

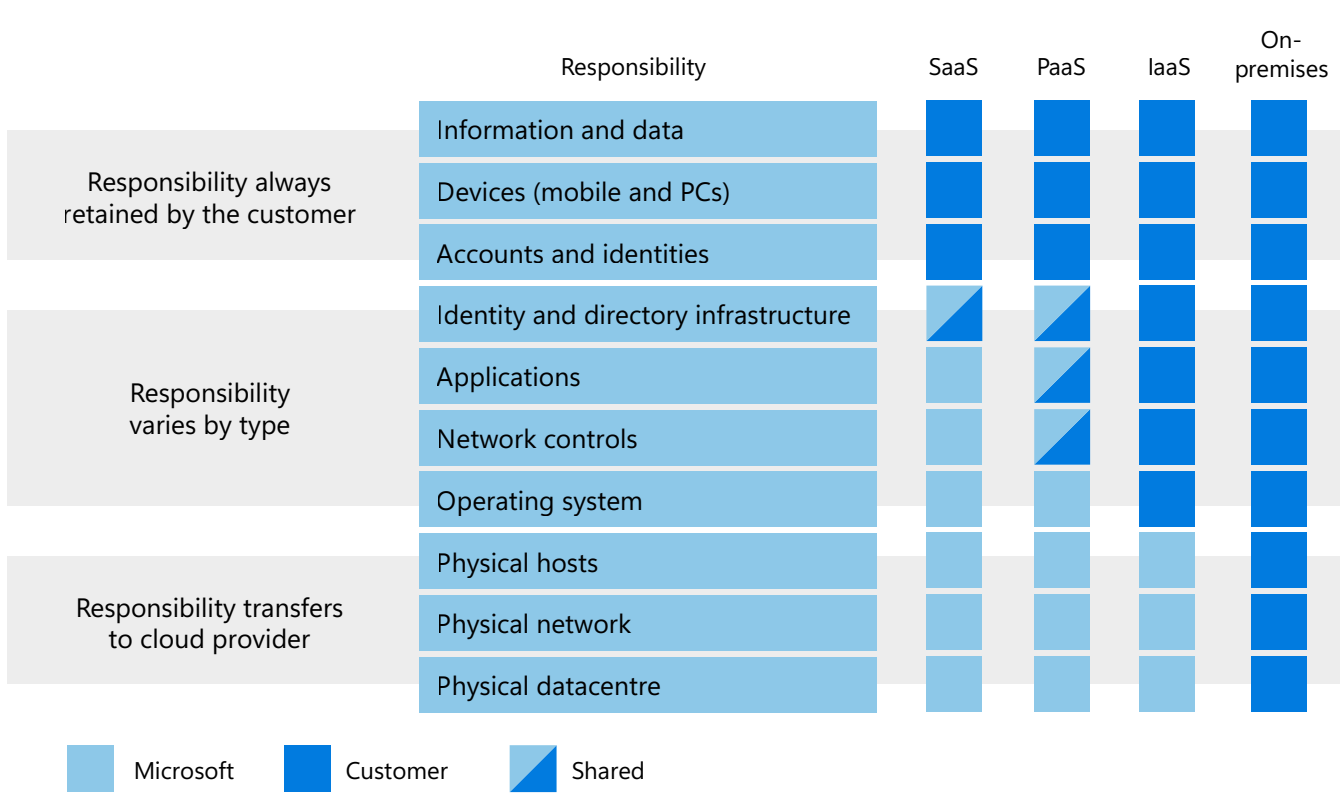
The cloud security mindset shift

Help protect your migration and modernisation efforts from day one.

As you start your move to the cloud, you need to ensure your entire IT estate remains secure. This requires a fresh approach to security that accounts for the cloud's unique security landscape. Understanding this landscape, and the tools and capabilities the cloud offers, is key to successfully and safely making this transition.

A shared security model

The cloud operates under a shared security model, where the cloud provider secures many aspects of the underlying infrastructure, while you remain responsible for securing your workloads.



How is cloud security different?

To be successful in the cloud, you'll need to understand the unique security concerns that apply to cloud-based workloads.

- Expanded points of access**
Cloud services increase the number and variety of access points, making it more important to secure workloads across environments.
- Fragmented security tools**
Using separate tools for cloud and on-premises environments can create visibility gaps and slow threat detection and response.
- Evolving compliance regulations**
The distributed nature of the cloud can introduce cross-region or provider-specific compliance requirements that you may not have applied to your legacy environments.

- Configuration and permissions errors**
Misconfigurations and overly broad access permissions in the cloud can lead to serious security and compliance breaches.
- Connecting DevOps and security**
When dev and security teams aren't aligned, your cloud apps can be exposed to preventable vulnerabilities, or fixes can be delayed.
- Risk identification and prioritisation**
Without proactive, centralised insights, it's difficult to spot and quickly act on your most critical vulnerabilities.

How does your mindset need to change?

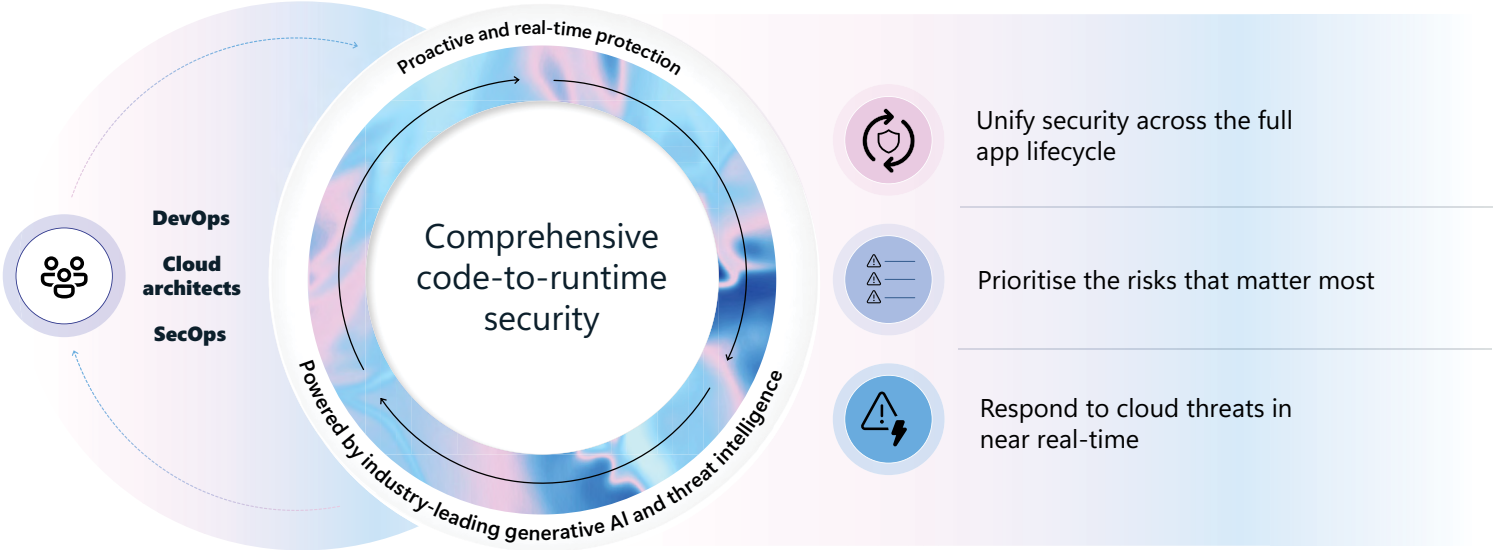
The cloud requires you to adjust how you approach security.

Traditional security	Cloud Security
Physical infrastructure at on-premises locations	Infrastructure distributed across multiple platforms and services
Perimeter-based security (firewalls, VPNs)	Identity and context-based security
Security is a separate concern, often acting to slow change	Security is integrated into your IT processes, capable of enabling business goals
Reactive threat response	Proactive and continuous threat detection and avoidance

Adopt unified security tooling

To help you make these adjustments, you should adopt a cloud-native application protection platform (CNAPP). CNAPPs simplify security across hybrid and multicloud environments, allowing you to mitigate risk, while also proactively detecting and dealing with threats.

How a CNAPP improves your security



A successful move to the cloud depends on both understanding the unique security environment of the cloud and developing a unified strategy to address these concerns. By taking advantage of the unified security solutions available on a cloud platform like Azure, you can feel confident meeting these challenges.

Download the eBook
[Secure the shift: Navigating security challenges in migration and modernisation](#) to learn more about how adopting a new security mindset, along with the right tools, can help you protect your cloud transformation from day one.

Get the eBook