Devolutions

7 QUICK WINS FOR SMB CYBERSECURITY IN 2025

MARCH 19, 2025

Today's **small and mid-sized businesses (SMBs) are under relentless attack** from hackers who are finding it both practical and profitable to target smaller vs. larger organizations. Consider the following:

- According to a study by Accenture, **43% of all cyberattacks worldwide now target SMBs**.
- A report by IBM and the Ponemon Institute found that the **average data breach cost for SMBs has climbed to $2.98 million per incident**.
- The Devolutions State of IT Security in SMBs in 2023/24 Survey revealed that **78% of SMBs are more concerned about cybersecurity than they were a year ago**, and **69% of SMBs have experienced at least one cyberattack in the last year**.

Indeed, for every data breach in a large enterprise that makes international headlines such as the notorious SolarWinds hack in 2019-2020, there are thousands of cyberattacks carried out against SMBs ranging from costly to outright catastrophic. In fact, **60% of SMBs go out of business within six months** of a data breach.

EFFECTIVE, AFFORDABLE AND MANAGEABLE

This White Paper highlights seven quick wins to **help SMBs strengthen their cybersecurity profile, reduce the size of their attack surface, and lower their chances of being victimized in 2025 and ahead**. What's more, the seven strategies discussed in this White Paper take into consideration that SMBs typically do not have the large cybersecurity budgets or in-house specialized teams found in large enterprises. As such, the advice and recommendations herein are not just very effective, but they are also **highly affordable and easily manageable for SMBs**.

#1

IMPLEMENT PRIVILEGED ACCESS MANAGEMENT (PAM)

PAM refers to a class of solutions that help **secure, control, manage, and monitor privileged access to critical accounts** — a.k.a. "the keys to the kingdom." These accounts can include:

- Domain administrator accounts
- Privileged user accounts
- Local administrator accounts
- Emergency access accounts
- Application accounts
- System accounts
- Domain service accounts

Whenever these types of accounts are accessed, a PAM solution logs the session and tracks the actions performed — and ultimately helps ensure and verify that only authorized users are accessing the right accounts at the right time.

When evaluating and ultimately choosing a PAM solution, SMBs should avoid solutions that offer expensive and complex "bells and whistles," and instead focus on solutions that deliver core features and functionality such as:

- **Versatile account management:** Integrate Active Directory, Entra ID (formerly Azure AD), local SSH users, and databases (MySQL, Oracle, Microsoft SQL).
- **Password rotation and propagation:** Rotate passwords and propagate changes across systems automatically.
- **Granular role-based access controls:** Enforce the Principle of Least Privilege (POLP) effectively by defining roles and associating them with specific access rights and permissions. We look deeper at POLP later in this White Paper.
- **Just-in-time (JIT) elevation:** Grant users temporary elevated permissions within Active Directory or Azure groups for a specific task or time frame.
- **Customizable approval processes:** Regulate access with customizable approval requirements and recipients.

Devolutions PAM is an essential security platform designed to control, monitor, and secure elevated access for users, accounts, processes, and systems. This makes it particularly valuable for SMBs, which typically have smaller cybersecurity budgets and lack in-house resources or specialists compared to large enterprises. Devolutions PAM stands out for being affordable, easy to use, and scalable.

#2

USE A PASSWORD MANAGER TO ENFORCE STRONG PASSWORD POLICIES

According to research by LastPass, **81% of confirmed breaches are due to weak, reused, or stolen passwords**. And speaking of weak passwords: NordPass in collaboration with NordStellar has released the 2024 edition the top 200 most common passwords. Yet again, taking the #1 spot it 123456. In fact, **the vast majority of passwords on the list can be cracked in less than a second**. Naturally, cyber criminals are aware of this enormous vulnerability, and are exploiting it with ease

Despite this threat, many SMBs are not doing enough to establish full password visibility, which is absolutely critical to enforce access rules, monitor compliance, and ensure governance. The Devolutions State of IT Security in SMBs in 2023/24 Survey found that **less than 60% of SMBs are using essential cybersecurity measures such as a password manager solution**.

A robust password management solution gives SMBs full visibility into the password practices of all users. At the same time, the solution makes it easy for users to generate complex and unique passwords that are virtually impossible to crack.

What's more, users are not burdened by having to remember multiple long, difficult passwords. Instead, they conveniently store all of their credentials (along with other sensitive data and corporate secrets such as alarm codes and software license keys) in secure data vaults, which are accessed on an as-needed basis.

SMBs in the market for a password management solution should focus on the following features and capabilities:

- **Enhanced password security:** Create, vault, share and manage passwords — without the risk of data breaches, leaks and hacks.
- **Enterprise-grade protection:** Highly secured with the latest AES 256-bit encryption standards and data security best practices (applicable for SMBs that choose a cloud-based password management solution).
- **Enhanced toolset:** Access easy-to-use tools such as a strong password generator, browser access with automatic credential injection, and password analyzer.
- **Comprehensive reports:** Quickly generate comprehensive reports for compliance, governance and auditing purposes, including activity logs, usage reports, and administration logs.

Devolutions' Hub Business ensures strong password hygiene by providing centralized password management on a highly-secure cloud-based platform. In addition, **Devolutions Hub Business**, uses zero-knowledge encryption, and is built with encryption schemes and algorithms that surpass many other cloud-based password managers. And like all of our solutions, **Devolutions Hub Business** is easily affordable for SMBs that need enterprise-grade password management, yet do not have enterprise-grade cybersecurity budgets.

#3

BUILD YOUR CYBERSECURITY FOUNDATION ON THE PRINCIPLE OF LEAST PRIVILEGE AND ZERO TRUST

The principle of least privilege (POLP) is a policy in which end users are only given the amount of access they need to carry out their jobs. The guiding principle of zero trust is «never trust, always verify.» Every user, device, and application regardless of physical location must be authenticated and authorized before access is granted. Both of these concepts are related, and it could be said that zero trust is a key element of POLP. **They compliment each other to create a strong, reliable cybersecurity foundation**.

To establish and enforce POLP, SMBs should carry out the following activities:

- Make least privilege the default starting point, and add higher-level access as needed through analysis and in consultation with users.
- Communicate the purpose of POLP to all users. Help them understand it is not intended to stifle their productivity, but rather protect the organization.
- If temporary privileged access is required, use one-time-use credentials. These are granted at the last moment, and then revoked immediately after use. This approach (called “privilege bracketing”) can be used for individual users, as well as processes and systems.
- Separate administrator accounts from standard accounts.
- Separate higher-level system functions from lower-level system functions.
- Automatically track all login attempts (including unsuccessful ones) and activity. It is critical to have full visibility and see precisely what users do and when.

- Regularly audit user privileges to ensure that access is appropriate.
- Ensure that a process is in place to remove access for departing employees. A Beyond Identity survey found that 1 in 4 ex-employees said they could still access accounts from past jobs — including former IT staff and managers who had access to privileged accounts.
- Have the option to automatically revoke privileged access in the event of an emergency.

To establish and enforce zero trust, SMBs should carry out the following activities:

- Add prioritized cloud technologies to replace unauthenticated legacy services and systems.
- Design zero trust architecture based on how data moves across the network, and how users and apps access sensitive information.
- Verify trust upon access to any network resource by using multi-factor authentication in real-time.
- Extend identity controls to the endpoint to recognize and validate all devices. Merely verifying users is not enough!
- Organize users by group/role to support device policies. For more insight on implementing Privileged Identity Management (PIM.
- Leverage automatic de-provisioning, along with the capacity to wipe, lock and un-enroll stolen or lost devices.
- Regularly update end user rights based on changes to roles/jobs, as well as changes to prevailing security policies and compliance requirements.

Devolutions' **Remote Desktop Manager** and **Devolutions PAM** enable SMBs to configure and implement granular access controls that support POLP and zero trust. These solutions are easy-to-use, scaleable, affordable, and designed specifically for SMBs that need to establish strong cybersecurity, but without compromising efficiency or productivity.

#4

AUTOMATE THREAT DETECTION WITH AI

AI-driven security tools are a game changer for SMBs, enabling real-time threat detection and response. These tools **minimize manual oversight**, while **enhancing incident detection capabilities**. Some of the most important and impressive applications include:

- **Adaptive learning** that leverages machine learning models to continuously improve threat detection capabilities.
- **Advanced pattern recognition** engines that that analyze vast amounts of data at remarkable speeds to identify attacker patterns and anomalies, including subtle signs of malicious activity.
- **Launching automated responses** to mitigate and contain threats.
- **Using predictive analytics** to proactively detect future threats by analyzing trends and patterns.
- **Reducing the amount false positives** by more accurately assessing and classifying safe vs. malicious activities.

At Devolutions, we're currently working on integrating AI insights into our tools to help SMBs proactively protect their assets without needing a large IT team.

#5

SEND BUSINESS SECRETS THROUGH A SECURE MESSAGING PLATFORM.

For many SMBs, free instant messaging chat apps such as Slack, Microsoft Teams, and Facebook Messenger have become essential communication and collaboration tools. However, many of these apps do not encrypt messages, which means that hackers can covertly intercept them. Eliminating this risk is straightforward: **SMBs should only use an encrypted messaging service for all private, confidential, and sensitive messaging and file transfers.**

SMBs should focus on an encrypted messaging service that aligns with the following:

- **Strong standalone encryption:** The service should use XChaCha20Poly1305 with random nonces. In addition, encryption should run in-browser via a memory-safe Rust program compiled to WASM (WebAssembly). Payloads should also be stored encrypted at rest and in transit with TLS1.2+ through a strong cipher set, and GUID (UUID) v4 should be used for link uniqueness only.
- **Secure file transfer:** The service should make it easy to encrypt and transfer files (including larger files e.g., 10MB in size).
- **Enhanced security:** The service should give senders the option to add an extra security layer with a passphrase. Only those with the passphrase can access your link, protecting it from being re-shared and falling into the wrong hands.
- **User customization:** The service should give senders the option to select the duration of their encrypted message. If the message is not retrieved by the receiver during this period, it should automatically and permanently expires. In addition, recipients should be allowed to delete messages once they are read or no longer needed (senders should have the option to prohibit deletion if they wish).

Devolutions Send checks all of these boxes, and is the safe and smart way for SMBs to share sensitive information and files. **Devolutions Send** is easy-to-use and available as a standalone (web-based) service, as well as integrated into several Devolutions' solutions including **Remote Desktop Manager**, **Devolutions Sever**, **Devolutions Hub Business**, and **Devolutions Workspace**. And budget-conscious SMBs will be happy to learn that using **Devolutions Send** is 100% free!

#6

MAINTAIN SYSTEM UPDATES AND PATCH MANAGEMENT

Unpatched software is like an open door for hackers. A Sophos survey conducted in 2024 revealed that **32% of ransomware attacks targeting respondents in the past year started with an exploited vulnerability**. Overall, **60% of all breaches are attributable to unpatched vulnerabilities**, and **50% of vulnerabilities remain unremediated after 50 days** – giving hackers ample time and opportunity to gain a foothold in their victims' networks.

Multiple tools are available to help SMBs stay on top of system updates and patch management. The simplest tools essentially provide push notifications that a new update or patch is available. This is helpful, but it is important to keep in mind that it is still necessary to manually perform the update or apply the patch. More comprehensive — and not surprisingly, more expensive — tools proactively scan network systems and software to detect updates and patches, and can be configured to automatically download and install them on scheduled days/times.

Devolutions' **Remote Desktop Manager** enables SMBs to track software versions, and automate updates and patches. This proactive approach ensures that the infrastructure stays resilient against the latest exploits.

#7

REGULARLY TRAIN USERS ON CYBERSECURITY

Users either strengthen or undermine cybersecurity. Furthermore, in many cases cybersecurity events are not driven by malicious intent. In fact, Verizon's 2023 Data Breach Investigations Report found that 74% of known data breaches were caused by user error, such as clicking on a phishing link in an email. Simply put: providing users with regularly training on cybersecurity is essential.

There is no definitive list of what should be included in cybersecurity training, since the threat landscape is constantly changing. Generally, at a minimum training should cover the following, whether is it delivered online, in-person, or a combination) :

- Access control
- Bring your own device (BYOD)
- Cloud services
- Data leakage
- Identity theft
- Incident reporting
- Intellectual property

- Malware
- Mobile devices
- Open Wi-Fi risks
- Password management
- Phishing (including the emergence of AI-driven deepfake attacks)
- Physical security
- Privacy
- Protecting payment card data
- Ransomware
- Responsible internet use
- Social engineering
- Social networks
- Traveling securely

Devolutions partners with SMBs to integrate training programs that are tailored to their specific environments, ensuring that the members of their workforce **become active partners in strong, reliable cybersecurity**.

THE BOTTOM LINE

By adopting these low cost, high impact strategies, SMBs can **effectively navigate the evolving threat landscape throughout 2025** and into the future. Remember, cybersecurity doesn't have to be overwhelming — **quick wins like these can make a big difference!**

Want cybersecurity quick wins for your SMB? DEVOLUTIONS CAN HELP!

At Devolutions, we empower SMBs with affordable solutions that simplify complex cybersecurity challenges, and deliver powerful quick wins that drive security, compliance, and productivity across the organization.

Contact Devolutions today at sales@devolutions.net. Free 30-day trials of our solutions are also available.