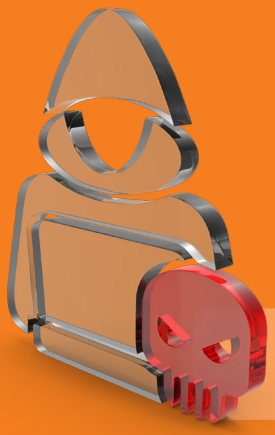
in time tec

CREATING ABUNDANCE

The Integrated Security Stack

How SMBs Can Build Enterprise Protection Without Enterprise Budgets

Executive Summary & Why Now

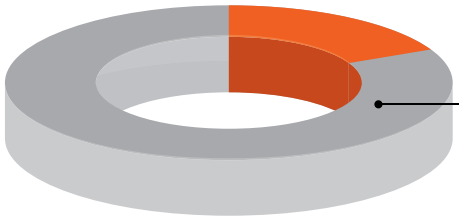


Enterprise-grade security, sized (and priced) for SMBs

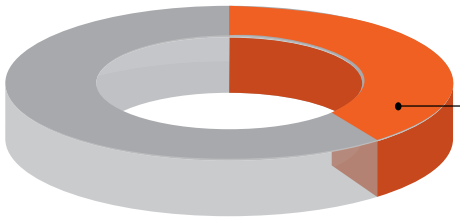
Modern attacks are faster, cheaper, and more automated than ever. Ransomware and credential abuse dominate initial access, and third-party breaches are rising yet SMBs can reach enterprise-level protection by integrating a right-sized stack:

Identity + Endpoint + Email/Cloud + Vulnerability/Patch +Backup/BCP + Response

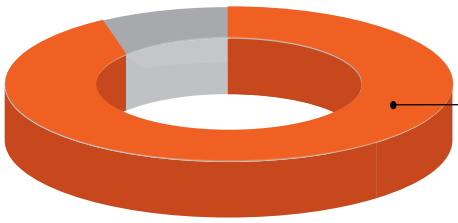
44% of breaches involved ransomware, signaling a worrying surge



22% of breaches were driven by credential abuse, targeting weak passwords



30% of breaches are tied to third-party involvement, doubling year over year.



83% of APAC breaches involved malware, with email as the primary delivery vector.

Threat Landscape Snapshot

What hits SMBs first and hardest

Stolen Credentials, **55%**

Exploited Vulnerabilities, **18%**

Phishing / Social Engineering, **20%**

What these trends mean for SMBs

Prioritize identity hardening (phishing resistant MFA, conditional access).

Close edge/VPN exposure and improve patch latency.

Invest in tested backups + BCP to reduce ransom pressure.

88% of SMB breaches involve ransomware versus 39% in large organizations, while payment amounts continue to decline as more victims refuse to pay.

34% growth in exploited vulnerabilities, with edge/VPN flaws rising eightfold and only 54% patched within an average 32-day window.

Hundreds of millions of daily identity-attack signals are tracked by Microsoft, with password attacks dominant and MFA adoption uneven among SMBs.

APAC breaches show doubled third-party involvement and eightfold growth in edge/VPN flaws, amplifying global SMB patterns

The Integrated Security Stack

Unified Build. Continuous Integration

Why: >99% of identity attacks remain password-based; MFA adoption gaps keep SMBs exposed.

Key Measures: MFA (phishing resistant), conditional access, least privilege, automated provisioning.

Why: Ransomware prevalence in breaches is rising, modern EDR reduces dwell time and stops encryption.

Key Measures: EDR with behavioral detection, web filtering, email threat protection (anti-phish, DMARC).

Why: Human error drives most breaches, proactive training and reporting reduce phishing risk and accelerate response.

Key Measures: Phishing simulation (TSAT), gamified awareness training (TLMS), DMARC enforcement (TDMARC), one-click threat reporting (TPIR).

Why: Third-party/supply-chain exposure doubled globally and is acute in APAC, where diversification strategies ('China Plus One') increase vendor complexity.

Key Measures: MFA everywhere, RBAC/Least Privilege,misconfiguration scanning, centralized cloud logs.

Why: In APAC, exploited vulnerabilities, especially in VPNs and edge devices, rose 34%, with 22% of attacks targeting those devices. Only 54% were patched, taking a median of 32 days to fix.

Key Measures: Weekly vulnerability scans, SLA-based patching (critical ≤7 days), fixed processes for edge/VPN.

Why: Payment refusal rises with reliable recovery; encrypted backups are prime ransomware targets without isolation.

Key Measures: 3-2-1 rule, immutable/air-gapped copies, quarterly restore tests, documented RTO/RPO. documented RTO/RPO.

Why: Faster detection lowers breach cost and impact; integrated response reduces median dwell times.

Key Measures: Centralized logging mapped playbooks (BEC, ransomware), tabletop drills, out-of-band communications.

Sources: 2025 Multi-Factor Authentication (MFA) Statistics & Trends to Know

Sources: Verizon's 2025 Data Breach Investigations Report Notes Alarming Cyberattack Surge Through Third Parties Security Today

Sources: Verizon DBIR: Patch Delays on VPNs and Edge Devices Fuel 34% Spike in Exploited Vulnerabilities - All Time Cybersecurity

What to Buy on an SMB Budget

Spend where ROI is proven

High-ROI Essentials ▸ Why it matters

Phishing-Resistant MFA & SSO	▸ Cuts credential abuse and reduces successful identity attacks.
EDR + Email Security Bundle	▸ Ransomware present in 51% of breaches, endpoint/email are first lines.
Vuln/Patch orchestration for edge/VPN	▸ Exploitation surged, patch lag (median 32 days) is costly.
Immutable backups + quarterly restore tests	▸ Enables ransom refusal (median payouts falling).
SIEM-lite + managed detection (MDR/MSP)	▸ Reduces detection/containment time, lowers costs.

Nice-to-haves (later) ▸ Rationale

Advanced SOAR & bespoke XDR

Start with MDR/EDR, scale orchestration after core hygiene. (general best practice, inferential omit citation)

Quantum-safe crypto pilots

Plan ahead, but prioritize present exposure first.

Sources: Ransomware hits APAC hard, driving 51% of regional data breaches | Communications Today

Sources: Cost of a data breach 2025 | IBM

90-Day Implementation Roadmap

Quick wins to “Established” maturity in one quarter

Phase 0 (Week 0): Readiness

App inventory, privileged accounts, backup topology, IR contacts (legal, MSP, regulators).

Phase 1 (Weeks 1–4): Identity & Email First

Enforce MFA for all admins & critical apps, set conditional access, deploy email anti-phish + DMARC.

Outcome: Reduced credential abuse risk (top initial vector).

Phase 2 (Weeks 5–8): Endpoint + Patch Discipline

Roll out EDR; define patch SLAs, remediate edge/VPN vulns, centralize cloud logs.

Outcome: Exposure to exploited vulnerabilities reduced, faster detection.

Phase 3 (Weeks 9–12): Backups + IR Drills

Implement 3-2-1 with immutable storage; run quarterly restore test; conduct a tabletop ransomware drill with out-of-band communications.

Outcome: Higher confidence to refuse ransom, faster recovery.

Foundation — **Developing** — **Established**
(target end of 90 days)

KPI Dashboard, Checklists & Sources

Measure resilience like an enterprise

Top KPIs

MFA coverage
(% of users & apps)
privileged account hygiene

Patch latency
(median days to remediate
critical edge/VPN vulns)

EDR coverage
(% endpoints)
+ **mean time to detect/contain**

Backup integrity
(quarterly restore success rate,
RTO/RPO adherence)

Phishing simulation
click-through rate
(monthly), **user report rate.**
(training KPI; general)

Quick checklists:

- **Identity:** MFA everywhere (admins first), conditional access, break-glass accounts secured.
- **Endpoint/Email:** EDR deployed, block macros, DMARC enforced.
- **Vulnerability/Patch :** Weekly scans, SLA playbook for perimeter devices, VPN hardening/alternatives.
- **Backup/BCP:** 3-2-1, immutable store, quarterly restores, documented RTO/RPO.
- **IR:** Playbooks (ransomware/BEC), out-of-band comms, annual tabletop.

Sources : https://www.itpro.com/security/cyber-attacks/microsoft-logs-600-million-identity-attacks-per-day-as-threat-actors-collaborate-more

Sources:https://www.techrepublic.com/article/news-verizon-data-breach-investigations-report-2025/