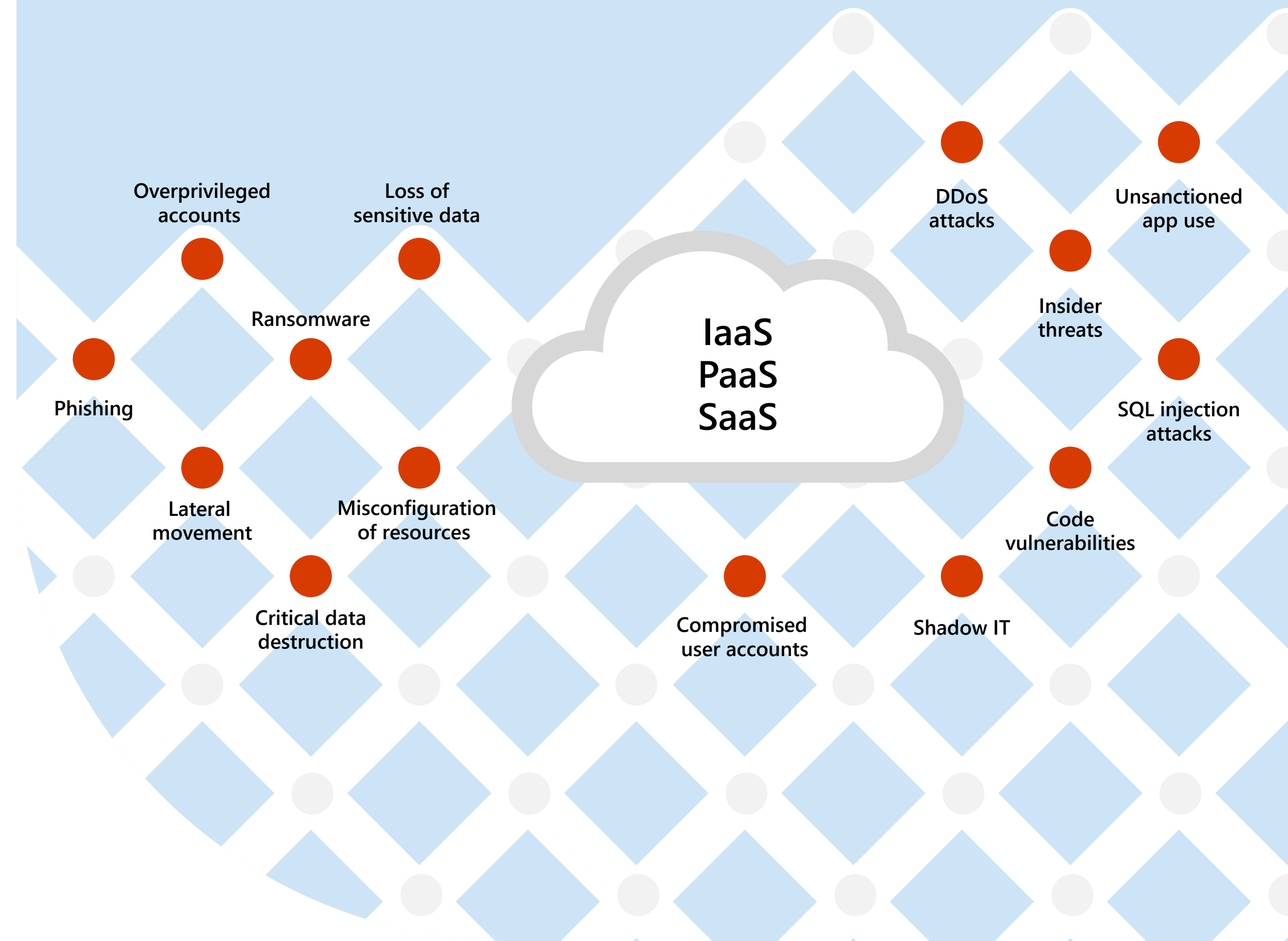
Protect your cloud workloads with advanced threat protection technologies and leading threat intelligence



Microsoft Defender for Cloud provides advanced protection for servers, containers, and other cloud workloads. Its built-in behavioral analytics and machine learning help you identify vulnerabilities and advanced persistent threats, and you can monitor your cloud resources for known attack patterns and post-breach activity. With prioritized security alerts and incidents, Microsoft Defender for Cloud can help you detect and protect against new and emerging threats.

Microsoft Defender for Cloud is designed to protect your multicloud estate, including Azure-native services, workload protection for Amazon Elastic Kubernetes Service and Amazon Elastic Container Service, along with Google Kubernetes Engine Standard clusters and Google Compute Engine virtual machines (VMs).

Evolving cloud threats and risks



Protect your multicloud and hybrid workloads

Protection isn't limited to just your cloud workloads, however. Depending on where you are in your journey to the cloud, you may have workloads and services running on on-premises servers that still must be protected. You can benefit from cloud-based intelligence and automation to extend protection to these on-premises services, including enabling protection on Windows- or Linux-based servers.



Take advantage of broad workload coverage

Microsoft Defender for Cloud, backed by the power of leading threat intelligence capabilities, provides broad coverage of your cloud workloads, such as:

- VMs, including Windows, Linux, and machines running in AWS and GCP.
- Containers, including [Azure Kubernetes Service](#), Amazon Elastic Kubernetes Service, and Google Kubernetes Engine.
- Databases, including SQL, MariaDB, and [Azure Cosmos DB](#).
- [Azure App Service](#).
- Cloud Service Layer functions, such as DNS and [Azure Key Vault](#).

Identify, prioritize, and secure sensitive data in cloud workloads

Microsoft Defender for Cloud integrates with [Microsoft Purview](#), a unified data governance solution that helps you manage your multicloud and SaaS data. The integration enables you to use Microsoft Defender for Cloud to better discover, classify, track, and secure sensitive information across your workloads and improve your security posture through better prioritization and recommendations. Just as Microsoft Defender for Cloud gives you a bird's-eye view of your cloud environments, Azure Purview extends that view into your data and data storage systems, broadening your ability to prioritize actions based on the sensitivity of your data.

Next steps >>

- Turn on Microsoft Defender for Cloud workload protection capabilities for all resources.
- Connect your AWS and GPC services to Microsoft Defender for Cloud to protect critical workloads running on these services.
- Use [Azure Arc](#) to extend threat protection to hybrid (on-premises) servers, including Windows and Linux servers.



Priority area 3:
Control access
to critical apps
and resources



Enable streamlined, secure, and controlled access to data and services in the cloud

Another critical element of a comprehensive cloud security strategy is controlling and managing user access to apps, data, and services. According to Forrester Consulting, the average enterprise has more than 1,000 cloud apps and services, half of which go unmonitored by IT.⁴



Simplify user access



Azure AD centralizes identity and access management across your environments. You can use single sign-on capabilities to provide streamlined access to SaaS apps, on-premises apps, and custom apps that reside on any cloud platform for any user type and any identity so that users need just one set of credentials and have fewer prompts to sign in. With a seamless single sign-on experience, users can quickly access applications from anywhere, for yearly savings of up to 8.5 hours for users and up to \$2.4 million for the organization.⁵

In addition to single sign-on, conditional access in Azure AD enables you to enforce fine-tuned adaptive access controls, such as requiring multifactor authentication, based on user context, device, location, and session risk information. Move beyond simple access/block decisions and tailor decisions based on risk level, such as allowing, blocking, or limiting access, or requiring additional authentication methods, such as a one-time passcode or a biometric input. Augment this by ensuring that only healthy, trusted devices are allowed access to your corporate resources by checking the device health and security posture of registered devices.

⁴Forrester Consulting. The Total Economic Impact™ of Microsoft Cloud App Security. Published May 2020.

<https://tools.totaleconomicimpact.com/go/microsoft/CloudAppSecurity>

⁵Ibid.

Ensure least-privilege access for all identities in your multicloud environment



IT administrators are no longer the only users who have permissions to access critical cloud apps, data, and services. Developers; third-party contractors; and workload identities, such as bots, API keys, and VMs, also have access to your cloud resources. Today, more than 40,000 permissions can be granted to identities across the major cloud platforms, and nearly 50% of these permissions can be classified as high risk, with the ability to cause catastrophic damage if used improperly. To add to this, more than 90% of identities are using less than 5% of their granted permissions to perform their job function.⁶ The result is a significant—and highly exploitable—permissions gap.

CloudKnox Permissions Management is a cloud infrastructure entitlement management solution that provides comprehensive visibility into permissions assigned to all entities—users and workloads—actions, and resources across cloud infrastructures. It detects, right-sizes, and monitors unused and excessive permissions and enables Zero Trust security through least-privilege access in Azure, AWS, and GCP.

⁶Microsoft Security. 2021 State of Cloud Permissions Risks Report. Published 2021. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWSvP2>

Right-size permissions and entitlements with CloudKnox Permissions Management

Strengthen the security of your multicloud environment by preventing and addressing permissions creep



Visibility

Gain insights into effective permissions of identities and their usage



Remediation

Right-size permissions across clouds with the click of a button

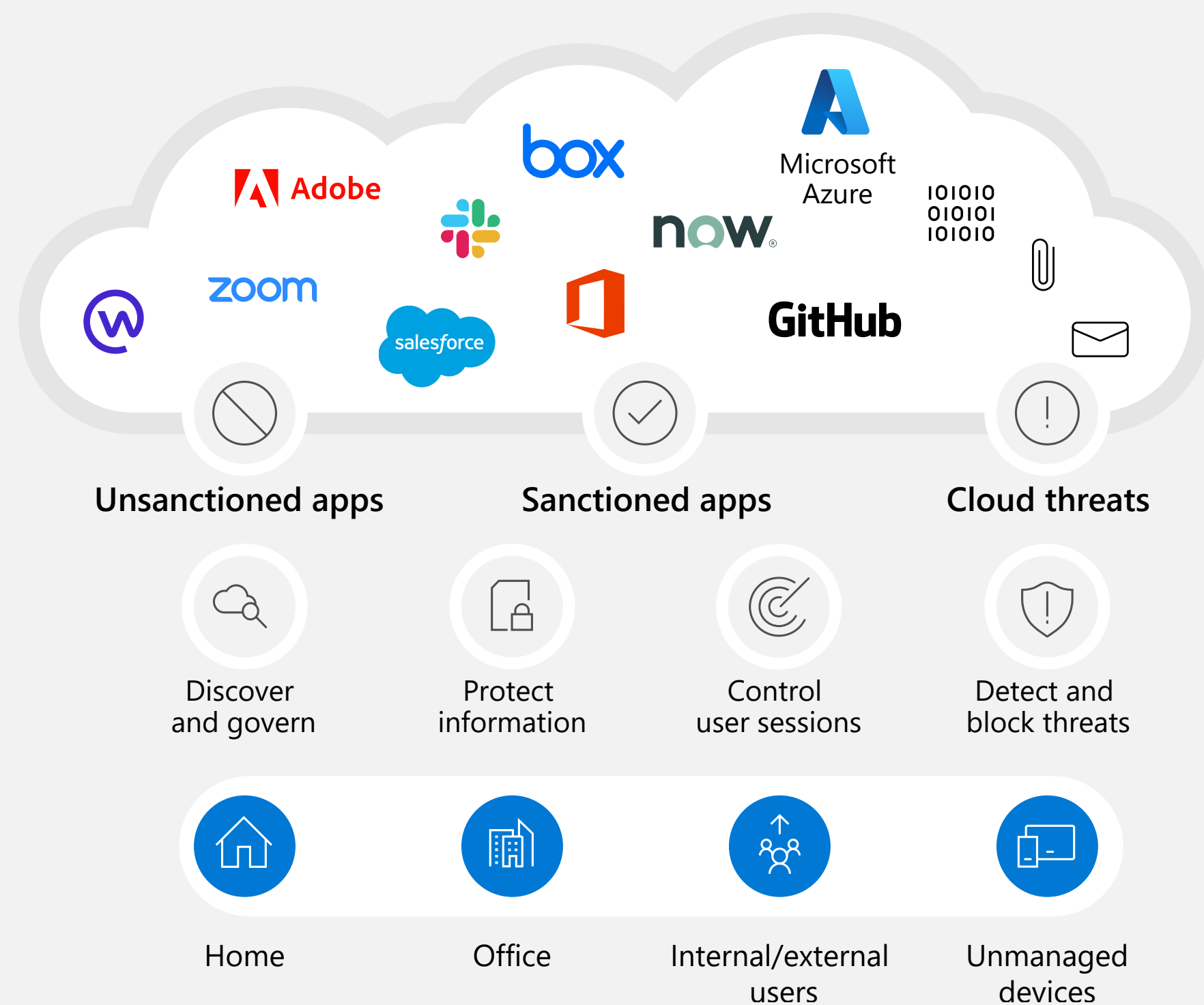


Monitoring

Continuously monitor activity, alert on anomalies, and measure sprawl

Microsoft Defender for Cloud Apps

- Discover cloud apps and understand usage patterns
- Enable secure access to SaaS apps and resources
- Protect sensitive information with real-time controls
- Policy-driven governance for Microsoft 365 apps



Control the access and use of SaaS apps

Microsoft Defender for Cloud Apps, Microsoft’s leading cloud access security broker, gives you visibility into apps used in your environment and the ways workers are using and interacting with these apps. This helps you identify unsanctioned apps, assess their compliance risk, and make informed decisions about allowing ongoing use. Microsoft Defender for Cloud Apps continues to expand its support for SaaS apps and now covers more than 26,000 apps.

With Microsoft Defender for Cloud Apps, you can:

- Monitor cloud apps for threats, such as compromised accounts, malicious insiders, malware, and rogue cloud apps.
- Implement policy-driven governance for Microsoft 365 apps to detect and remediate inappropriate app behaviors.
- Discover the use of cloud apps across your organization and identify shadow IT.
- Control the access and use of apps, including preventing inappropriate sharing of sensitive information.



You can also take advantage of native API integrations for deeper app insights and more granular control of the apps in your environment. For example, you can use API connectors to enable instant, out-of-the-box protection through Microsoft’s built-in anomaly detection engine and gain deep insights into the app’s behavior and potentially risky user activity. Native API integrations include Box, Dropbox, Google Cloud, Salesforce, and more.

Microsoft Defender for Cloud Apps also integrates with other Microsoft security solutions to provide even more insights and protection. It can display additional data in the Microsoft 365 Defender portal to improve advanced threat hunting research and, when used with Microsoft Defender for Endpoint, can extend app discovery to devices running Windows and macOS.

Protect resources and applications with cloud-native network security

Protecting your network infrastructure against network-based risks and threats plays an important role in controlling access to apps and resources. Azure provides highly secure, reliable, and performant network access to your cloud and hybrid workloads and data. [Azure network security](#), Microsoft's cloud-native network security services, is built on a robust software-defined network foundation that you can connect and extend to the cloud as part of your overall cloud security strategy.



Next steps >>


- Enable single sign-on, multifactor authentication, and conditional access policies within Azure AD to streamline secure access to cloud apps and services.
- Use CloudKnox Permissions Management to identify and remediate permissions risks across your multicloud estate.
- Deploy Microsoft Defender for Cloud Apps to better manage and govern SaaS apps in use in your organization.

⁷Ibid.

Azure network security consists of several key network security services, including:

- **Azure Firewall**, a stateful, cloud-native firewall as a service that secures and governs traffic between virtual networks.
- **Azure Web Application Firewall**, an easy-to-deploy service that helps protect web apps by filtering and monitoring HTTP traffic from the internet.
- **Azure DDoS Protection**, which provides layer 3/4 and layer 7 protection against distributed denial of service (DDoS) attacks.

With Azure network security, you can reduce the risk of network-based breaches by 30%.⁷



Priority area 4:
Secure every step
of your cloud-native
development lifecycle



Build, deploy, and operate secure code and apps in the cloud



Microsoft Defender for Cloud Apps, and other tools to better secure Microsoft and third-party apps, but what about the apps and code that your organization develops, deploys, and operates? Securing your code and apps is just as important as securing other aspects of your cloud environment. This can be accomplished by integrating security into the entire app-development and operations lifecycle—an approach commonly called *DevSecOps*.



In a world where 83% of code vulnerabilities are caused by development errors⁸, an integrated DevSecOps approach helps developers integrate security into every step of the lifecycle. GitHub Advanced Security is a developer-first, community-driven service that makes it easier to secure your apps. It provides:

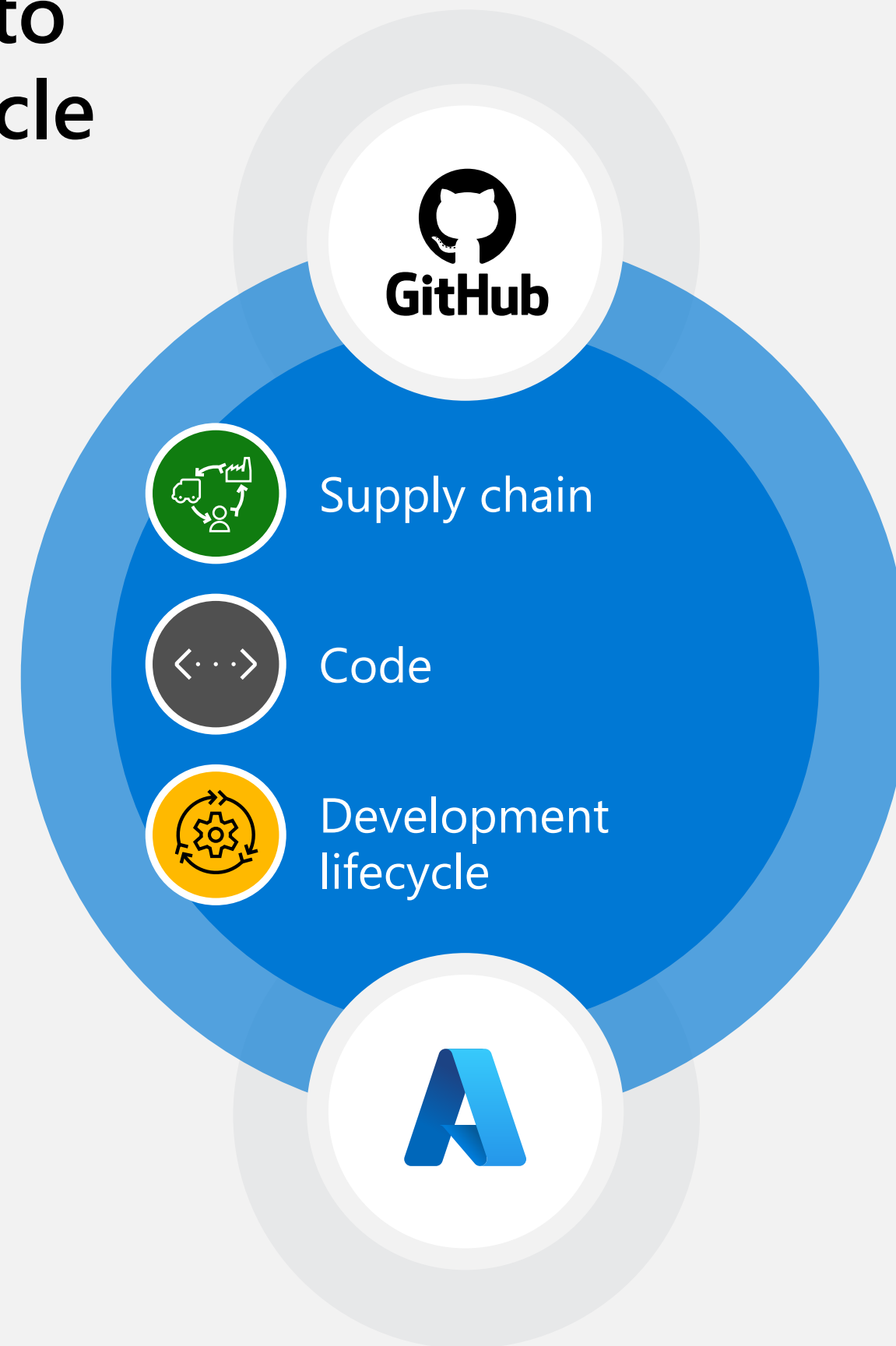
- **Dependency scanning.** The service continuously assesses the risk levels of dependencies the code uses.
- **Code scanning.** As code is generated, GitHub Advanced Security scans it and displays the results for easy remediation.
- **Secret scanning.** The service scans the code for hard-coded credentials or tokens.

⁸Synopsys Cybersecurity Research Center. 2019 Open source security and risk analysis. Published April 22, 2019. <https://www.gcomtw.com/mailshot/Synopsys/2002BlackDuck/reposra19.pdf>

Integrate security into entire DevOps lifecycle

Shift left with secure DevOps

- Increase development speed and improve application security
- Deploy secure code across clouds
- Focus on high-priority security issues
- Work within the standard developer workflow



Fixing a security defect in production can be up to 60 times more expensive than during the development cycle
(source: <https://securityboulevard.com/2020/09/the-importance-of-fixing-and-finding-vulnerabilities-in-development/>).

Take advantage of the integration between GitHub and Microsoft Defender for Cloud to better connect DevOps and SecOps

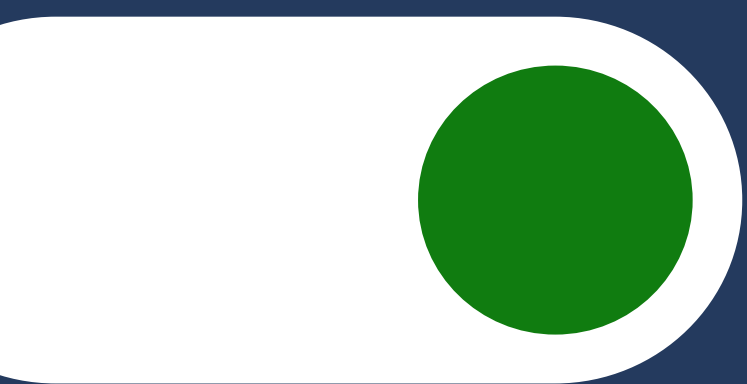


As powerful as GitHub is, it's even better when used along with Microsoft Defender for Cloud. Together, these solutions provide the tools and visibility to help developers kickstart DevSecOps practices. For example, the results from container scans appear in Microsoft Defender for Cloud, giving security teams a better understanding of the source of vulnerable container images and the repositories they came from. Developers can scan for common vulnerabilities before pushing images to a container registry or deploying them to a containerized web app or Kubernetes cluster.

Next steps

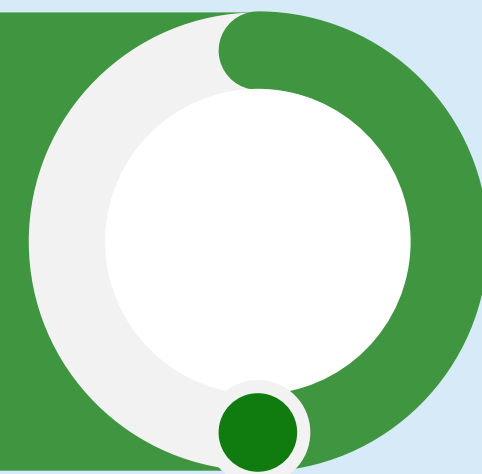
- Use GitHub Advanced Security for dependency scanning, code scanning, and secret scanning.
- Use GitHub actions to enable your development teams to create secure and automated workflows to build, test, package, release, and deploy apps to any cloud.
- Use GitHub integration with Microsoft Defender for Cloud to give security and development teams better visibility into vulnerability scanning and container scan results.

Secure the
cloud, secure
the organization



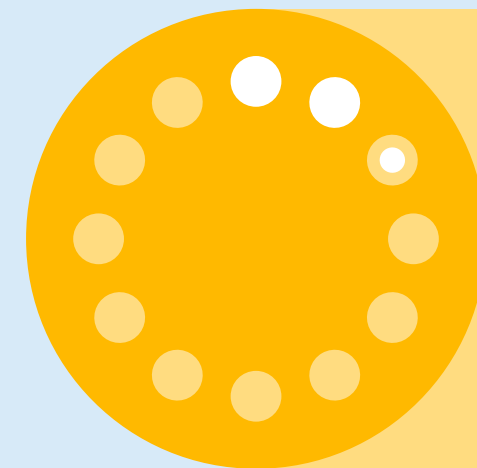
Total Economic Impact™ of Microsoft solutions

Reduction in time to threat mitigation
with Microsoft Defender for Cloud



50%

<3 months



Playback on investment
with Microsoft Defender
for Cloud Apps

ROI with Azure
network security



165%

Integrated protection for your multicloud resources, workloads, and apps



Microsoft provides a comprehensive set of Cloud Security solutions and capabilities to help you protect your multicloud and hybrid environments. Using solutions such as Microsoft Defender for Cloud, Microsoft Defender for Cloud Apps, CloudKnox Permissions Management, and GitHub Advanced Security, you can:

- Control access to critical apps and resources.
- Strengthen your security posture.
- Secure every step of the development lifecycle.
- Defend against evolving threats.

The Total Economic Impact™ of Microsoft solutions is clear:

- 50% reduction in time to threat mitigation with Microsoft Defender for Cloud.⁹
- A return on investment (ROI) of less than 3 months with Microsoft Defender for Cloud Apps.¹⁰
- 165% ROI with Azure network security.¹¹

No matter where you are in your cloud security strategy—just getting started or looking to take it to the next level—Microsoft’s flexible and complementary solutions can help.

⁹Doerr, Eric. Forrester Consulting TEI study: Azure security center delivers 219 percent ROI over 3 years and a payback of less than 6 months. Microsoft Security Blog. Posted February 18, 2021. <https://www.microsoft.com/security/blog/2021/02/18/forrester-consulting-tei-study-azure-security-center-delivers-219-percent-roi-over-3-years-and-a-payback-of-less-than-6-months/>

¹⁰Johnson, Ann. New study shows customers save time, resources and improve security with Microsoft Cloud App Security. Microsoft Security Blog. Posted July 7, 2020. <https://www.microsoft.com/security/blog/2020/07/07/new-study-customers-save-time-resources-improve-security-microsoft-cloud-app-security/>

¹¹Chew, Albert. Azure network security helps reduce cost and risk according to Forrester TEI study. Microsoft Security Blog. Posted October 12, 2021. <https://www.microsoft.com/security/blog/2021/10/12/azure-network-security-helps-reduce-cost-and-risk-according-to-forrester-tei-study/>

Resources

- [Get started](#) with a 30-day free trial.
- Visit the [Cloud Security website](#) for all the latest information.
- Try the interactive demo [Secure your Azure, hybrid, and multicloud environment](#).
- Read the e-book [6 tips to integrate security into your DevOps practices](#) on securing the development lifecycle.



Visit aka.ms/multi-cloud-security to learn more

<http://www.azure.com/enter>

©2022 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

