CLOUD SECURITY ADVICE FOR NONPROFIT LEADERS

ACCELERATE YOUR MISSION WHILE STAYING SECURE

Digital transformation provides many benefits for nonprofits. It can empower your staff to collaborate more effectively from anywhere, on any device, knowing that vital data is protected against cyberthreats. It can also reduce the time required to manage your technology infrastructure so more resources can be dedicated to your organization's mission. Cloud technology is central to achieving these benefits.

aleson ITC
data thinking

5 WAYS THAT MICROSOFT 365 CAN HELP YOU FURTHER REALISE THE POSSIBILITIES OF THE CLOUD WHILE ACHIEVING A STRONG FOUNDATION IN SECURITY AND COMPLIANCE

01 Give your staff more flexibility while maintaining control over data usage with a single, unified identity solution

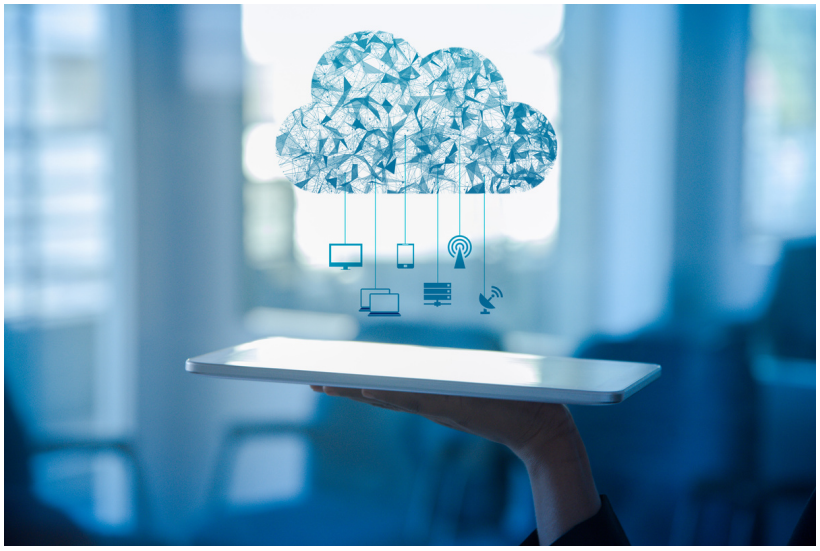
02 Gain the power of intelligent security

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

04 Minimize privileged access

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

aleson ITC
data thinking



01. Give your staff more flexibility while maintaining control over data usage with a single, unified identity solution

You want your employees to be able to work anywhere, on any device, without an overly cumbersome IT process. And employees are not the only users you want to be able to connect to your systems. Volunteers, donors, beneficiaries, and other outside partners also may need access to some parts of your organization. Today the “outside” of your organization's network is no longer defined by your firewall, but by the credentials your employees, donors, volunteers, and other external associates use to log onto your network, often from remote locations. In this environment, identity is the new difference-maker, enabling you to provide broad access while staying in control of data and identifying user activity across your entire infrastructure.

Organizations with Microsoft 365 can use Azure Active Directory (Azure AD) to centralize identity and access management and enable deep compliance management, governance, and productivity, across devices, data, apps, and infrastructure. Azure AD simplifies compliance and security, and is built to work for apps in the cloud, on mobile devices, or on-premises.

Learn more about AZURE

aleson ITC
data thinking

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. Your nonprofit needs intelligent security that can identify emerging threats before they cause problems. Microsoft 365 can help. Using vast computational analytics resources, Microsoft analyzes 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 organization to detect anomalies within your IT ecosystem and protect against zero-day threats automatically.

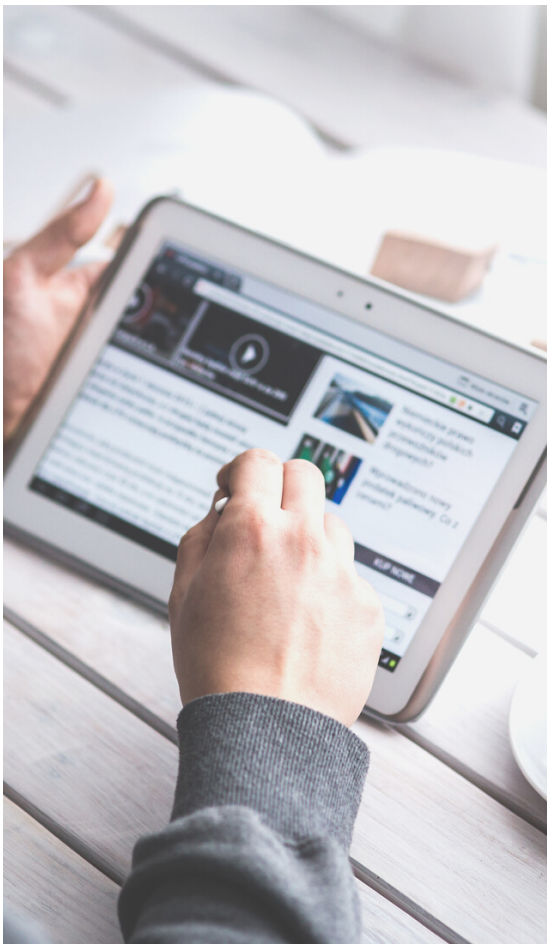
By connecting the insights gained from the Intelligent Security Graph with the data gathered about threats on your specific network, Microsoft 365 provides a two-way street of improvement driven by machine learning and big data.

aleson ITC
data thinking

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

Your staff is probably relying on an ever-growing number of internal and third-party tools to get their jobs done, including cloud-based software as a service (SaaS) apps, such as Citrix and Dropbox. In the past, maintaining visibility and control over mobile applications required 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.

With MAM, your employees can stay productive and securely access necessary information using the Office mobile and line-of-business apps they already know. MAM ensures data security by helping to restrict actions like copy, cut, paste, and save as to only those apps managed by Intune



aleson ITC
data thinking

04. Minimize 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 authorized 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. You can also see a history of administrator activation, including any changes administrators made to Azure resources.

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

Many organizations rely on SaaS applications such as Office 365, Box, and Salesforce to help boost staff productivity. Historically, the IT department needed to create and update user accounts in each SaaS application individually, and employees 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 applications, you can help reduce the risks and headaches associated with having multiple identities.

Many organizations rely on SaaS applications such as Office 365, Box, and Salesforce to help boost staff productivity. Historically, the IT department needed to create and update user accounts in each SaaS application individually, and employees 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 applications, you can help reduce the risks and headaches associated with having multiple identities.

MICROSOFT 365

LEARN MORE ABOUT CLOUD SECURITY

CONTACT US

+34 962 681 242

INFO@ALESON-ITC.COM

WWW.ALESON-ITC.COM

aleson ITC

data thinking