Best practices Cloud security Microsoft Purview
6 min read

11 best practices for securing data in cloud services

By Pramiti Bhatnagar, Data Security and Privacy GBB
Abbas Kudrati, Chief Security Advisor

July 5, 2023

Data protection

Data security

Zero Trust

Microsoft Defender

Microsoft Defender for Cloud

Microsoft Entra

Microsoft Purview Data Loss Prevention

Microsoft Purview Information Protection

Microsoft Sentinel

In today's digital age, cloud computing has become an essential part of businesses, enabling them to store and access their data from anywhere. However, with convenience comes the risk of data breaches and cyberattacks. Therefore, it is crucial to implement best practices to secure data in cloud services.

1. Choose a reliable cloud service provider

Choosing a reputable cloud service provider is the first step toward securing data. The provider should offer secure data storage, encryption, and access controls. Look for providers that are compliant with relevant security standards and regulations, such as ISO 27001, HIPAA, and PCI DSS. Microsoft Cloud has several certifications making it a trusted choice for customers. For an exhaustive list of the compliance offerings, refer to compliance offerings for Microsoft 365, Azure, and other Microsoft services.

2. Understand your security responsibilities

When you move your data to cloud services, it's important to understand who is responsible for securing it. In most cases, the cloud provider is responsible for securing the infrastructure, while the customer is responsible for securing the data stored on that infrastructure. Make sure you know your responsibilities and take the necessary steps to secure your data. The below picture shows how the responsibility shifts from the customer to the cloud provider as the customers move their applications to cloud services. While customers maintain end-to-end responsibility of maintaining the environment on-premises, as they move to cloud services, more and more responsibilities are taken over by the cloud provider. However, maintaining and securing data, devices, and identities is always the customer's responsibility.

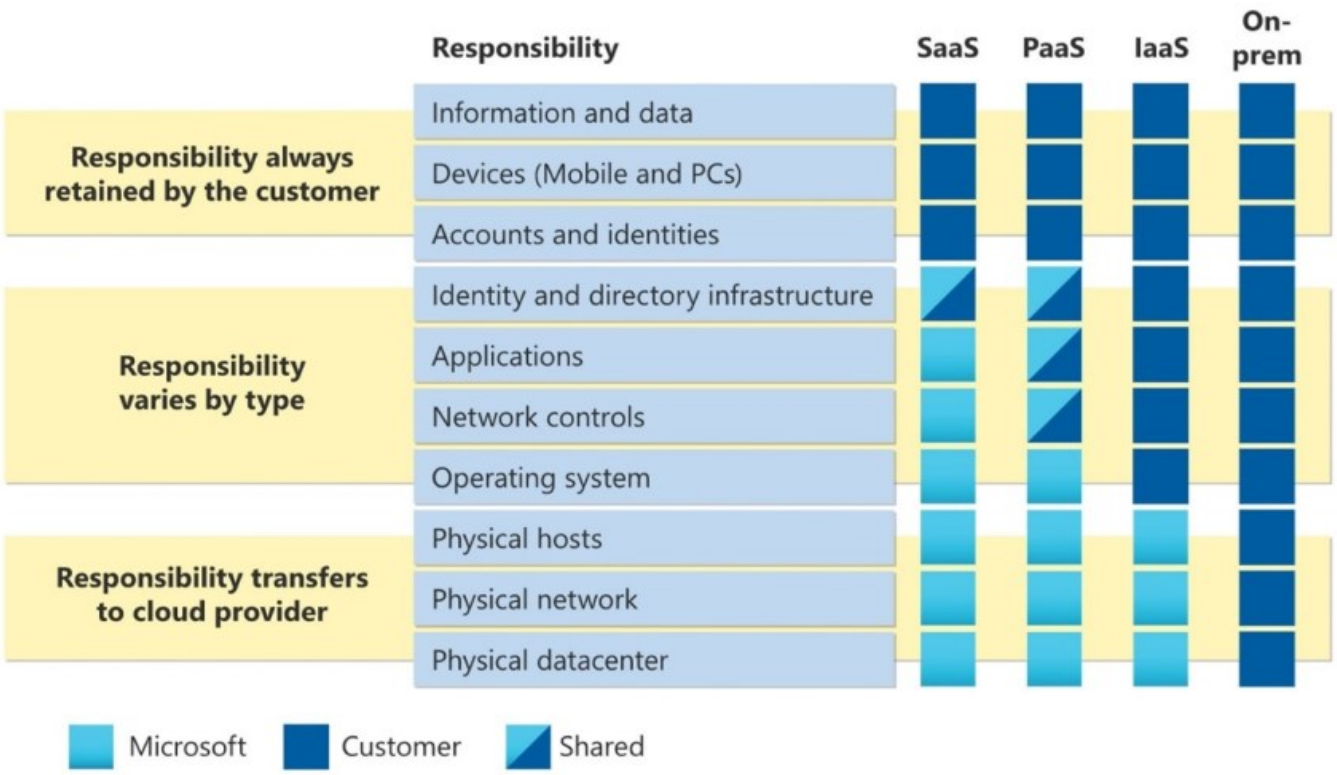

Figure 1. Shared responsibility model in the cloud.

3. Use strong authentication

While passwords are the first line of defense against unauthorized access, we are aware that passwords can be stolen, leaked, or compromised. Using strong authentication methods, such as multifactor authentication, can significantly reduce the risk of unauthorized access to data. Multifactor authentication requires users to provide multiple forms of authentication, such as a password and a code sent to a mobile app, before gaining access to the cloud environment. However, the best defense is provided by passwordless technologies like facial recognition, fingerprints, or mobile apps. Microsoft provides a host of such technologies like Windows Hello, Microsoft Authenticator, or FIDO2 Security keys. Using these methods, you can mitigate the risk of password theft.

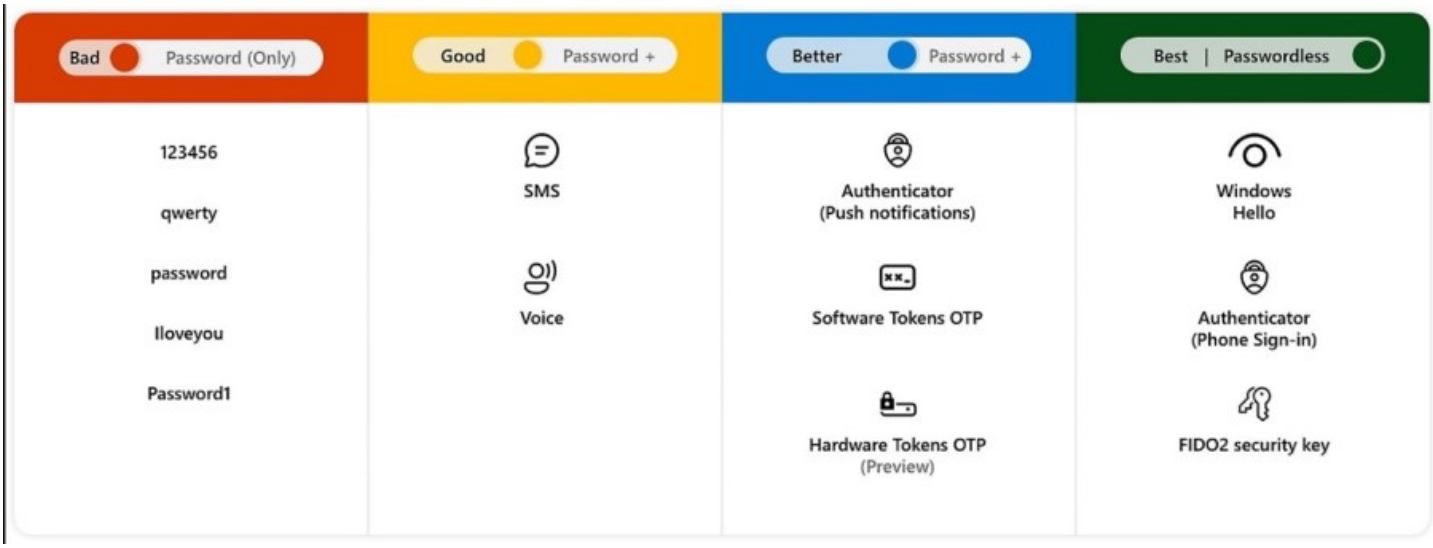

Figure 2. Authentication methods.

4. Implement encryption

Encryption is a critical component of cloud security. It involves encoding data in such a way that only authorized users can access it. Implementing encryption for data in transit and data at rest can help protect sensitive data from unauthorized access and data breaches. In the Microsoft Cloud, data is always encrypted at rest, in transit, and in use. **Microsoft Azure Storage Service Encryption** provides encryption for data at rest with 256-bit AES using Microsoft Manage Keys. It encrypts data in Azure

Managed Disks, blob storage, Azure files, Azure queues and table storage. **Azure Disk Encryption** provides encryption for data at rest in Windows and Linux VMs using 256-AES encryption. **Transparent Data Encryption** provides encryption for Microsoft Azure SQL Database and Azure Data Warehouse.

5. Protect data wherever it lives or travels

The biggest problem faced by businesses today is discovering where their sensitive data is. With more than 80 percent of corporate data "dark", organizations need tools to help them discover this data. Microsoft Purview Information Protection helps you scan data at rest across Microsoft 365 applications, SharePoint Online, Exchange Online, Teams, non-Microsoft Cloud apps, and on-premises file shares and SharePoint servers using the Microsoft Purview Information Protection scanner tool, to discover sensitive data. Identifying the data is not enough. Organizations need to be aware of the risk associated with this data and protect the data by applying things such as encryption, access restrictions, and visual markings. With Microsoft Purview Information Protection you can automatically apply sensitivity labels to identify the data as highly confidential, confidential, or general, depending on your label schema by using more than 300 Sensitive Information Types and Trainable Classifiers.

Organizations also suffer from inadvertent or malicious data loss. They need to have controls in place to prevent sensitive data from being accessed by unauthorized individuals. Microsoft Purview Data Loss Prevention helps prevent data loss by identifying and preventing risky or inappropriate sharing, transfer, or use of sensitive information across cloud, apps, and on endpoint devices. It is a cloud-native solution with built-in protection so that you no longer need to deploy and maintain costly on-premises infrastructure or agents.

Data doesn't move itself; people move data. That is why understanding the user context and intent behind data movement is key to preventing data loss. Microsoft Purview Insider Risk Management offers built-in, ready-to-use machine learning models to detect and mitigate the most critical data security risks around your data. And by using Adaptive Protection, organizations can automatically tailor the appropriate data loss prevention controls based on a user's risk level, ensuring that the most effective policy—such as blocking data sharing—is applied only to high-risk users, while low-risk users can maintain their productivity. The result: your security operations team is now more efficient and empowered to do more with less.

Learn more about data protection for businesses.

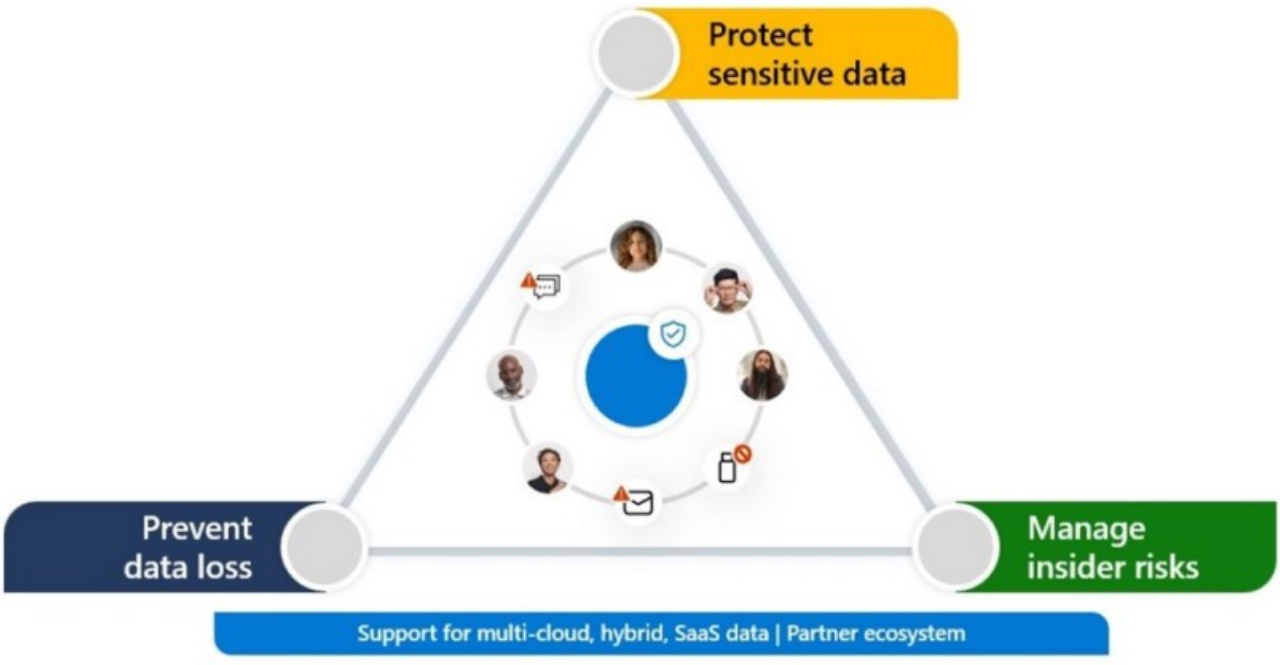

Figure 3. Microsoft's approach to data security.

6. Implement access control

Implementing access controls can help limit access to sensitive data in cloud services. Access controls should be based on the principle of least privilege, where users are granted the minimum access required to perform their tasks. Role-based access control can be used to assign roles and permissions to users based on their job responsibilities. Microsoft Entra encompasses all such Identity and Access capabilities from Microsoft.

7. Monitor cloud activity and know your security posture

Monitoring cloud activity can help detect and prevent unauthorized access to data. Cloud service providers offer monitoring services that can alert administrators when suspicious activity is detected. Regularly reviewing cloud logs and audit trails can help identify potential security threats. Microsoft Defender for Cloud is a cloud-native application protection platform that combines the capabilities of Cloud Security Posture Management with integrated data-aware security posture and Cloud Workload Protection Platform to help prevent, detect, and respond to threats with increased visibility into and control over the security of multicloud and on-premises resources such as Azure Storage, Azure SQL, and open-source databases.

Figure 4. Microsoft Defender for Cloud.

In addition, Microsoft Sentinel, Microsoft's AI-enriched, cloud-native security information and event management, can uncover sophisticated threats and automate response. It acts as a centralized hub across multicloud environments to monitor attackers as they move across vectors.

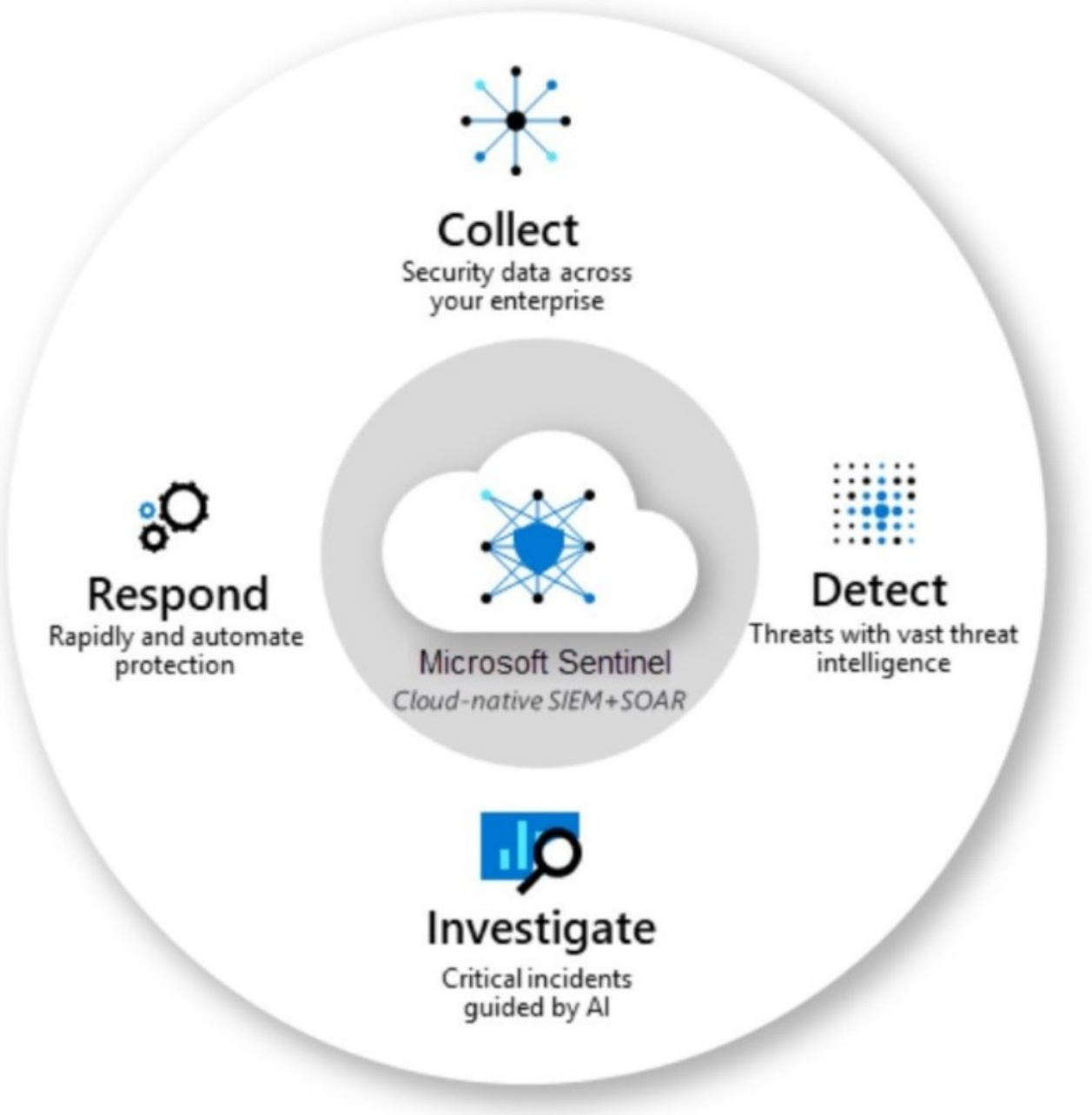

Figure 5. Microsoft Sentinel.

8. Use secure APIs

APIs are used to access cloud services, and they can be vulnerable to attacks if not secured properly. Secure APIs should be implemented with strong authentication and encryption to prevent unauthorized access to cloud services.

9. Conduct regular security assessments

Conducting regular security assessments can help identify security vulnerabilities and assess the effectiveness of security measures. Regular security assessments can be conducted internally or by third-party security experts.

10. Train your employees

Ensure that your employees are aware of the security risks associated with storing data in cloud services and are trained on best practices for securing data. This includes regular security awareness training and policies for reporting suspicious activity.

11. Implement principles of Zero Trust

Zero Trust is a security strategy. It is not a product or a service, but an approach in designing and implementing the following set of security principles:

- **Verify explicitly** – Always authenticate and authorize based on all available data points.
- **Use least privilege access** – Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
- **Assume breach** – Minimize blast radius and segment access.

A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy. This is done by implementing Zero Trust controls and technologies across six foundational elements of identity, endpoints, data, apps, infrastructure, and network.

Figure 6. Zero Trust across the vectors.

Each of these is a source of signal, a control plane for enforcement, and a critical resource to be defended. Here is Microsoft's guide to securing data with Zero Trust.

What's next

In conclusion, securing data in cloud services is essential for businesses to protect their sensitive information from unauthorized access and data breaches. End-to-end security design and implementation is the foundation of securing data in cloud services. Microsoft recommends a defense in depth approach implementing the principles of Zero Trust across identity, endpoints, data, apps, infrastructure, and network.

Learn more

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and Twitter (@MSFTSecurity) for the latest news and updates on cybersecurity.

Learn more

Connect with us on social

What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy