Microsoft Azure

5 cloud security essentials every growing business needs

Secure sensitive data and stay ahead of evolving threats with Azure

1 Reimagine, don't replicate

Cloud migration is a chance to reimagine—not replicate—legacy trust models. The same security concepts apply, but it's a shared responsibility. Cloud providers secure the infrastructure; you secure your configurations, data, and access.

Count on Azure's defense-in-depth strategy to handle core infrastructure security, including network defenses, DDoS protection, storage encryption, and operating system hardening.

Follow the Zero Trust **model** as you add layers, always verifying access for every identity, device, and workload. Doing so can reduce the risk of breaches and simplify compliance.

Find new ways to be proactive. Continuously monitor cloud resources, using automated tools like Microsoft Defender for Cloud, so you can detect issues early.

2 Close visibility gaps

Consistency matters in protecting apps, data, and connected resources, whether hosted on premises or across multiple cloud platforms. Disconnected security tools slow detection, create more maintenance work, and make it hard to track and report on compliance.

- Use automated tools and workflows to reduce manual effort and catch issues early. For example, set baseline security policies and automate enforcement.
- Keep systems and apps updated. Automate routine tasks like patching, scanning, reporting, security checks, and compliance enforcement.
- Ensure that older applications, systems, or workloads are integrated into your threat detection, identity management, and compliance capabilities.
- Conduct a cybersecurity risk assessment to understand gaps in security and determine steps to resolve them.
- Protect hybrid work settings, including data and internet-connected devices. Ensure mobile applications are downloaded from legitimate app stores, and never share credentials over email or text.

3 Secure the application lifecycle

End-to-end cloud security requires a holistic view of your applications and data—and the people who work on them. Early security integration can reduce remediation costs by up to 73% and cut critical incidents nearly in half.[1]

Remediation costs 73%

Critical incidents 50%

- Start simply by enabling automated security checks in your development tools to reduce risk before deployment.
- Use GitHub's built-in security features like secret scanning and code scanning to catch issues early and keep your code secure without adding complexity.
- Get AI-powered security insights using tools like Copilot Autofix, which suggests code changes so you can resolve issues quickly, without switching tools.
- Review the top web application security risks compiled by the OWASP, the standard in computer security information.
- Automate vulnerability management in production using a cloud-native application protection platform (CNAPP) like Defender for Cloud.
- Clean up unused resources that could become targets.

Better, more responsive protection with Defender for Cloud[2]

50% reduction in false positives

30% reduced time to remediate threats

4 Build a strong foundation

Make sure that people, processes, and policies align by following these simple, cost-effective steps—built into Microsoft tools you may already have.

Turn on multifactor authentication by requiring two or more of the following authentication factors:

- Something you are, like a fingerprint
- Something you know, like a password
- Something you have, like a phone

Remind employees how to recognize and report phishing and to avoid reusing passwords. Consider using a password manager.

Take advantage of built-in cloud features to apply security policies and updates, and set up automatic alerts for suspicious activity.

Help secure assets against ransomware attacks with air-gapped immutable backups, encryption, and secure access controls.

Prioritize the cybersecurity investments that meet your business goals:

- **Data loss prevention (DLP)** tools help identify suspicious activity and prevent sensitive data from leaving leaking outside of the business.
- **Endpoint detection and response (EDR)** helps protect devices and defend against threats.
- **Identity and access management (IAM)** helps ensure only the right people get access to the right information.

5 Get proactive protection and response

Defender for Cloud helps you take a proactive approach to security by automating checks, responses, and compliance tasks—saving time, reducing human error, and strengthening your security posture without adding IT overhead.

- Unify security management to centrally manage, monitor, and enforce security and compliance rules.
- Gain in-depth and continuous security assessments of your cloud resources running in DevOps pipelines, Azure, Amazon Web Service, and Google Cloud Platform.
- Detect, investigate, and respond to cyberattacks in real time to protect your multicloud, hybrid, and on-premises workloads.
- Bring together security alerts from other sources so you can correlate insights and coordinates enforcement for your workloads across cloud and on-premises environments.

Simplify and strengthen security

These security best practices represent some first crucial steps for protecting your business on premises and in the cloud. To go further, Microsoft and partners provide extensive guidance and support tailored to your goals.

Learn how Azure helps businesses of all sizes migrate and modernize with confidence:

Find a trusted Microsoft partner

Fuel transformation with experts and investments using Azure Accelerate

Learn more about cloud solutions for small and medium businesses

[1] Kalithe, Bhanu Kiran. Shift Left Security: A Paradigm Shift in Software Development Security Integration. IJCSIT. May 20, 2025.
[2] The Total Economic Impact™ Of Microsoft Defender For Cloud, a commissioned study conducted by Forrester Consulting, January 2025

© 2025 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.