Devolutions

10 security controls to prioritize for SMBs (and 1 bonus)

OCTOBER 2025

TABLE OF CONTENTS

In the distant past, small and mid-sized businesses (SMBs) could comfort themselves by saying that their relatively smaller size and less valuable data were, paradoxically, an advantage since it meant that hackers and other bad actors focused on attacking large enterprises. **Unfortunately, those days are over.**

Today, SMBs are firmly in the cyberthreat crosshairs. Research by Microsoft found **the average total cost of a cyberattack on an SMB was roughly $255,000 per incident** (all figures in this white paper are USD), with some incidents reaching $7 million when investigation, recovery, and reputation damage are included. Given this real and present danger, it would be logical to assume that SMBs around the world have made it a top priority to strengthen their cybersecurity. In theory, yes. But in practice, no.

The Devolutions' State of IT Security in SMBs 2024–2025 survey revealed that the majority of SMBs remain highly vulnerable to a cyberattack:

- **68% of SMBs say that they do not have an advanced cybersecurity posture.**
- **Only 20% of SMBs have a comprehensive insider-risk plan, and just 18% actively monitor for insider risk.**
- **52% of SMBs still manage privileged access manually with spreadsheets, basic vaults, or have no formal system at all.**
- **61% of SMBs do not provide continuous security awareness training, and 17% provide no training whatsoever.**

What is behind this lack of awareness, attention, and most importantly, action from SMBs? Often, it is not intentional. For many SMBs, cybersecurity is viewed as complex, costly, and difficult to staff; especially amid tool sprawl, legacy systems, and day-to-day operational pressures. In other words, SMBs look out into the marketplace and see a maze of tools, solutions, and products that are aimed at enterprises with large IT teams and significant annual IT security budgets. **This is simply not the reality that most SMBs face.**

This white paper meets SMBs where they actually are. Here is our path:

- We look at 10 practical and affordable security controls that SMBs can implement in the near-term future – some as rapidly as within days – to dramatically strengthen their cybersecurity posture.
- We share one "people-centric" bonus tip that could mean the difference between fending off vs. being victimized by a potentially catastrophic cyberattack.
- We wrap up our journey with guidance to help SMBs move from intention to execution quickly and confidently.

SECURITY CONTROL #1: SECURE REMOTE ACCESS MANAGEMENT

Remote connectivity is indispensable for support, maintenance, and operations, yet it remains a primary intrusion path when unmanaged. The usual suspects are common: an exposed portal, inconsistent multi-factor authentication (MFA), and sessions that launch without policy or audit. Verizon's 2025 Data Breach Investigations Report (DBIR) highlights the primary role of stolen credentials in common breach patterns.

Action items

- Remove all direct RDP, SSH, and VNC exposure from the internet. Require access through a broker or gateway only.
- Enforce MFA at connection time for every privileged or external session, not just at portal sign-in.
- Standardize session policies by protocol. Set clipboard, drive mapping, file transfer, recording, and idle timeout rules per risk level.
- Use credential injection so users and vendors never see or copy passwords during connection.
- Segment administration pathways. Restrict remote admin to dedicated jump hosts or gateway relay networks that do not overlap with user subnets.
- Patch and harden the remote access stack first. Keep gateway, agents, clients, and plugins current and disable unused protocols and ciphers.
- Monitor and log everything. Forward gateway, session, and authentication logs to your SIEM and alert on after-hours or unusual source locations.
- Time-box access. Require ticket or change ID, approval for high risk systems, and automatic session termination on expiry.
- Lock down vendor and third-party access with separate accounts, least privilege roles, and restricted maintenance windows.
- Define and rehearse break glass procedures. Store emergency credentials in a separate vault, rotate immediately after use, and document approval and notification steps.

SECURITY CONTROL #2: USE A SECURE DIGITAL VAULT FOR CREDENTIALS AND SECRETS

A secure vault is a control boundary that turns chaotic, copy-paste credentials into governed secrets with lineage and recovery. Cloudflare's analysis that **41% of logins on websites that it manages used compromised passwords is a blunt reminder that stolen secrets are already in circulation.**

Action items

- Consolidate every secret into one vault. Sweep spreadsheets, browser stores, password files, code repos, ticket attachments, and shared drives, then import and securely delete the originals.
- Design a clear vault structure and ownership model. Separate areas for user credentials, privileged accounts, service accounts, and vendor access, with least privilege roles and delegated owners.
- Enforce strong authentication at the vault. Require multi-factor authentication (MFA), conditional access, and device checks for admins and any external users.
- Apply rotation policies inside the vault. Schedule rotations for privileged and service accounts, trigger event-based rotations from Human Resources and Information Technology Service Management (ITSM) events, and propagate changes to dependent systems.
- Protect recovery materials. Generate emergency kits, maintain more than one valid emergency key, store copies offline, and run periodic validation tests.
- Restrict reveal and export. Require masked view for sensitive items, prefer use through credential injection as established in Control 1, and limit who can export or create API tokens.
- Run quarterly hygiene reviews. Remove stale users and orphaned secrets, rotate anything unused for 90 days, scan for shadow stores, and attest that legacy files were securely destroyed.
- Require approval and justification for high-risk secrets. Use check-out with short timers, automatic check in, and dual control for the most sensitive entries.

- Enable full auditing and alerts. Forward immutable vault logs to your security information and event management (SIEM) platform and alert on bulk export, after-hours access, unusual geolocations, and repeated failed attempts.
- Integrate with your stack. Tie role-based access control (RBAC) to directory groups, enable single sign-on (SSO), connect webhooks to ticketing, and expose secret providers for continuous integration (CI) or automation that need machine access.

SECURITY CONTROL #3: SECURE PASSWORD MANAGEMENT AND ROTATION

Static or shared passwords turn a single compromise into a campaign. Generation, rotation, and propagation close that window. Tie changes to time and to events such as role change, vendor off-boarding, or incident containment.

Action items

- Adopt strong, consistent generation rules. Use unique, high-entropy passwords for every account and system; prefer long passphrases where supported and set minimum lengths that exceed vendor defaults.
- Screen new passwords against known-breached credentials. Block passwords found in breach datasets and enforce history rules to prevent reuse across accounts or over time.
- Tie rotations to both time and events. Schedule rotations for privileged and service accounts and trigger immediate changes on incidents, role changes, vendor off-boarding, or scope elevation.
- Propagate changes reliably. Map dependencies so a rotated credential updates all linked services, applications, connection entries, and scripts without manual edits or outages.
- Eliminate shared admin accounts. Replace shared credentials with individual accounts tied to identity and audit; where shared secrets are unavoidable, pair usage with approval and post-use rotation.

- Shorten the life of temporary credentials. Issue time-bound, task-specific passwords for maintenance windows and auto-expire them at the end of the window.
- Harden service and application accounts. Use random, non-interactive passwords, deny interactive logon, restrict network logon where possible, and rotate on a tighter cadence than user accounts.
- Stage and test rotations safely. Validate rotation procedures in a non-production environment, define rollback steps, and stagger production rotations to reduce blast radius.
- Monitor for rotation failures and drift. Alert on failed updates, mismatched secrets, or services that fall out of policy, and remediate within defined Service-Level Objectives (SLOs).
- Document ownership and attestation. Assign an owner to each high-value credential, require quarterly attestation that rotation and dependency mappings are accurate, and record evidence for audits.

SECURITY CONTROL #4: USE MULTI-FACTOR AUTHENTICATION (MFA) EVERYWHERE

MFA reduces successful account takeovers. CISA's guidance on phishing-resistant MFA urges FIDO2 or passkeys over weaker factors, and public sector deployments demonstrate the model at scale.

Action items

- Standardize preferred methods. Prioritize FIDO2 security keys and passkeys, then authenticator apps; avoid SMS except as a temporary fallback.
- Enforce MFA at high-risk points. Require MFA at vault sign-in, gateway connection, VPN entry, session launch for RDP/SSH, privileged actions, and self-service security changes.
- Cover all identities appropriately. Enroll administrators, employees, and third-party vendors; replace MFA-incompatible service accounts with scoped tokens or managed identities and lock them down separately.

- Eliminate legacy bypass paths. Disable basic authentication protocols such as legacy POP/IMAP, remove app passwords, and require Network Level Authentication (NLA) or equivalent for remote protocols.
- Protect enrollment and recovery. Require identity proofing for new-factor enrollment, separate approval for resets, and store recovery codes or backup keys securely in the vault from Control 2.
- Harden push-based MFA. Enable number matching or verification codes, rate-limit prompts, and auto-block repeated denials to prevent push fatigue attacks.
- Apply risk-based, step-up challenges. Trigger MFA based on unusual geo locations, device posture, new browsers, off-hours access, or impossible travel signals.
- Integrate with single sign-on (SSO) and conditional access. Centralize policy in your identity provider, and force re-authentication for privileged tasks as established in Control 1.
- Measure coverage and effectiveness. Track enrollment percentage, factor mix, failure rates, and exception counts; investigate spikes and remediate gaps within set timelines.
- Time-bound exceptions. Document any MFA exceptions with an expiration date and compensating controls, then review and retire them on schedule.

SECURITY CONTROL #5: IMPLEMENT LEAST PRIVILEGE AND JUST-IN-TIME (JIT) ACCESS

Standing admin rights are a gift to intruders. Least privilege with just-in-time elevation changes the physics of an attack. Rights exist only for the task and only for a short window.

Action items

- Discover and classify privilege. Inventory all accounts with elevated rights across domains, cloud tenants, SaaS admins, databases, and network devices; tag by role, system criticality, and required privilege.

- Define role-based access control (RBAC) baselines. Create narrow role profiles for administrators, operators, and auditors; map each system action to the minimum role that can perform it.
- Eliminate standing admin memberships. Replace permanent privileged group memberships with JIT elevation that grants rights only for a task and only for a limited window.
- Require ticket and approval for elevation. Bind elevation requests to a change, incident, or maintenance ticket; route high-risk systems through multi-party approval with clear justification.
- Time-box and scope elevation. Set default durations in minutes, not hours; restrict elevation to specific systems, commands, or management scopes and terminate automatically on expiry.
- Rotate on check-in. When elevated access ends, rotate the underlying credential or token immediately to prevent reuse and to contain lateral movement.
- Segregate privileged workstations. Require privileged tasks to run from hardened administrative workstations that are separate from daily user devices and internet browsing.
- Minimize and monitor service account privilege. Replace broad privileges with the least set of rights, deny interactive logon, and review each service account's permissions quarterly.
- Log and review privileged activity. Capture who elevated, when, for what ticket, and what actions were taken; forward records to your security information and event management (SIEM) and sample weekly for anomalies.
- Attest and re-certify regularly. Run quarterly access reviews with system owners to remove unused roles, retire stale elevation workflows, and document attestation for audits.

SECURITY CONTROL #6: SESSION RECORDING, AUDITING, AND LOGGING

Evidence shortens investigations. For high-risk work, session video with sensitive-data redaction removes ambiguity, while immutable logs support compliance and trending. IBM's analysis ties faster identification and containment to lower breach costs, which makes disciplined logging a financial control as well as a security control.

Action items

- Define scope and risk tiers. Identify which systems, protocols, and vendors require recording and enhanced logging; prioritize privileged RDP, SSH, web admin consoles, and changes to security controls.
- Enable recording with privacy guardrails. Turn on session recording for high-risk work and configure redaction for passwords, tokens, and sensitive fields; disable clipboard capture where not needed.
- Normalize and time-sync everything. Standardize log formats and ensure tight clock sync using Network Time Protocol (NTP) so timelines align across gateway, vault, identity provider, and endpoint sources.
- Set retention and legal hold policy. Define retention by record type, meet regulatory requirements, and document legal hold procedures for incidents or investigations.
- Forward to your SIEM and alert on signals. Stream gateway, session, elevation, and vault events to the security information and event management (SIEM) platform; alert on after-hours admin activity, unusual geolocation, bulk export, and repeated failures.
- Store evidence in tamper-evident repositories. Write logs and recordings to immutable or Write Once Read Many (WORM) storage in a separate account or tenancy; restrict delete rights and require change control for retention edits.
- Harden access to audit data. Protect log and recording access with role-based access control (RBAC), multi-factor authentication (MFA), and just-in-time investigator access; record who viewed or exported what and when.

- Automate integrity and chain of custody. Hash recordings and critical logs, verify checksums on a schedule, and preserve a chain-of-custody record for any evidence you export.
- Review and report on a cadence. Sample a subset of high-risk recordings weekly, run a quarterly audit of privileged actions, and publish metrics such as mean time to review and number of policy violations.
- Integrate with incident response playbooks. Link recording IDs and log search queries to tickets; predefine export formats for regulators and insurers, and test the end-to-end workflow during tabletop exercises.

SECURITY CONTROL #7: AUTOMATION AND ORCHESTRATION

SMB teams typically cannot scale manual security work. Automate joiner-mover-leaver changes, trigger rotations from HR events, expire just-in-time elevation automatically, and wire ticket approvals to access grants.

Action items

- Identify high-impact candidates first. Choose workflows with frequent errors or delays such as joiner–mover–leaver changes, privileged password rotations, and vendor access provisioning.
- Standardize approvals and evidence. Bind automated actions to tickets, capture approver identity, justification, and timestamps, and attach logs or recording IDs automatically to the record.
- Use least-privilege automation accounts. Create scoped service principals or tokens with only the permissions required for each workflow and rotate their secrets on a short cadence.
- Build idempotent, fail-safe steps. Ensure rerunning a workflow produces the same end state, add retries with backoff, and define explicit rollback actions for partial failures.

- Document ownership and recovery. Assign an owner for every automation, publish runbooks for manual fallback, and test handoffs so operations can complete the task if the pipeline is down.
- Connect source systems to triggers. Use Human Resources (HR) and Information Technology Service Management (ITSM) events to kick off automations through webhooks, message queues, or REST APIs.
- Template repeatable tasks as code. Encode connection entries, policies, and remote workflows using infrastructure as code (IaC) or configuration templates so changes are versioned and peer reviewed.
- Instrument and monitor the pipelines. Emit metrics and logs for each step, forward to your security information and event management (SIEM) platform, and alert on failures, timeouts, or unexpected side effects.
- Guardrails for production changes. Require change windows for high-risk automations, add dry-run modes for preview, and enforce manual confirmation for actions that affect privileged groups or critical systems.
- Continuously improve with post-action reviews. After incidents or large rollouts, review automation performance, tune thresholds and timeouts, retire unnecessary steps, and record lessons learned.

SECURITY CONTROL #8: FOCUS ON PATCH AND VULNERABILITY MANAGEMENT

Attackers weaponize new CVEs quickly, often chaining misconfigurations and known flaws with stolen credentials. Internet-facing services, remote access components, and management consoles need an accelerated patch lane.

Action items

- Build a real-time asset inventory. Track every internet-facing system, server, workstation, network device, application, and firmware version in one source of truth tied to ownership.

- Scan continuously and verify coverage. Run authenticated vulnerability scans on a fixed cadence and after major changes; validate that all subnets, cloud accounts, and remote sites are included.
- Prioritize by exploitability, not only severity. Combine Common Vulnerability Scoring System (CVSS) with threat intelligence and proof-of-concept exploitation to raise priority for actively exploited issues.
- Define patch service-level agreements (SLAs). Set targets such as 72 hours for internet-facing and remote access components, 7 days for business-critical systems, and 30 days for the rest; document approved exceptions with expiry dates.
- Stage, test, and roll back safely. Use a pre-production ring to test vendor updates, document rollback steps, and schedule maintenance windows that minimize business disruption.
- Address third-party and firmware updates. Include browser, PDF, runtimes, drivers, network device firmware, and out-of-band management controllers in the same program and track their status.
- Mitigate when you cannot patch immediately. Apply compensating controls such as configuration hardening, firewall rules, virtual patching with a web application firewall (WAF) or intrusion prevention system (IPS), and temporary feature disablement.
- Retire or isolate end-of-life (EOL) systems. Replace unsupported platforms; if replacement is delayed, isolate them on dedicated network segments with restricted access and heightened monitoring.
- Prove closure with validation. After patch deployment, rescan to confirm remediation, spot-check system versions, and record evidence linked to tickets for audits.
- Measure and report program health. Track time to remediate, exception volume, percentage of assets compliant with SLA, and repeat offenders; review trends monthly and assign actions to system owners.

SECURITY CONTROL #9: RUN BACKUPS (AND TEST THEM!)

Resilience is the final safety net. Adopt 3-2-1, isolate copies from the domain, encrypt, and test restores. Modern ransomware blends encryption with data theft and pressure campaigns.

Action items

- Define business targets. Set Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each critical system and align backup frequency and retention to meet them.
- Adopt the 3-2-1 model with immutability. Keep three copies on two media types with one offsite; use immutable or Write Once Read Many (WORM) storage so ransomware cannot alter backups.
- Isolate backup infrastructure. Place backup servers, repositories, and consoles on a separate management network and restrict admin access with Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC).
- Encrypt everywhere. Enable encryption in transit and at rest; manage keys in a Hardware Security Module (HSM) or vault and restrict who can export or rotate keys.
- Automate and stagger schedules. Run frequent incrementals with periodic fulls; stagger job start times to avoid resource contention and ensure remote sites and laptops are covered.
- Test restores by stopwatch. Perform monthly restore tests for at least one business-critical system; record restore time, validate data integrity, and update the runbook with lessons learned.
- Back up more than data. Include configuration states, infrastructure-as-code files, directory and identity configs, vault exports, logging and recording repositories, and licensing files.
- Scan before you restore. Stage restores in a quarantine environment, scan for malware, and validate application behavior before reconnecting to production networks.

- Enforce retention and legal hold. Apply tiered retention policies per system and regulatory requirement; document legal hold procedures and protect held backups from pruning.
- Monitor and prove success. Alert on failed jobs, slow throughput, and capacity thresholds; generate monthly reports that show success rates, tested systems, and gaps tied to owners and remediation dates.

SECURITY CONTROL #10: IMPLEMENT CONTINUOUS MONITORING AND INCIDENT RESPONSE READINESS

You cannot respond to what you do not see. Centralize logs from identity, vaults, gateways, PAM, and directories. Write short, explicit playbooks for the most likely event: a compromised admin credential opening a remote session. Run quarterly tabletops and include after-hours escalation. The goal is fewer surprises and faster containment.

Action items

- Centralize telemetry where it matters. Ingest identity, gateway, vault, Privileged Access Management (PAM), endpoint, and cloud logs into your Security Information and Event Management (SIEM) platform; tag privileged activity and remote sessions for higher priority.
- Define high-fidelity detections. Write detections for the top abuse paths such as impossible travel logins, after-hours admin access, mass credential failures, vault exports, and privileged session launches without approvals.
- Codify actionable runbooks. Create short, step-by-step playbooks for events like "compromised admin credential," "suspicious remote session," and "vault anomaly"; include who does what, in what order, with which tools.
- Establish clear escalation paths. Publish on-call rotations, contact methods, and decision thresholds; ensure business leadership knows when and how they will be paged.

- Rehearse regularly. Run quarterly tabletop exercises and at least one live technical drill per year that validates end-to-end steps from alert triage through containment and credential rotation.
- Instrument response metrics. Track mean time to detect (MTTD), mean time to respond (MTTR), percentage of alerts investigated within service levels, and recurrence of the same root cause; review trends monthly.
- Harden alert intake and noise controls. Tune rules to reduce false positives, add suppression for known-good automation, and require justification for any rule disabled longer than a defined window.
- Prepare for evidence handling. Standardize log retention, hashing, and chain-of-custody procedures; predefine export formats for regulators, insurers, and law enforcement.
- Enable containment at the push of a button. Pre-stage capabilities to disable accounts, revoke tokens, quarantine devices with Endpoint Detection and Response (EDR), and block sources at firewalls; require approvals only where risk justifies delay.
- Use early-warning tripwires. Deploy canary accounts, decoy credentials, and honeytokens in sensitive paths; alert immediately on use and link the alert to the relevant runbook.

BONUS SECURITY CONTROL: EDUCATE STAFF

People remain a decisive factor. Phishing creates the opening and password reuse magnifies it. Replace once-a-year lectures with role-specific micro-training, live simulations, and immediate coaching. Pair this with practical guidance on passkeys, MFA prompts, and suspicious login notifications.

Action items — fundamental (implement ASAP)

- Build a year-round program, not a one-off. Establish continuous Security Awareness Training (SAT) with quarterly themes and monthly micro-lessons that take five minutes or less.

- Tailor content by role. Provide scenario-based modules for Finance, Human Resources (HR), IT, and executives; cover real risks they face such as invoice fraud, data handling, and remote admin hygiene.
- Run realistic phishing simulations. Launch quarterly campaigns with varied lures, immediate coaching on click, and required follow-up for repeat offenders; increase difficulty only as performance improves.
- Make reporting frictionless. Add a one-click "Report Phish" button in mail clients, route submissions to your Security Information and Event Management (SIEM), and publicly recognize timely, accurate reports.
- Onboard and re-certify. Require SAT within the first week of employment, then annual re-certification with policy acknowledgments tracked in your Learning Management System (LMS).
- Embed just-in-time prompts. Surface brief reminders when users create weak passwords, share files externally, or request Multi-Factor Authentication (MFA) resets; link to micro-lessons rather than long documents.
- Measure what matters. Track Key Performance Indicators (KPIs) such as phishing failure rate, median time to report, MFA enrollment, policy acknowledgment completion, and reduction in repeat risky behavior.
- Localize and include everyone. Offer training in the languages your teams speak, provide captions and accessible formats, and schedule sessions that work for frontline and shift workers.
- Engage leadership and managers. Have leaders introduce training, share real incident lessons, and include a five-minute security topic in staff meetings each month.
- Refresh content after incidents. Convert recent internal or industry events into anonymized lessons within two weeks so training reflects current tactics and reinforces relevant controls.

ADVICE FOR IMPLEMENTING ACTION ITEMS

SMBs are advised to start with the actions that cut the most risk with the least disruption, then layer in governance and automation where they deliver clear value. This sequencing keeps momentum high, contains change management, and shows measurable progress early.

Large budgets and large teams are not prerequisites for meaningful progress. Clarity of priorities, disciplined sequencing, and visible evidence of control performance matter more. For most SMBs:

- **The highest return comes from identity and remote access first, because that is where attackers begin.**
- **Secrets, privilege, and audit follow, because that is how attackers persist.**
- **Automation, patching, backup, and monitoring then wrap the environment so detection accelerates and recovery is predictable.**

Drilling deeper into the specific action items for each security control, SMBs are advised to:

- **Do the fundamentals across all controls first. This creates a foundation and stops the most common attack paths.**
- **Promote advanced items onto the roadmap. Prioritize by risk, compliance deadlines, and ease of integration with your stack.**
- **Move an advanced item up if there is an active threat, a new regulatory need, or if prerequisites are already met.**

A two-tier plan turns ambition into steady progress. Lock in the fundamentals across every control to create a uniform baseline, then advance along a documented roadmap that balances risk, effort, and dependency. Review results at regular intervals, retire blockers, and promote ready items forward. **The outcome is a defensible program that reduces exposure quickly and matures predictably over time.**

THE FINAL WORD

Cybersecurity for SMBs is not an abstract ideal. It is a set of repeatable habits that protect revenue, customers, and reputation every day. **The ten controls in this white paper, plus the people-focused bonus, translate strategy into execution.**

Security is never finished, but it can be consistent, auditable, and affordable. With the controls outlined here, SMBs strengthen reliability across daily operations, limit exposure to common attack paths, and show that cybersecurity is not only a cost to manage. **It is a business capability that sustains trust and enables growth.**

FROM BASELINE TO EXECUTION

SMBs in search of a direct and proven path from baseline to execution are invited to explore Devolutions' solutions and products, which are designed and priced for SMB realities. Free trials are available of all of the following solutions:

- **Remote Desktop Manager:** Centralize connections and inject vaulted credentials at launch.
- **Devolutions PAM:** Explore purpose-built privileged controls that rotate secrets, enforce check-out with approval, and provide just-in-time elevation.
- **Devolutions Server and Devolutions Hub Business:** Establish your policy backbone (self-hosted or cloud). Establish robust and reliable single sign-on, RBAC, MFA, conditional access, and reporting.
- **Devolutions Gateway:** Broker secure access to internal resources without a VPN, and keep vendor sessions scoped, time-bound, and recorded.
- **Devolutions Starter Pack:** Pilot the full stack with up to five users and no feature limits. Validate workflows from credential injection to session recording and rotation.

Prefer a guided path? Book a live, guided demo or launch a 30–90 day proof of concept with minimal time investment focused on your privileged workflows. Our experts will map roles and systems, configure policies, and show your teams how to measure time to connect, audit readiness, risk reduction, and more.