2B1 INC.

Beyond Antivirus: A Practical Cybersecurity White Paper for Law Firms

A clear, business-first reference that explains modern safeguards in plain language. Built for managing partners, COOs, legal operations, and IT leads.

Published: **August 2025** •

Summary. Client confidentiality now includes how you protect systems and data. This paper lays out the essential safeguards that reduce real risks like ransomware, email compromise, data leakage, and vendor exposure. Each topic begins with a definition, then explains the problem and how the control reduces it, followed by practical steps and simple measures.

Table of Contents

1 Endpoint protection and anti-malware (EPP/EDR)

2 Ransomware protection

3 Cryptomining protection

4 Email security (inbound and outbound)

5 Backup and disaster recovery (DR)

6 Data Loss Prevention (DLP)

7 Patch and vulnerability management

8 User awareness and training

9 Password policy and Multi-Factor Authentication (MFA)

10 Data encryption (devices and servers)

11 Vendor and service-provider management

12 Physical security of hardware

13 Incident response plan (IRP)

14 Logging, monitoring, and managed detection (SIEM/MDR)

15 Zero Trust access model

16 Privileged Access Management (PAM)

17 Mobile Device Management (MDM) and BYOD

18 Network segmentation

19 Secure file transfer and client

collaboration

20 Attack Surface Management (ASM) and continuous scanning

21 Penetration testing and tabletop exercises

22 Data classification and retention

23 Cyber insurance readiness

24 Framework alignment for client questionnaires

1) Endpoint protection and anti-malware (EPP/EDR)

Definition

Endpoints are user devices such as laptops and desktops. An **EPP** (Endpoint Protection Platform) blocks known malware. **EDR** (Endpoint Detection and Response) adds 24x7 monitoring, detects suspicious behavior, and can isolate an infected device.

The problem in a law firm

Phishing attachments and malicious links often land first on a lawyer's machine. That foothold can be used to move laterally and reach document management or billing systems.

What it does

- Real-time scanning and behavioral analysis to stop known threats.
- Automated isolation of compromised devices to prevent spread.
- Device controls such as script, macro, and USB restrictions.

Implementation essentials

- Deploy centrally managed EDR to 100 percent of firm devices.
- Integrate alerts with a 24x7 monitoring service or SOC.
- Block admin rights for daily use and require approvals for elevation.

Measures

- Time to detect and isolate an endpoint.
- Percent of endpoints with EDR active and updated.
- Blocked incidents per month and repeat offender trend.

> **Example.** A partner opens a malicious invoice PDF. EDR sees the PDF launching PowerShell, auto-isolates the laptop, and emails IT with a one-click restore workflow.

---

2) Ransomware protection

Definition

Ransomware encrypts files and often steals data, then demands payment for a key or for silence.

The problem in a law firm

Ransomware can stop filings, delay closings, and force breach notification. It also risks attorney-client privilege.

What it does

- Combines hardened endpoints, email filtering, network segmentation, and MFA.
- Uses offline or immutable backups and a rehearsed response playbook.

Implementation essentials

- Disable or restrict macros, remove local admin, enforce MFA everywhere.

- Segment servers and restrict lateral movement.
- Tabletop exercises that practice a ransomware runbook.

Measures

- Restore time in a mock drill.
- Backup restore success rate and last validation date.
- Number of privileged accounts reviewed and reduced.

---

3) Cryptomining protection

Definition

Cryptomining attacks (also called cryptojacking) hijack your systems to mine cryptocurrency without permission.

The problem in a law firm

Even if no data leaves the firm, mining degrades performance, increases cloud bills, and may indicate a deeper breach.

What it does

- EDR flags mining processes and unusual CPU spikes.
- DNS and web filters block known mining pools.
- Browser and server hardening blocks mining scripts.

Implementation essentials

- Alert on sustained CPU spikes and outbound connections to mining domains.
- Review cloud cost anomalies weekly.

Measures

- Number of blocked mining attempts.
- Mean time to remediate a mining alert.

---

4) Email security (inbound and outbound)

Definition

Inbound screening reduces spam, phishing, and malware. Outbound controls prevent accidental or unauthorized sharing.

The problem in a law firm

Email is the primary path into the firm and out of it. Business email compromise and mis-addressed messages are common.

What it does

- Inbound: anti-phishing engines, attachment sandboxing, and URL protection.
- Outbound: DLP rules for sensitive data, encryption on demand, and journaling.

- Email authentication: publish SPF, DKIM, and DMARC records to prevent spoofing.

Implementation essentials

- Enforce TLS for mail transport and block auto-forwarding to personal accounts.
- Quarantine high-risk attachments and impersonation attempts.

Measures

- Phishing click-through rate and report rate.
- DMARC policy enforcement level (monitor, quarantine, reject).
- Outbound DLP prevents and most common triggers.

---

5) Backup and disaster recovery (DR)

Definition

Backups are protected copies of your data. **Disaster recovery** is the plan to restore systems and keep the firm operating after an outage or attack.

The problem in a law firm

Hardware failure and ransomware can make primary data unusable. Paying a ransom does not guarantee recovery.

What it does

- Follows the 3-2-1 principle: three copies, two media types, one offline or immutable.
- Defines RPO (how much data you can afford to lose) and RTO (how quickly you must be back).
- Requires regular test restores.

Implementation essentials

- Tier systems by criticality and assign RPO/RTO targets.
- Protect backups with MFA and separate admin credentials.

Measures

- Restore success rate per system.
- Average restore time and last test date.

---

6) Data Loss Prevention (DLP)

Definition

DLP detects and prevents unauthorized sharing by monitoring endpoints, email, cloud storage, and network traffic.

The problem in a law firm

Many incidents are accidental. Examples include sending to the wrong recipient or sharing a link with public access.

What it does

- Pattern matching for client names, matter numbers, and regulated data.
- Contextual prompts that nudge users before sending. Blocking when required.

Implementation essentials

- Start with alert-only policies to tune false positives.
- Label files by sensitivity to improve accuracy.

Measures

- Prevented incidents by type. False positive rate.
- Top rule triggers and policy tuning trend.

---

7) Patch and vulnerability management

Definition

Routine updates to systems and applications plus prompt fixes for known vulnerabilities.

The problem in a law firm

Most intrusions exploit already known flaws. Attackers move faster than monthly cycles.

What it does

- Maintains an asset inventory and scans regularly.
- Prioritizes risk based on what is being actively exploited.

Implementation essentials

- Monthly patch windows and out-of-band fixes for high-risk items.
- Service owners accountable for patch SLAs.

Measures

- Time to patch high-risk items. Percent of systems current.
- Scan coverage across assets.

---

8) User awareness and training

Definition

Structured education that forms secure habits for lawyers and staff.

The problem in a law firm

Phishing succeeds when people are rushed. Partners, finance, and docketing are frequent targets.

What it does

- Short, role-based modules and simulated phishing with coaching.
- Simple reporting buttons and executive briefings.

Implementation essentials

- Track completion and behavior change, not only attendance.
- Recognize and reinforce positive reporting.

Measures

- Phish report rate and repeat-clicker reduction.
- Training completion and assessment scores.

---

9) Password policy and Multi-Factor Authentication (MFA)

Definition

Passwords are "something you know." **MFA** adds "something you have" (token or app) or "something you are" (biometric).

The problem in a law firm

Credential theft remains a top cause of breaches.

What it does

- Uses longer passphrases and checks against known-breached passwords.
- Requires MFA everywhere feasible. Phishing-resistant MFA for admin and remote access.

Implementation essentials

- Enable MFA on email, VPN, practice and document management, e-billing portals, and backup consoles.

Measures

- Percent of users and applications protected by MFA.
- Adoption of phishing-resistant methods for admins.

---

10) Data encryption (devices and servers)

Definition

Encryption makes data unreadable without the key. It applies to data at rest and in transit.

The problem in a law firm

Lost laptops and server breaches can expose client data.

What it does

- Full-disk encryption on laptops and workstations.
- Encryption at rest for file servers and databases. TLS for data in transit.

- Central key management and access controls.

Implementation essentials

- Require full-disk encryption on all firm-owned laptops and enable automatic lock.
- Disable legacy, insecure protocols.

Measures

- Percent of devices encrypted. TLS coverage across services.
- Key rotation cadence and access reviews.

---

11) Vendor and service-provider management

Definition

Due diligence and oversight of third parties that store, process, or can access your data. This includes e-discovery partners, cloud apps, and contract IT.

The problem in a law firm

Breaches often occur via vendors. Clients expect proof of controls and contractually enforceable protections.

What it does

- Risk-tiers vendors and requires minimum security controls.
- Reviews reports such as SOC 2 Type II or ISO 27001 and builds requirements into contracts.

Implementation essentials

- Track all vendors with data access in a register.
- Require breach notification timelines, encryption, MFA, and limits on subcontractors.
- Review high-risk vendors annually.

Measures

- Percent of high-risk vendors with current assessments.
- Number of unresolved findings and time to remediation.

---

12) Physical security of hardware

Definition

Protections for offices, server rooms, and devices such as badge access, cameras, and locked storage.

The problem in a law firm

Physical access can bypass software controls. Devices travel to court, client sites, and home offices.

What it does

- Controls entry, logs visitors, and deters theft or tampering.

- Protects chain-of-custody for evidence and exhibits.

Implementation essentials

- Asset inventory with assigned owners. Cable locks in shared spaces.
- Secure media destruction and privacy screens for travel.

Measures

- Lost or stolen device incidents and time to disable.
- Visitor log exceptions and media destruction certificates.

---

13) Incident response plan (IRP)

Definition

A pre-agreed plan with roles, decision trees, and checklists for detection, containment, investigation, notification, and recovery.

The problem in a law firm

Without a plan, response is slow, errors multiply, and privilege may be jeopardized.

What it does

- Assigns who does what and when. Coordinates communications and preserves evidence.
- Aligns with insurance, client, and regulatory duties.

Implementation essentials

- Counsel-directed forensics to preserve privilege.
- Insurer notification steps and client/regulator decision criteria.
- Tabletop exercises two times per year.

Measures

- Mean time to contain and recover.
- After-action items closed on time.

---

14) Logging, monitoring, and managed detection (SIEM/MDR)

Definition

SIEM (Security Information and Event Management) centralizes logs from endpoints, servers, cloud apps, and network devices. **MDR** (Managed Detection and Response) provides 24x7 analysts who investigate and respond.

The problem in a law firm

Attacks often go undetected for weeks. Without logs, investigations stall and notifications are harder.

What it does

- Aggregates and correlates events and alerts on suspicious behavior.
- Accelerates investigation and supports incident response.

Implementation essentials

- Send logs from identity, EDR, email, cloud suites, and critical servers.
- Define retention aligned to legal holds and client requirements.

Measures

- Coverage percent across sources and time from alert to review.
- Alert fidelity and false positive rate.

---

15) Zero Trust access model

Definition

Zero Trust is a design approach that treats every access request as untrusted until validated. It focuses on user identity, device health, and least-privilege access, with continuous evaluation instead of one-time authentication at the perimeter.

The problem in a law firm

Remote work, cloud apps, and vendor portals have stretched the "office network." A castle-and-moat mindset is no longer enough.

What it does

- Requires strong identity and MFA for all access.
- Checks device posture such as encryption and EDR before allowing connections.
- Limits access to the minimum needed and segments sensitive systems.

Implementation essentials

- Put all web apps behind SSO with conditional access. Block legacy protocols.
- Use groups and roles tied to matters and functions. Review access quarterly.

Measures

- Percent of apps behind SSO and MFA.
- Number of users with broad, non-role-based access reduced over time.

> **Example.** A laptop without disk encryption cannot access the document system until encryption and EDR are verified.

---

16) Privileged Access Management (PAM)

Definition

PAM controls administrator accounts and other high-risk credentials. It stores them in a secure vault, rotates them automatically, records sessions, and grants elevation only when needed and only for a short time.

The problem in a law firm

Shared admin passwords and always-on privileges let attackers move quickly and quietly if one account is compromised.

What it does

- Eliminates standing admin rights and replaces them with just-in-time access.
- Provides full audit trails of privileged activity for investigations and compliance.

Implementation essentials

- Vault all domain, server, and cloud admin accounts. Enforce MFA and session recording.
- Create emergency "break glass" accounts stored offline and tested quarterly.

Measures

- Percent of admins without standing privileges.
- Frequency of password rotation and number of privileged sessions reviewed.

---

17) Mobile Device Management (MDM) and BYOD

Definition

MDM or **UEM** (Unified Endpoint Management) enforces security on phones and tablets. **BYOD** means employees use personally owned devices for firm work with managed controls that protect firm data without overreaching into personal content.

The problem in a law firm

Email, messaging, and document access on mobile create risk if devices are lost, jailbroken, or out of date.

What it does

- Requires screen lock, encryption, and automatic wipe after failed attempts.
- Allows remote wipe of firm data only on BYOD through containerization.

Implementation essentials

- Register all devices that access firm email or files. Block unmanaged devices.
- Set minimum OS versions and patch cadence. Prohibit rooted or jailbroken devices.

Measures

- Percent of mobile devices managed and compliant.
- Time to remote-wipe lost devices.

---

18) Network segmentation

Definition

Segmentation separates networks and systems so that a compromise in one area does not easily spread. This includes VLANs, firewalls, and micro-segmentation in data centers and cloud.

The problem in a law firm

Flat networks let attackers jump from a receptionist's PC to file servers, finance, or litigation support.

What it does

- Places sensitive systems such as document management and finance in restricted zones.
- Limits lateral movement and reduces blast radius for ransomware.

Implementation essentials

- Enforce allow-list rules between segments and disable legacy SMB where possible.
- Separate guest Wi-Fi and vendor access from internal networks.

Measures

- Number of permitted paths into sensitive segments and change trend over time.
- Results from segmentation tests during tabletop or pen tests.

---

19) Secure file transfer and client collaboration

Definition

Secure portals or managed sharing platforms replace email attachments for large or sensitive exchanges. Controls include link expiration, access by identity, watermarking, and upload scanning.

The problem in a law firm

Attachments are easy to misaddress and hard to revoke. Large evidence sets and expert exchanges need structured tracking.

What it does

- Shares files with expiring links and identity-based access instead of open links.
- Logs who accessed what and when, supporting legal holds and audits.

Implementation essentials

- Set default sharing to “specific people” and require MFA for external collaborators.
- Enable virus scanning on upload and DLP checks before sharing.

Measures

- Percent of external transfers using the secure portal.
- Number of revoked links and DLP prevents per month.

> **Example.** Experts receive expiring links to a matter folder that watermark downloads with their email and timestamp.

---

20) Attack Surface Management (ASM) and continuous scanning

Definition

ASM inventory tracks every internet-facing asset such as domains, cloud services, VPN portals, and web apps. Continuous scanning looks for weaknesses as they appear, not only during scheduled maintenance.

The problem in a law firm

Shadow IT, forgotten subdomains, and quick cloud trials often remain exposed and unpatched.

What it does

- Discovers new or changed assets automatically and flags risky configurations.
- Pairs with vulnerability scanning to prioritize fixes by exposure and criticality.

Implementation essentials

- Enable external scans of domains and IP ranges. Monitor certificate transparency logs for new hosts.
- Establish a change process that registers any new public endpoint before it goes live.

Measures

- Time to close externally exposed critical findings.
- Number of unknown assets discovered and remediated.

---

21) Penetration testing and tabletop exercises

Definition

Penetration testing is a controlled, ethical attempt to exploit weaknesses to see what an attacker could achieve. **Tabletop exercises** are guided discussions that walk through an incident scenario to test roles and decisions without touching systems.

The problem in a law firm

Annual audits and paperwork do not show how your defenses perform in practice or how your team will respond under pressure.

What it does

- Validates controls end to end and reveals gaps in detection, segmentation, and response.
- Builds muscle memory so decisions are faster and clearer during real incidents.

Implementation essentials

- Scope tests for internal, external, and phishing vectors. Include high-value targets like DMS and finance.
- Run tabletop exercises for ransomware and vendor breach scenarios at least twice per year.

Measures

- Findings closed within target timelines.
- Tabletop after-action items completed and retested.

---

22) Data classification and retention

Definition

Classification assigns a sensitivity label to information such as Public, Internal, Confidential, or Restricted. **Retention** defines how long data is kept and how it is disposed of, with exceptions for legal holds and client agreements.

The problem in a law firm

Excess data increases breach impact and discovery costs. Without labels, DLP and access controls are blind.

What it does

- Improves accuracy of DLP and access rules by giving content context.
- Reduces risk and cost with defensible deletion once obligations end.

Implementation essentials

- Adopt simple labels and default everything to at least Internal.
- Tie retention to matter lifecycle with clear triggers for hold, archive, and destruction.

Measures

- Percent of content labeled. Volume of data archived or deleted per quarter.
- Number of access violations prevented by labels.

> **Example.** “Restricted” files require MFA for access and cannot be shared externally without a partner’s approval.

---

23) Cyber insurance readiness

Definition

Cyber insurance transfers some financial risk of cyber incidents. Readiness means you can demonstrate the controls carriers require and you can document them quickly during underwriting and claims.

The problem in a law firm

Carriers increasingly require proof of MFA, EDR, offline backups, and documented response plans. Lack of evidence can delay or limit claims.

What it does

- Aligns minimum controls with policy requirements and reduces premiums over time.
- Streamlines claims with pre-collected evidence such as logs and playbooks.

Implementation essentials

- Create an underwriting packet: network diagrams, control summaries, IR plan, backup tests, vendor list.
- Keep proof artifacts current. Assign ownership to risk or compliance staff.

Measures

- Number of required controls evidenced and verified.
- Time to produce documentation during renewal or claim.

---

24) Framework alignment for client questionnaires

Definition

NIST CSF and **CIS Controls** are widely used frameworks that organize security outcomes. Mapping your controls to them creates a common language for client due-diligence and audits.

The problem in a law firm

Security questionnaires vary by client and industry. Ad-hoc answers are slow and inconsistent.

What it does

- Provides reusable, framework-mapped responses to common questions.
- Reduces friction in client onboarding and panel renewals.

Implementation essentials

- Maintain a control catalog mapped to NIST CSF functions and CIS Controls.
- Publish a one-page “Security at 2b1 Inc.” summary for business users and a detailed appendix for technical reviewers.

Measures

- Average turnaround time for questionnaires.
- Number of follow-up questions and exceptions requested by clients.

90-day quick start

1. Now Turn on MFA for email, remote access, and administrator actions.
2. Week 1–2 Verify offline or immutable backups. Run a test restore of your document system.
3. Week 2–4 Deploy EDR to 100 percent of firm devices and integrate alerts with a monitoring service.
4. Month 2 Publish SPF, DKIM, and DMARC. Move to quarantine, then reject after monitoring.
5. Month 2–3 Patch high-risk vulnerabilities first. Cross-check findings with active exploitation reports.
6. Month 3 Run a ransomware tabletop exercise and close gaps found.

12–18 month maturity roadmap

Foundation (0–3 months)

- MFA everywhere. EDR on all endpoints.
- Offline or immutable backups tested.
- Email filtering with SPF/DKIM/DMARC.
- Basic IR plan and full-disk encryption on laptops.

Strengthening (3–9 months)

- DLP for email and endpoints. Vulnerability scanning with SLAs.
- Vendor risk program and network segmentation.
- MDM for mobile and BYOD.

Advanced (9–18 months)

- Central logging and MDR. Phishing-resistant MFA for admins.
- PAM with just-in-time access.
- Data classification and retention. Zero Trust roadmap.
- Regular penetration tests and tabletop exercises.

Sample policy snippets (plain language)

- **Passwords.** Use a passphrase of at least 14 characters. Do not reuse passwords. The firm checks new passwords against lists of known-breached passwords. Change only if compromise is suspected or required.
- **MFA.** MFA is required for email, remote access, administrator actions, and any system containing client confidential data.
- **Encryption.** All firm laptops must use full-disk encryption. Servers hosting client files and databases must use encryption at rest and TLS in transit.
- **Vendors.** Before onboarding a vendor with data access, evaluate controls, require contractual security

clauses, and record approval in the vendor register.
- **Remote work.** Access firm systems only through managed devices or approved virtual desktops. Store client data in firm repositories, not locally.

One-page control-to-risk map

Risk in legal practice	Control(s) that reduce it
Phishing to account takeover	Email filtering, SPF/DKIM/DMARC, MFA, user training
Ransomware halting matters	EDR, segmentation, backups, patching, incident response plan
Confidentiality breach via mis-send	DLP, secure portals, least privilege access
Vendor breach exposure	Vendor risk management and contractual controls
Lost laptop in transit	Full-disk encryption, MDM, rapid disable
Discovery cost and over-retention	Classification, retention, defensible deletion

---

Glossary (plain language)

AV. Antivirus. Legacy term for tools that block known malware.

DLP. Data Loss Prevention. Detects and blocks unauthorized sharing.

DMARC, DKIM, SPF. Email authentication records that prevent domain spoofing.

EDR. Endpoint Detection and Response. Monitors endpoints and isolates threats.

MDR. Managed Detection and Response. A third party monitors alerts 24x7.

MFA. Multi-Factor Authentication. Requires a second factor beyond a password.

NIST CSF. A framework that organizes security outcomes into Identify, Protect, Detect, Respond, and Recover, plus Governance practices.

PAM. Privileged Access Management. Controls admin accounts and access.

RPO/RTO. Recovery Point Objective and Recovery Time Objective.

SIEM. Security Information and Event Management. Central log collection and analytics.

Zero Trust. Default deny. Verify identity and device health for every access request.
