Secure your business when staff are working from home

In times like these, cyber security may not be at the top of our priority lists. But it's important to be aware of the threats that switching from on-premises to remote working conditions pose to organizations across the world.

As we seek to rapidly deploy cloud-based collaboration services to help professionals work from home, we may lose sight of the security threats that can accompany this shift. Your chosen applications may have a limited set of security controls.

1.1 HOW YOU CAN BOOST SECURITY TODAY

Without additional security controls, you rely on user awareness to prevent impactful mistakes and on targeted monitoring with whatever logs are available. This is not an ideal situation.

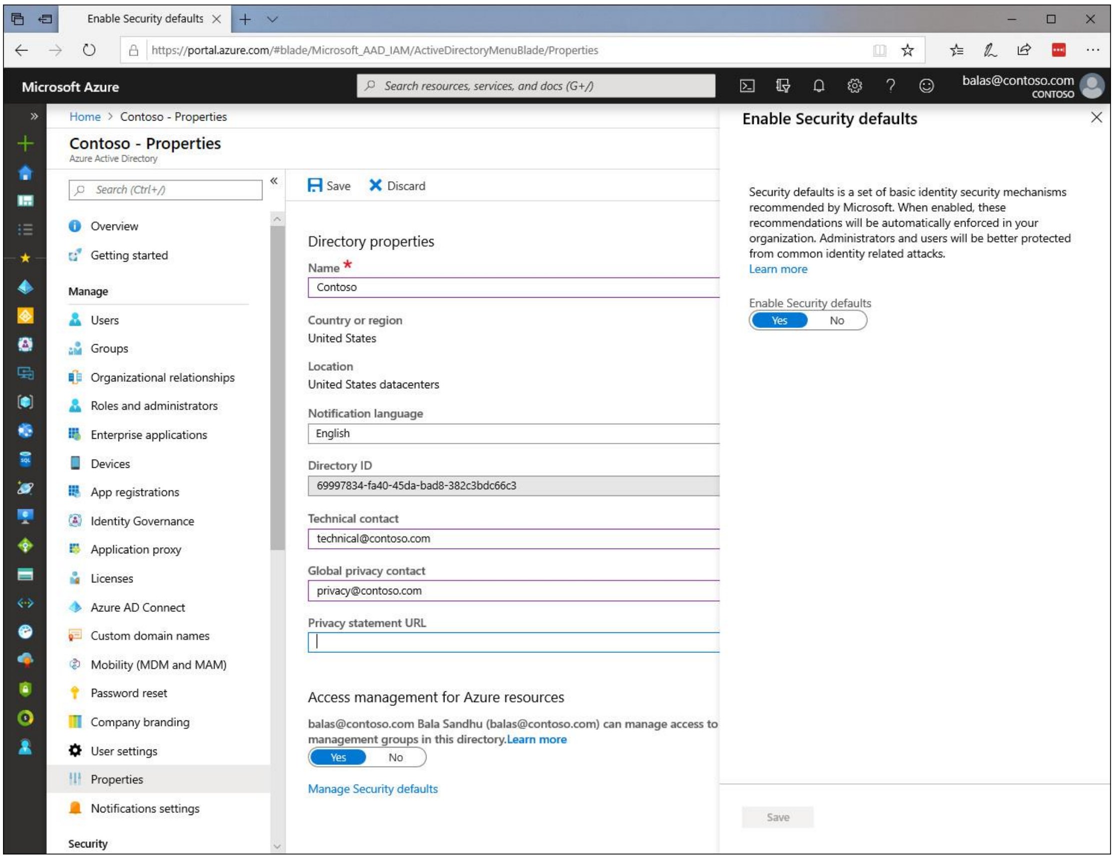
But in the Microsoft cloud, the gatekeeper for all cloud security-related things is Azure Active Directory (Azure AD). And it makes sense to focus efforts there first, even if the collaboration service you wish to provide your users is not from Microsoft. Then, once you have established secure access, it really depends on the chosen solution as to which controls are available. So, being aware of what's in the box is important.

In this article, we will list some of the security controls available to our customers. All with the goal of helping you to bolster security quickly – while reducing the impact on productivity.

1.2 SECURITY DEFAULTS – AZURE ACTIVE DIRECTORY

For Azure AD, we recently introduced security defaults. These fall under the category of what we feel are the most basic and yet the most important controls to consider. These defaults help you enforce multi-factor authentication (MFA) for administrative accounts and then give you the option of enabling the Microsoft Authenticator mobile app for users. Note that it is not granular, so it will either be on or off (by user state). However, you can give users the option to 'remember my device' to reduce the amount of times they are asked to perform 2-step authentication.

To see what the configuration and user experiences look like before you start configuring, take a look at this video one of my colleagues made.



https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Properties

Contoso - Properties
Azure Active Directory

Directory properties

Name *
Contoso

Country or region
United States

Location
United States datacenters

Notification language
English

Directory ID
69997834-fa40-45da-bad8-382c3bdc66c3

Technical contact
technical@contoso.com

Global privacy contact
privacy@contoso.com

Privacy statement URL

Access management for Azure resources

balas@contoso.com Bala Sandhu (balas@contoso.com) can manage access to management groups in this directory.Learn more

● Yes ○ No

Manage Security defaults

Enable Security defaults

Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks.
Learn more

Enable Security defaults
● Yes ○ No

Azure security

Security defaults in Azure AD make it easier to be secure and help protect your organization because they contain preconfigured security settings for common attacks.

These are configurable controls on top of our platform in the area of accounts and identities. Read about the shared responsibilities model to understand which security tasks are handled by Microsoft as the cloud provider and which tasks are handled by you.

If there's nothing else you can do, the above is a strong starting point. If your organization has access to Premium features in Azure AD, it is definitely advisable to use those as they provide you with additional options that greatly increase account security, as well as offering more fine-grain controls that increase usability.

1.3 POWERFUL QUICK WINS WITH OFFICE 365 AND MICROSOFT TEAMS

So, let's talk about what we can do for Microsoft's collaboration platform, Office 365. This includes Microsoft Teams. In fact, Microsoft is currently offering an extended trial to support remote workers using Microsoft Teams. Since these workloads are connected to Azure AD, the controls mentioned above also apply.

Our Enterprise Cybersecurity Architects Mark Simos and Matt Kemelhar provided the input for our Office 365 Security Roadmap. This roadmap contains a prioritized overview of recommended security configurations and practices and gives you a clear path of where to focus.

While we strive to achieve as much as possible in the long-term, some of the best first steps to take can be found here: 30 days – powerful quick wins.

1.4 MICROSOFT SECURE SCORE

When it comes to security, it's increasingly difficult to know what you should be doing first or next. There are a multitude of considerations around information protection, security management, security monitoring and so on – and we certainly don't recommend taking any shortcuts around these areas. This is where Microsoft Secure Score – free for all customers – can help.

By following your Security Score recommendations, you can protect your organization from threats. From a centralized dashboard in the Microsoft 365 security center, you can monitor and work on the security of your Microsoft 365 identities, data, apps, devices and infrastructure.

Secure Score gives you a way to improve your security posture in a structured way by providing visibility and actionable recommendations. Security posture management is a complex topic for any organization. And if you want to enable continuous security posture improvement (which you do!) – you'll need to make sure it's well rooted in your organization.

So, even though this article started with recommendations to cover the basics quickly, we've seen there's always something more to do. Microsoft Secure Score is an excellent tool for you to work on your organization's security posture. It's free to use, and a great starting point.

1.5 FIND OUT MORE ABOUT MULTIFACTOR AUTHENTICATION (MFA)

As mentioned above, MFA is a vital piece of the security puzzle. By requiring multiple forms of verification to prove identity when signing into an application, MFA can immediately help secure your business against breaches. And with Azure AD, you can enable MFA at no extra cost.

Click here to find out more about boosting security with MFA.

1.6 ENABLE REMOTE WORKING WITH ZERO TRUST SECURITY

Understanding “Zero Trust” security and how companies can build cloud strategies around it is crucial as staff increasingly is work remotely.

With a Zero Trust model, instead of assuming everything behind your corporate firewall is safe, you assume breach and verify each request as though it originates from an open network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches you to ‘never trust, always verify.’

Click here to find out more about Zero Trust security.