Endpoints and email: which settings stop the attacks that actually land?

This month, run EDR with tamper protection on every laptop, remove users' local admin rights and turn on Microsoft's three standard attack surface reduction rules; this quarter, take your mail domains to DMARC enforcement and confirm every bank detail change by phone. Judge the rest by whether it stops pasted commands, fake sign-in pages or fake payment requests.

Reviewed	Next review	Version
4 Nov 2026	**4 Dec 2026**	**1.0**

Written for

IT teams in small and mid-size organizations managing Windows and Mac laptops, phones and Microsoft 365 or Google Workspace mail, often without security staff

Latest version

sheets.einblick.dev/endpoints-email/

If you only do five things

1. **Run EDR on every device, and lock it.**
   Defender for Endpoint Plan 1 lacks EDR; Defender for Business (in Business Premium) and Plan 2 have it[1]. Turn on tamper protection, and on Macs move Defender's from audit mode to block[2].
2. **Take away local admin rights.**
   Entra join makes the joining user a local admin. Turn that off in the device registration policy or Autopilot profile, and fix joined devices with an Intune account protection policy[3]. Manage the built-in admin with Windows LAPS, which needs only Intune Plan 1[4].
3. **Turn on attack surface reduction rules.**
   Microsoft recommends block mode for its three standard protection rules without extensive testing, and audit mode first for the rest. The rules need Defender Antivirus in active mode[5].
4. **Take every mail domain to DMARC enforcement.**
   Set up SPF and DKIM for every sender, then step DMARC from `p=none` via `p=quarantine` to `p=reject`, Microsoft's goal for every domain[6]. RFC 9989 advises against `p=reject` where users post to mailing lists[21]. Today, publish `v=DMARC1; p=reject;` on domains that never send mail, including onmicrosoft.com if unused[6].
5. **Confirm payment changes on a known number.**
   Call a known number before changing bank details or a payroll account. Microsoft saw over 46 million attacks posing as business contacts in a year, most opening with bland small talk[7].

Roll out the device baseline in this order

1. **Find the devices nobody manages.**
   Compare the device lists in Intune, Entra ID and your EDR console. Treat any device missing from one of them as unprotected until it is enrolled.
2. **Replace or pay for what's out of support.**
   Windows 10 support ended on 14 October 2025. Commercial ESU costs $61 per device for the first year, doubles each year, lasts three years at most, and joining late means paying for the years you missed[8]. Office LTSC 2021 support ended on 13 October 2026[23]. Patch the rest within the patching sheet's deadlines.
3. **Audit the other ASR rules, then block.**
   Run them in audit mode for a few weeks, plus the WMI rule if you use Configuration Manager. Add per-rule exclusions only for named business apps, then switch to block[5].
4. **Add application control in audit mode.**
   In Intune's App Control for Business, trust Windows components and Store apps, apps with a good reputation and apps from the Intune managed installer. Apps installed before you enable the managed installer aren't tagged, so audit first[9].
5. **Encrypt, escrow the keys, then enforce.**
   Require BitLocker to store its recovery key in Entra ID before it encrypts[10], and FileVault to escrow its key. Then make encryption a compliance rule and require compliant devices, as the passkeys and MFA sheet describes.

Device settings that close the common paths

- **Block macro and script paths.** Office on Windows blocks macros in files from the internet by default, but the policy that enforces it works only in Microsoft 365 Apps for enterprise, not for business[12]. Add the ASR rules against macro Win32 API calls, obfuscated scripts and scripts launching downloads[5].
- **Limit what pasted commands can do.** ClickFix lures, which get users to paste a command into Run, Terminal or File Explorer, ran on over 1.1 million devices from February to early May 2026. Restrict PowerShell and JavaScript and enforce application control in user-writable folders[7].
- **Allow remote support tools for IT only.** Vishing callers get victims to grant access through one, then finish reconnaissance in two minutes or less[7]. Block the rest with application control.
- **Allowlist browser extensions.** Set Edge's ExtensionInstallBlocklist to * and list approved ones in ExtensionInstallAllowlist[13]. At the average company, over 15% of users had unauthorized AI extensions[11].
- **Give Macs the same baseline.** Atomic macOS Stealer topped the infostealer families Defender Experts saw[7]. macOS has no ASR rules[5], so rely on EDR, FileVault and standard accounts.

Email settings against spoofing and fraud

- **Turn on the preset policies.** Assign Microsoft's Standard preset security policy to everyone and Strict to admins, finance and executives; until you turn them on, they apply to no one[15]. In Google Workspace, turn on every option under Gmail **Safety**[16].
- **Remove the Safe Links click-through.** Microsoft advises time-of-click URL checks without a user override; 89% to 96% of malicious attachments each month led to phishing pages, not malware[7].
- **Mark external mail.** `Set-ExternalInOutlook -Enabled $true` adds an External tag in supported versions of Outlook on every platform[17].
- **Block automatic external forwarding.** Set the outbound spam policy to **Off - Forwarding is disabled**; the default, Automatic, varies by tenant. Off also disables inbox rules that forward outside, which attackers add to compromised accounts[18].
- **Reject Direct Send.** Run `Set-OrganizationConfig -RejectDirectSend $true` once every scanner or app that uses Direct Send has an inbound connector[19].

- **Protect work data on personal phones.** Intune app protection Level 2 blocks copy and paste to unmanaged apps, outdated OS versions and jailbroken devices. Require it in Conditional Access[14].

- **Require TLS with MTA-STS.** Publish the policy in testing mode, then enforce. Exchange Online already checks other domains' policies on outbound mail[20].

What changed in 2026

- **DMARC became a standards-track RFC.** RFC 9989 replaced RFC 7489 and RFC 9091 in May 2026. It swaps the `pct` tag, which Microsoft's guide still uses[6], for `t` (testing), and requires DKIM signing on domains that publish `p=reject`[21].

- **Windows 11 24H2 Home and Pro lost support.** They no longer get updates, and Enterprise 23H2 stops on 10 November 2026[22].
- **Administrator protection shipped.** The October 2026 update turns it on where Microsoft's Windows security baselines apply. Microsoft says not to use it on LAPS-managed devices[24], so set the policy explicitly on those.

What you can skip

- **More email phishing simulations.** Email phishing opened only 6% of Mandiant's 2025 intrusions, voice phishing 11%[25]. Spend the time on call-back rules for finance and the help desk.
- **A second antivirus beside Defender.** ASR rules don't run while Defender Antivirus is in passive mode[5].
- **DMARC forensic reports.** Microsoft 365 doesn't send them; start with aggregate reports only[6].

Mistakes that cost the most

- **Exclusions without an owner.** Excluded files run, and no ASR events are recorded for them[5]. Give each exclusion an owner and a review date.
- **Trusting a whole share or site for macros.** Anyone who can add files there can add macros[12]. Sign the macros you need instead.
- **Deleting a device before saving its keys.** Deleting it in Entra ID loses its LAPS password[4]; deleting its Intune object suspends BitLocker[10].
- **Changing bank details because an email thread says so.** Attackers reuse old threads to get bank accounts changed before a wire transfer[11].

What this looks like at your size

Small team, no security staff

- Use Business Premium's Defender for Business[1] and the Standard email preset.
- Make every user a standard user.
- Use a DMARC reporting service and a call-back rule for every payment change.

Growing, with IT or security staff

- Audit the other ASR rules for a month, then block.
- Pilot App Control for Business with the Intune managed installer.
- Use Strict presets for finance and admins; enforce MTA-STS and reject Direct Send.

Enterprise or regulated

- Enforce App Control on all workstations.
- Handle elevation requests with Endpoint Privilege Management, not admin accounts.
- Report weekly coverage: EDR with tamper protection, ASR in block mode, encryption, supported OS.

Version history

4 Nov 2026, version 1.0	Published after a copy edit and a source-by-source fact check, which aligned the DMARC advice with RFC 9989 and narrowed 9 statements to what the sources say.

Sources

1. What is Microsoft Defender for Business?. Microsoft Learn, 27 Aug 2025. learn.microsoft.com
2. Tamper protection overview. Microsoft Learn, 9 Sep 2026. learn.microsoft.com
3. Manage local administrators on Entra joined devices. Microsoft Learn, 17 Jun 2026. learn.microsoft.com
4. Windows LAPS with Microsoft Intune. Microsoft Learn, 29 May 2025. learn.microsoft.com
5. ASR rules overview. Microsoft Learn, 4 Aug 2026. learn.microsoft.com
6. Set up DMARC in Microsoft 365. Microsoft Learn, 3 Jul 2026. learn.microsoft.com
7. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
8. Windows 10 ESU program. Microsoft Learn, 17 Nov 2025. learn.microsoft.com
9. App Control for Business and managed installers. Microsoft Learn, 17 Sep 2025. learn.microsoft.com
10. Encrypt Windows devices with BitLocker. Microsoft Learn, 26 Nov 2025. learn.microsoft.com
11. 2026 Data Breach Investigations Report. Verizon, 19 May 2026. verizon.com
12. Macros from the internet blocked by default. Microsoft Learn, 17 Jul 2026. learn.microsoft.com
13. Manage Edge extensions with policies. Microsoft Learn, 12 Jan 2024. learn.microsoft.com
14. App protection data protection framework. Microsoft Learn, 12 Jun 2025. learn.microsoft.com
15. Preset security policies. Microsoft Learn, 3 Jul 2026. learn.microsoft.com
16. Advanced phishing and malware protection. Google Workspace Help, updated 26 Oct 2026. knowledge.workspace.google.com
17. Set-ExternalInOutlook. Microsoft Learn, updated 27 Feb 2026. learn.microsoft.com
18. Control external email forwarding. Microsoft Learn, 18 Aug 2026. learn.microsoft.com
19. Set-OrganizationConfig. Microsoft Learn, updated 29 Oct 2026. learn.microsoft.com
20. Enhance mail flow with MTA-STS. Microsoft Learn, 21 Jul 2026. learn.microsoft.com
21. RFC 9989: DMARC. IETF, May 2026. rfc-editor.org
22. Windows 11 release information. Microsoft Learn, 28 Oct 2026. learn.microsoft.com
23. End of support resources for Office. Microsoft Learn, 20 Oct 2026. learn.microsoft.com
24. Administrator protection. Microsoft Learn, 13 Oct 2026. learn.microsoft.com
25. M-Trends 2026. Google Cloud (Mandiant), 23 Mar 2026. cloud.google.com