

Step up your enterprise security: 5 strategies for advanced cloud security

Meeting the security challenge

As an IT decision maker, you're at the forefront of the technology changes that drive digital transformation – especially the adoption of cloud technology. With the right approach, you can enable deeper knowledge of customers, access to new markets, fresh ways for employees to work in collaborative teams, increased efficiency and dramatically faster innovation.

At the same time, it's more important than ever to protect information, comply with regulations and protect privacy. A more diverse ecosystem of devices and applications, the growing trend of working remotely and proliferating cyberthreats combine to create a uniquely challenging environment. Having the right tools and processes

in place can have a long-lasting positive impact on your organisation's ability to create value and thrive in an ever-more-competitive global market.

Leveraging the investment and experience of cloud providers in security, compliance and privacy can enable you to reduce risk while gaining time and resources to focus on technology that differentiates your business. The cloud computing revolution is driven by the realisation among enterprise leaders – from Fortune 50 giants to agile startups – that IT infrastructure and broad business software functions are no longer part of their core value-creating mission.

More protection, less complexity

Increasing your commitment to cloud technology by adopting Microsoft 365 gives you advanced security capabilities such as cloud-based identity, threat protection integrated at the operating system level and powerful tools for identifying and mitigating attacks. And by combining Enterprise Mobility + Security and Windows 10 with Office 365 ProPlus, Microsoft 365 provides one intelligent solution that works across your entire enterprise.

5 ways

Here are five ways that Microsoft 365 can help you achieve the strong security foundation you need to achieve your digital transformation goals.

- 01 Manage and secure access with a single, unified identity solution
- 02 Gain the power of intelligent security
- 03 Get control over mobile, SaaS and line-of-business applications
- 04 Minimise privileged access
- 05 Enable single sign-on for maximum security and user convenience

01 Manage and secure access with a single, unified identity solution



Employees expect to work anywhere, on any device, whether that device is approved by IT or not. And employees are not the only users who connect to your systems. Customers, suppliers and other outside partners may have to do so as well. Today, the 'outside' of your corporate network is no longer defined by your firewall, but by the credentials your employees, suppliers and customers use to log on to your network, often from remote locations. In this environment, identity is the new difference-maker, enabling you to provide and control access to critical business data and applications.

Organisations with Microsoft 365 can use Azure Active Directory (Azure AD) to centralise identity and access management, and enable deep security, productivity and management across devices, data, apps and infrastructure. Azure AD is built to work for apps in the cloud, on mobile devices or on-premises, and it connects seamlessly with your on-premises directory to simplify security in hybrid IT scenarios.

With Azure AD, you can also enable conditional access, which allows you to block users with non-compliant devices, or locations, to help keep attackers out of your network.

[Learn more about Azure AD](#)

02 Gain the power of intelligent security



Cyberthreats continue to evolve at a rapid pace, making it difficult for traditional signature-based malware identification tools to keep up. You need intelligent security that can identify emerging threats before they cause problems for your IT ecosystem.

Microsoft 365 can help. Using vast computational analytics resources, Microsoft analyses data from more than a billion Windows devices, and more than 400 million monthly email messages, to detect new cyberattacks in their earliest stages. The result is the Microsoft Intelligent Security Graph. With Windows Defender Advanced Threat Protection in Microsoft 365, this intelligence is applied to your business to detect anomalies within your IT ecosystem and protect against zero-day threats automatically.

By connecting the insights gained from the Intelligent Security Graph with the data gathered about threats on your specific network, Microsoft 365 provides a two-way street of improvement driven by machine learning and big data.

[Learn more about intelligent security with Microsoft 365](#)

03 Get control over mobile, SaaS and line-of-business applications



Your users are probably relying on an ever-growing number of internal and third-party tools, including cloud-based software as a service (SaaS) apps. Maintaining visibility and control over mobile applications used to require fully enrolling devices in a mobile device management solution.

Now, with Microsoft 365, you can use Mobile Application Management (MAM) in Intune to manage internal and external applications from a single cloud-based solution. Users don't have to enrol their devices for protection your organisation's data within an application.

MAM enables your users to more securely access corporate information using the Office mobile and line-of-business apps they know, while helping to ensure data security by restricting certain actions, like copy, cut, paste and save as, to only those apps managed by Intune.

[Learn more about MAM in Intune](#)

04 Minimise privileged access

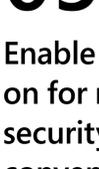


A key principle of modern security is ensuring least-privilege access, meaning that users are provided with the minimum administrative permissions for the shortest period necessary to do their jobs. This reduces the chance of a malicious user having high-level access or an authorised user inadvertently impacting a sensitive resource.

Using Azure AD Privileged Identity Management (PIM), you have granular control over access privileges to your IT resources. You can easily see which users are assigned and enable on-demand, 'just in time' administrative access to Microsoft Online Services such as Office 365, as well as see a history of administrator activation, including what changes administrators made to Azure resources.

[Learn more about Azure AD PIM](#)

05 Enable single sign-on for maximum security and user convenience



Many organisations rely on software as a service (SaaS) applications such as Office 365, Box and Salesforce for end-user productivity. Historically, IT staff needed to create and update user accounts in each SaaS application individually and users had to remember a different password for each SaaS application. The alternative is for users to create their own, potentially insecure credentials for each service. The more identities they have, the more likely they are to forget or lose one of them, creating a potential security risk.

By providing users with the convenience of single sign-on across all types of application, you can help reduce the risks and headaches associated with having multiple identities.

Azure AD extends on-premises AD into the cloud, enabling users to use their primary organisational account not only to log in to their domain-joined devices and company resources, but also all of the web and SaaS applications needed for their job. Application access can be automatically provisioned or de-provisioned based on group membership and employee status. Plus, Azure AD integrates out of the box with many of today's popular SaaS applications.

[Learn more about single sign-on with Azure AD](#)



As your organisation pursues the power of digital technology to transform its business, adopting the latest cloud solutions can make it easier for you to keep users, data and systems protected, while enabling better collaboration and greater creativity.

Enhancing your security capabilities by moving to Microsoft 365 gives you powerful new tools for providing highly secure yet seamless workplace experiences, while minimising administrative complexity and reliance on third-party applications.

[Discover Office 365](#)

[Test drive Office 365 today](#)