SMB Security Architecture – Controls & Flows (v1)

Context: ~50-person hybrid SMB; SaaS-centric; e-commerce/PII; limited IT budget.

---

0) How to read the diagrams

- We split the architecture into **four focused views** to avoid clutter.
- **Numbered arrows** show the **order of the flow**. Each diagram has a short caption that explains those numbers in words.
- Shapes: **User/Device (ellipse)**, **Service/Control (rounded box)**, **Trust zone (large rounded rectangle)**.
- Line styles: **Solid** = normal data path, **Dashed** = security-gated path (e.g., MFA, device posture), **Dotted** = logging/telemetry.

---

1) Identity & Access (SSO + MFA)

Purpose: One secure login to all apps, protected by MFA. Users get only the access they need.
Why: Stops most account-takeovers and makes onboarding/offboarding quick.

Non-technical

- Sign in once via company login + quick second check (MFA).
- You're then in email, files, CRM automatically.
- Disable one account = turn off access everywhere.

Implementers

- Central IdP/SSO (SAML/OIDC); **MFA for all**; break-glass admin.
- Role groups + SCIM; Conditional Access (device compliance, geo, risk).
- Block legacy auth; review OAuth grants; log sign-ins & privilege changes.

KPIs: MFA 100%; privileged accounts MFA 100%; stale accounts 0.

Diagram: `Identity_Access_v1.drawio`.

---

2) Endpoint Security (EDR + MDM + Encryption)

Purpose: Company devices are managed, patched, encrypted, and watched by an EDR agent.
Why: Malware is blocked/isolated; lost laptops don't leak data.

Non-technical

- Your laptop has a "guardian" that blocks suspicious behavior.
- If it's lost, the disk is encrypted; IT can wipe it remotely.

Implementers

- EDR on all endpoints; enable isolate/rollback; host firewall.
- Full-disk encryption; no daily local admin; patch rings (crit ≤7d).
- Device compliance gates SSO; USB controls as needed; browser auto-update.

KPIs: ≥95% devices compliant & encrypted; EDR coverage 100%.

Diagram: `Endpoint_Security_v1.drawio`.

---

3) Network & Remote Access (Segment, Filter, Contain)

Purpose: Office split into **Staff**, **Guest**, **IoT**; firewall filters traffic; remote users use ZTNA/VPN.
Why: Limits lateral movement; guests/IoT can't reach business data.

Implementers

- VLANs: Staff (802.1X), Guest (Internet-only), IoT (no east-west).
- NGFW/IPS: egress allow-list, geo/IP rep, DNS filtering.
- ZTNA/VPN with SSO+MFA & device posture; log denies and changes.

KPIs: 0 guest→staff routes; remote via ZTNA/VPN 100%.

Diagram: `Network_Segmentation_v1.drawio`.

---

4) Email/Web Protection (Phishing & Malicious Sites)

Implementers

- Safe Links/Attachments (or equivalent); external banner; block auto-forwarding.
- DMARC/DKIM/SPF at enforcement; domain monitoring.
- DNS filtering (DoH) for all segments; block risky categories.

KPI: Phish-fail ≤5%; DMARC rejects; DNS blocks tracked.

---

5) Data Protection & Backup

- SaaS/email/files backed up to a **separate tenant** with immutability.
- Quarterly restore tests; document RPO/RTO per data class.
- Encrypt in transit/at rest; legal-hold for PII where required.

KPI: 100% classes meet RTO/RPO in tests.

---

6) SecOps: Logging, Detection, & IR

- Send IdP, EDR, NGFW/DNS, SaaS audit logs to SIEM/MDR.
- Alerts: impossible-travel, risky OAuth, malware isolate, mass download, new admin.
- IR runbooks: BEC, ransomware, lost device, exposed SaaS. Tabletop quarterly.
- Pager (Sev-1), Chat (Sev-2), Ticket (all).

KPIs: MTTD <1h; MTTR <24h; ≥90% sources logging.

Diagram: `SecOps_Telemetry_v1.drawio`.