White paper

The best practices for Microsoft security

www.globalknowledge.com
info@globalknowledge.co.uk
0118 912 1929

Introduction

Defining and deploying strong operational security practices for your Microsoft environment should be an essential pillar of your business strategy. This is especially true if large parts of your IT environment reside in the Azure cloud. The reason? Cybercrime is more prevalent than ever and has gradually evolved into a professional and successful revenue model.

Luckily, Microsoft security provides a strong and useful framework for protecting your data, infrastructure and applications. This is especially true if you combine the security checks and tools in Azure with an essential set of best practices. In this article, we will take a closer look at the best practices for Microsoft security. All of these recommendations are based on lessons learned by customers and are directly applicable to Microsoft environments. Read on and use them to your advantage!

1. Educate teams about the cloud security journey

Moving to and strengthening your cloud environment is a journey, a never-ending project characterised by a process of continuous improvement and constant learning. Not getting lost along the way requires some effort, since moving to the cloud is a significant change that requires a shift in mindset and a different approach to security. While the outcomes that security provides to the organisation won't change, the best way to accomplish these outcomes in the cloud is often very different.

This means that educating your teams about the cloud security journey is absolutely essential. You should inform your people thoroughly on the following topics and aspects of the cloud security equation:

- Threats in the cloud. This includes the evolution of threat environments, roles and digital strategies.
- A shared responsibility model and its impact on security. How are security roles and responsibilities evolving in your organisation?
- The cultural changes that usually arise from cloud adoption.

Everyone within the organisation who has some kind of security task or responsibility has to be or become familiar with the Microsoft cloud security context.

2. Educate teams on cloud security technology

Getting to know cloud security technology is the second part of the equation. Technical teams need access to technical information to make sound, informed security decisions. Learning new technologies on the job is their bread and butter, but the volume of details in the cloud often overwhelms their ability to fit learning into their daily routines. So be sure to set aside enough dedicated time for technical learning.

This applies to all IT and security roles that directly interact with cloud technology. Ensure that your professionals can learn at their own pace and have access to experienced instructors and hands-on labs. Microsoft provides resources that allow your technical professionals to step up with regard to cloud security. Azure security, Azure AD authentication and Azure Active Directory are excellent examples.

3. Assign accountability for cloud security decisions

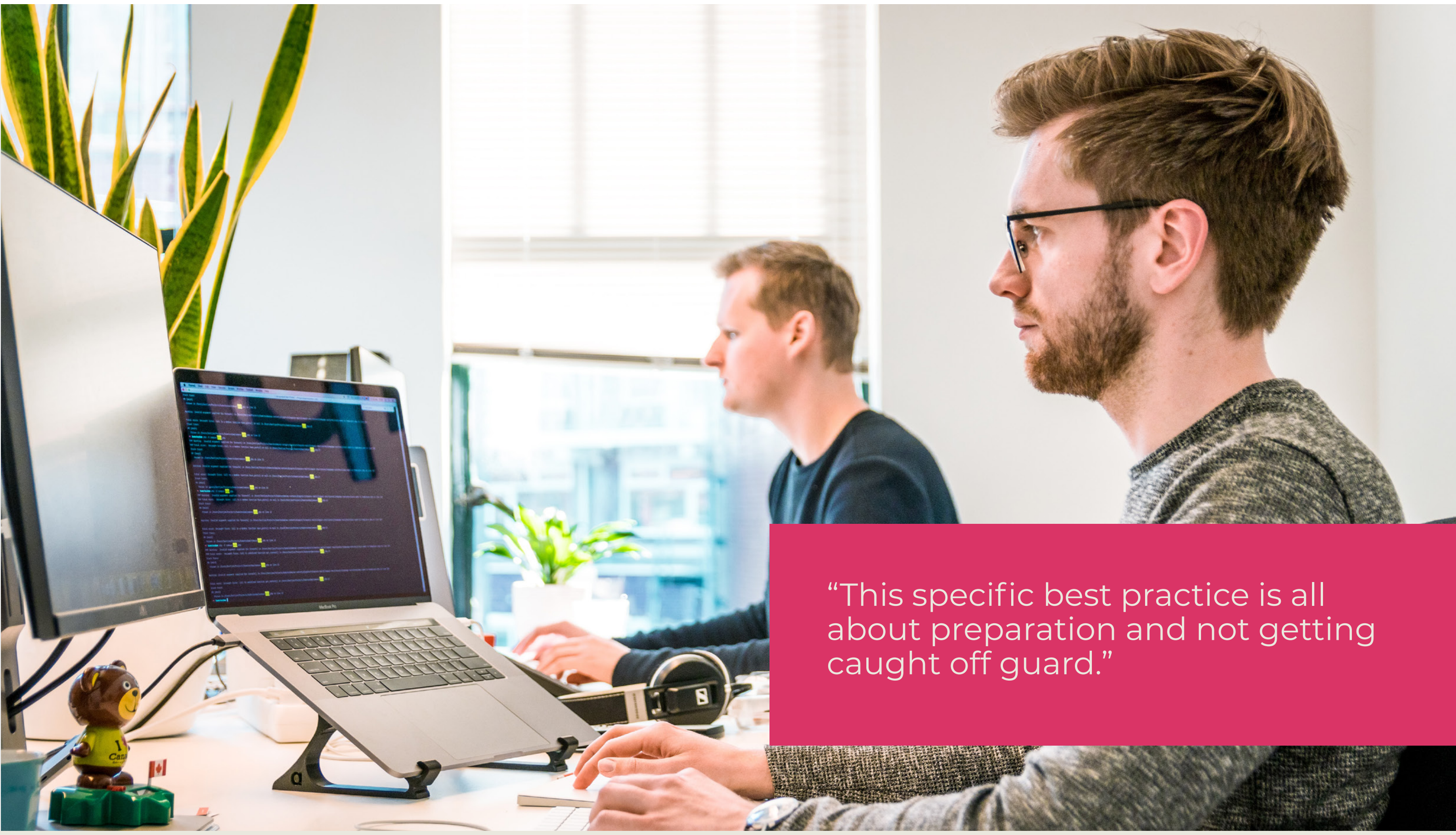
Security leadership and ownership are essential parts of good cloud security management. They speed up cloud adoption and increase the robustness of your security framework. Lack of ownership typically creates friction since nobody feels empowered to make decisions. So be sure to define which teams or individuals are accountable for making key security decisions about the cloud.

Subsequently, you should thoroughly document these owners and their contact information. Also, don't forget to socialise essential security accountability information with your IT, security, cloud and development teams. threats that present the biggest challenges and risks for your organisation.

4. Update incident response processes

This specific best practice is all about preparation and not getting caught off guard. Once you have fallen victim to a cyberattack, a risk can often become a difficult situation to control in the blink of an eye. This means that updating processes and preparing analysts to appropriately respond to security incidents is of the utmost importance.

Update processes, prepare your team, and practice with simulated attacks so your teams can work at their best during incident investigation, remediation and threat hunting. Perfecting incident response is a matter of creating the right processes and playbooks, providing education on threats and threat management, and getting the right insights into endpoint data, network and identity sources.



"This specific best practice is all about preparation and not getting caught off guard."

5. Assign accountability for cloud security decisions

Establishing a good framework for security posture management is another important security practice. Actively managing the security posture of your Azure environment involves two sets of responsibilities:

- **Security posture management.** Monitoring overall security posture using Microsoft Defender for Cloud's secure score and other data sources. It includes actively working with resource owners to mitigate risks and reporting them to security leadership.
- **Security remediation.** Be sure to assign accountability for addressing cloud security risks to the teams that manage your cloud (compute, application, data, storage, identity and access, networking, and IoT) resources

Secure score in Microsoft Defender is an excellent tool for security posture management. It provides an accurate and comprehensive assessment of the most important security information in Azure for a wide variety of assets.

6. Require passwordless and multi-factor authentication

Many organisations still heavily rely on the (faulty) premise that professional attackers can't guess or steal your administrators' passwords. Wrong. Just as your antique skeleton key is highly unlikely to protect you against modern-day burglars, traditional passwords won't protect accounts and cloud environments against a lot of attacks that are common in today's digital universe.

Implementing passwordless or multi-factor authentication is a big step in the right direction. Examples are Windows Hello, an authenticator app, Azure AD Multi-Factor Authentication, or a third-party multi-factor authentication solution. Tie these solutions to a solid and reliable identity, key management or security architecture, and train administrators on how to use them.

> "Traditional passwords won't protect accounts and cloud environments against a lot of attacks that are common in today's digital universe. "

7. Integrate native firewall and network security

Simplicity is a great asset in the field of security management. It prevents human errors like confusion and misconfigurations. You can greatly simplify your network security strategy and maintenance by integrating Azure Firewall, the Azure web firewall (WAF) and distributed denial of service (DDoS) into your network security approach and framework. Azure's native capabilities hugely simplify the implementation and operation of firewalls, which is typically a complex task.

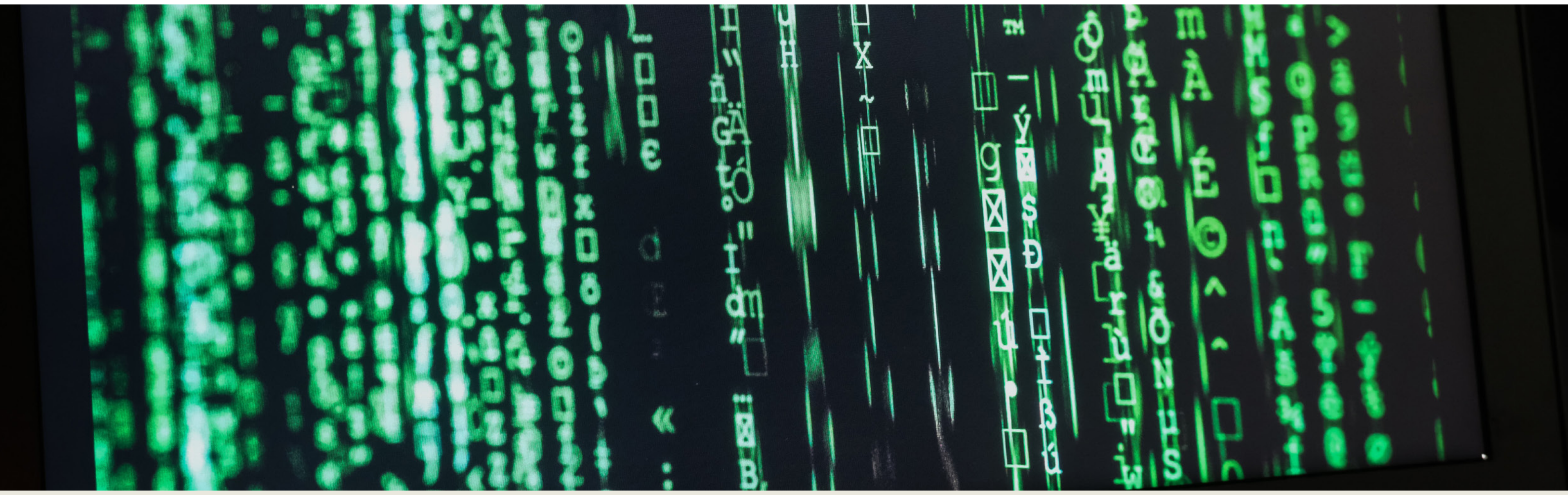
8. Integrate native threat detection

The impact of an attack or security breach is generally determined by two quantities: the mean time to acknowledge (MTTA) and the mean time to remediate incidents (MTTR). Integrating the native threat detection capabilities provided by **threat detection in Microsoft Defender for Cloud** allows you to focus on and speed up incident investigation and remediation. The implementation and management of native threat detection tools is usually handled and supervised by dedicated security operations teams within your organisation.

9. Standardise on a single directory and identity

Dealing with multiple identities and directories in your cloud security environment is a time-consuming hassle and often results in poor security practices (password reuse across accounts, a greater likelihood of stale or abandoned accounts). The good news? Microsoft's cloud technology allows you to standardise on a single Azure AD directory. It is possible to standardise a single identity for each separate user and application in Azure.

Properly standardising on a single Azure AD directory is usually a cross-team effort. It requires a solid security architecture, the creation of identity and key management teams and a strong set of policies and standards to secure optimal compliance.



10. Use identity-based access control instead of keys

Many organisations still use key-based authentication. Using keys to authenticate cloud services and APIs has its drawbacks. It requires extremely careful key management and is difficult for non-security IT professionals, such as developers and infrastructure specialists. Identity-based authentication overcomes many of these challenges with mature capabilities.

These include, amongst others, secret rotation, lifecycle management and administrative delegation. You can use Azure's managed identities to authenticate non-human services, such as services or automation. Do you have services that don't support managed identities? Then you can create a service principal with restricted permissions at the resource level instead.

11. Establish a single and unified security strategy

You can only move forward if everyone in your organisation is on the same page. Ensuring all teams are aligned to a single and unified security strategy is an important foundation for success. When teams work in isolation without being aligned to a common strategy, their individual actions can inadvertently weaken each other's efforts. The misalignment can create unnecessary friction between different teams (network security, identity, application) that slows down overall and asset-specific progress.

So, be sure to build and implement a security strategy that includes the input and active participation of all teams. This strategy should always include:

- Active input from all teams. You have to work out the cloud security journey together.
- A shared awareness of the security strategy. You can achieve this through clear communication and documentation.
- The application of enterprise asset segmentation.

> "Ensuring all teams are aligned to a single and unified security strategy is an important foundation for success."

How does Global Knowledge help?

Global Knowledge can provide you with the knowledge and tools that allow you to apply the aforementioned best practices for cloud security in your Microsoft Azure environment. We offer a wide range of Azure training courses. For example, the course “**Microsoft Security Administrator, M-AZ500, Microsoft Azure Security Technologies (AZ-500)**” teaches IT Professionals how to manage their Azure subscriptions, secure identities and administer the infrastructure.

The course “**Microsoft Identity and Access Administrator**” provides IT identity and access professionals, along with IT security professionals, with the knowledge and skills needed to implement identity management solutions based on Microsoft Azure AD and its connected identity technologies.

More information

Would you like to know more about security in Microsoft Azure and our courses? Then don’t hesitate to **contact us**. We are happy to make your acquaintance!

CONTACT US