ANONYMISED SAMPLE REPORT: Full 28-point output from our automated Microsoft 365 Security Hardening Audit tool, shown for the fictional practice **Severn Gate Legal LLP (severngatelegal.co.uk)**.

alphasec.uk · alphabyte.it · alphaops.biz

AUTOMATED MICROSOFT GRAPH & PUBLIC DNS SECURITY HARDENING AUDIT

Severn Gate Legal LLP

28-Control Traffic-Light Assessment · Cyber Essentials & Copilot Readiness

AlphaSec · Alphabyte Group
Connies House, Cardiff CF23 9AF
029 2240 4615 · ross@alphabyte.it
Audit Date: 30 October 2026

Automated read-only Microsoft Graph and DNS inspection across **28 security controls** identified **8 Red (Action Required)** findings, **14 Amber (Worth Hardening)** findings, and **6 Green (All Good)** controls — including **4 Cyber Essentials v3.3 blockers**.

Domain: severngatelegal.co.uk

Mailboxes: 26 licensed

Licences: 22 × M365 Business Standard · 4 × M365 Business Premium

Sector: Solicitors & Conveyancing Practice

46/100
OVERALL TENANT HARDENING SCORE

8	14	6
RED · FIX	AMBER · HARDEN	GREEN · GOOD

Priority Remediation Plan — 8 Urgent Red Fixes

Every Red control below can be locked down without disrupting legitimate day-to-day staff work (estimated remediation time: half a day).

1. **ID-04 · Conditional Access Baseline vs Security Defaults (M365 Business Premium / Entra ID P1)**
   Deploy Alphabyte's 6-Policy Conditional Access Baseline (Require MFA for All Users, Require Phishing-Resistant MFA for Admins, Block Legacy Auth, Block High-Risk Countries, Require Compliant Device for Finance/Partner data).

2. **ID-05 · Geolocation Sign-In Restrictions (UK + Approved Travel Group) (M365 Business Premium / Entra ID P1)**
   Create an Entra Named Location for 'United Kingdom & Ireland' and block sign-ins from all other countries unless a user is temporarily added to the `M365-Travel-Approved` security group.

3. **ID-07 · Dormant, Former-Staff & Unlicensed Sign-In Enabled Accounts (Included (All M365 Plans))**
   Convert the 2 former locum mailboxes to Shared Mailboxes, set `AccountEnabled = false` on all 4 dormant accounts, and remove £49/month in wasted licences.

4. **ADM-01 · Global Administrator Count (Target: 2 to 4 Maximum) (Included (All M365 Plans))**
   Reduce Global Administrators to 2 dedicated admin accounts + 2 emergency break-glass accounts. Remove Global Admin from the external web developer immediately.

5. **ADM-02 · Separate Non-Mailboxed Admin Accounts (No Daily Email/Web Use) (Included (Unlicensed Cloud Accounts))**
   Create separate unlicensed `admin-name@` accounts with no mailbox for administrative tasks, and strip all admin roles from daily email accounts.

6. **EXO-01 · External Email Auto-Forwarding Blocked Tenant-Wide (Included (Exchange Online))**
   Set `AutoForwardEnabled = Off` in Defender Outbound Spam Policy and set `AutoForwardEnabled = $false` on the default Exchange Remote Domain (`*`).

7. **EXO-05 · DMARC Policy Enforced (`p=quarantine` or `p=reject`) (Public DNS)**
   Once DKIM is enabled, update `_dmarc.severngatelegal.co.uk` to `v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@severngatelegal.co.uk;` for 14 days, then advance to `p=reject`.

8. **SPO-01 · Third-Party OAuth App Consent Restricted to Admin Approval (Included (Entra ID))**
   Switch Entra Enterprise Applications → User Consent Settings to 'Do not allow user consent' and enable the Admin Consent Request workflow so staff can request approval with 1 click.

Identity & Sign-In

3 Red · 3 Amber · 1 Green

ID-01 Multi-Factor Authentication (MFA) Enforced for All Users

Included (All M365 Plans) · Cyber Essentials Scope

● AMBER · WORTH HARDENING

Observed in tenant: 23 of 26 active user accounts have MFA registered and enforced, but 3 accounts (2 fee-earners and 1 accounts assistant) still have MFA enforcement in 'Disabled / Per-User Legacy' state.

WHY IT MATTERS / RISK

Any single mailbox without MFA can be compromised via password spraying or credential stuffing in minutes — and is an automatic fail under Cyber Essentials v3.3.

RECOMMENDED ACTION

Migrate from legacy per-user MFA to Entra ID Conditional Access (or Security Defaults), require registration within 24 hours for the remaining 3 users, and revoke active refresh tokens.

ID-02 Legacy Authentication Protocols Blocked (IMAP / POP / SMTP Basic Auth)

GREEN · ALL GOOD

Included (All M365 Plans) | Cyber Essentials Scope

Observed in tenant: Basic authentication and legacy protocols (IMAP4, POP3, Exchange ActiveSync basic) are disabled across the tenant except for 1 scanner account using Authenticated SMTP.

WHY IT MATTERS / RISK

Legacy authentication protocols cannot enforce MFA and are the #1 route attackers use to bypass MFA prompts.

RECOMMENDED ACTION

Keep legacy auth blocked tenant-wide; migrate the single multifunction copier from SMTP Basic Auth to Microsoft Graph High Volume Email or an isolated SendGrid relay.

ID-03 Phishing-Resistant Authentication Strength & Number Matching

AMBER · WORTH HARDENING

Included / Business Premium for CA Strength

Observed in tenant: Microsoft Authenticator Number Matching is active, but SMS and Voice Call fallback are still enabled as valid MFA methods for 19 users, and no Passkeys (FIDO2) are registered for Partners.

WHY IT MATTERS / RISK

SMS codes are vulnerable to SIM-swap and real-time Adversary-in-the-Middle (EvilProxy) phishing links.

RECOMMENDED ACTION

Enforce Microsoft Authenticator Push with Number Matching + Geo-Location display for all staff, register FIDO2 Passkeys for Partners/Admins, and disable SMS MFA once Authenticator enrolment is 100%.

ID-04 Conditional Access Baseline vs Security Defaults

RED · ACTION REQUIRED

M365 Business Premium / Entra ID P1 | Cyber Essentials Scope

Observed in tenant: Security Defaults was turned off historically to accommodate a third-party app, and only 1 partial Conditional Access policy exists (covering Global Admins only). 4 Business Premium licences are present in severngatelegal.co.uk, but tenant-wide Conditional Access policies are not configured.

WHY IT MATTERS / RISK

Because Security Defaults is off and no baseline Conditional Access policy covers all users, new accounts created in the tenant have zero automatic MFA or risk enforcement.

RECOMMENDED ACTION

Deploy Alphabyte's 6-Policy Conditional Access Baseline (Require MFA for All Users, Require Phishing-Resistant MFA for Admins, Block Legacy Auth, Block High-Risk Countries, Require Compliant Device for Finance/Partner data).

ID-05 Geolocation Sign-In Restrictions (UK + Approved Travel Group)

RED · ACTION REQUIRED

M365 Business Premium / Entra ID P1

Observed in tenant: Sign-ins are currently permitted from all 240+ countries worldwide. Sign-in logs show 142 failed login attempts against partner UPNs from Russia, Vietnam, and Brazil over the past 14 days.

WHY IT MATTERS / RISK

Without a Named Location country block, automated botnets can continuously probe user passwords and trigger MFA fatigue prompts from overseas.

RECOMMENDED ACTION

Create an Entra Named Location for 'United Kingdom & Ireland' and block sign-ins from all other countries unless a user is temporarily added to the `M365-Travel-Approved` security group.

ID-06 Password Expiration Disabled & NCSC Banned Password List

Included (All M365 Plans) | Cyber Essentials Scope

● AMBER · WORTH HARDENING

Observed in tenant: The tenant still forces a 90-day periodic password rotation policy (`PasswordValidityPeriodInDays = 90`).

WHY IT MATTERS / RISK

NCSC and Cyber Essentials v3.3 explicitly advise against periodic forced password expiry because it drives staff to choose predictable incremental passwords (`Autumn2026!`).

RECOMMENDED ACTION

Set passwords to never expire (`Set-MgDomain -PasswordValidityPeriodInDays 2147483647`) while enforcing MFA + Entra Smart Lockout (10 attempts / 60s lockout) and custom banned password words (`Severn`, `Cardiff`, `Legal`).

ID-07 Dormant, Former-Staff & Unlicensed Sign-In Enabled Accounts

Included (All M365 Plans) | Cyber Essentials Scope

● RED · ACTION REQUIRED

Observed in tenant: 4 user accounts with active sign-in enabled (`AccountEnabled = true`) have not logged in for over 90 days (including 2 former locum/contractor accounts and 1 unused `temp.reception@` account).

WHY IT MATTERS / RISK

Unmonitored ex-staff or contractor accounts are a prime target for quiet takeover and data exfiltration.

RECOMMENDED ACTION

Convert the 2 former locum mailboxes to Shared Mailboxes, set `AccountEnabled = false` on all 4 dormant accounts, and remove £49/month in wasted licences.

Privileged & Admin Access

2 Red | 2 Amber

ADM-01 Global Administrator Count (Target: 2 to 4 Maximum)

Included (All M365 Plans) | Cyber Essentials Scope

● RED · ACTION REQUIRED

Observed in tenant: 6 accounts currently hold permanent Global Administrator rights on severngatelegal.co.uk — including 3 daily partner mailboxes, 1 practice manager mailbox, 1 external web developer account, and 1 IT account.

WHY IT MATTERS / RISK

If any one of those 6 accounts is phished, the attacker has total control to delete all OneDrive/SharePoint data, disable MFA, and lock the firm out.

RECOMMENDED ACTION

Reduce Global Administrators to 2 dedicated admin accounts + 2 emergency break-glass accounts. Remove Global Admin from the external web developer immediately.

ADM-02 Separate Non-Mailboxed Admin Accounts (No Daily Email/Web Use)

Included (Unlicensed Cloud Accounts) | Cyber Essentials Scope

● RED · ACTION REQUIRED

Observed in tenant: Partners and the Practice Manager use their day-to-day email accounts (`j.davies@`, `s.morgan@`, `h.evans@`) with Global Admin privileges attached.

WHY IT MATTERS / RISK

Using an account that receives external emails and browses the web while holding Global Admin rights is an automatic fail under Cyber Essentials v3.3.

RECOMMENDED ACTION

Create separate unlicensed `admin-name@` accounts with no mailbox for administrative tasks, and strip all admin roles from daily email accounts.

ADM-03 Two Cloud-Only Emergency 'Break-Glass' Accounts Configured

Included (All M365 Plans)

● AMBER · WORTH HARDENING

Observed in tenant: No dedicated `.onmicrosoft.com` emergency break-glass accounts exist; all admins authenticate on the primary custom domain.

WHY IT MATTERS / RISK

If a Conditional Access policy misconfiguration or DNS/federation outage occurs, administrators can lock themselves out of the tenant completely.

RECOMMENDED ACTION

Create two cloud-only `bg-admin-01@` and `bg-admin-02@*.onmicrosoft.com` accounts secured with 24+ character random passwords stored in dual-custody physical/1Password vaults and FIDO2 hardware keys, excluded from Conditional Access.

ADM-04 Admin Session Lifetime & Re-Authentication Frequency

M365 Business Premium / Entra ID P1

● AMBER · WORTH HARDENING

Observed in tenant: Admin centre browser sessions currently use the default 90-day rolling refresh token with persistent browser cookies.

WHY IT MATTERS / RISK

An unattended laptop or stolen session cookie keeps full Entra/Exchange Admin Center privileges alive for months.

RECOMMENDED ACTION

Configure a Conditional Access Session Control policy requiring Sign-In Frequency of 8 hours and `Persistent Browser Session = Never` for all directory admin roles.

Email & Anti-Phishing

2 Red · 4 Amber · 2 Green

EXO-01 External Email Auto-Forwarding Blocked Tenant-Wide

Included (Exchange Online)

● RED · ACTION REQUIRED

Observed in tenant: The default Outbound Spam Filter policy currently has `AutoForwardEnabled = On`, allowing any user or attacker-created inbox rule to silently forward all incoming client emails to an external Gmail/Outlook address.

WHY IT MATTERS / RISK

In Business Email Compromise (BEC) attacks, criminals set up a hidden auto-forward rule so they can monitor conveyancing/invoice threads for weeks even after a password reset.

RECOMMENDED ACTION

Set `AutoForwardEnabled = Off` in Defender Outbound Spam Policy and set `AutoForwardEnabled = $false` on the default Exchange Remote Domain (`*`).

EXO-02 Hidden Mailbox Forwarding & Suspicious Inbox Rules Audit

Included (Exchange Online)

● AMBER · WORTH HARDENING

Observed in tenant: 2 mailboxes have active client-side inbox rules: 1 forwards copies of invoices to a personal `@btinternet.com` address, and 1 moves messages containing 'remittance' to an archive folder.

WHY IT MATTERS / RISK

Forwarding firm financial emails to personal consumer mailboxes leaks client data outside M365 governance and mimics BEC persistence rules.

RECOMMENDED ACTION

Review and remove the `@btinternet.com` forwarding rule with the staff member, and enable Defender alerting on creation of new inbox forwarding/redirect rules.

EXO-03 SPF Record Hardened (Single Record, `-all` or `~all`, <10 Lookups)

Public DNS

● GREEN · ALL GOOD

Observed in tenant: Valid single SPF record published (`v=spf1 include:spf.protection.outlook.com -all`) using 2 of 10 allowed DNS lookups.

WHY IT MATTERS / RISK

Missing or overly permissive SPF records allow external servers to spoof emails from your domain.

RECOMMENDED ACTION

No change required — SPF is properly hardened with `-all`.

EXO-04 DKIM Cryptographic Signing Enabled on Custom Domain

Included (Exchange Online + DNS)

● AMBER · WORTH HARDENING

Observed in tenant: Microsoft 365 is signing outbound mail with the default `.onmicrosoft.com` key because `selector1._domainkey.severngatelegal.co.uk` and `selector2._domainkey.severngatelegal.co.uk` CNAME records have not been enabled.

WHY IT MATTERS / RISK

Without custom-domain DKIM signing, DMARC alignment fails when emails are forwarded and major receivers (Gmail, Yahoo, enterprise gateways) downgrade deliverability.

RECOMMENDED ACTION

Publish the `selector1` and `selector2` CNAME records in DNS and enable 2048-bit DKIM signing in the Defender Portal for `severngatelegal.co.uk`.

EXO-05 DMARC Policy Enforced (`p=quarantine` or `p=reject`)

Public DNS

● RED · ACTION REQUIRED

Observed in tenant: `_dmarc.severngatelegal.co.uk` is currently set to `v=DMARC1; p=none;` with no `rua=` aggregate reporting mailbox configured.

WHY IT MATTERS / RISK

`p=none` is monitoring-only: anyone on the internet can send a fake payment-redirection or invoice email pretending to be `@severngatelegal.co.uk` and receiving mail servers are instructed not to block it.

RECOMMENDED ACTION

Once DKIM is enabled, update `_dmarc.severngatelegal.co.uk` to `v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@severngatelegal.co.uk;` for 14 days, then advance to `p=reject`.

EXO-06 External Sender Warning Banner (`Set-ExternalInOutlook`)

Included (Exchange Online)

● GREEN · ALL GOOD

Observed in tenant: Native Outlook `External` sender tag and top-of-message warning banner are enabled across Outlook Desktop, Web, and Mobile.

WHY IT MATTERS / RISK

Without external tagging, staff cannot easily spot display-name spoofing where an attacker sets their display name to a Managing Partner's name.

RECOMMENDED ACTION

Keep `Set-ExternalInOutlook -Enabled $true` active and add the firm's trusted sister domains to the allow list if needed.

EXO-07 Shared Mailboxes Blocked from DirectInteractive Sign-In

Included (Exchange Online) Cyber Essentials Scope

● AMBER · WORTH HARDENING

Observed in tenant: 5 of 7 shared mailboxes (`accounts@`, `enquiries@`, `conveyancing@`, `reception@`, `archiveteam@`) still have `AccountEnabled = true` in Entra ID with unknown legacy passwords.

WHY IT MATTERS / RISK

Shared mailboxes should only be accessed via delegated permissions from a named user's MFA-protected account. Leaving direct sign-in enabled creates backdoor accounts.

RECOMMENDED ACTION

Set `AccountEnabled = $false` on all 7 shared mailboxes in Entra ID (this does not affect delegated mailbox access or email delivery).

EXO-08

Defender for Office 365 Safe Links, Safe Attachments & Executive Impersonation

● AMBER · WORTH HARDENING

M365 Business Premium / Defender for Office 365 P1

Observed in tenant: Standard Exchange Online Protection (EOP) anti-malware is active, but Defender Safe Links real-time URL detonation and Partner/Accounts User Impersonation protection are not enabled for the 22 Business Standard users.

WHY IT MATTERS / RISK

Modern phishing emails use delayed weaponized links (clean at delivery, malicious 20 minutes later when clicked) and display-name impersonation of Senior Partners asking Accounts to pay an urgent supplier.

RECOMMENDED ACTION

Enable the Defender 'Standard/Strict Preset Security Policy' with User Impersonation protection for all Partners + Accounts staff (either via Business Premium upgrade or a £1.60/user Defender for Office 365 Plan 1 add-on).

SharePoint, OneDrive & OAuth

1 Red · 2 Amber · 1 Green

SPO-01 **Third-Party OAuth App Consent Restricted to Admin Approval**

● RED · ACTION REQUIRED

Included (Entra ID)

Observed in tenant: Users can currently grant consent to any third-party OAuth application requesting access to their mailbox and OneDrive files (`ManagePermissionGrantsForOwnedResource` is open to all users). 11 unverified 3rd-party apps (including browser PDF converters and an AI meeting notetaker) hold active Graph tokens.

WHY IT MATTERS / RISK

Consent phishing ('Illicit Consent Grant') tricks a user into clicking 'Accept' on a fake Microsoft 365 app prompt, giving attackers persistent API access to read emails and files without needing the user's password or MFA.

RECOMMENDED ACTION

Switch Entra Enterprise Applications → User Consent Settings to 'Do not allow user consent' and enable the Admin Consent Request workflow so staff can request approval with 1 click.

SPO-02 **SharePoint & OneDrive Anonymous 'Anyone with the Link' Sharing**

● AMBER · WORTH HARDENING

Included (SharePoint Online)

Observed in tenant: SharePoint Tenant Sharing Capability is currently set to `ExternalUserAndGuestSharing` (Anyone links allowed) with no mandatory link expiration date.

WHY IT MATTERS / RISK

An 'Anyone with the link' URL created 2 years ago remains open forever and can be forwarded to unintended recipients without authentication.

RECOMMENDED ACTION

Change default sharing link type from 'Anyone' to 'Specific People (Authenticated OTP)', or enforce a mandatory 14-day expiry and view-only default on all external links.

SPO-03

Internal SharePoint Permissions & Microsoft 365 Copilot Oversharing Check

● AMBER · WORTH HARDENING

Included (SharePoint Online)

Observed in tenant: 3 SharePoint sites (`Management & HR`, `Partner Drawings & Accounts`, and `Client Archive`) include the `Everyone except external users` group in their Member/Visitor permissions.

WHY IT MATTERS / RISK

Any junior member of staff — or Microsoft 365 Copilot if enabled — can search and surface confidential HR, payroll, and partner financial documents.

RECOMMENDED ACTION

Remove `Everyone except external users` from the 3 restricted SharePoint sites and lock access down to role-based security groups (`SG-Partners`, `SG-HR-Finance`).

SPO-04 **External Guest Account Hygiene & Stale Guest Access Review**

Included (Entra ID)

● GREEN · ALL GOOD

Observed in tenant: Only 6 external `#EXT#` guest users exist in Entra ID, all associated with current counsel and auditing firms.

WHY IT MATTERS / RISK

Unreviewed guest accounts accumulate over time and retain access to shared Teams channels and folders.

RECOMMENDED ACTION

Keep guest invitations restricted to Member/Admin roles and review the 6 external guests every 6 months.

Audit, Backup & Governance

1 Amber · 2 Green

GOV-01 **Unified Audit Log (`AdminAuditLogEnabled`) & Mailbox Auditing Active**

Included (All M365 Plans — 180-Day Retention)

● GREEN · ALL GOOD

Observed in tenant: Microsoft Purview Unified Audit Logging (`AdminAuditLogEnabled = True`) and per-mailbox audit logging (`AuditEnabled = True`) are active across all 26 mailboxes.

WHY IT MATTERS / RISK

Without Unified Audit Logging enabled prior to an incident, forensic investigators cannot see which emails or files were accessed during a breach (and ICO reporting becomes far harder).

RECOMMENDED ACTION

No change required — 180-day Unified Audit Log is active and recording.

GOV-02

Independent Cloud-to-Cloud Backup for Exchange, OneDrive & SharePoint

Add-On (Dropsuite / Cove / Acronis M365 Backup)

● AMBER · WORTH HARDENING

Observed in tenant: The tenant relies solely on Microsoft's native 30–93 day recycle bin with no independent off-tenant M365 backup configured.

WHY IT MATTERS / RISK

Microsoft's Shared Responsibility Model covers infrastructure uptime, not accidental mass deletion, malicious insider purging, or ransomware encryption synced via OneDrive.

RECOMMENDED ACTION

Enable immutable daily cloud-to-cloud backup for all 26 Exchange mailboxes, OneDrive accounts, and SharePoint sites (~£3/user/month).

GOV-03 **UK Data Residency & GDPR Tenant Location Verification**

Included (All M365 Plans)

● GREEN · ALL GOOD

Observed in tenant: Tenant Country/Region is set to `GB (United Kingdom)` with Exchange Online, SharePoint Online, and Teams data stored at rest in UK data centres (London & Cardiff/Newport).

WHY IT MATTERS / RISK

Misconfigured tenant regions can store UK client personal data outside the UK/EEA in breach of client engagement terms.

RECOMMENDED ACTION

Record the UK data-at-rest verification screenshot in the firm's GDPR / Law Society compliance folder.

Devices & Endpoint Compliance

2 Amber

DEV-01 Intune MDM Enrolment & BitLocker Encryption Key Escrow

M365 Business Premium / Intune P1 | Cyber Essentials Scope

AMBER · WORTH HARDENING

Observed in tenant: 26 Windows 11 laptops are Entra-registered/joined, but only 4 are enrolled in Microsoft Intune with BitLocker recovery keys escrowed in Entra ID. The remaining 22 laptops are managed manually.

WHY IT MATTERS / RISK

If a laptop is lost or stolen on a train and you cannot prove via central escrow that BitLocker encryption was active at the time of loss, the ICO treats it as a reportable data breach.

RECOMMENDED ACTION

Escrow all 26 BitLocker recovery keys into Entra ID immediately (supported even on Entra-joined devices) and consider full Intune compliance policies for remote wipe.

DEV-02 Personal Mobile & Unmanaged Home PC Access Controls (MAM / App Protection)

M365 Business Premium / Intune P1 | Cyber Essentials Scope

AMBER · WORTH HARDENING

Observed in tenant: Staff can currently sign into Outlook Web and download full PST/client bundles onto unmanaged personal home PCs, and access work email via Apple Mail/Samsung Mail without an App Protection PIN.

WHY IT MATTERS / RISK

Client files downloaded onto an unmanaged home computer infected with info-stealer malware bypass all office firewall controls.

RECOMMENDED ACTION

Block full file downloads on unmanaged browser sessions (allow web-only preview) and enforce Outlook Mobile App Protection policies on iOS/Android phones.

Want this 28-point Traffic-Light Audit run on your own Microsoft 365 tenant — free of charge?

We run this read-only check on a 10-minute screen-share (or delegated Global Reader session) and send you the full Red/Amber/Green action sheet with zero obligation.

Ross Owen · Alphabyte Group
029 2240 4615 · 07885 972 512
ross@alphabyte.it · alphasec.uk/m365-security-audit/