Microsoft Azure

Cloud Security Essentials

5 best practices for migration and modernization

Contents

Introduction: Reframing security for the cloud era

Top cloud challenges for businesses[1]

77%
struggle with security

75%
lack resources or expertise

Modern cloud infrastructures and applications are the foundation of business value. Today's small and medium businesses host nearly two-thirds of their workloads and data on cloud platforms.[2] They also benefit from new cloud-based security models.

Security is always a priority. But a 2025 report revealed that 43% of cyber issues now target small or medium businesses, and the average cost of a breach is $4.5 million.[3]

Hosting workloads in the cloud can help improve security, but it takes thoughtful planning. In addition to familiar services like Microsoft 365, cloud computing offers servers, storage, databases, networking, and more—flexible resources that offer economies of scale but also require security. As a global cloud provider, Microsoft is a recognized leader in cybersecurity, providing solutions for identity and network access, information protection and governance, risk management, and cyberthreat detection. Years of experience have taught that layers of protection across Microsoft solutions—from the productivity apps in Microsoft 365 to all cloud platform technologies—work best to help safeguard against different types of threats. Azure reflects that defense-in-depth strategy with multiple layers of security controls across every stage of its cloud architecture—from physical infrastructure to applications and data.

Five essential practices can help you build a more secure, resilient, and manageable business infrastructure as you adopt cloud services. These best practices help you get more impact—businesses that modernize on Azure can realize a substantial **344% return on investment** (ROI) over three years. Using automation and built-in cloud-native tools, you can enhance existing defenses no matter where your workloads run—on-premises, in cloud environments, or both—and drive greater value from your investment.

1 Do reimagine, don’t replicate

Microsoft is a global leader in cybersecurity

84
trillion security signals processed per day

10K
security and threat intelligence experts

Cloud migration is a chance to reimagine—not replicate—legacy trust models. Familiar concepts still apply, such as encryption, access control, and compliance. But you share security responsibilities with your cloud service provider, and that changes the way you assess and respond to risks.

Generally, cloud service providers the underlying infrastructure that your workloads run on, allowing you to offload the security burden for these resources. If you use managed platform and data services, you can offload even more of the security and configuration burden to the provider.

That shift in responsibility represents tangible value. In a recent IDC survey of businesses that modernized on Azure, participants cited enhanced security as a top benefit.[4] One reason for this is the Zero Trust approach to security: Never trust, always verify. That means starting to shift protection to identity, device, and workload layers to help safeguard your people, devices, apps, and data.

Tips to get started

Identify which security tasks you can offload. As the chart shows, responsibility varies by service type.

In addition to traditional defenses, start following Zero Trust principles. Microsoft is a named leader in Zero Trust platform providers.[5]

Promote a mindset of continuous monitoring rather than waiting for issues to arise before addressing them. Built-in Azure security and observability services like Azure Monitor are a first step.

Compared to on-premises management, you share responsibilities for tasks with your cloud service provider. Responsibility varies depending on the type of service you use—software as a service (SaaS) like Microsoft 365, platform as a service (PaaS) like Azure Databases, and infrastructure as a service (IaaS) like Azure Virtual Machines.

	Responsibility	SaaS	PaaS	IaaS	On-Premises
Responsibility always retained by the customer	Information and data	🟩	🟩	🟩	🟩
	Devices (mobile and PCs)	🟩	🟩	🟩	🟩
	Accounts and identities	🟩	🟩	🟩	🟩
Responsibility varies by type	Identity and directory infrastructure	◩	◩	🟩	🟩
	Applications	🟨	◩	🟩	🟩
	Network controls	🟨	◩	🟩	🟩
	Operating system	🟨	🟨	🟩	🟩
Responsibility transfers to cloud provider	Physical hosts	🟨	🟨	🟨	🟩
	Physical network	🟨	🟨	🟨	🟩
	Physical datacenter	🟨	🟨	🟨	🟩

🟨 Microsoft (cloud service provider) 🟩 Customer ◩ Shared

2 Unify threat detection and response across all your environments

A layered approach to security helps defend your workloads from threats at all levels. Point solutions offer a quick fix, but as cloud environments grow more complex, relying on a patchwork of security tools begins to weaken your defenses. Fragmented solutions limit your visibility, context, and coordination—especially in multicloud and hybrid setups, where diverse vulnerabilities and attack types demand unified protection.

You need a solution for keeping everything in view across your environments, so you can improve your response time. Integrated tools help simplify a complex task. They bolster your existing defenses with continuous scanning and monitoring across all your cloud environments. You get up-to-the-minute information from correlated logs, telemetry, and event data. You can save time and manual effort using automated workflows that help orchestrate the right response.

To help you create a cohesive, effective security operations workflow, Microsoft Defender for Cloud helps unify protections into one experience. It collects data from your cloud and development environments to give insights, recommendations, and actions that help you protect your cloud workloads and resources. And it’s backed by Microsoft security research and data science teams, who continuously monitor the threat landscape.

Tips in detection and response

Get personalized recommendations for security, performance, reliability, and cost from Azure Advisor in the Azure portal.

Don’t rely only on a patchwork of disconnected security tools that detract with their siloed alerts, inconsistent policies, and gaps that cyberattackers can exploit. Instead, consider using Defender for Cloud to bring together security alerts from other systems so you can correlate insights.

To reduce manual effort and response time, use tools that automate and centralize security information. Consider using Microsoft Sentinel with Defender for Cloud, so you can centralize monitoring, correlate alerts, and automate responses.

3
Build resilience with best practices and training

Technology alone doesn’t secure workloads. Prioritizing risk is also a strategic and cultural task. Employees must be trained to recognize threats and understand their role in security, as insider threats and human error are major causes of breaches. To help reduce risks, make sure that people, processes, and policies align, and automate governance to ensure they stay aligned.

To shift from reactive to proactive security, you need smart, automated technology and the right practices. Resilience requires:

Visibility so you know what you have and who can access it.

Governance so you can enforce policies before problems arise.

Automation and rules that reduce manual effort.

Integration across identity, data, apps, and infrastructure.

Tips for risk management

Continuously monitor your cloud and on-premises resources, identities, and network configurations. Maintain an up-to-date view of potential risks, such as exposed endpoints, weak configurations, and excessive permissions, using a solution like Defender for Cloud.

Unify security management using tools like Azure Policy and Azure Monitor, which work with Defender for Cloud to help you centrally manage, monitor, and enforce compliance policies.

Reduce the risk of data exposure by scanning and classifying sensitive data. To simplify the task, consider Microsoft Purview, a unified data governance, compliance, and risk management platform for all your data—whether on-premises, in Azure, or in other clouds.

> We don't have to worry about patching those apps and tools nearly as much, given they're cloud-based, and Microsoft and our partner Quorum take care of most necessary updates on demand, 24/7. It really reduces the footprint of things our small IT team maintains."

Dan Collins

Director of Information & Communications Technology, Newington College

Read the full story

4 Address visibility gaps in your environment

As you migrate workloads in phases to cloud-based virtual machines (VMs) and services, you may continue to manage on-premises assets for a while. Maybe legacy integrations are too complex to move, or data residency requirements prevent migration. Whatever the reason, the result is a hybrid cloud environment until you complete the move. But hybrid environments can leave blind spots that expose vulnerabilities in your security.

In a hybrid world, you must protect your applications, data, and cloud resources consistently no matter where they reside. In recent years, small and medium businesses have increasingly turned to cloud-native application protection platforms (CNAPPs) like Microsoft Defender for Cloud. Defender for Cloud helps you maintain visibility across hybrid and multicloud environments. This means that whether your workloads run in the cloud, stay on-premises, or even use multiple providers, such as Azure, Amazon Web Services, or Google Cloud Platform, you can use one solution to improve compliance efforts and protect your workloads from code to runtime.

Tips for hybrid and multicloud visibility

Be aware that diverse and connected workloads across multiple environments create more entry points for attackers. Automate advanced protection using Defender for Cloud to continuously assess your cloud resources running across cloud and on-premises platforms. And make sure that legacy resources are included.

Make sure to deepen protection for the VMs you use. Consider automating scans using Defender for Cloud to assess VM configurations.

Extend protection to all your data. Take advantage of the way Azure encrypts data at rest and in transit, helping to reduce your attack surface.

If you have a hybrid environment, consider an extended detection and response (XDR) solution that collects, correlates, and analyzes threat data from across multiple cloud providers and on-premises environments. Defender for Cloud includes XDR capabilities to help you detect and respond to complex threats efficiently.

> ”
>
> We look at the automated reports from Defender to review findings and perform necessary actions, which helps us to manage security efficiently without needing additional personnel.”

John Meister

Vice President of Technology, Puritan Life

Read the full story →

5 Secure the entire application lifecycle

Developer benefits on Azure[6]

39%

higher developer productivity

43%

faster to market new products and solutions

Modern cloud development gives you an edge. You can optimize existing workloads and pilot new solutions using the latest technologies, including AI, infrastructure-as-code (IaC), the Internet of Things (IoT), containers, and serverless computing. You can also optimize security, extending it to cloud-based code repositories, build pipelines, and development workflows. The modern application lifecycle boosts productivity, streamline operations, and makes your applications and services more reliable. Automating threat detection and using continuous scanning helps you keep each step in the lifecycle secure.

Cloud security requires a holistic view of your applications and data—and the people who work on them. The goal is to protect the entire application lifecycle from code to cloud, detect issues before they snowball, and empower your business to move quickly without compromising on security.

Tips for lifecycle security

Adopt *shift-left security* and start performing security testing earlier in the software development lifecycle—that is, to the left end of the timeline—while the code is still fresh in your mind. Avoid waiting, as it's exponentially more expensive to remediate errors detected later in the cycle.

Embed security controls, testing, and guardrails throughout the development process. Scan for risks early and enforce security policies throughout development pipelines, so you can make secure decisions without slowing delivery. Try GitHub Advanced Security or Azure DevOps with integrated security scanning.

Protect code after it moves to production through continuous monitoring and threat detection. Consider automating vulnerability management using Defender for Cloud.

Consider using secure-by-design cloud services that require less upfront configuration, such as Azure App Service or Azure Functions.

Remember to clean up—identify unused virtual machines, outdated roles and permissions, and any other forgotten resources that could become targets.

What's up in your cloud? Security-first thinking asks:

? Where are my resources? Where is my data? What is internet-facing?

? Should these resources be exposed to the internet?

? Who can access my data?

? Does my code have any exposed credentials?

? Where are the critical vulnerabilities?

? Is there an active exploit in my cloud environment?

? How do I respond quickly?

Conclusion

Comprehensive security across the full lifecycle, from development to runtime

Cloud security requires proactive scanning and monitoring, layered defenses from design to delivery, and real-time responses across hybrid and multicloud environments. Microsoft is recognized for its leadership in multiple Gartner Magic Quadrants for security, making us the only cloud operated by a leading security vendor.[7] By incorporating automation and cloud-native defenses, you can migrate and modernize with confidence while building a secure foundation for your business.

Next steps

→ Find a trusted Microsoft partner

→ Fuel transformation with Microsoft experts and investments using Azure Accelerate

→ Learn more about Azure solutions

[1] Flexera 2025 State of the Cloud Report. Flexera. June 2025
[2] Flexera 2025 State of the Cloud Report. Flexera. June 2025
[3] Shepherd, Maggie. 30 Surprising Small Business Cyber Security Statistics. Fundera. 2025.
[4] The Business Value of Migrating and Modernizing IT Estate with Microsoft Azure. IDC. April 2025.
[5] Rivera, Carlos; Blankenship, Joseph; Born, Faith; Harrington, Peter. The Forrester Wave™: Zero Trust Platform Providers, Q3 2025. July 7, 2025.
[6] The Business Value of Migrating and Modernizing IT Estate with Microsoft Azure. IDC. April 2025.
[7] Industry-Recognized Cybersecurity Leader. Microsoft Security website.