A Journey Through Microsoft/Office 365 Security

By: Kyle Haas

Friday, January 26, 2024

Where Are You In Your Journey?

HOW MUCH SURFACE AREA DOES YOUR ORGANIZATION HAVE?

ARE YOU FOLLOWING BEST PRACTICES?

ARE YOU PREPARED TO RESPOND IN AN EMERGENCY?

DO YOUR USERS KNOW WHAT TO DO IN AN EMERGENCY?

ARE YOU GETTING THE MOST OUT OF YOUR LICENSING?

Goals For Today:

- Are Security Defaults A Good Fit for You?
- MFA / Conditional Access & Best Practices
- Making the most of your licensing
- Increase your security posture over time
- How to respond to an emergency

…

And we'll end with some open discussion regarding 365 administration – we can even talk about Windows 11.

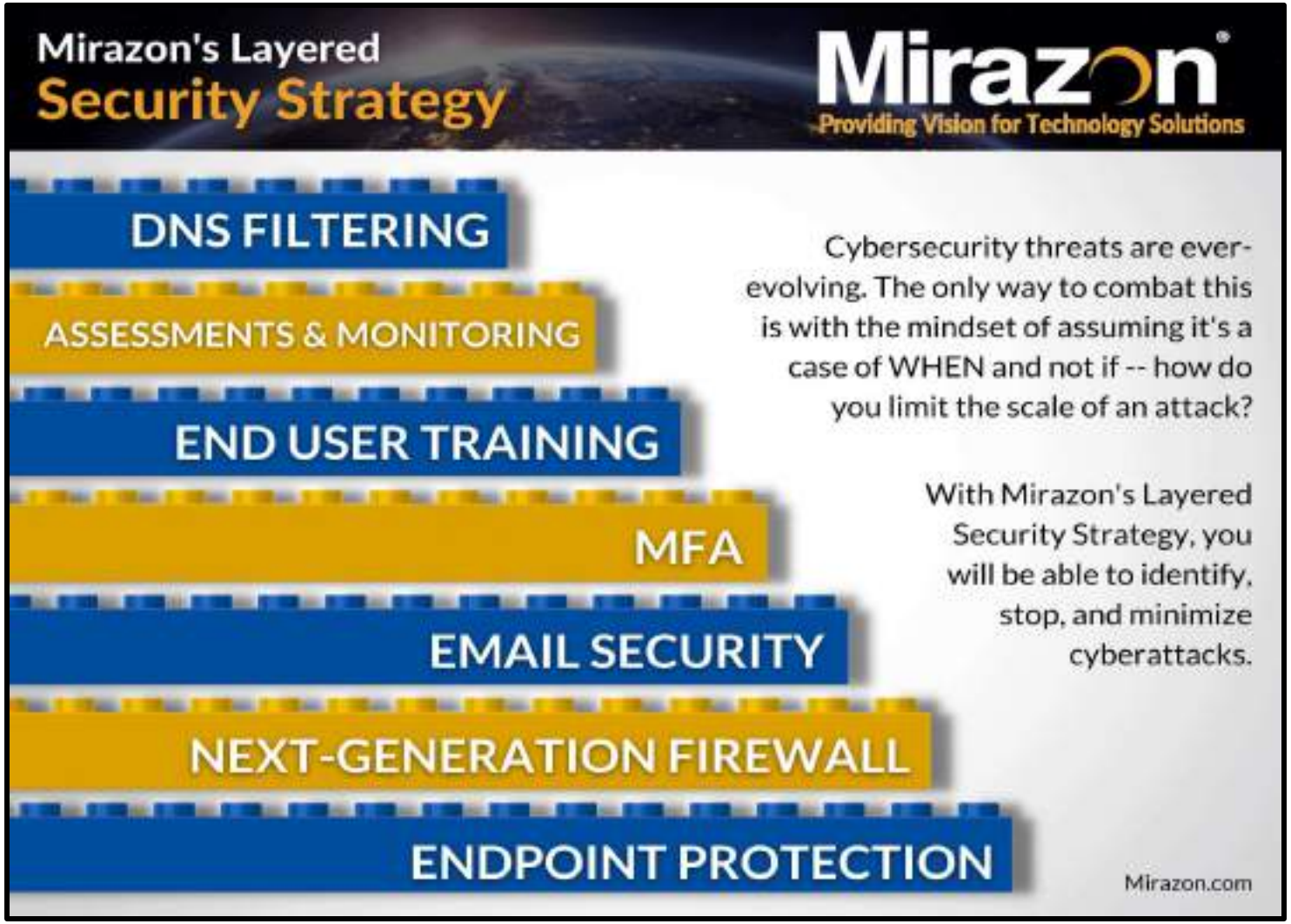
What's The Big Picture?

- Our online/cloud surface area keeps growing exponentially.
- Phishing threats through email continue to be a major issue, although they are mostly negated through the usage of MFA.
- Hackers are getting smarter and are working together. They are performing more intricate attacks than we've seen in previous years and will wait until the moment is right.
- Cyber security insurance coverage requires MFA for email as a bare minimum, and MFA is preferred across the board.
- Some companies are already moving to "passwordless" auth.

Security In Layers

- Multiple layers shown on the right overlap with Microsoft 365…

- **Want better security?**
- Start with your weakest layer!



Security Defaults: Perfect for Small Orgs

- What comes with every new 365 Tenant?
  Security Defaults! Since October 2019!
- For many, this is the very first feature that gets disabled!
  - But what does it do?
    - Requires ALL users to register for MFA within 14 days of account creation.
    - Requires admin role-holders to always use MFA.
    - Requires users to use MFA “when necessary.” (Location, Device, role, and task.)
    - All legacy authentication is blocked, with no exceptions.
    - Entra (Azure AD) Portal is blocked for non-admins.
  - Where is it? Azure AD (Entra) > Overview > Properties

https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults

Security Defaults: Use Case

- Who should use Security Defaults?
  - Organizations with Free Azure AD, who are wanting to cover their bases with otherwise simple security requirements and no exclusions. This is perfect for ticking the box "We Require ALL Users to use MFA."

  NOTE: If you are not using Security Defaults, and you're not using Conditional Access, you **MUST** enable **MFA PER USER.**
- Who should not (*or cannot*) use Security Defaults?
  - Any organization which is paying for and using Entra P1/P2 licensing, or using Conditional Access policies.
  - Any organization who needs to tweak the default settings, including making exclusions for legacy authentication or to bypass MFA.

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

Let's talk licensing for a minute…

Click here for full feature breakdown and comparison.

Azure/Entra Active Directory Premium Licensing:

- Available as addon P1/P2 or through the following:
  - M365 Business Premium (P1)
  - EMS E3 (P1) – Enterprise Mobility and Security Addon
  - EMS E5 (P2) – Enterprise Mobility and Security Addon

P1 = 6$/User/Month – No Limit
P2 = 9$/User/Month – No Limit
BP = 22$/User/Month – 300 User Limit
EMS E3 = 11$/User/Month – No Limit
EMS E5 = 17$/User/Month – No Limit

Azure AD Free:

✓ Basic user and group management, AD-Sync, basic reports/logs (7-Days), and cloud Self-Service Password Reset (SSPR). Must use **Per-User MFA** if not using Security Defaults.

Azure P1:

✓ **Conditional Access**, extended logs (30-Days), dynamic groups, password-writeback for AD.

Azure P2:

✓ **"Risk-Based" Conditional Access**, PIM, MFA Registration Policy, etc.

"The new standard" for security-conscious organizations.

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

Conditional Access

With P1 Templates:

- “Require all admins to use MFA.”
- “Require all users to use MFA.”
- “Block legacy authentication.”
- “Block unsupported or unknown device platforms.”
- “Require compliant or Azure-AD/Hybrid joined device.”
- “Require security info registration” or “Require Terms of Use!”

With P2 licensing we can use AI for “Risky Sign-Ins” and “Risky Users” as conditional access variables!

Common Custom Policies:

- “Block all NON-USA sign-ins” or “Block sign-ins outside of our HQ!”
- “Block all sign-ins from untrusted IP addresses.”

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Org Settings Best Practices

365 Admin > Settings > Org Settings

- Services:
  - Modern Authentication (Enable – And use Conditional Access)
  - User Consent to Apps (Require Admin Consent?)
- Security & Privacy:
  - Customer Lockbox – Enable
  - Idle Session Timeout – Enable
  - Password Expiration – Does Passwordless still weird you out, too?
  - Self-Service Password Reset (SSPR)
  - Sharing – Let Users Invite Guests?
- Organization Profile:
  - Help Desk Contact Information

Take Time to Review Admin-Role Holders!

Avoid using any admin account as a "Daily Driver"

Don't make every admin a global admin!

What about Teams? SharePoint? Exchange?

We aren't going to cover individual settings for every single app…

Teams:

- Who is allowed to call us? Who are we allowed to call?
  - Allow external calls, or allow only trusted domains? Block Skype/Personal calls?
- Who is allowed to control a meeting? Do we allow screen-sharing and remote control?

SharePoint/OneDrive (Policies > Sharing / Access Control):

- Should public links to files be allowed? Should external access be blocked?
- Default permissions when sharing?

Exchange:

- Make the most of transport rules!
  - Label External Mail and check out the "Preset Security Policies" for Email!

Security / Compliance Admin Centers

"Defender" / Security Center / Security.Microsoft.com

- Logs and tools to simulate, review, and respond to threats.
- Security Awareness Training / Simulated Phishing
- Threat Policy Templates: Standard and Strict
- Learn about malware trends

"Purview" / Compliance Center / Compliance.Microsoft.com

- Set labels, policies, alerts and reports regarding sensitive data.
- Perform investigations – search your whole tenant for specific activity.

"Entra" Identity Secure Score / Entra.Microsoft.com

All have unique "Scores" with recommendations from Microsoft.
Check out Microsoft's recommendations over time and increase your score.

Responding To Emergencies As An Admin

As an Admin who is investigating another user:

- Review Sign-In Logs (Why Not Do Monthly Checks?)
- Anything suspicious? Reset password and **require MFA**.
- Check for rules in Outlook, then look elsewhere.
- Educate the end-user.

As an admin who is investigating the breach of another admin:

- Same as above, but also check for newly created users, delegated partner access, check admin-role holders, check Exchange connectors, Sharepoint sites, etc. Seek help. ☺
- Review Audit Log

  https://learn.microsoft.com/en-us/purview/audit-log-activities

Responding To Emergencies As an End User

- Please notify IT if you have a suspicion that something is wrong.

Take notes if it is necessary for you to remember events that are occurring.

Sign in to Office.com → Click Your Name in Top-Right → View Account

- Check My Sign-Ins (https://mysignins.microsoft.com/)
- Reset Password
- Manage Devices → Check devices registered with your account.
- Verify your Security Info (MFA) is correct, and you are using the best method. (https://mysignins.microsoft.com/security-info)

Works for Personal Accounts, too!

Before We Demo: Some Current Events

- Azure AD Now Called “Entra” (On-Truh, Inn-Truh?)
- New Authentication Methods (**Legacy Methods Die 30 Sept 2024**)
- Microsoft Managed Registration Campaigns (Anybody fight that?)
- Azure AD Sync – Server 2016 and newer now required.
- Windows 10 End of Support – Now Coming October 2025

Anybody got any other Microsoft 365 News before we demo?

Let’s Demo!

- Review User-Sign Ins
- Conditional Access templates
- New MFA Methods (Migration Process, etc.)
- Azure/Entra MFA Tips
- Peek at Secure/Compliance Score
- Anything else??

Thanks! Q&A

Kyle Haas | kyle.haas@mirazon.com | (502) 432-5825