Microsoft Azure

Secure the Shift

Navigating security challenges in migration and modernization

Contents

Introduction

The cloud can offer significant advantages over traditional on-premises environments, including the potential for cost savings, improved scalability and performance, better resiliency, and the ability to more rapidly develop and deploy innovative products and services. However, the cloud also introduces novel security challenges that you'll need to address as you move to the cloud.

The cloud security landscape is fundamentally different from that of your legacy infrastructure. Traditional on-premises security models that focus on the perimeter or network edge are insufficient. You need to adopt a fresh approach to security, one that is better suited to the more dynamic and distributed nature of cloud environments.

Making this adjustment is critical to migration and modernization efforts in the cloud, along with preparing you to safely adopt the latest AI-powered cloud technologies. It requires that you break down silos among your security, operations, and dev teams to establish a unified security approach. You also need to integrate the cloud's shared responsibility model into your strategy. In this model, both the cloud provider and your staff play integral roles in securing your IT infrastructure.

These efforts are worth it. Applying a security-first approach to cloud migration and modernization can help you take full advantage of the cloud's power and flexibility while rationalizing your overall security strategy. It can give your organization confidence in adopting new technologies to fuel business agility, trust, and resilience going forward.

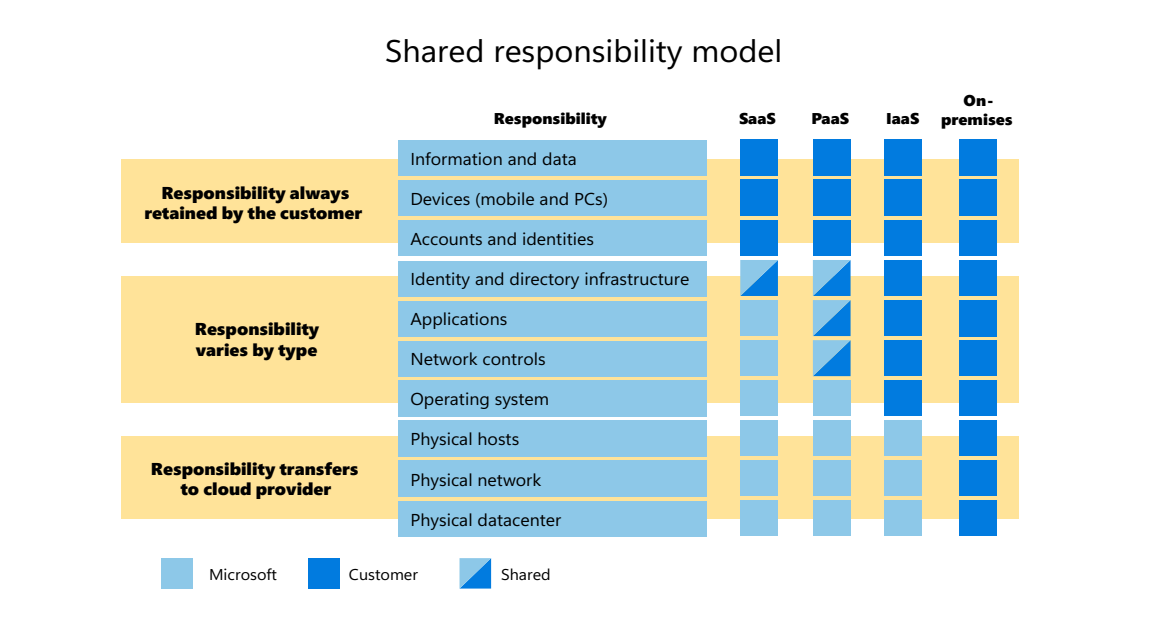
You've likely already explored the benefits that the cloud can bring to your business from an operations and development perspective, but have you fully considered how your security needs will change as you move to the cloud? This guide aims to give you a head start on identifying and dealing with some of the more common issues you might face, how you can avoid them, and how Azure and Microsoft Defender for Cloud can help you establish a secure, unified foundation for your cloud, multicloud, or hybrid IT infrastructure.

How can moving to the cloud improve your security?

One of the biggest misconceptions about moving to the cloud is the assumption that traditional on-premises strategies translate directly to the cloud. Although security has always been an essential part of IT, your existing security practices may not be suited to the dynamic environment that your cloud and hybrid infrastructure faces.

Adapting to this changed landscape requires a fresh mindset—one that embraces automation, continuous monitoring, and a security-first approach to operations. Many core concepts, like encryption, access control, and compliance, still apply in the cloud, but you need to adapt them for distributed cloud-based workloads. In hybrid environments, where workloads span on-premises datacenters and the cloud, you also need to establish consistent visibility and security controls across all of your environments.

Given these changes, it may appear that the cloud just introduces complexity and additional vulnerabilities to your infrastructure. However, the truth is that a well-planned cloud security strategy can actually streamline and simplify your security processes, while improving the security posture for both your cloud and on-premises environments. The key to this is the cloud's shared responsibility model, paired with the adoption of powerful security tools that can help unify how you manage both environments.



With the shared responsibility model, your cloud provider is in charge of some aspects of security, while your team is accountable for others. Generally, cloud providers secure the underlying infrastructure that your workloads run on, allowing you to offload the security burden for these resources. Managed app and data services enable you to offload even more of the security and configuration burden to the provider, so your security team can focus on higher-value concerns, like securing data and applications, managing identities, and enforcing policy.

In addition, powerful security tools offered by major cloud platforms can improve and simplify security across your entire IT estate. These tools offer centralized visibility for your workloads, posture and risk management, and unified threat protection. They can also extend cloud-based security capabilities to your on-premises infrastructure, providing consistent identity and access management, threat detection, compliance monitoring, and data protection across your hybrid and multicloud infrastructure.

By rethinking your security strategy approach and making the most of the strengths of the cloud, you can build a more agile, resilient, and manageable security foundation.

Understand how cloud security is different

Before you can take full advantage of the security capabilities that the cloud offers, you need to understand the unique security concerns that apply to cloud-based workloads. The most successful migration and modernization efforts take these concerns into consideration from day one and create security strategies and processes to protect their cloud infrastructure investments as early as possible.

As you plan your move to the cloud or review your existing cloud estate, make sure that you understand and address each of these core cloud security issues:

- **Expanded points of access**
  Moving to the cloud means managing more diverse types of workloads, potentially connected across multiple environments. Without proper planning and security considerations, this can add vulnerabilities to your infrastructure by creating more access points for attackers to exploit. The ongoing adoption of AI-powered applications further complicates this issue by increasing the total number of the entry points that you need to protect.

- **Fragmented security tools for threat detection and response**
  Your cloud and on-premises environments will face different types of potential threats, attacks, and vulnerabilities. Employing a variety of tools to protect your various cloud and on-premises resources can lead to inefficiencies and gaps in threat detection, response, and security management. This can hinder your ability to detect and respond to security events across your multicloud and hybrid infrastructure.

- **Evolving compliance regulations**
  Since your cloud or hybrid workloads may span multiple environments, cloud workloads may face a different set of regulatory requirements than what you've dealt with previously. Failure to comply with evolving regulations can bring hefty fines, legal penalties, and loss of customer trust. Expanding your business to new geopolitical regions or multiple cloud providers can further increase regulatory complexity, since you need to account for the different security standards of each jurisdiction and provider.

- **Cloud configuration errors and excessive permissions**
  Misconfigurations in cloud workloads can allow improper access or lack proper oversight of access. This can lead to data breaches and compliance violations.

- **Bridging the gap between DevOps and security teams**
  Delivering secure and reliable applications without compromising development speed or quality requires unified security responses between teams. If security teams are accountable for securing cloud apps, data, and infrastructure, but aren't responsible for making fixes in code, vulnerabilities may not be fixed promptly, resulting in leaks or breaches.

- **Risk identification and prioritization**
  Without the ability to proactively identify and prioritize vulnerabilities in complex, multicloud environments, issues may remain undetected and fixes may not be applied in a timely manner.

Address common cloud security challenges

A successful cloud migration and modernization effort requires that you shift how you think about security. You need to address the unique security concerns inherent in the cloud, while also integrating your legacy infrastructure into a unified security strategy. In this section, we highlight some common challenges that show how changing your approach to security in the cloud and adopting new strategies can strengthen your organization's overall security posture.

Although not an exhaustive list, these examples can help you rethink outdated assumptions and avoid problems as you move to the cloud. By meeting these challenges proactively, you get a head start on establishing a stronger, more future-ready cloud foundation.

Challenge #1: Own your role in the shared responsibility model

As we've mentioned, the cloud operates under a shared responsibility model, in which the cloud provider is in charge of some aspects of security, while your team is accountable for others. This model can offload many of your traditional security tasks, but misunderstanding the detailed breakdown of responsibilities is a risk as you start moving workloads to the cloud.

The particulars of which side is responsible for what depends on the provider and the type of cloud services you're using. For example, the cloud platform handles more security areas for fully managed platform as a service (PaaS) resources than for infrastructure as a service (IaaS) offerings, such as virtual machines (VMs).

Failing to properly map out which side is responsible for managing specific security areas can often lead to gaps in coverage, since your teams might incorrectly assume that the platform is covering more than it is. This can leave you with unmonitored workloads, improperly configured services, or unmanaged user permissions. The risk compounds in multicloud and hybrid setups, where each provider or environment may define responsibilities slightly differently.

To avoid these issues, your organization must clearly identify, define, and validate which security tasks your teams are responsible for. With the help of security posture management tools, establish internal review processes to ensure that you're validating your cloud configurations, data protection, access controls, and monitoring. Also make sure to educate your staff on how the shared responsibility model works and what they're accountable for.

Challenge #2: Address visibility gaps between cloud and hybrid environments

In most organizations, cloud transformation is a gradual process, resulting in hybrid environments that blend legacy systems with modern cloud infrastructure. However, during cloud adoption efforts, IT teams commonly make the mistake of focusing security efforts solely on new cloud assets. In the process, they can overlook the risks posed by their aging on-premises systems, applications, data stores, and legacy identity providers.

These older resources often lack modern defenses, remain unpatched, or are incompatible with newer security tools, making them prime targets for cyberattackers seeking an easy entry point into your infrastructure. Effective cloud security requires a holistic approach that spans the entire IT estate, covering not only your new cloud assets but also your remaining on-premises or hybrid infrastructure.

Ignoring these older assets results in vulnerabilities that can undermine even the most advanced cloud defenses. To ensure that your migration and modernization efforts are successful, you need to make sure that these legacy systems continue to be assessed, monitored, and accounted for in your broader security strategy. This includes integrating them into your threat detection, identity management, and compliance enforcement systems.

Challenge #3: Secure your DevOps processes across the entire application lifecycle

Modern application development techniques can introduce new vulnerabilities in addition to what you deal with as you protect your traditional production environments. They add cloud-based code repositories, build pipelines, and DevOps workflows. These components can offer superior developer productivity, streamline operations, and make your applications and services more reliable, but if they aren't properly secured, they can become attractive targets for cyberattackers.

Vulnerabilities can originate early in the development lifecycle through exposed secrets, insecure configurations, or unvetted third-party code. If these risks go undetected, they can silently propagate these vulnerabilities into the production environment. To address this, you need to adopt a *shift-left* security approach, in which security activities are integrated as early as possible in the software development lifecycle (that is, *as far left on the timeline as possible*). This helps to ensure that you're embedding security controls, testing, and guardrails throughout the development process.

Securing the development pipeline is just as critical as securing the final product. By integrating tools and practices that scan for risks early and that enforce security policies throughout the continuous integration/continuous delivery (CI/CD) lifecycle, your teams can minimize security issues, reduce exposure, catch issues sooner, and deliver safer software more quickly and efficiently.

Challenge #4: Prioritize the most important risks

One of the most dangerous mistakes in cloud security is failing to actively identify, prioritize, and manage risks before they compound.

A key benefit of the cloud is that your infrastructure can easily and quickly evolve to support your changing business goals or technical requirements. However, without continuous oversight, this type of change can result in small issues quietly growing into serious vulnerabilities. Failure to evaluate the severity of issues or inability to prioritize fixes for high-risk vulnerabilities can further compound this problem.

For example, a failure to ensure that your resources have up-to-date permissions (often a result of previous development or troubleshooting efforts) can leave your systems exposed to misuse or attack. Inactive or forgotten resources, such as unused VMs, improperly secured data stores, or outdated roles or user permissions, can become low-hanging fruit for bad actors seeking overlooked entry points. Even worse, cloud environments often contain hidden attack paths, where minor misconfigurations in identity, storage, or networking can chain together, resulting in high-impact breaches.

Managing cloud risks early and consistently is essential to preventing small oversights from turning into major incidents. To address these risks, you need to move from a reactive security approach to a more proactive one. By developing a unified strategy that can continuously audit permissions, identify and clean up unused assets, and map potential vulnerabilities, you can minimize the risk that continuous change can introduce.

Challenge #5: Unify threat detection and response across all of your environments

As your cloud environments grow in scale and complexity, you need to avoid falling into the trap of managing security with a patchwork of disconnected tools. Fragmented security solutions often lead

to fragmented defenses, with individual tools offering only partial visibility or protection and limited context across the broader environment.

In multicloud and hybrid environments, this lack of integration can become even more problematic. Different environments can offer different vulnerabilities and are subject to different types of attacks. Relying on a collection of disconnected tools to protect your infrastructure can slow down or prevent threat detection, response, and remediation.

In these scenarios, your security teams can be overwhelmed by siloed alerts, inconsistent policies, and gaps between tools that cyberattackers can exploit. To keep pace with modern threats and help ensure that you've minimized risks across your entire IT estate, you need unified security platforms that can provide end-to-end visibility, correlated insights, and coordinated enforcement for your workloads across the cloud and on-premises environments.

To help accomplish this, you should plan to adopt a unified cloud security solution that integrates an extended detection and response (XDR) solution. XDR solutions are integrated security tools that collect, correlate, and analyze threat data from across multiple cloud providers and your on-premises environments to help you detect and respond to complex threats efficiently. These systems provide unified capabilities that not only can strengthen your security posture but also can streamline operations, enabling you to move faster and more confidently in the cloud.

Build a secure cloud foundation

You may have noticed some common threads among these challenges. Legacy security strategies, tools, and siloed areas of responsibility can often lead to vulnerabilities, fragmented defenses, and increased risk. Without a holistic, proactive, and integrated security strategy, you'll be playing a time-consuming game of catch-up as you adapt to your new hybrid and multicloud reality in an improvisational manner.

The truth is that organizations that lead with security are better equipped to compete in the modern business environment. They can grow faster, adopt new technologies more rapidly, and adapt to change more effectively. To take full advantage of the cloud and to build a more resilient business in the process, you need to reevaluate your entire security strategy and examine how you can make the most of modern automation tools, identity-first principles, continuous monitoring, and unified security tooling.

What are the biggest challenges you face when securing your hybrid and cloud environments?

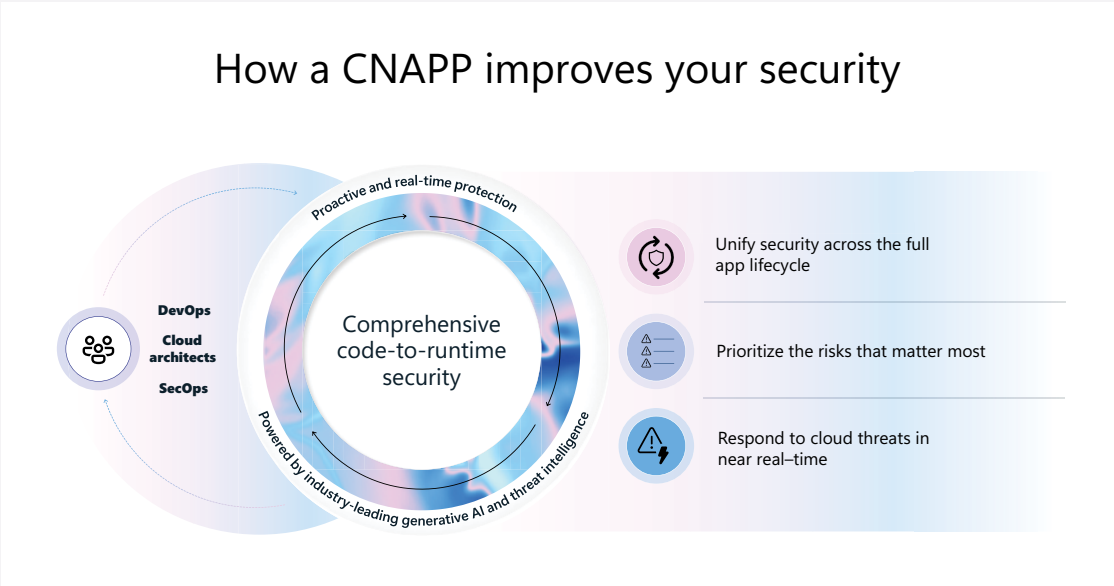
- **Cumbersome security onboarding and enablement.** Complicated or inconsistent security processes across your cloud and on-premises environments, in addition to a lack of standardized security automation or templates, can make applying security controls to new users or workloads much more difficult and time-consuming.
- **Lack of visibility.** You have various types of workloads that are built using an array of services and technologies. These workloads can also be hosted in multiple on-premises and cloud-based environments. Without tools to help you centrally inventory and manage all of these resources, it can be extremely difficult to understand the full scope of your exposure or to detect threats in a timely manner.
- **Lack of integration.** Without unified security operations tooling, your security teams can be left operating in silos, making it harder to correlate signals, prioritize risks, and respond quickly to emerging threats.

Adopt a unified security strategy to secure your entire IT estate

To be successful, your migration and modernization efforts need a unified security strategy that addresses the ever-changing threat environment that cloud services face. This strategy needs to account for the full diversity of your applications, services, databases, containers, and APIs, all of which can span multiple cloud platforms and on-premises datacenters. At the same time, you need to secure your modern DevOps and CI/CD-based processes that demand tighter collaboration between your developers and security teams.

Additionally, reactive legacy security strategies are no longer adequate in the face of modern cloud-based threats. You need to employ a more comprehensive, efficient, and scalable approach for securing cloud-native and hybrid environments. And this approach must deliver full application lifecycle protection, streamline operations, and empower teams to move quickly without compromising on security.

To meet these needs, you should consider adopting a cloud-native application protection platform (CNAPP) for your combined IT estate. A CNAPP is a unified security solution designed to simplify securing your workloads across hybrid and multicloud environments, providing the tools and services you need to help mitigate risk to your workloads and infrastructure, while also proactively detecting and mitigating emerging threats.



An effective CNAPP is built on three pillars:

→ Unify security across the full cloud app lifecycle

A CNAPP can prevent cyberattacks with built-in, natively integrated security controls across the entire cloud and AI application lifecycle.

This starts before code gets deployed, by integrating security tools directly into your DevOps workflows and CI/CD pipelines to detect vulnerabilities, misconfigurations, and exposed secrets as early as possible. It can also scan infrastructure as code (IaC), databases, containers, APIs, and third-party dependencies during build and test stages, enabling developers to make secure decisions without slowing delivery.

Just as critically, these protections continue after your code moves to production, providing continuous monitoring and threat detection after workloads are live. By applying consistent security across every stage of the lifecycle, you can reduce risk, respond to threats more quickly, and help ensure that your applications and data remain secure from code to cloud.

→ Prioritize the risks that matter most

The modern threat environment is constantly evolving, with newly discovered vulnerabilities, configuration drift, identity changes, and dynamic cloud architectures all making your security team's job more difficult. However, by offering unified posture management capabilities paired with constantly updated threat insights covering your entire hybrid and multicloud estate, a CNAPP can proactively minimize cloud security risks.

The CNAPP continuously monitors your cloud and on-premises resources, identities, and network configurations to maintain an up-to-date view of potential risks. It can help you centrally manage, monitor, and enforce compliance policies. It can also correlate data from development and runtime environments, helping to identify which known vulnerabilities and misconfigurations pose the greatest potential real-world threat to your workloads.

These context-aware insights help your security teams proactively harden high-risk areas, while avoiding wasting time on low-priority issues. With prioritized risk management, you can mitigate vulnerabilities, maintain a stronger overall security posture, and prevent minor problems from escalating into serious incidents.

→ Respond to cloud threats in near–real time

CNAPPs centralize threat detection for workloads, services, and identities across all your cloud and on-premises environments. They can also integrate with XDR solutions to take advantage of globally compiled threat data, allowing them to detect new threats more quickly. On detection of threats or issues, CNAPPs can provide context-rich alerts that help security teams to rapidly understand the scope and severity of problems.

A CNAPP can also automate response workflows (for example, disabling compromised accounts, rolling back changes, or isolating workloads), where possible, and integrate third-party tools to further support investigation and remediation efforts. These capabilities can reduce the time to detect and respond to issues, helping you to stay ahead of bad actors and to minimize business impact.

Together, these pillars can ensure that a CNAPP not only helps to reduce the risk of vulnerabilities across your entire IT estate but also continuously strengthens your security posture, while enabling rapid, effective responses to attacks.

Establish unified security across your IT estate with Defender for Cloud

Defender for Cloud is the integrated CNAPP solution from Microsoft. It's powered by industry-leading generative AI and threat intelligence capabilities, and it offers unified security for your workloads and data, across the entire cloud app lifecycle. With full visibility, real-time cloud detection and response, and proactive risk prioritization, it can protect your cloud, multicloud, and hybrid applications and data from code to runtime.

Following are some of the Defender for Cloud features that help you to strengthen your overall security posture and provide solid threat protection for your workloads:

→ Gain visibility into your workloads across your IT estate

Defender for Cloud provides centralized insight into your cloud and on-premises environments, offering a comprehensive view of workloads, configurations, and security status to help you identify potential vulnerabilities and misconfigurations early.

→ Manage compliance

Continuously track your infrastructure, apps, and data, for compliance with industry standards and regulatory requirements, with built-in compliance assessments,. Defender for Cloud can help you address gaps and demonstrate alignment with security frameworks, like International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), and Center for Internet Security (CIS).

→ Continuously assess and reduce cloud risks

Defender for Cloud automatically identifies risks across your cloud resources, such as exposed endpoints, weak configurations, and excessive permissions, and offers prioritized recommendations to reduce your exposure over time.

- **Strengthen application security posture using unified DevOps, security visibility, and infrastructure security**

Integrate security into the software development lifecycle by scanning IaC, containers, and dependencies for vulnerabilities, and enable collaboration between development and security teams to catch and fix issues before deployment.

- **Protect your compute workloads, APIs, and data in the cloud and on-premises**

Defend critical assets with advanced protection that spans VMs, containers, databases, and APIs, whether they're running in Azure, other clouds, or your on-premises datacenter.

- **Detect and respond to threats across all your environments using a unified platform**

Defender for Cloud integrates with Microsoft Defender XDR to provide threat detection and response capabilities so you can monitor your infrastructure for new threats, receive contextual alerts, activate automation to proactively deal with issues, and more. With Defender XDR, you can quickly investigate and respond to threats across your entire hybrid and multicloud infrastructure, helping to reduce response times and strengthen your overall security.

By securing your migration and modernization efforts with Defender for Cloud, you lay the foundation for agility, trust, and resilience in the cloud. With integrated tools that streamline risk management, enforce compliance, secure the full development lifecycle, and deliver intelligent threat detection, Defender for Cloud empowers your organization to move faster, operate with confidence, and lead with a security-first mindset as you integrate the cloud into your IT estate.

Secure your cloud and hybrid environment from day one

Effective migration and modernization is about more than simply moving workloads to the cloud. It also requires a fundamental transformation in your security strategy. As we've discussed, overlooking that shift can cause time-consuming and potentially financially harmful complications. Applying legacy assumptions to modern infrastructure, leaving legacy systems exposed, failing to secure dev workflows, or relying on fragmented security tooling can all increase the risks to your IT estate.

Addressing these challenges early can position your organization for long-term success. When you apply good security practices from the start, you enable greater agility, strengthen resilience, and reduce internal friction that can hinder innovation. A unified, cloud-native security approach, like that offered by Defender for Cloud, helps you to simplify complexity, maintain visibility across hybrid and multicloud environments, improve compliance efforts, and protect your workloads from code to runtime.

Ultimately, applying a security-first mindset to your migration and modernization efforts isn't just a technical imperative—it's critical for your organization's ongoing success in an ever-changing, increasingly cloud-powered business world.

Learn more about safeguarding your IT estate as you move to the cloud

Explore Defender for Cloud

Talk to an Azure sales specialist