Strengthening the Gates to Your M365 Stack

By: Kyle Haas

Friday, March 27th, 2026

WARMUP

Where Are You In Your Journey?

How big is your attack surface?

On-prem only? Hybrid? Fully cloud?
Every cloud workload is a potential entry point.

Are you following best practices?

Security Defaults, Conditional Access, MFA…
What do you have enabled?

Are you prepared to respond?

What steps would you take in a crisis?
Are you and your end-users educated?

Are you maximizing your licensing?

Are you using the features available to you?

AGENDA

Goals For Today:

01 **Essentials & Baseline Protections**

Security Defaults vs. Conditional Access, strengthening MFA, and Secure Score quick wins

02 **Features & Licensing**

What you get with M365 Basic, Business Premium, or Enterprise — and where to upgrade

03 **Incident Response Playbook**

Sign-in logs, Entra ID, Purview audit logs, and AI-assisted triage

04 **Stopping a Breach**

Revoking sessions, forcing password resets, hunting forwarding rules and token abuse

05 **Open Q&A**

Bring your real-world scenarios, war stories, and questions

What's The Big Picture?

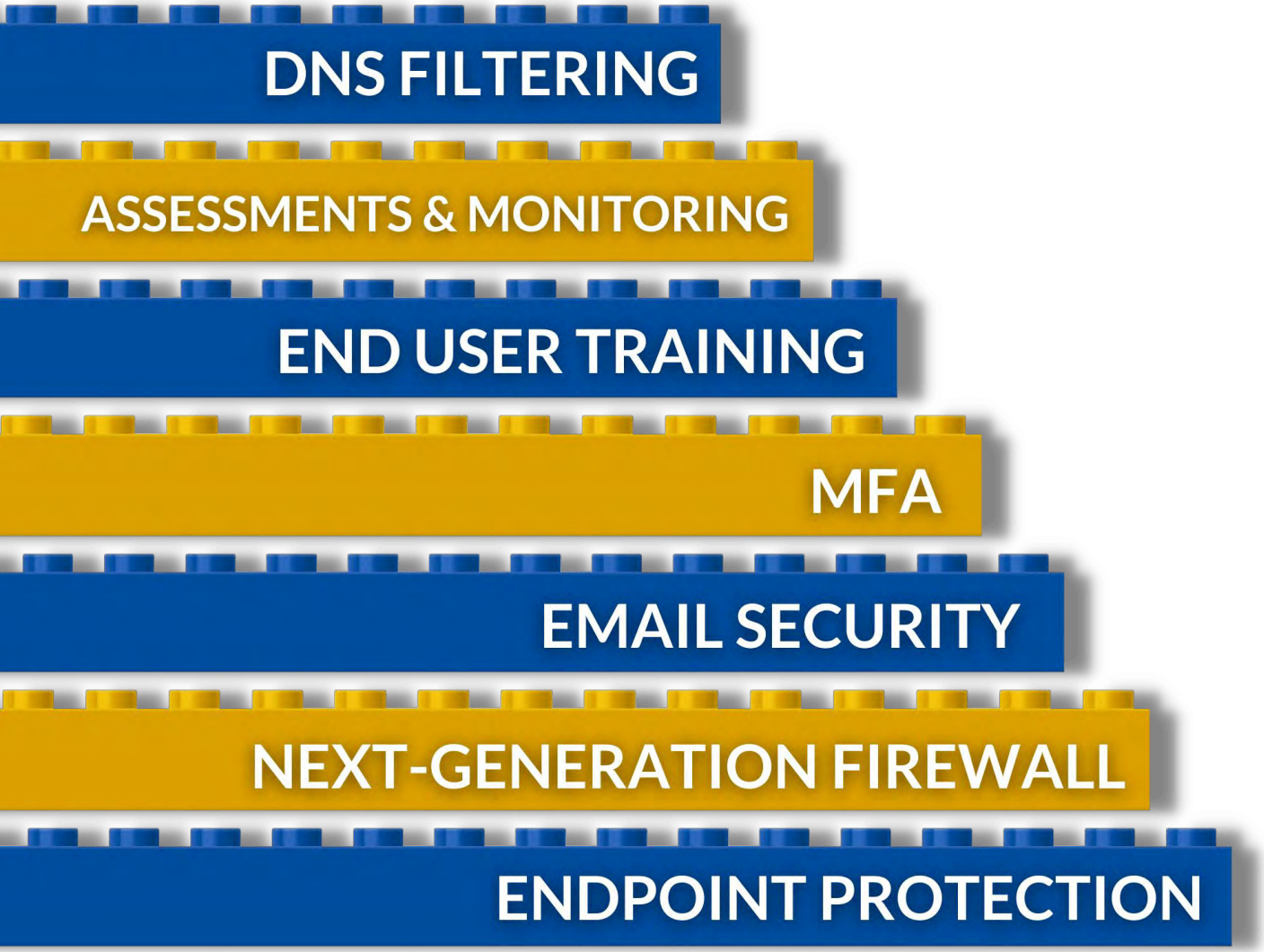
- Our online/cloud surface area keeps growing exponentially.
- 99% of breaches are preventable with MFA.
- Current AiTM (Adversary In the Middle) & Token Replay Attacks can sidestep MFA. These just keep getting more sophisticated!
- Threat actors now using AI for hyper-personalized attacks – at nearly every opportunity.
- Automated scripting and malicious OAuth app consent can grant hackers persistent footholds.

If you are not requiring MFA for all of your cloud accounts, you are likely uninsurable – and a disaster is waiting to happen!

https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/

GOOD ADVICE

Security In Layers



Multiple layers shown on the right overlap with Microsoft 365…

Want better security?

Start with strengthening your weakest layer!

BASELINE PROTECTION

Security Defaults Versus Conditional Access

Security Defaults (Free)	Conditional Access (P1/BP)
✓ All users must register MFA in 14 days	✓ Full control over every sign-in condition
✓ Admins always require MFA	✓ Block sign-ins by country, IP, device
✓ MFA triggered by location/device risk	✓ Require compliant or Hybrid-joined device
✓ Legacy authentication fully blocked	✓ Risk-based policies with P2 (AI-driven)
✓ Azure portal blocked for non-admins	✓ Phishing-resistant MFA enforcement
✗ Not configurable — all or nothing	✓ Token protection policies (NEW)
✗ Cannot exclude specific users or apps	✓ Require Terms of Use / app consent
✗ Cannot allow legacy auth exceptions	✓ Named locations, trusted networks
→ Best for: simple orgs, Azure AD Free	→ Best for: any org wanting real control

⚠ ***Without Security Defaults OR Conditional Access, you must enable MFA per-user manually.***

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

In my opinion, Conditional Access is no longer optional – ESPECIALLY if you have disabled Security Defaults.

BASELINE PROTECTION

Microsoft's Out-of-Box Protection Templates

Likely included in your current licensing— many orgs have them available and simply don't use them.

Security Defaults

Entra ID → Properties

Free (Entra ID Free)

01 The starter pack — forces MFA registration, blocks legacy auth, protects admin logins. All-or-nothing but zero cost. Right fit for simple orgs not yet on Conditional Access.

Use when: No Entra P1. No CA. You just want MFA enforced!

Preset Security Policies for Email

security.microsoft.com → Email & Collaboration → Policies & Rules → Threat Policies → Preset Security Policies

Defender for Office 365 P1 (Business Premium+)

02 Standard and Strict Protection bundles configure anti-phishing, anti-spam, Safe Links, and Safe Attachments in one click. Strict is ideal for exec and finance users; Standard covers everyone else.

Use when: BP or E3/E5. Apply Strict to high-risk users.

Defender for Endpoint / Business Security Baselines

security.microsoft.com → Configuration Management → Security Baselines (or Intune → Endpoint Security)

Defender for Business / MDE Plan 1+ (included in BP)

03 Intune-pushed hardening templates for Windows. Covers Attack surface reduction rules, firewall policy, credential guard, controlled folder access, and Defender settings — pre-tuned to Microsoft's recommended values.

Use when Defender/Intune-enrolled, Start with MDM Security Baseline.

Conditional Access Policy Templates

Entra ID → Security → Conditional Access → New Policy → Templates

Entra P1 (Business Premium+)

04 Many ready-made CA policy templates: require MFA for all users, block legacy auth, require compliant device, MFA for risky sign-ins, and more. Always deploy in report-only mode first to preview impact before enabling.

Use when: Moving off Security Defaults. Start report-only.

https://learn.microsoft.com/en-us/defender-office-365/preset-security-policies

https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-

https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policy-common?tabs=secure-foundation

IDENTITY CONTROLS

MFA: From SMS to Phishing-Resistant

Not All MFA is Equal

- **Email OTP** – Should only be used for basic guest access.

- **SMS/Voice OTP** – Vulnerable to SIM swap attacks!

- **Generic Authenticator TOTP** – Still phishable via AiTM!

- **Push Notification via MS Authenticator** – Enable Number Matching to prevent fatigue!

- **FIDO2 / Passkeys / Windows Hello** –Hardware bound and Microsoft-Recommended.

https://learn.microsoft.com/en-us/security/zero-trust/sfi/phishing-resistant-mfa

Are you still using Legacy Authentication Methods? Are you bypassing MFA requirements for any locations/IPs?

FEATURES & LICENSING

What Do You Actually Get?

M365 Business Basic

~$6/user/mo

- Entra ID Free (7-day logs)
- Security Defaults
- Per-User MFA
- Basic Exchange Online Protection (EOP)
- Basic anti-malware & anti-spam

No Conditional Access

No Defender for Business

M365 Business Premium

~$22/user/mo ★ Recommended SMB

- Entra P1 (30-day logs + CA)
- Conditional Access — full control
- Defender for Endpoint (EDR)
- Defender for Office 365 P1
- Intune device management
- Azure Information Protection P1
- Purview audit logs (90 days)

300-user limit

M365 E3 / E5 Enterprise

E3 ~$36 · E5 ~$57/user/mo

- Entra P2 (risk-based CA, PIM)
- Defender for Office 365 P2
- E5: Defender XDR full suite
- E5: Copilot for Security**
- Purview audit (1–10 yr logs)
- eDiscovery & Compliance Center
- Advanced Threat Analytics
- No user-count limit

https://m365maps.com/matrix.htm#0000010000010010000000

***Copilot for Security requires separate license on top of M365 E5.*

Most Common Mistake: Paying for Premium/Enterprise but Conditional Access and other features are not enabled!

BASELINE PROTECTION

Microsoft Secure Score: Your Ongoing Dashboard

Where Do You Find Your Scores?

security.microsoft.com → Secure Score
entra.microsoft.com → Identity Secure Score
compliance.microsoft.com → Compliance Manager Score

https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score

What Does It Measure?

Various controls across Identity, Devices, Apps, Data, and Infrastructure.
Each control has an assigned point value.

https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-identity-secure-score

High-Impact Quick Wins

Require MFA for all admins

Block legacy auth via CA policy

Enable SSPR for all users

Enable audit log retention

Deploy Preset Security Policies for email

https://learn.microsoft.com/en-us/purview/compliance-manager-scoring

How Do You Use it?

Mark items as 'risk accepted' or 'third-party mitigation' to keep your score meaningful.
Review monthly — Microsoft adds new controls regularly.

WHAT'S NEW?

Newly Added: Baseline Security Mode

- New in M365 Admin Center under Org Settings → Security & Privacy
- Centralizes approximately 20 Microsoft-Recommended Security Checks
- Allows you to automatically apply low-impact controls
- Can generate an "impact simulation report" using audit data
- Like with the Secure Score, you can track each control and whether you are aligning with Microsoft's recommendations.

https://learn.microsoft.com/en-us/microsoft-365/baseline-security-mode/baseline-security-mode-settings?view=o365-worldwide

Investigating Incidents

1. Sign-In Logs (Entra ID – Entra.Microsoft.com)
   - Check user locations, device(s), MFA Registration – both interactive and non-interactive
   - Export .CSV for easier review!

2. Purview Audit Log (Compliance.Microsoft.com)
   - Search for common malicious activities: MailboxLogin, Set-Mailbox, New-InboxRule, Add-MailboxPermission, FileDownloaded, ConsentToApplication, etc.
   - Again, export a .CSV!

3. Defender XDR Alerts (Security.Microsoft.com)
   - Check Incidents & Alerts
   - Look for new Inbox Rules, forwarding rules, App Registrations.

4. Utilize Artificial Intelligence!
   - Copilot for Security
   - Take your .CSV logs and analyze using Copilot, Claude, or ChatGPT!

https://learn.microsoft.com/en-us/defender-office-365/detect-and-remediate-illicit-consent-grants

https://learn.microsoft.com/en-us/defender-office-365/detect-and-remediate-outlook-rules-forms-attack

INCIDENT RESPONSE

Stopping a Breach: Lock It Down Fast

CONTAIN:

- Disable the breached user account (Block Sign In)
- Revoke Active Sessions
- Force a password reset (Two for Entra-Sync)
- Remove Admin roles from breached account

INVESTIGATE:

- Check Inbox Rules (Forwarding, Move to Folder, Delete)
- Check for new app registrations/consents granted
- Check for mailbox permission changes / delegation
- Review Sharepoint/OneDrive activity

1. Alert Fires Off
2. Block Sign-In
3. Revoke Sessions
4. Reset Credentials
5. Hunt for Persistence

RECOVER:

- Re-enable account with new password and re-register a resistant MFA method
- Audit and remove forwarding rules found
- If admin account was breached: audit all role assignments, new users, partner access, exchange connectors
- Document the timeline; notify stakeholders; educate your team

https://learn.microsoft.com/en-us/defender-office-365/responding-to-a-compromised-email-account

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

Proactive Response: Alert Yourself!

Set Alerts in the Compliance Admin Center – Policies → Alert Policies

“Creation of forwarding/redirect rule”

“Elevation of Exchange admin privilege”

“Suspicious email forwarding activity”

“Email Messages removed after delivery”

Use Powershell to hunt for rules or forwarding!

Want to place a bet? ☺

https://learn.microsoft.com/en-us/purview/compliance-manager-alert-policies

TAKE-HOME ACTION ITEMS

Homework

Open these tabs when you're back at your desk — check each one off.

Scores & Posture

- [ ] **Review your Microsoft Secure Score**
  security.microsoft.com → Secure Score — quick wins with high point value
- [ ] **Check your Entra Identity Secure Score**
  entra.microsoft.com → Identity Secure Score (separate from Defender score)
- [ ] **Check Out Baseline Security Mode**
  M365 Admin Center → Org Settings → Security & Privacy → run the report

Identity & Admin Hygiene

- [ ] **Audit every admin role holder / No Daily Drivers!**
  Entra → Roles & Admins — does every Global Admin truly need Global Admin?
- [ ] **Check for stale guest accounts**
  Entra → Users → filter Guest — are former vendors or contractors still here?
- [ ] **Review PIM activation requirements – If Entra P2!**
  Are eligible roles requiring just-in-time activation, or are they always-on?
- [ ] **Confirm no shared admin accounts**
  Every admin: named individual, unique password, own MFA method enrolled

Alerts, Notifications & Consent

- [ ] **Verify alert emails are being received**
  security.microsoft.com → Settings → Email notifications — test one now
- [ ] **Confirm admin consent request recipients**
  Entra → Enterprise Apps → Consent & Permissions → real inboxes only
- [ ] **Review configured alert policies**
  compliance.microsoft.com → Policies → Alert policies — critical ones enabled?
- [ ] **Audit OAuth app consent grants**
  Entra → Enterprise Apps → filter 'User consent' — anything unexpected?

Quick Wins to Enable Today

- [ ] **Enable SSPR for all users**
  Entra → Password reset — reduces helpdesk load, ties resets to MFA
- [ ] **Turn on Number Matching for push MFA**
  Entra → Authentication Methods → Microsoft Authenticator → configure
- [ ] **Check for inbox rules org-wide**
  PowerShell: Get-InboxRule — look for forwarding or auto-delete rules
- [ ] **Subscribe to M365 Service Health alerts**
  M365 Admin → Health → Service Health → set alert preferences

Homework, Part 2

Entra Connect Versions Being Sunset Later This Year:

- Versions older than 2.5.79.0 WILL STOP WORKING September 30th of this year; the current build is 2.6.3.
- What is SyncJacking?

Good news: Entra Backup and Recovery Now in Preview!

- Requires Entra ID P1/P2
- Backups taken automatically once enabled, once per day, retaining up to five days.
- Admins can view backups, create difference reports, recover all or select objects.
- Recovery history is logged, showing all in-progress and completed recovery operations.

https://docs.azure.cn/en-us/entra/identity/hybrid/connect/how-to-upgrade-previous-version

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/reference-connect-version-history

https://learn.microsoft.com/en-us/entra/backup/overview

Key Links:

security.microsoft.com

entra.microsoft.com

compliance.microsoft.com

aka.ms/securescore

aka.ms/CATemplates

aka.ms/mfasetup

Thanks! Q&A

Kyle Haas | kyle.haas@mirazon.com | (502) 240-0404