



# STATE OF IT SECURITY IN SMBs IN 2022-2023



# TABLE OF CONTENTS

|  |    |
|--|----|
| PART 1   | 10 |
| Cybersecurity Threats in SMBs                  |    |
| PART 2   | 17 |
| Privileged Access Management in SMBs           |    |
| PART 3   | 23 |
| IT Security Awareness in SMBs                  |    |
| PART 4   | 30 |
| Remote Access Management in SMBs               |    |
| PART 5   | 35 |
| IT Security Management in SMBs                 |    |
| PART 6   | 43 |
| Recommendations                                |    |
| PART 7   | 76 |
| Profile of Respondents                         |    |
| DEVOLUTIONS HELPING SMBs STAY SAFE AND SUCCEED | 80 |
| OUR SUITE OF SOLUTIONS                         | 81 |
| CONTACT  | 83 |

# EXECUTIVE SUMMARY

Small and mid-sized businesses (SMBs) around the world are emerging from the worst of the pandemic and finding their way forward in the “new normal.” And while much has changed and shifted in the last couple of years, the importance of strong IT security has not diminished. On the contrary, it is even more vital as SMBs rely more on remote workers and cloud-based solutions.

Today, hackers are using advanced methods to infiltrate networks and accounts, so that they can steal data and commit identity theft. In many cases, they are carrying out their illicit aims with alarming ease, and remaining undetected for weeks, months — or even years. In addition to this, SMBs need to defend themselves from internal “rogue” users, as well as users who trigger a data breach due to ignorance or negligence.

**The bottom line? The attack surface is now larger than ever before, the volume and variety of threats is unprecedented, and SMBs need to be proactive instead of reactive when it comes to IT security.**

The average cost of a data breach for organizations of all sizes has climbed to an average of \$4.24M USD per incident, which is the highest amount ever recorded.

[[source](#)]

Focusing exclusively on the impact on SMBs, the financial toll can range from \$120,000 USD to \$1.24 USD million per incident. [[source](#)]

To help SMBs grasp the scope and dynamics of the post-pandemic IT security landscape, for the third consecutive year **Devolutions surveyed executives and decision-makers in SMBs<sup>1</sup>** worldwide across five core topics:

- **Cybersecurity Threats in SMBs**
- **Privileged Access Management in SMBs**
- **IT Security Awareness in SMBs**
- **Remote Access Management in SMBs**
- **IT Security Management in SMBs**

Here are some notable findings of the Devolutions' State of IT Security in SMBs in 2022-2023 survey:



67%

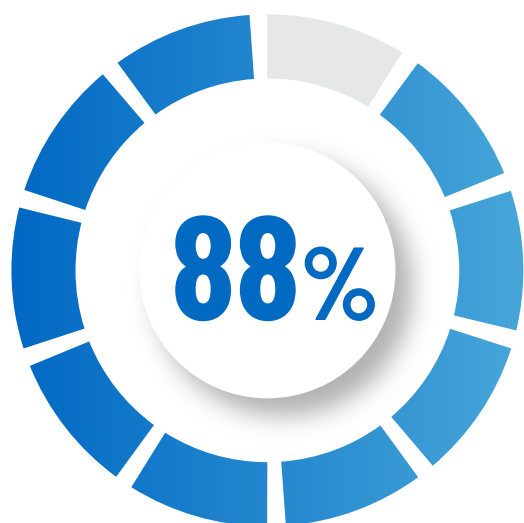
of SMBs **are more concerned about cybersecurity threats** now compared to last year.

<sup>1</sup> Organizations that participated in the survey are those that self-identified as SMBs. This approach reflects the fact that the definition of SMB varies depending on the industry and sector.

# 60%



of SMBs experienced at least one cyberattack in the last year, and **18% of them experienced six or more.**



of SMBs **do not**  
**have a fully-deployed**  
**PAM solution**  
in place.



of SMBs have added  
**staff to take care of IT**  
**security** since the  
pandemic began.



**A virtual private network (VPN) is the most popular tool** that SMBs are using to manage remote access.

Remote work is triggering IT security challenges for SMBs in four key areas: **security, efficiency, governance, and affordability.**

**32% of SMBs are allocating less than 5% of their IT budget to IT security, which is below the recommended minimum amount.**

These are just a few of the many insights that are revealed and explored in this report, which answers critical questions such as:

- What cybersecurity threats are SMBs the most concerned about?
- How are SMBs protecting themselves against hackers and internal threats?
- How do SMBs manage privileged accounts?
- How do SMBs educate end-users about IT security?
- How is the rise of remote working affecting IT security concerns for SMBs?



# RECOMMENDATIONS

This report also explores 10 targeted recommendations to help SMBs reduce cybersecurity threats, strengthen privileged access management, increase IT security awareness, strengthen remote access management, and enhance IT security management.

1

SMBs need to protect themselves against the biggest threats, especially: ransomware, phishing, malware, cloud computing vulnerabilities, and supply chain attacks.

2

SMBs need to implement five core IT security principles: the principle of least privilege (POLP), zero trust, segregation of duties, defense-in-depth, and the four-eyes principle.

3

SMBs need to fully implement a privileged access management (PAM) solution and bridge the gap between authentication and authorization.

4

SMBs need a comprehensive plan to ensure cybersecurity objectives are properly communicated and consistently enforced.

5

SMBs need to provide users with cybersecurity awareness training that focuses on the most fundamental issues, risks, and threats.

6

SMBs without in-house IT security and cloud security expertise should partner with a Managed Service Provider (MSP).

7

SMBs should implement a just-in-time gateway solution to eliminate vulnerabilities caused by virtual private networks (VPNs).

8

SMBs need to address the increased security vulnerabilities caused by remote working.

9

SMBs should focus on getting four core benefits from their remote access tools: improved security, efficiency, governance, and affordability.

10

To get more security budget, IT professionals should focus on five elements: trust, compliance, insurance, employees, and ethics.

The advice and action steps for each recommendation is proven, practical, and affordable for SMBs.



## FROM THE RECOMMENDATION SECTION:

“SMBs need to appreciate that the level of IT security is not only measured by budget, but also by consistency of approach. Otherwise, SMBs can lull themselves into a false sense of safety — which is a sentiment that hackers and rogue end users are ready, willing, and able to exploit.”



## ABOUT THIS REPORT

**In total, 262 respondents answered 24 questions.** All answers, along with insights, commentary, sources of further information, and targeted recommendations are presented in the remainder of this report.

# PART 1

## CYBERSECURITY THREATS IN SMBs

Stating that IT security is important is hardly insightful or original. However, what is new and notable is how frequent, severe, sophisticated, and costly IT threats — which include cybersecurity threats — have become.

Indeed, long gone are the days when only government agencies and big enterprises had to worry about “script kiddies” aiming to destroy machines and wreak havoc. Today’s hackers are sophisticated, well-connected, and seem to have an endless pool of resources. Their goal is to commit identity theft and generate financial gain — and some of them are remarkably successful.

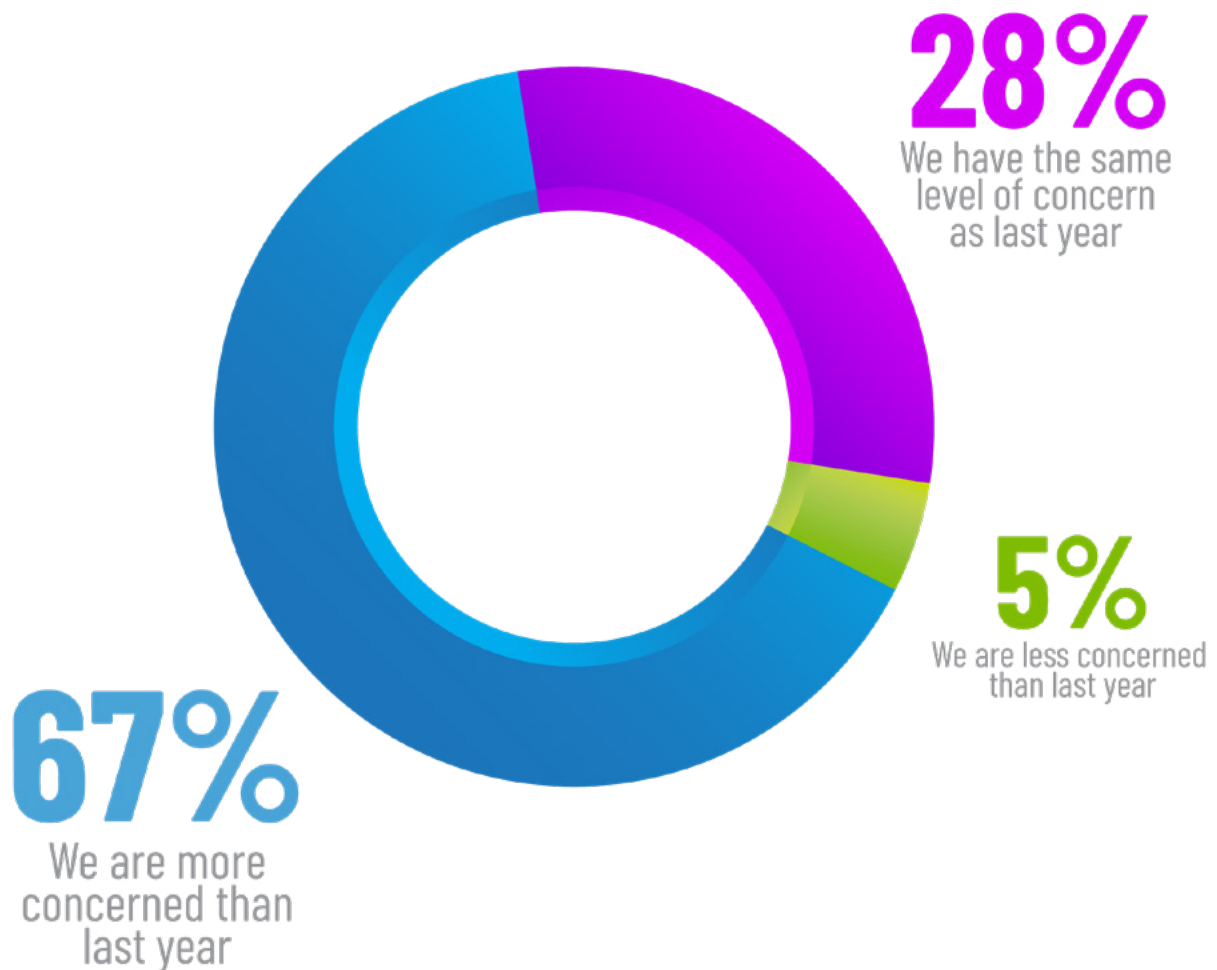
What’s more, they are not limiting their attacks to large organizations. Increasingly, they are targeting SMBs and exploiting vulnerable IT security defenses; especially those related to remote workers. Given the potentially catastrophic impact of just a single breach, it should be clear to all SMBs that paying attention to IT security is not just “yet another technology matter.” It is a fundamental business priority.

## QUESTIONS

In the Devolutions’ State of IT Security in SMBs in 2022-23 survey, we asked executives and decision-makers in SMBs worldwide to describe their overall perspective on IT security, including: what they have experienced in the last year, what concerns them the most today, and what they are doing to protect themselves.

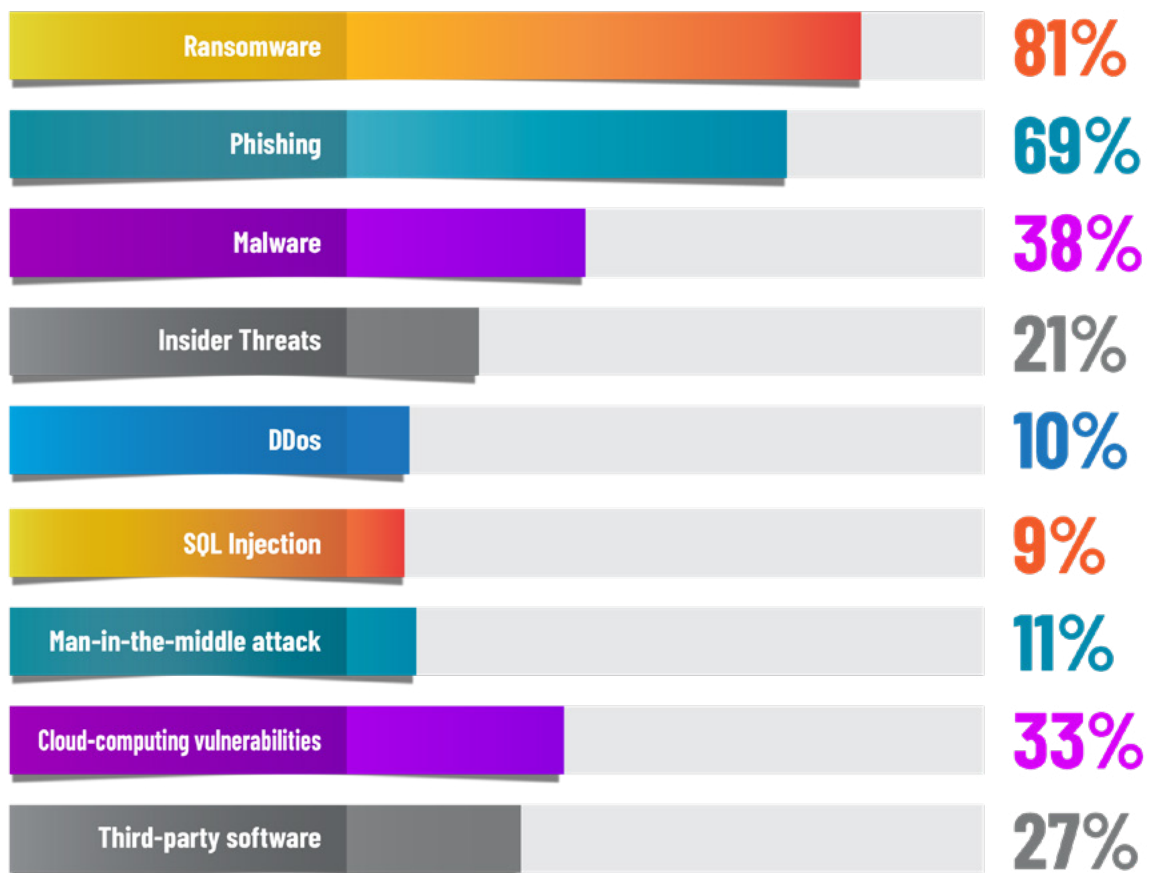
# QUESTION 1

Compared to last year, how concerned are you about cybersecurity threats toward your organization?



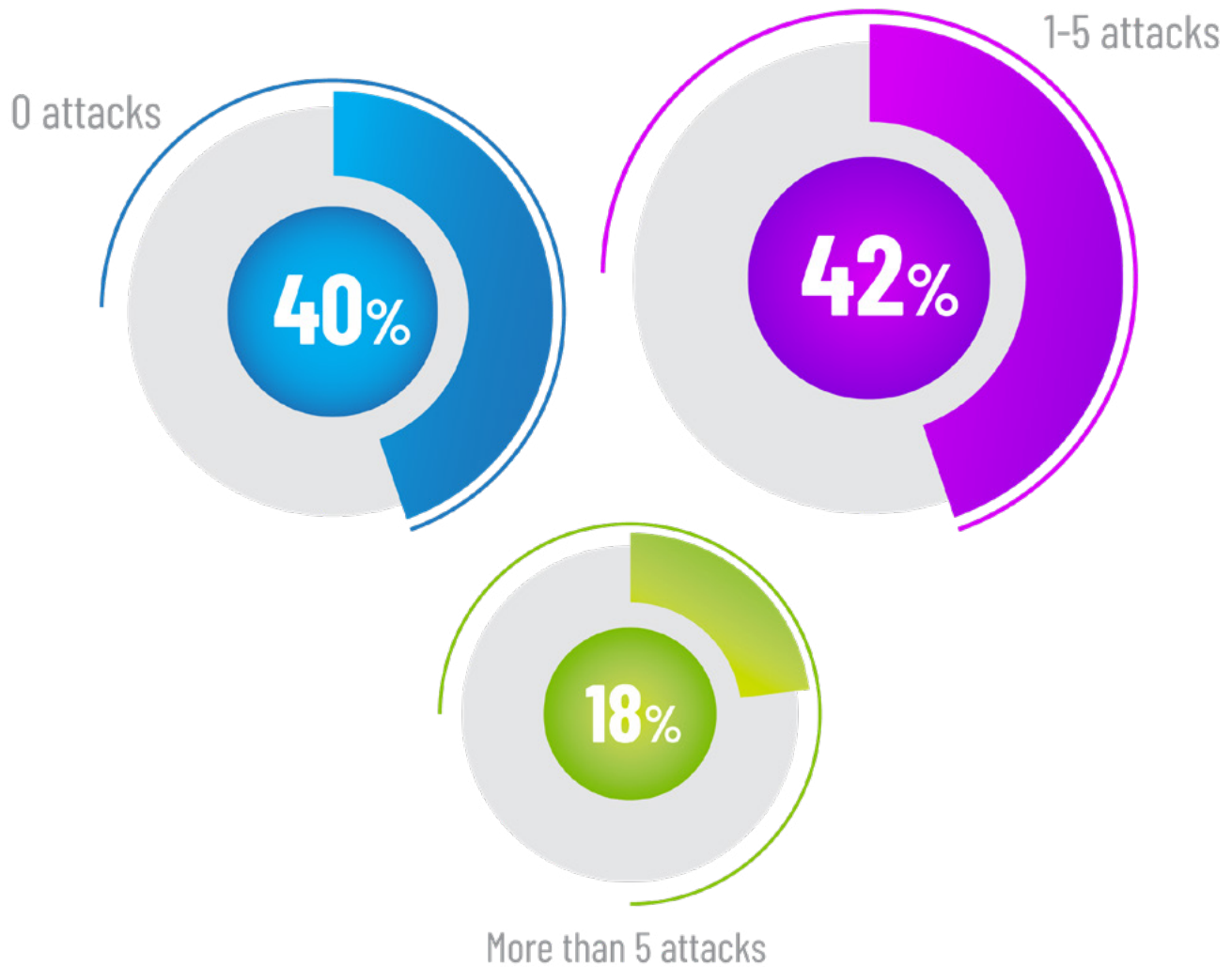
# QUESTION 2

Please select the 3 cybersecurity threats you are most concerned about:



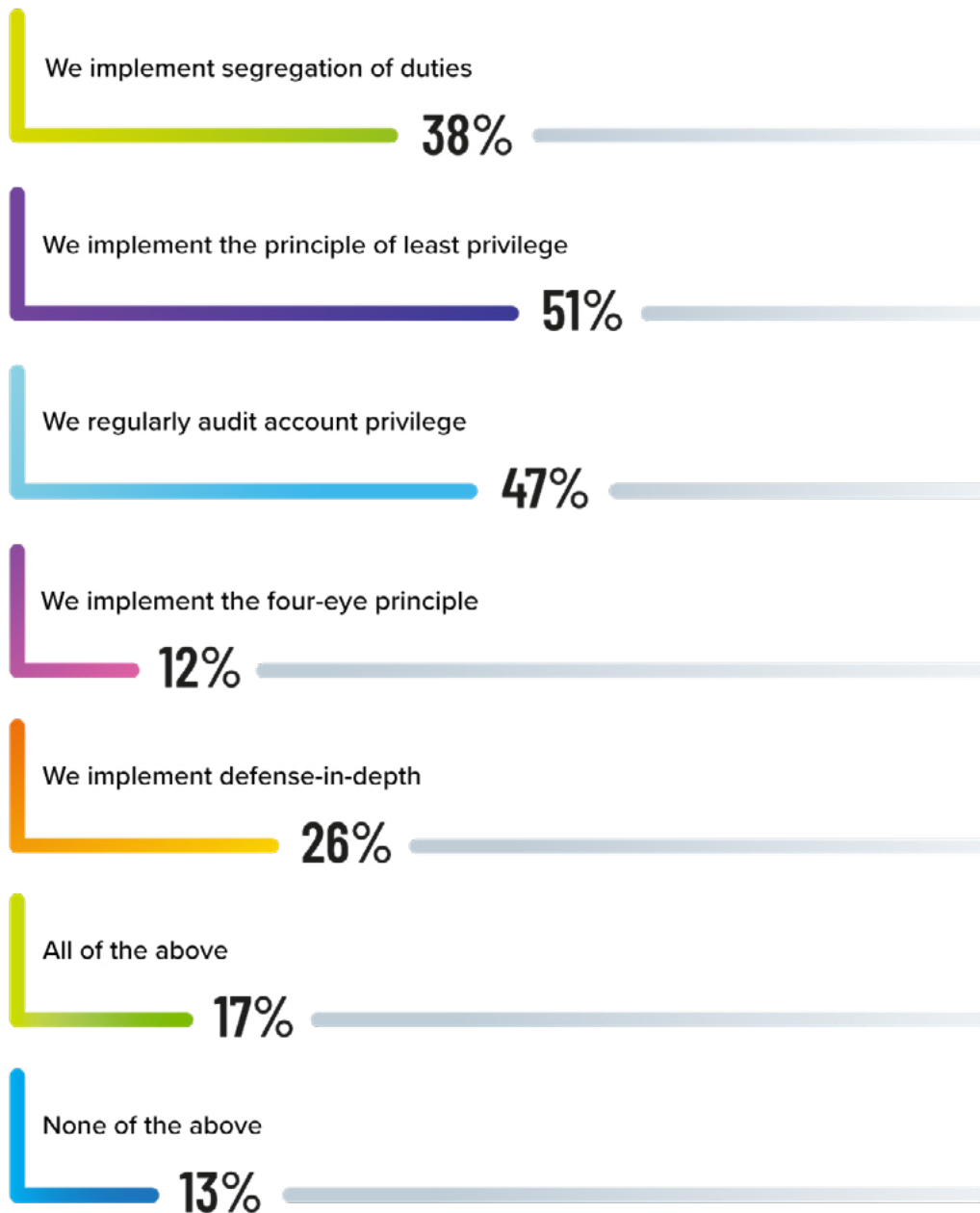
# QUESTION 3

In the last year, how many cybersecurity attacks has your organization faced?



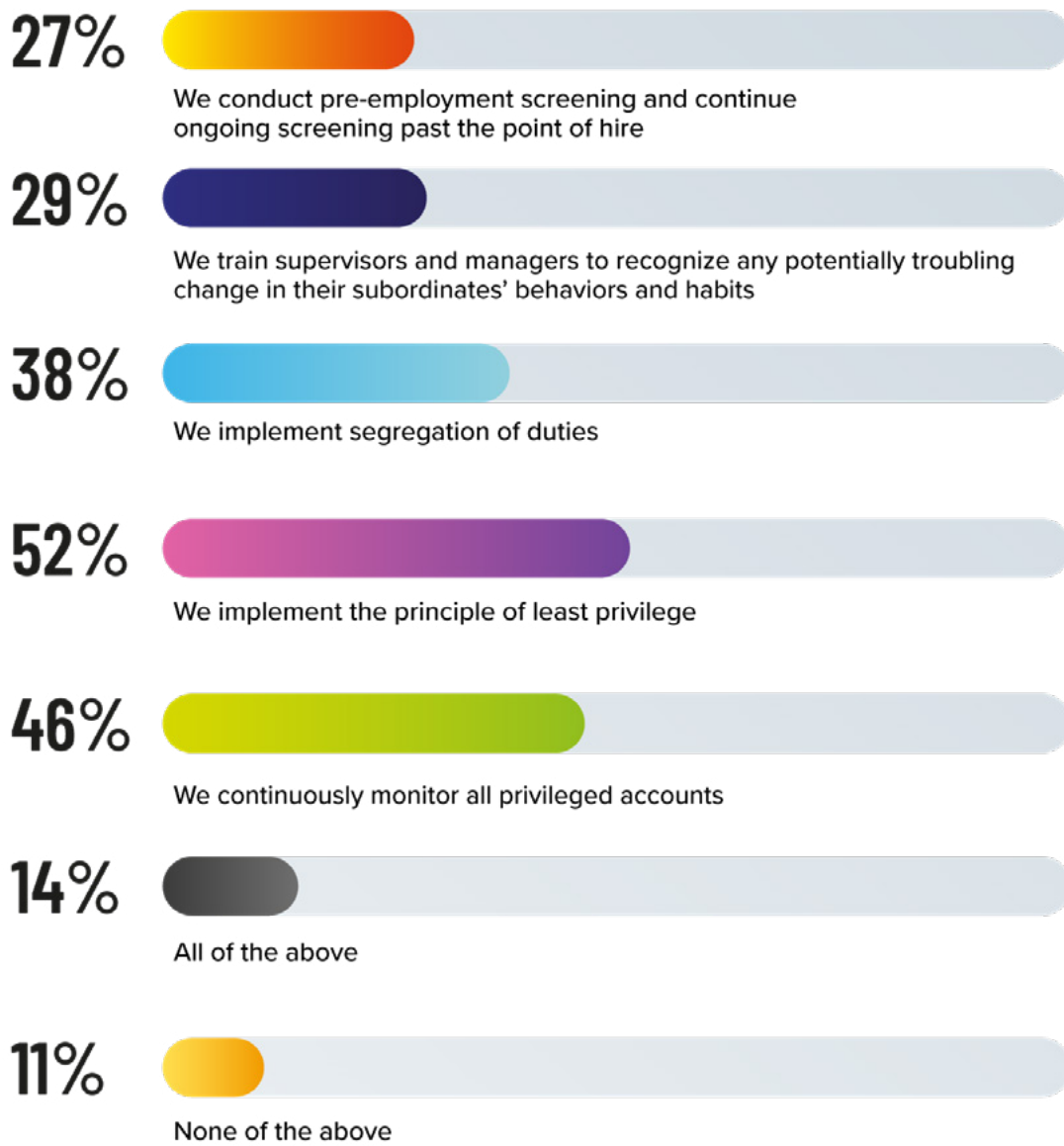
# QUESTION 4

What measures do you have in place to prevent cyberattacks or data breaches from hackers?  
Please select all that apply:



# QUESTION 5

What measures do you have in place to prevent insider threats? Please select all that apply:



# COMMENTARY

Two-thirds (67%) of SMBs said that they are more concerned about IT security this year compared to a year ago. This is 5% lower than the 2021-22 survey. However, the slight dip in anxiety levels is likely because many remote workers over the past year have been called back into the office (full-time and hybrid), which is enabling SMBs to tighten some security controls and governance practices.

SMBs also said that their top three cybersecurity concerns at this time are ransomware (81%), phishing (69%), and malware (38%). All these concerns are valid — especially phishing, which is exploding both in prevalence and cost. Yet, only 27% of SMBs rated third-party software in their top three cybersecurity concerns, which suggests that it is not viewed as a primary threat at this time. However, it should be: [Gartner](#) predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021. And although it happened in 2020, the long, dark shadow of the [SolarWinds/Solarigate supply chain attack](#) — which is still hailed as the most sophisticated hack ever — has not faded. It continues to inspire hackers to develop tools to exploit this threat vector.

The survey also found that 60% of SMBs experienced at least one cyberattack in the last year, and 18% of these experienced six or more. These numbers — which may in reality be higher, given that not all cyberattacks are registered (including those that are in-progress) — further emphasize that SMBs literally cannot afford to take IT security and cybersecurity lightly. The average cost of a data breach for organizations of all sizes has climbed to an average of [\\$4.24M USD per incident](#), which is the highest amount ever recorded. And focusing exclusively on the impact on SMBs, the financial toll can range from [\\$120,000 USD to \\$1.24 million USD per incident](#) (depending on a variety of factors such as the number of compromised records involved).

Given the severe — and potentially catastrophic — consequences of a single data breach, it might seem safe to assume that, at the very least, all SMBs are implementing what are now considered fundamental, basic IT security measures including: segregation of duties, principle of least privilege, regularly auditing account privilege, the four-eye principle, and defense-in-depth. However, this is not the case: the survey found that only 18% of SMBs can check all of these boxes. And of even greater concern, 13% of SMBs do not implement any of these essential measures!

---

**In the Recommendations Section of this report, we take a closer look at measures that help SMBs protect themselves on an increasingly dangerous threat landscape — including breaches that are carried out by internal rogue users.**



# PART 2

## PRIVILEGED ACCESS MANAGEMENT IN SMBs

Privileged access refers to an entity — human or nonhuman (machine/application) — that uses an administrative account, or a credential with elevated rights, in order to perform maintenance, make changes, or carry out any other type of privileged operation.

Privileged accounts are referred to as “the keys to the kingdom,” because they typically govern access to highly valuable, confidential, and proprietary information that is often targeted by hackers and rogue users.

In addition, privileged accounts and credentials typically exist all over the place: [17% of companies](#) make sensitive files available to every employee, and [60% of companies](#) have more than 500 accounts with non-expiring passwords.

SMBs that prioritize privileged access management (PAM) as part of their overall IT security program benefit in several ways, including:

- Reducing security risks
- Shrinking the overall size of the attack surface
- Lowering operational costs and complexity
- Increasing visibility and situational awareness
- Improving regulatory compliance

Furthermore, a growing number of insurance carriers that offer cybersecurity policies are insisting that customers have a robust PAM solution in place as a prerequisite for coverage.

## QUESTIONS

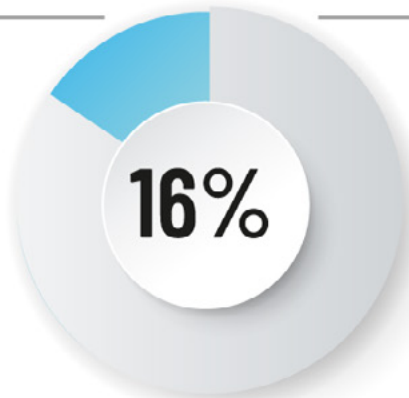
In the Devolutions’ State of IT Security in SMBs in 2022-23 survey, we asked executives and decision-makers in SMBs worldwide to describe how they are approaching, handling, and experiencing privileged access management in their company.

# QUESTION 6

How do you primarily manage access to privileged accounts in your company?



We use a directory service  
(e.g., Azure, Active Directory, etc.)



We use a password manager

**12%**

We have a PAM solution,  
and it is fully deployed

**9%**

We have a PAM solution, and it is  
partially deployed (i.e., we are using  
some of the features/functions,  
but not all of them currently)

**3%**

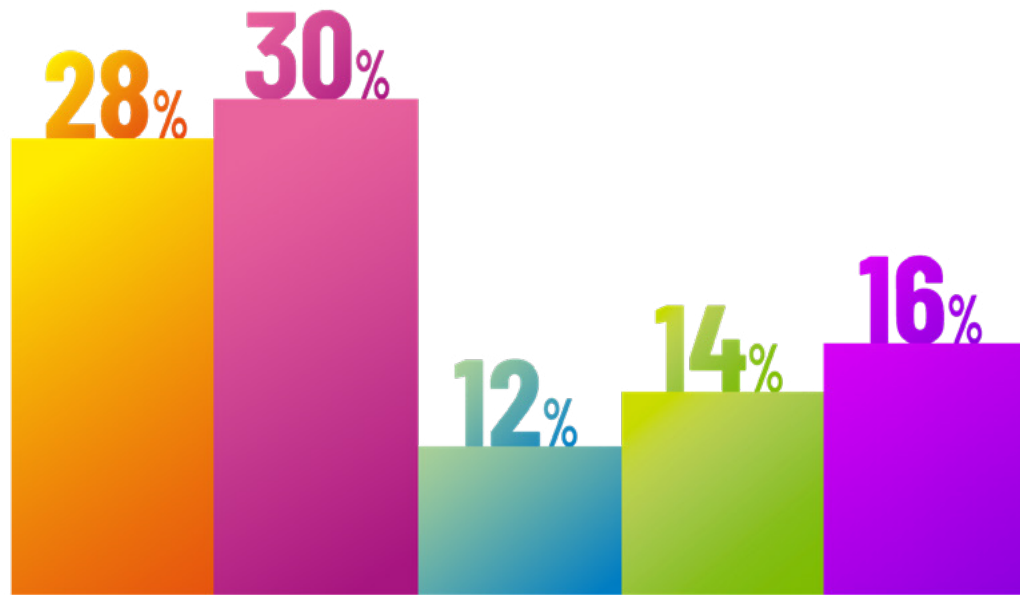
We use endpoint operating  
systems tools

**2%**

We are not managing access  
to privileged accounts

# QUESTION 7

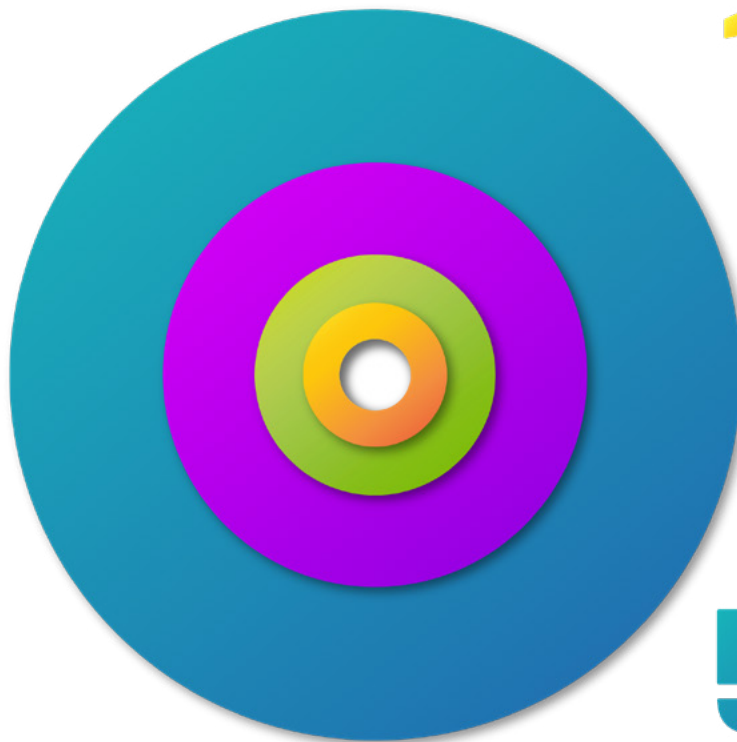
If your organization does not have a fully deployed PAM solution in place, what is the main reason why?



- We do not have the budget
- Our existing access and password management tools are sufficient
- PAM is too complex to implement and manage
- At this time, no PAM solution that we have evaluated has met our requirements
- Other (the 5 most popular “other” responses are listed below)
  - We are in the process of migrating to a new PAM solution.
  - While implementing a PAM solution is a goal of ours, it is not a critical priority at this time.
  - There is a lack of management focus and buy-in regarding PAM/PAM solution.
  - It is not the right time for our business to implement a PAM solution.
  - We use our client’s PAM solution to access privileged accounts.

# QUESTION 8

Have PAM controls affected the velocity and productivity of work in your organization?



11%

Yes: the impact has been negative, and it is taking longer and/or is more complicated to access certain resources

15%

Yes: the impact has been positive - our approval workflow is better, and we improved productivity

22%

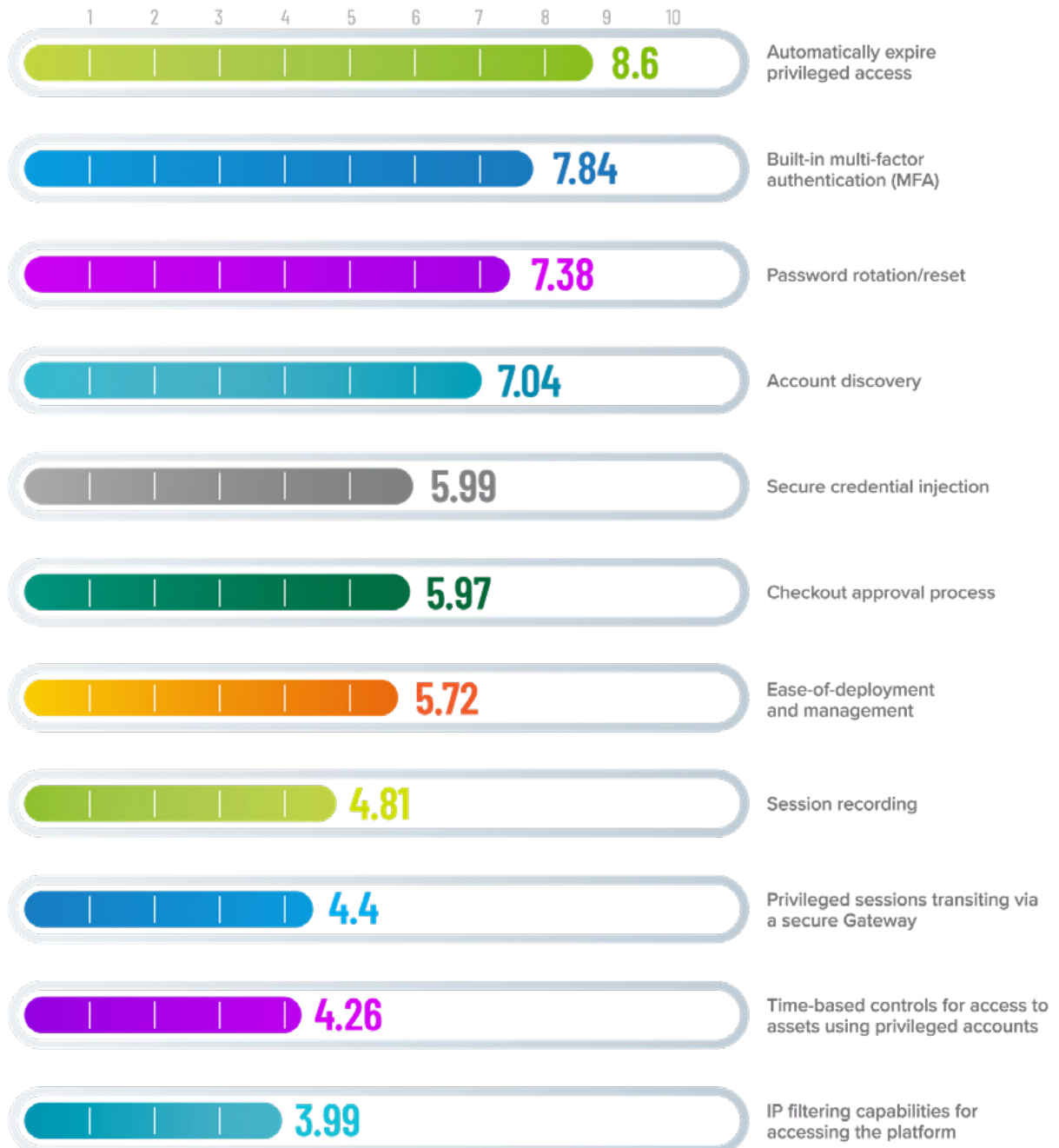
No: we have not experienced any impact (positive or negative)

52%

We have not yet implemented PAM controls

# QUESTION 9

Please rank the following features and capabilities of a PAM solution from the most important (1) to the least important (11) based on your organization's IT security strategy:



# COMMENTARY

We start the PAM story in SMBs with some good news, and some bad news. The good news is that only 2% of SMBs are not managing access to privileged accounts. This is a 5% drop from the 2021-22 Survey, and the improvement is a cause for cautious optimism.

Why “cautious”? Because of the bad news: only 12% of SMBs have a fully deployed PAM solution in place. This is 1% fewer than last year, and frankly it is 88% lower than it should be. Just as SMBs would not leave their office doors unlocked during non-business hours, they should not operate without a robust, comprehensive PAM solution. Indeed, a breach can be far costlier than a burglary!

What is blocking SMBs from putting a fully deployed PAM solution in place? The survey found that 28% do not have the budget, and 12% think that PAM is too complex to implement and manage. Both of these perceptions are understandable, yet outdated. Granted, for many years comprehensive PAM solutions were priced for large organizations and enterprises — which meant that most SMBs could not afford them. What’s more, SMBs could not afford a team of in-house cybersecurity specialists to configure, use, and continuously update the solution. Thankfully, things have changed for the better!

Affordable and easy-to-use PAM solutions are now available for SMBs that need the same comprehensive privileged account governance as large organizations and enterprises. The rallying cry for this long overdue democratization in the global PAM marketplace is called [“PAM for the rest of us!”](#)

Still, some SMBs are reluctant to fully deploy a PAM solution, because they fear that doing so will reduce efficiency and productivity. However, the survey found that 15% of SMBs credit PAM controls for enhancing their approval workflow, improving productivity, and overall accelerating the velocity of work. A further 22% of SMBs did not register any post-PAM negative or positive impact, while 11% said that they experienced some drawbacks. However, this is likely because (as noted earlier) their PAM solution is needlessly complicated, and not designed for the requirements of SMBs.

The survey also revealed that slightly more than half of SMBs (52%) have not yet implemented PAM controls. The only people happy about this are hackers and rogue users. And since neither of these groups are part of any SMB’s target market, SMBs should make implementing PAM controls a top priority.

And to wrap things up, the three most important features that SMBs want in a PAM solution are: automatically expiring privileged access, built-in MFA, and password rotation reset. Not surprisingly, all these features are rooted in automation, which is crucial for SMBs that need to boost efficiency and productivity in an affordable manner.

---

**In the Recommendations Section of this report, we take a closer look at what features and functions SMBs should look for in a PAM solution.**

# PART 3

## IT SECURITY AWARENESS IN SMBs

It is widely understood that despite the ongoing threats posed by hackers and rogue insiders, negligent end users have always been — and unfortunately, will always be — the weakest link in the IT security chain.

Indeed, whether they are clicking on suspicious links, carelessly sharing passwords, accessing networks through insecure public Wi-Fi connections — and the list of security transgressions goes on — end users can trigger costly data breaches and leaks.

And the story gets worse: negligent end users are not the only culprits behind preventable IT security incidents. [Research](#) has found that a whopping 60% of organizations that experience a data breach put the blame on a known vulnerability that they had not yet patched. And separate [research](#) has found that two-thirds of IT decision-makers do not believe that their IT Operations teams and IT Security teams work in a cohesive manner to secure the organization against internal and external threats and risks.

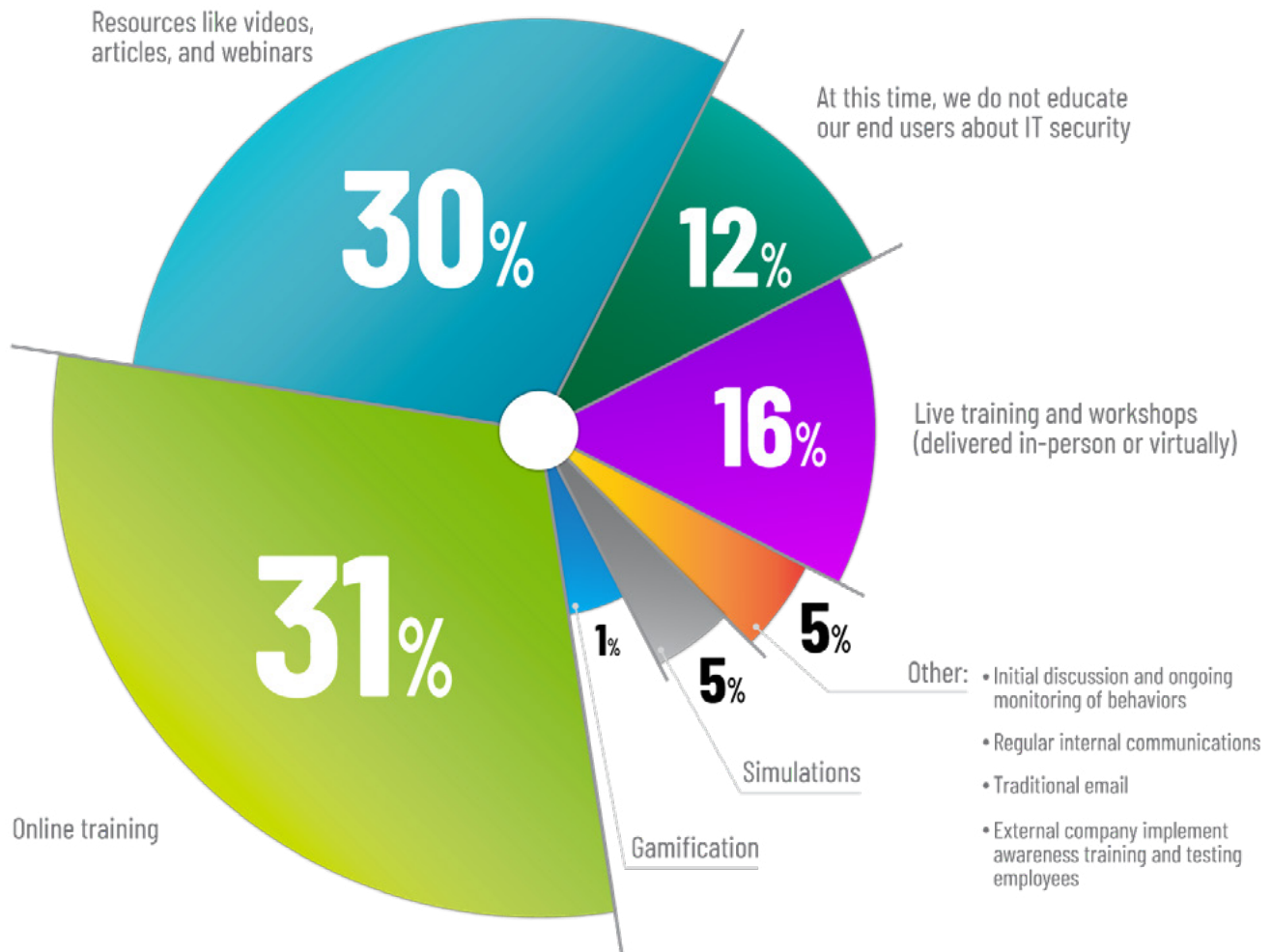
It is crucial to ensure that everyone in the organization — from end users to IT professionals to leadership — plays an active role in strengthening IT security. Otherwise, they will unwittingly but invariably increase the risk.

## QUESTIONS

In the Devolutions' State of IT Security in SMBs in 2022-23 survey, we asked executives and decision-makers in SMBs worldwide to share how they are prioritizing, implementing, and measuring efforts to improve IT security awareness in their companies.

# QUESTION 10

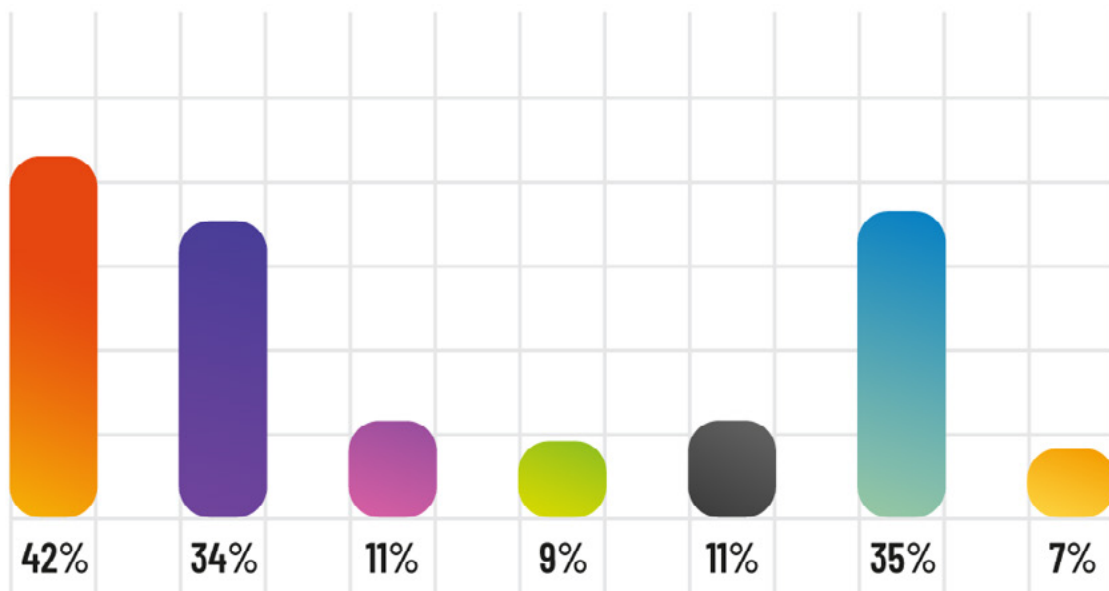
How does your company primarily educate end users about IT security?





# QUESTION 11

How is your company measuring the impact of IT security training?



- Monitoring training results and risk scores over time
- Conducting end-user perception and knowledge assessments
- Comparing results to industry peers
- Saved time on security incidents
- Reduced cost on security incidents
- At this time, we do not measure impact
- None of the above

# QUESTION 12

Does your organization have a comprehensive and updated cybersecurity incident reporting response plan in place?



Yes  
**56%**



No  
**44%**

# QUESTION 13

Since the pandemic began in early 2020, have you added staff to take care of IT security?

36%

Yes, we have added one or more employees to address our IT security needs

8%

Yes, we are working with an external vendor to address our IT security needs

56%

No, we have not hired additional employees to address our IT security needs

# COMMENTARY

We begin on a positive note: 88% of SMBs are providing some form of IT security education to their end users. This is a 14% jump compared to last year's survey, and suggests that more executives and decision-makers are realizing that investing in good IT security hygiene is not just a technical matter: given the potentially enormous consequences and costs of breaches and leaks, it is a fundamental business priority.

It is also interesting to see that online training has emerged as the number one option (31%) in SMBs for educating end users about IT security. This trend is likely driven by two complimentary factors:

- SMBs may be required to offer formal vs. *ad hoc* IT security training for end users, in order to meet the training requirements imposed by third parties such as compliance programs (e.g. SOC 2, ISO/IEC 27001:2013, etc.), customer contracts, and cybersecurity insurance policies.
- Online training features dashboards and reports that make it easy for managers to track end user activity and performance. Instead of guessing and hoping that end users are making progress, managers can clearly see who is moving ahead and who needs additional coaching — or, in some cases, stern warnings.

Unfortunately, the situation is not entirely positive: 35% of SMBs do not measure the impact of IT security training on end users. Assuming rather than knowing that end users are trained and compliant is unwise. For example, in a phishing simulation to verify IT security awareness, [39% of end users](#) — including some that had access to privileged accounts — simply gave away their password!

The survey also revealed that 44% of SMBs do not have a comprehensive and updated cybersecurity incident response plan in place. This is 4% more than last year, which is concerning given that the risks and potential consequences are increasing vs. decreasing. What could be behind this worrisome trend?

The most likely reason is that SMBs are still reeling from the unprecedented disruption of the pandemic and have not had the opportunity to focus on this. However, SMBs that continue to overlook this priority are, as the old saying goes, “playing with fire.” By some counts, hackers carry out an [estimated 2,200 cyberattacks per day](#) — or one every 39 seconds. It only takes a single cyberattack to realize how invaluable a comprehensive and updated incident response plan is (for those that have one!), or would have been (for those that don't!).

Lastly, the survey found that 36% of SMBs have added staff to take care of IT security since the pandemic began, and 8% are working with an external vendor such as a Managed Service Provider (MSP). We anticipate that the volume of SMBs partnering with MSPs will increase for two reasons:

- The widespread IT security skills shortage is getting worse. In fact, there will be an estimated [3.5 million IT security jobs unfilled worldwide by 2025](#) — up from one million in 2014. And while remote work is enabling SMBs to find experienced professionals outside of their local geographic labor market, the price for these skilled individuals is surging. While the exact cost varies based on multiple factors, it is not uncommon for IT security professionals to make twice the median income of all other workers. The bottom line for many SMBs is partnering with an MSP is the only affordable way to maintain a strong and compliant IT security profile.
- MSPs that traditionally focused on serving large and mid-sized organizations, are realizing that SMBs are an untapped and lucrative market. There are approximately [400 million SMBs worldwide](#) — and the vast majority of them do not have sufficient IT security.

---

**In the Recommendations Section of this report,** we highlight best practices for SMBs to prepare, communicate, and update their comprehensive incident response plan. We also look at core topics that should be included in IT security awareness training, and explore what SMBs should look for when choosing an MSP.

# PART 4

## REMOTE ACCESS MANAGEMENT IN SMBs

In order to connect to remote systems and perform various management tasks, IT professionals often require administrative credentials. While this method is expedient and convenient, it also poses security risks. If a privileged account is abused or compromised in any way, the result could be a costly breach.

Hackers use multiple methods to steal privileged account credentials. Two of the most common are snooping on insecure remote connections and deploying malware on end-user devices. And speaking of end users: many of them — including some [high-ranking executives](#) and [IT professionals](#) — still use the same password across multiple accounts, which makes things even easier for hackers and worse for their victims.

Plus, no discussion of remote access management would be complete without referencing the biggest global event in generations: the COVID-19 pandemic. In the last couple of years, the number of SMBs using remote access tools has skyrocketed to accommodate remote workers and/or clients. Unfortunately, this has also greatly expanded the size of the attack surface and provided hackers with more threat vectors to exploit.

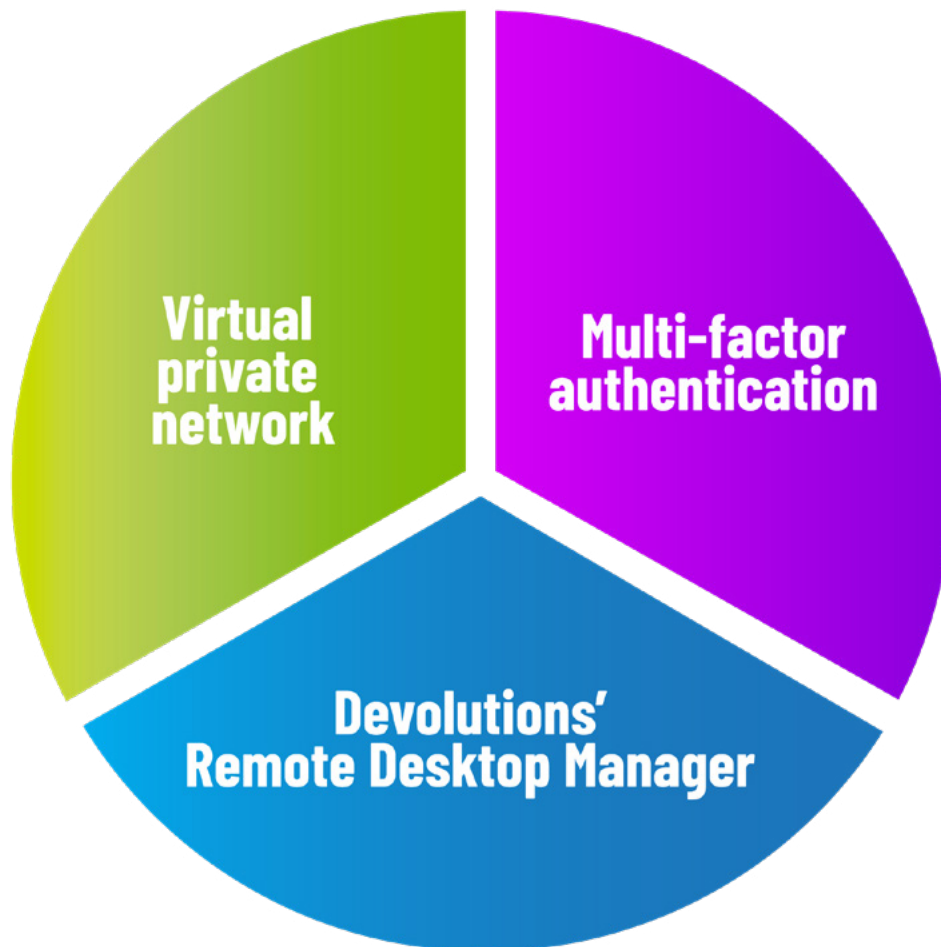
## QUESTIONS

In the Devolutions' State of IT Security in SMBs in 2022-23 survey, we asked executives and decision-makers in SMBs worldwide to describe how they are managing remote access, and to share some of the IT security challenges and concerns they face due to remote access.

# QUESTION 14

What IT security tools and technologies is your organization currently using to manage remote access?

By a significant margin, the three most popular responses were:



# QUESTION 15

What is your organization's employee deployment situation right now?



75%

We are allowing some/all employees to work hybrid (both corporate office and home)



19%

All of our employees are working in the office full-time



6%

We are totally remote



# QUESTION 16

Remote working has significantly increased in the last few years. In your organization, please share the IT security challenges that remote work is creating or driving.

We received many responses, which we have grouped in the following four main categories:

|                               |  |
|-------------------------------|--|
| <b>SECURITY CHALLENGES:</b>   | Controlling vulnerabilities caused by remote workers using personal devices.   |
| <b>EFFICIENCY CHALLENGES:</b> | Dealing with the additional workload burden on IT staff who are responsible for monitoring network traffic, and improving IT security without reducing remote worker efficiency. |
| <b>GOVERNANCE CHALLENGES:</b> | Difficulty distributing policies and updates to all workers and customers/clients, and governing external suppliers accessing the network with their own equipment.              |
| <b>COST CHALLENGES:</b>       | Dealing with increased infrastructure costs of ensuring remote worker security.  |

# COMMENTARY

A virtual private network (VPN) is the most popular tool that SMBs are using to manage remote access. The pandemic dramatically accelerated VPN usage worldwide, with especially high implementation in countries that recorded a [high number of COVID-19 cases](#). However, while VPNs can help reduce risks, they can also pose drawbacks for SMBs regarding deployment, management, and security. We explore these problems and provide solutions in the recommendation section of this report.

The survey also found that the vast majority of SMBs are using multi-factor authentication (MFA) as an extra layer of security. Remote workers must verify their identity by providing their login credential, along with another piece of information that could be:

- Something known (answer to a secret question, PIN, or password).
- Something owned (smartphone or a token).
- Something biometric (fingerprint, voice recognition, or eye scan).

The idea is that even if a remote worker's login credentials are stolen, it is less likely (though not impossible) that hackers will be able to supply the additional information and gain unauthorized access to a device, application, network, or system.

In addition, many SMBs are using Devolutions' Remote Desktop Manager<sup>2</sup> to manage remote access. By centralizing all passwords and enterprise data in one secure location, IT professionals can quickly access the information they need, when they need it, while also keeping remote sessions secure.

With regards to the current employee deployment situation, 75% of SMBs are allowing some or all employees to work hybrid, while 6% now have a completely remote workforce. While there are several significant advantages to remote work — most notably cost-savings for employers and convenience for employees — this approach greatly expands the size of the attack surface. SMBs need to proactively address these vulnerabilities to ensure that remote work is safe and compliant.

Finally, we asked executives and decision-makers to share the IT security challenges that remote work is creating or driving in their company. Most responses related to four types of challenges: security, efficiency, governance, and affordability. The valuable and practical insight here is that when evaluating (and ultimately choosing) tools for managing remote access, SMBs must ensure that all four of these boxes are checked. In other words, any potential remote access tool must significantly improve security, efficiency, and governance, while being affordable. If any of these core aspects are overlooked, then SMBs will face unexpected gaps, problems, and obstacles.

---

**In the Recommendations Section of this report, we explore why SMBs should implement a just-in-time Gateway solution to eliminate problems and issues caused by VPNs. We also highlight practical and effective approaches to address security vulnerabilities triggered by remote workers, and provide a checklist to help SMBs get four core benefits from their remote access tools: improved security, efficiency, governance, and affordability.**

<sup>2</sup>By way of transparency and to verify the integrity of the survey, we wish to point out that we did NOT include "Devolutions' Remote Desktop Manager" as a potential response to question #14. This was an open-ended/fill-in-the-blank type of question, and participants were invited to submit any response that they wished. The fact that Remote Desktop Manager was among the most popular responses was entirely driven by participants and not in any way directly or indirectly influenced by us.

# PART 5

## IT SECURITY MANAGEMENT IN SMBs

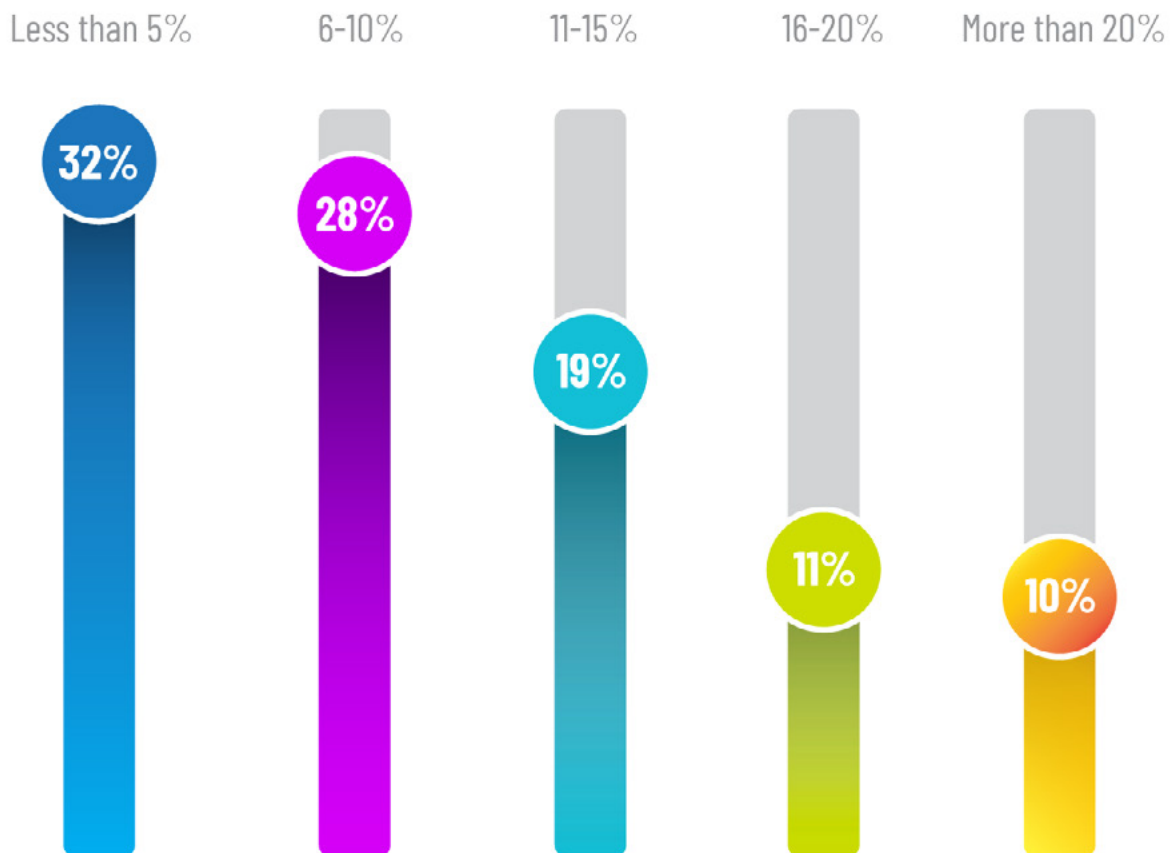
IT security management consists of strategies, policies, processes, technologies, and tools that ensure the confidentiality, protection, integrity, and availability of IT systems. In many SMBs, IT security and cybersecurity are managed by the same team. And even when they are managed by separate departments, it is common for IT security professionals and cybersecurity professionals to work closely and collaboratively on establishing, enforcing, and evolving robust security across the organization — which is an ongoing commitment and not a one-time objective.

### QUESTIONS

In the Devolutions' State of IT Security in SMBs in 2022-23 survey, we asked executives and decision-makers in SMBs worldwide to share their experiences and expectations in IT security management, with a focus on spending and planning.

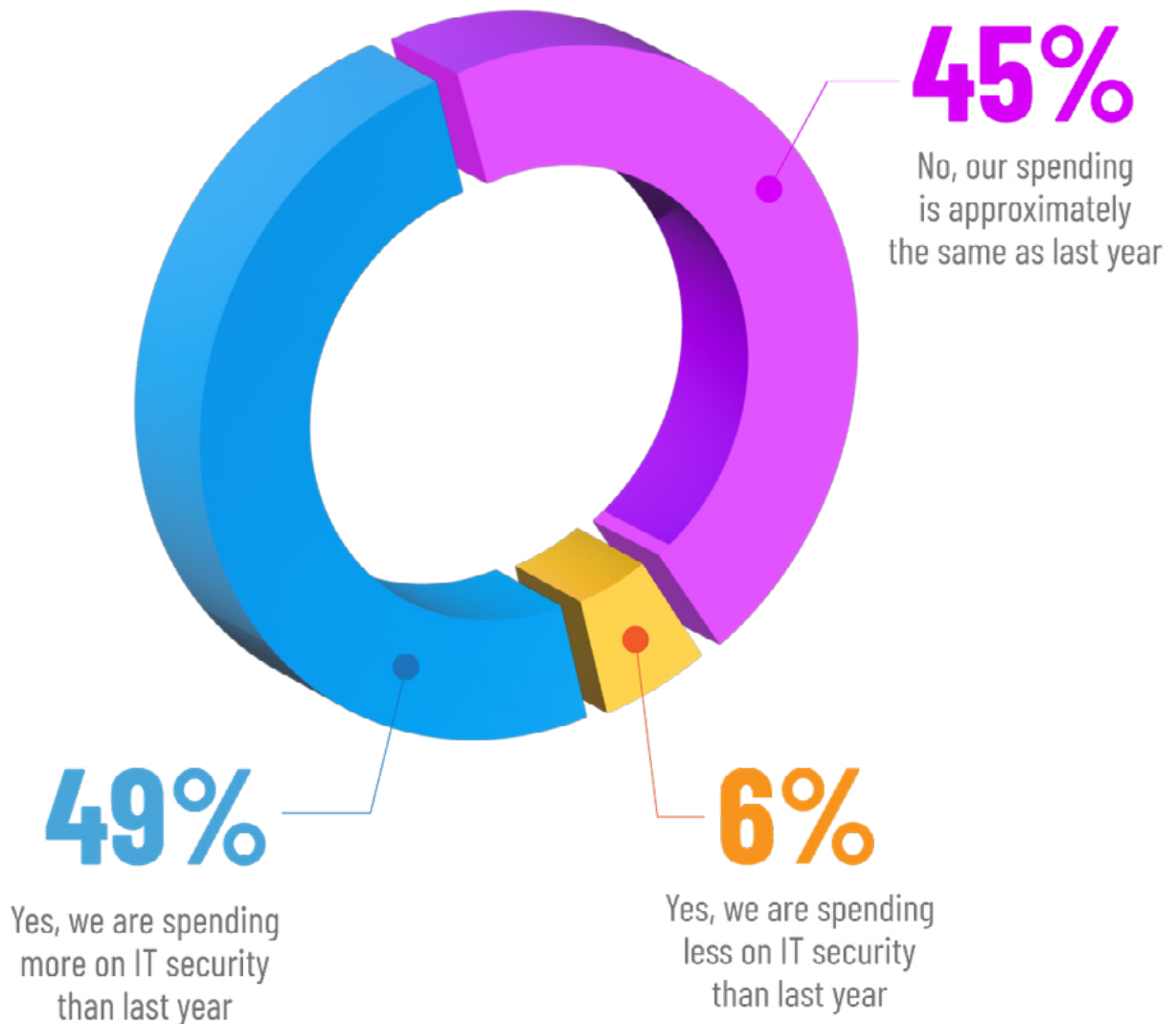
# QUESTION 17

Of your organization's overall IT budget, how much is allocated for IT security (e.g., technology, training, etc.)?



# QUESTION 18

In the last year, has your total overall spending on IT security changed?



# QUESTION 19

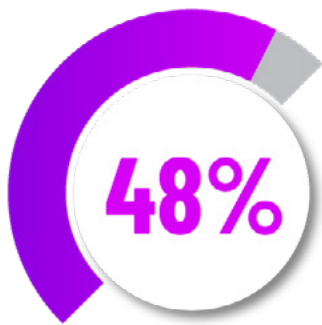
In the next 12 months, do you anticipate that your overall spending on IT security will change?



**Yes**, we plan on spending **more** on IT security in the next 12 months



**Yes**, we plan on spending **less** on IT security in the next 12 months



**No**, we plan on spending **approximately the same** on IT security in the next 12 months

# QUESTION 20

What IT security projects do you plan on exploring and potentially implementing in the next 12 months?

The top 18 IT security projects are listed below (in order of popularity):

- Implementing a PAM solution
- Introducing or fully-integrating 2FA
- Providing (directly or through a third-party) end user training
- Updating VPN strategies
- Implementing automatic password rotation
- Expanding a password management tool for use by all employees (not just IT staff)
- Hardening email security
- Hardening Active Directory
- Adding cybersecurity insurance
- Implementing more granular and just-in-time access to resources
- Moving data backups to the cloud
- Conducting penetration testing and red teaming
- Getting vendors to conduct in-depth, objective vulnerability assessments
- Implementing a SIEM solution
- Establishing a SOC solution
- Shifting to a passwordless authentication
- Expanding security team with experienced and certified members
- Segregating network infrastructure

# COMMENTARY

When it comes to spending on IT security, how much is the “right” amount? There is no specific, standard number. SMBs have different dynamics and face various risks and challenges regarding:

- **The size, depth, and details of their attack surface.**
- **The type of data they store, share, and transmit.**
- **The threats they face now, and the threats they are likely to face in the future.**
- **Various compliance and regulation standards they must meet.**
- **The availability and cost of qualified IT security specialists.**

All of these factors could mean that SMB #1 may need to spend X amount on IT security, while SMB #2 may need to spend less or more than X amount. Again, there is no definitive price tag. Optimal spending in one SMB could be under-spending or over-spending in another.

Yet with this being said, many experts — including those at Devolutions — recommend that SMBs allocate between 6-15% of their organization’s IT budget on IT security (which includes cybersecurity).


Using this standard, the question we need to answer is: are SMBs spending below, within, or above the recommended range? Let us start with the latter two scenarios (within and above the recommended range), before looking at the first (below the recommended range).

The survey found that in 68% of SMBs, IT security spending as a portion of overall IT budget falls within the recommended 6-15% range. This is significantly higher than what was reported in last year’s survey, which found that just 32% of SMBs were allocating 6-15% of their overall IT budget to IT security. Clearly, this is a positive development, and it is likely driven by a combination of three factors:

- The expansion of remote work during the pandemic has alerted SMBs (ideally proactively rather than as a result of a security incident) to the growing external and internal risks they face.
- More cybersecurity insurance carriers are insisting that policyholders spend money on providing formal end user training, and implementing solutions such as PAM.
- More customers — especially those in the B2B space — are demanding that the companies they do business with have strong IT security measures. And SMBs that participate in request-for-proposal competitions typically discover that they (along with all other bidders) must provide proof of having strong IT security measures in place. Otherwise, they will not be considered for funding.

The survey also found that 21% of SMBs are allocating more than 16% of their overall IT budget to IT security. Is this also a positive development? Perhaps — but not necessarily. In some SMBs, the overall IT budget may be smaller than it should be. Such cases would skew the weighting and make IT security spending seem sufficient, when in reality it may be inadequate (and possibly by a considerable extent).





It is also possible that some SMBs are legitimately allocating a significant amount on IT security, but they are not necessarily optimizing their spending. SMBs that suspect this may be the case — and even those who do not, but nevertheless wisely want to assess their IT security profile and infrastructure — should work with reputable IT security vendors that specialize in serving SMBs. These vendors understand that SMBs face financial realities and limitations that differ from those in large organizations and enterprises.

And what about SMBs that are spending below the recommended range on IT security? The survey found that 32% of SMBs fall into this category, which is 6% more than last year. What could be driving this year-over-year decline? Again, we turn to the most likely factor: the pandemic.


As discussed above, the pandemic persuaded — and in some cases, forced — SMBs to increase IT security spending as a proportion of their overall IT budget. But the pandemic also unleashed an unprecedented amount of financial damage. For example, between April 2020 and April 2021, an estimated [200,000 SMBs in the U.S. permanently closed](#) as a direct result of the pandemic. And many SMBs that survived the financial onslaught were forced to significantly scale back operations, which often included hiring freezes and layoffs, along with postponed or cancelled spending and expansion plans.

Per these pressures and risks — which for many SMBs have not completely disappeared — it is understandable that reducing IT security spending may be viewed as a pragmatic decision at this time. However, SMBs need to realize that the potential financial damage of just a single cyberattack could be vastly more expensive than proactively investing in IT security technologies, tools, and training. Indeed, while there are many prudent ways for SMBs to spend less and get lean, putting IT security on the budget “chopping block” is unwise — and could be extremely regrettable.

The survey also found that nearly half (49%) of SMBs are spending more on IT security this year vs. last year. This is most likely driven by increased labor costs. Recall that Part 3 of this report highlighted that in the last year, 36% of SMBs have added one or more employees to address their IT security needs.

In addition, 45% of SMBs are spending approximately the same amount now on IT security vs. a year ago. While this is not necessarily shocking or alarming, it is a potential red flag — because the threat landscape has worsened and become more dangerous in the last year; especially when it comes to ransomware and supply chain attacks. SMBs need to appreciate that the level of IT security is not only measured by budget, but also by consistency of approach. Otherwise, SMBs can lull themselves into a false sense of safety. This is a sentiment that hackers and rogue end users are ready, willing, and able to exploit.

We also see from the survey that 6% of SMBs are spending less on IT security now vs. last year. Again, we can reasonably discern that this reduction is not the result of executives and decision-makers saying “we are spending too much on IT security and need to cut back,” but rather “we need to reduce overall spending in our company, and cutting back on IT security can help us achieve this objective.” As discussed earlier, this approach is understandable — but unwise. And surprisingly, it may also be unnecessary. As discussed earlier, SMBs who choose reputable IT security vendors that specialize in serving SMBs are likely to get advice and solutions that strengthen their IT security profile, while lowering their overall costs. Essentially, they will get more for less, which is always welcome in SMBs.



What does the road ahead look like for SMBs when it comes to IT security spending? The survey revealed that 46% of SMBs plan on increasing their IT security spending in the next 12 months, while 48% plan on spending about the same on IT security over the next year. The five most common projects in the pipeline include:

- Implementing a PAM solution
- Introducing or fully integrating 2FA
- Expanding a password management tool for use by all employees (not just IT staff)
- Implementing automatic password rotation
- Updating VPN strategies

It is interesting to note that all of these frequently-mentioned IT security projects are related to identity and access management.

Identity management combines digital elements and entries in a centralized database to create a unique designation for each individual user. Administrators can monitor, change, and remove these designations as needed to enforce security, as well as grant end users the permissions needed to carry out various work-related tasks. Access management governs whether or not end users have permission to access networks, resources, apps, databases, etc. This concept embraces all of the policies, processes, methods, systems, and tools required to maintain access that is privileged within a digital environment. Essentially, identity management is concerned with who an end user is, while access management is concerned with what an end-user is authorized to do.

Lastly, 6% of SMBs plan to spend less on IT security in the next 12 months. This aligns with what we highlighted in Part 1 of this report, which is that 5% of SMBs are less concerned about IT security now vs. a year ago. Is this reduction in concern justified? We do not believe so. The volume and potential severity of risks and threats are increasing, not decreasing. SMBs that neglect to adjust accordingly — which may involve spending more money on IT security and/or spending more intelligently on IT security — could find themselves on the wrong side of a massive and possibly ruinous attack.

---











**In the Recommendations Section of this report,** we provide practical advice that can help IT Security professionals get more budget and executive buy-in for priorities and projects (e.g., PAM, MFA, etc.).

# PART 6

## RECOMMENDATIONS

In this section, we provide 10 targeted recommendations to help SMBs reduce cybersecurity threats, strengthen privileged access management, increase IT security awareness, strengthen remote access management, and enhance IT security management.

The advice and action steps that we provide for each recommendation is proven, practical, and affordable for SMBs:

-  **Recommendation #1:**  
SMBs need to proactively protect themselves against cybersecurity threats rather than take a “wait-and-see” approach, or unwisely assume that they are “too small to be attacked.” Hackers are increasingly targeting SMBs, to exploit weaker — and in some cases virtually non-existent — cybersecurity defenses.
-  **Recommendation #2:**  
SMBs need to implement a suite of principles and policies that significantly reduce cybersecurity risks, while increasing visibility, governance, and control. These principles and policies include: the principle of least privilege, zero trust, segregation of duties, defense-in-depth, and the four-eyes principle.
-  **Recommendation #3:**  
To fortify their IT security posture and reduce the risk of a potentially catastrophic breach, SMBs need to fully implement a privileged access management (PAM) solution that bridges the gap between authentication and authorization.
-  **Recommendation #4:**  
SMBs need a comprehensive plan to ensure that cybersecurity objectives and requirements are communicated in a timely manner to all required stakeholders, and continually monitored and enforced.
-  **Recommendation #5:**  
SMBs should provide users with cybersecurity awareness training that focuses on fundamental issues, risks, and threats.
-  **Recommendation #6:**  
SMBs that lack in-house IT security and cloud security expertise, and at this time either do not want to hire additional staff or cannot hire additional staff, should partner with a Managed Service Provider (MSP) to close the skills gap.
-  **Recommendation #7:**  
SMBs should implement a just-in-time gateway solution to eliminate vulnerabilities caused by virtual private networks (VPNs).
-  **Recommendation #8:**  
SMBs need to address security vulnerabilities triggered by remote workers.
-  **Recommendation #9:**  
SMBs must get four core benefits from their remote access tools: improved security, efficiency, governance, and affordability.
-  **Recommendation #10:**  
To get more IT security budget, IT professionals should ensure that any pitch, proposal, or presentation focuses on five elements: trust, compliance, insurance, employees, and ethics.

# RECOMMENDATIONS FOR SMBs TO REDUCE CYBERSECURITY THREATS

1

SMBs need to proactively protect themselves against cybersecurity threats rather than take a wait-and-see approach, or unwisely assume that they are “too small to be attacked.” Hackers are increasingly targeting SMBs, to exploit weaker — and in some cases virtually non-existent — cybersecurity defenses.

The survey found that the top five cybersecurity threats that SMBs are most concerned about include: [ransomware](#), [phishing](#), [malware](#), [cloud computing vulnerabilities](#), and [supply chain attacks](#). This is not very surprising, since these threats are closely linked. For example, ransomware is typically malware that is delivered through phishing, an exploited vulnerability, or a compromised supply chain.

Preventing all possible cyberattacks is an enormous — and for many businesses, unrealistic — challenge. Fortunately, however, the impact of ransomware and other threats can be greatly reduced with appropriate preparation. A good starting point for SMBs is to develop a defense strategy that:

- Limits a hacker’s ability to move freely within the environment.
- Enables visibility and response capabilities.
- Prevents unnecessary exposure.
- Implements a robust and efficient recovery of operations.

We dive deeper into each of these elements below:

## Limiting a Hacker's Ability to Move Freely Within the Environment

Once initial access is obtained, hackers will try to seek (if they do not already have) high value credentials, in order to gain administrative access in the environment. Vertical elevation often requires moving from system to system. For example, a user desktop might be compromised with no other valuable access. In this case, a hacker will try to connect on other desktops or servers, in an attempt to extract administrative accounts credentials (connecting on other systems is called lateral movement).

Strong account hygiene, along with suitable privileged access control and governance makes it harder for hackers to achieve their objective without being detected. Core action items that SMBs should adopt include:

- Fully deploying a comprehensive, but easy to use and manage PAM solution (we explore this in recommendation #3).
- Implementing dual authorization, also known as the “four eyes principle” (we explore this in recommendation #2).
- Establishing relevant approval workflows, in which individuals must approve data or tasks at specific points in a process.
- Implementing the Local Administrator Password Solutions (LAPS), which provides management of local account passwords of domain joined computers. Passwords are stored in Active Directory (AD) and protected by an access control list (ACL), so that only eligible users can read/request a reset.

## Enabling Visibility and Response Capabilities

It is not pessimistic, but rather it is pragmatic to acknowledge that, at some point, hackers can — if they are persistent and sophisticated enough — penetrate even a robust cybersecurity defense system. Thankfully, solutions to detect and respond to threats have evolved significantly from the days when many organizations (and most SMBs) relied on conventional antivirus software.

**Nearly 1.5 million new phishing sites are created each month.**  
[[source](#)]

Today, endpoint detection and response (EDR) solutions are essential for detecting and preventing known and unknown malware. Other measures that SMBs should adopt to greatly enhance their visibility and response capabilities include:

- Behavioral analysis, which uses machine learning, artificial intelligence, big data, and analytics to identify malicious behavior by analyzing differences in normal, everyday activities.
- Containment capability, which is a method whereby access to information, files, systems, and networks is controlled via access points.
- Centralized monitoring, in which cybersecurity processes are managed across the organization using a single, centralized set of tools, procedures, and systems. This approach eliminates silos between cybersecurity departments and uses a centralized network to put everything under one umbrella.
- Outsourcing some or all IT security tasks to a Managed Service Provider (we explore this in recommendation #6).

## Preventing Unnecessary Exposure

Reducing the size of the attack surface is critical for blocking initial access, elevation, and lateral movement within the environment. Systems that are not required for business operations, or are not patched in a timely manner, may expose vulnerabilities. Systems that are unnecessary, or that are unavailable for patching, should be managed in such way that hackers will not have the opportunity to exploit them.

## Implementing a Robust Backup and Recovery Plan

To reduce impacts on business continuity and operations, a robust backup and recovery plan should be put in place to facilitate rapid recovery from highly disruptive ransomware. The following best practices are advised<sup>3</sup>:

- **Increase backup frequency.** Due to ransomware, only backing up data once a night is no longer sufficient. All data sets should be protected multiple times per day.
- **Align backup strategy to service-level demands.** For example, if the service level is 15 minutes, then backups should be performed at least every 15 minutes.
- **Adhere to the “3-2-1 backup rule.”** This involves keeping three complete copies of data: two of which are local but on two different types of media (or two different local on-premises backup storage systems), and one copy stored off site.
- **Exercise caution when moving data to the cloud.** Scrutinize a vendor’s claim of offering disaster recovery as a service (DRaaS). While there are significant advantages of DRaaS, it is not a magic wand. SMBs need to remember that “push button” disaster recovery does not necessarily mean “instant” recovery.
- **Automate disaster recovery runbooks.** This involves pre-setting the recovery order and executing the appropriate recovery process with a single click. This approach can be highly beneficial for SMBs with multi-tier applications using interdependent servers, as it helps ensure recovery where and when it is most needed.
- **Don’t use backup for data retention.** Remember that most recoveries come from the most recent backup, and not from a backup that is several months — or possibly years — old.
- **Protect endpoints and SaaS applications.** Laptops, desktops, smartphone, and tablets can contain unique and valuable data, which is never stored in a data center storage device unless it is specifically and deliberately backed up.

<sup>3</sup>These best practices on creating and managing a robust backup and recover plan are based on guidance published by [TechTarget](#).



# 2

SMBs need to implement a suite of principles and policies that significantly reduce cybersecurity risks, while increasing visibility, governance, and control. These principles and policies include: the principle of least privilege, zero trust, segregation of duties, defense-in-depth, and the four-eyes principle.

## Principle of Least Privilege (POLP)

POLP means that end users only get the access they need to carry out their day-to-day activities. If elevated privileges are necessary for a specific project or activity, these should be temporarily granted, and then removed immediately once they are no longer required. Best practices include:

- In consultation with end users, evaluate each role to determine the right access level. The default should be set to “least privilege,” and greater access should only be granted as required.
- Explain the purpose of POLP to all end users, so they grasp that this policy is not meant to frustrate them or stifle their productivity, but rather to protect the organization from a costly – and potentially catastrophic – breach.
- When temporary privileged access is required, use one-time-use credentials that are granted at the last possible moment, and then revoked immediately after use. This approach, which is known as privilege bracketing, can be implemented for individual users, as well as processes and systems.
- Separate administrator accounts from standard accounts, and separate higher-level system functions from lower-level system functions.
- Establish full visibility to see what end users do, and when they do it.
- Regularly audit end user privileges to ensure that access is appropriate.
- Immediately remove access for end users who leave the organization.
- Have the capacity to automatically revoke privileged access in the event of an emergency.

## Zero Trust

Zero trust means that nobody is automatically trusted from the outset. Instead, the approach is to “trust, but verify.” Access management should be evaluated with contextual data, rather than simply trusting authentication secrets provided at login.

This strategy is very relevant for the new work-from-home (WFH) reality, which blurs the boundary between the corporate network and cloud usage as workers connect from anywhere and access many decentralized resources. Controls must be focused on end user context, behavior, and location. Best practices include:

- Use multi-factor authentication (MFA) in real-time to verify trust when attempting to access new network resources or when context changes.
- Extend identity controls to the endpoint, in order to recognize and validate all devices.
- Organize users by group/role to support device policies.
- Use automatic de-provisioning, and have the capacity to wipe, lock, and un-enroll stolen/lost devices.
- Regularly update end user rights based on changes to roles/jobs, as well as changes to security policies and compliance requirements.
- Monitor behavior and allow alerts when suspicious activities are detected.

## Segregation of Duties

Segregation of duties is rooted in the view that when multiple people are involved in a sensitive workflow, there is a lower risk that an individual will manipulate or misuse organizational resources. Best practices include:

- Establish and assign roles in a manner that minimizes risk and prevents conflicts of interest (real or apparent), wrongful acts, fraud, and abuse when assigning one or multiple roles to an employee.
- Align tasks with roles by configuring permissions and access rights to align with task and role segregation, which should be based on the POLP (as discussed above).

- Analyze access levels for escalation to ensure that no single individual could combine multiple accesses to promote himself or herself to a higher (and unauthorized) access level on a system or domain.
- Integrate HR policies to support a comprehensive program. This includes training supervisors and managers to recognize when a subordinate (or any other colleague) has been assigned, or has assumed, tasks involving the use of organizational resources that should be transferred to another, more appropriate role.

## Defense-in-Depth

Defense-in-depth uses multiple layers of protection to effectively slow hackers down, as they attempt to snake their way to the perimeter, and from there to mission-critical assets. Best practices include:

- Design control layers as if a breach has already happened (i.e., answering the “what if?” question), and implement defenses to prevent or contain a hacker’s next move.
- Combine security principles and strategies to generate synergies. For example, segregation of duties and POLP contain threats to a subset of the entire business environment, which creates an ideal opportunity to implement control layers between them.
- Implement the four-eyes principle (discussed below) for privileged access using an approval workflow to prevent/detect unauthorized access attempts.
- Implement cybersecurity solutions that function differently and represent dissimilar controls. For example, while an anti-malware network filter, a whitelisting app, and an email attachment scanner are all anti-malware tools, they do different things, and as such can cover a wider area of the attack surface.
- Don’t forget to monitor! Slowing a hacker down with multiple prevention controls is not enough if unauthorized access or attempts to elevate are not monitored and detected.

## Four-Eyes Principle

The four-eyes principle (sometimes referred to as the two-person principle/rule) requires that any activity by an employee that involves material risk must be reviewed and confirmed by a second employee who is independent and competent. Best practices include:

- Implement dual authorization workflows to access sensitive information or perform elevated actions.
- Review audit trails of actions performed on risky systems or data.
- Assign business roles that involve high-risk procedures or access to multiple employees.
- Record actions performed on systems when external users access corporate resources. These recordings should be reviewed to ensure that no suspicious actions were attempted.

# RECOMMENDATIONS FOR SMBs TO STRENGTHEN PRIVILEGED ACCESS MANAGEMENT

# 3

To fortify their IT security posture and reduce the risk of a potentially catastrophic breach, SMBs need to fully implement a privileged access management (PAM) solution that bridges the gap between authentication and authorization.

Identity management combines digital elements and entries in a centralized database in order to create a unique designation for each individual user. These designations are monitored, changed, and removed as needed in order to enforce security, while at the same time granting end users the permissions that they need to carry out various work-related tasks.

Access management governs whether or not end users have permission to access networks, resources, apps, databases, etc. This concept embraces all of the policies, processes, methods, systems, and tools required to maintain access that is privileged within a digital environment.

Essentially, identity management is concerned with *who* a user is, while access management is concerned with *what* a user does.

However, [a big problem that SMBs face when they attempt to enforce identity and access management \(IAM\)](#) is that certain technologies — such as legacy systems, phones, and cameras — cannot use a federated system. And while in theory it is possible to manually create and maintain unique identity accounts for each user, this is highly impractical.

So why don't SMBs simply avoid this problem entirely by eliminating privileged accounts that are shared across roles, teams, and/or groups? The answer is that [some privileged accounts are necessary](#), such as:

- Domain Administrator Accounts
- Local Administrator Accounts
- Emergency Access Accounts
- Application Accounts
- System Accounts
- Domain Service Accounts

The solution to this dilemma is for SMBs to fully implement a PAM solution extends the protection offered by an IAM system into the non-federated identity space.

## Key Elements of a Robust PAM Solution

SMBs should focus on a robust PAM solution that offers all of the following:

- A vault that stores passwords (and other sensitive data, such as building alarm codes, software license keys, etc.), and which is securely shared between multiple end-users.
- Account checkout, which allows Admins to grant or reject an access request on a case-by-case basis, and if necessary, set time limits.
- Notifications that alert Admins when certain events or actions take place involving end users, roles, vaults, etc.
- Automated mandatory password rotation.
- Account brokering, which automates workflows (e.g., opening a VPN client, launching a remote access protocol, and accessing a privileged account) without providing end-users with passwords in the first place.
- Session activity recording.
- Enables credential rotation on and after every check-out for an RDP session, which mitigates the potential exploitation of the RDP credentials (credentials do not need to be passed to users, as each authentication occurs one time – thereby eliminating the need to rotate credentials).
- Ease-of-deployment and management.
- Affordably priced to suit SMB IT security budgets, which are significantly smaller than large enterprise budgets.

In addition to the above, some more sophisticated PAM solutions support privileged session management (PSM), which utilizes a specialized server that brokers authentication behind-the-scenes, and can also record the activity of remote sessions.

PSM is especially important for SMBs that have contractors and “boomerang” employees (i.e., employees who leave the organization and then return). These end users typically need more scrutiny and limited access.

## RECOMMENDATIONS FOR SMBs TO INCREASE IT SECURITY AWARENESS

# 4

SMBs need a comprehensive plan to ensure that cybersecurity objectives and requirements are communicated in a timely manner to all required stakeholders, and continually monitored and enforced.

Policies that lack technical controls to enforce them are ineffective. Even worse, poorly communicated policies are neither enforced nor applied. To avoid these pitfalls, it is crucial for SMBs to:

- Define and document objectives.
- Define roles and responsibilities.
- Communicate downstream and monitor upstream.

We explore each of these below:



**Organizations with a comprehensive and well-tested cybersecurity incident response plan reduced the cost of a breach by an average of \$2 million USD, compared to organizations without a robust plan and suitable plan in place. [\[source\]](#)**

## **Defining and Documenting Objectives**

Cybersecurity objectives must be clearly defined and documented. They also must be specific, measurable, achievable, realistic, and anchored within a defined time frame (a.k.a. “SMART”).

IT security awareness at all levels of the organization cannot be optimized without proper objectives. Indeed, many organizations focus entirely on end user vigilance (e.g., avoiding phishing, applying cybersecurity controls, etc.) but neglect to confirm that objectives are understood or clearly known in the first place.

## **Define Roles and Responsibilities**

Defining roles and responsibilities are at the heart of an effective policy and plan. To ensure that key internal stakeholders understand cybersecurity requirements across the business, these roles and responsibilities should be mapped to a RACI chart (Responsible, Accountable, Consulted, Informed).

### Example of RACI Chart for High Level Cybersecurity Roles and Responsibilities

|   | Board | Executives | IT Director | Team Leader |
|---|-------|------------|-------------|-------------|
| Evaluate, Direct and Monitor cybersecurity objectives                           | A     | R          | I           |             |
| Align, Plan and Organize cybersecurity initiatives                              |       | A          | R           | I           |
| Build, Acquire and Implement cybersecurity initiatives                          |       |            | A           | R           |
| Deliver, Service and Support cybersecurity services                             |       |            | A           | R           |
| Evaluate, Monitor and Assess cybersecurity initiatives and services performance | I     | A          | R           |             |

RACI charts can also be used for more specific cybersecurity requirements to define who is accountable for accepting cybersecurity risks, or who is responsible to report a new cybersecurity risk.

## Communicate Downstream and Monitor Upstream

Policies must be available for all stakeholders (e.g., employees, suppliers, vendors, customers, etc.), and updates should be communicated in a timely matter. Establishing bi-directional communication channels is critical. Committees are a good and practical way to collect stakeholder feedback, validate alignment, and make continuous adjustments and improvements as necessary.

# 5

SMBs should provide users with cybersecurity awareness training that focuses on fundamental issues, risks, and threats.

While there are several ways for SMBs to increase their workforce's cybersecurity awareness, the most practical, effective, and cost-efficient — especially for SMBs with remote workers — is an online training platform. This provides employees with self-paced, hands-on, skills-based threat detection and mitigation training in a live and dynamic simulated environment.

One of the key advantages of online training is that employees get immediate feedback on their decision-making and move forward through the training based on their performance. Supervisors and managers can also access a dashboard and monitor the progress of each employee, in order identify strengths and weaknesses.

Nearly half of all data breaches are caused  
by employee negligence or carelessness.

[[source](#)]

There are many reputable online cybersecurity training programs available. At a minimum, we recommend that SMBs choose a program that covers several or all of the following fundamental issues, risks, and threats<sup>4</sup> :

- **Access Control**
- **Bring Your Own Device (BYOD)**
- **Cloud Services**
- **Data Leakage**
- **Identity Theft**
- **Incident Reporting**
- **Intellectual Property**
- **Introduction to Information Security**
- **Malware**
- **Mobile Devices**
- **Open Wi-Fi Risks**
- **Password Management**
- **Phishing**
- **Physical Security**
- **Privacy**
- **Protecting Payment Card Data**
- **Responsible Use of the Internet**
- **Social Engineering**
- **Social Networks**
- **Traveling Securely**
- **Working Remotely**

<sup>4</sup> These fundamental cybersecurity issues, risks, and threats are mapped to the [“Security Awareness — General Knowledge”](#) training curriculum offered by cybersecurity training firm Terrnova Security.

# 6

SMBs that lack in-house IT security and cloud security expertise, and at this time either do not want to hire additional staff or cannot hire additional staff, should partner with a Managed Service Provider (MSP) to close the skills gap.

MSPs help SMBs increase their capacity and skillset, reduce costs and risks, take advantage of growth opportunities, enhance user experience, manage uncertainty, and proactively plan for the future.

## To choose the right MSP, SMBs should focus on these seven core factors:

- **Services:** an MSP must have the proven capacity to serve the SMB's specific needs and goals. Not all MSPs focus or specialize in the same areas. For example, some MSPs can provide IT security-related services, but they lack the ability to provide cloud security-related services.
- **Advice:** an MSP must be committed to providing informed and objective advice. The focus must be on strengthening and securing their SMB client — not increasing the MSP's profits.
- **Affordability:** an MSP must demonstrate a clear understanding that SMBs typically have a significantly smaller IT security budget compared to large organizations and enterprises. As such, the focus should be on recommending essential vs. nice-to-have strategies and solutions, and helping SMBs optimize their limited IT security budget so they “get the most for the least.”

- **Fearlessness:** an MSP must not be afraid of telling executives and decision-makers what they need to hear vs. what they want to hear. If SMBs are making uninformed — or just plain bad — decisions and choices, then an MSP has a duty to escalate their concerns and observations, and recommend superior alternatives.
- **Responsiveness:** SMBs should never feel as though an MSP is treating them as a “second class citizen” compared to their large enterprise clients. Responsiveness standards should be included in the Service Level Agreement (SLA), and an MSP should consistently meet or exceed them.
- **Business Continuity & Disaster Recovery:** an MSP must have the tools, staff, and policies to monitor the SMB’s infrastructure 24/7/365, and support business continuity and disaster recovery. The notion of an SMB “going off the grid” for an extended period of time due to a cyberattack or any other event (including those not related to IT security) is not an option.
- **Technology & Vendor Neutral:** if necessary or upon request, an experienced MSP will provide informed and objective recommendations related to hardware, software, training providers, and other aspects related to their scope of services. However, at no time should an MSP insist on a specific product or vendor. An MSP’s loyalty must be to their client, not to a third-party.
- **Communication:** a competent MSP will have no problem having expert-to-expert discussions with members of an SMB’s in-house IT team and/or IT Security team. However, an MSP must also be capable and comfortable communicating (verbally and in writing) with “non-techies.” An MSP that cannot effectively engage diverse audiences is a part of the problem, not the solution.

# RECOMMENDATIONS FOR SMBs TO STRENGTHEN REMOTE ACCESS MANAGEMENT

## 7

SMBs should implement a just-in-time gateway solution to eliminate vulnerabilities caused by virtual private networks (VPNs).

Most SMBs are using a VPN to establish a protected network connection when using public networks — which is especially critical for remote workers. However, while VPNs are helpful, they trigger three major problems:

- VPN servers are notoriously difficult and time-consuming to deploy.
- VPN clients tunnel traffic through the private network, which can significantly degrade network performance.
- When granting temporary access, Admins must spend time updating and keeping track of VPN and firewall rules.

Fortunately, there is a practical solution to help SMBs close the security gap and strengthen remote access management: implement a Gateway solution to provide just-in-time access to resources in segmented networks. As a result, users can securely access the company's internal network from home. A gateway is also highly beneficial for Managed Services Providers (MSPs), as it allows them to connect rapidly and securely to separate customer networks.

With respect to the major VPN-triggered problems highlighted above, a Gateway solution:

- Deploys quickly and easily, which is vital for SMBs that do not have the budget or bandwidth to get bogged down with deployment-related issues and hassles.
- Improves network performance by restricting tunneling to RDP connections, which means there is no negative impact on other network traffic.
- Uses dynamic access rules, which eliminates the need for Admins to manually update VPN and firewall rules when granting temporary access.

For additional insight on a robust and affordable solution that checks all of these boxes, we invite SMBs to learn more about [Devolutions Gateway](#).



# 8

**SMBs need to address security vulnerabilities triggered by remote workers.**

Many SMBs worldwide have been in a mad scramble to find a safe and secure solution to deploy and maintain remote access. Even as some SMBs return to a physical office building, a substantial portion of the workforce is expected to remain remote on a full or part-time basis. This means that there are hundreds of new entry points that need to be safeguarded against potential hackers. It is a daunting challenge — especially since most SMBs do not have large IT teams in place. To address this priority, SMBs should implement and enforce a remote worker cybersecurity policy that includes the following elements:

## **Secure Remote Access with Just-in-Time Gateways and/or VPNs**

IT professionals constantly need secure access to critical corporate assets. Whether they need to update machines in the computer network or to assist users remotely, SMBs should choose a comprehensive and highly secure just-in-time gateway or VPN solution that is quick, robust, secure, and easy to deploy.

## Multi-Factor Authentication (MFA)

MFA is an extra layer of security that requires remote workers to verify their identity by providing their login credential, along with another piece of information that could be:

- Something they know, such as the answer to a secret question, a PIN, or a password
- Something they have, such as a smartphone or a token
- Something biometric, such as their fingerprint, voice recognition, or an eye scan

The idea is that even if a remote worker's login credentials are stolen, it is less likely that hackers will be able to supply the additional information to access a device, application, network, or system.

## Password Manager

To strengthen security, remote workers (along with in-office workers) should be provided with a robust, yet easy-to-use password manager that offers features such as:

- Password rotation
- Strong password generator
- Automatic checks against passwords that have been exposed during hacks
- Real-time email alerts in the event of unauthorized access attempts.

## Endpoint Security

Endpoint security is a critical line of defense to keep hackers from launching attacks against devices, and penetrating networks and integral systems. Key endpoint security tools include:

- Network firewalls for both on endpoints and home networks
- Anti-virus software
- Software updaters. Note: as a best practice, we recommend that SMBs put remote devices on a standard image and activate automatic updates for all apps and programs (especially security software)

## Ongoing Cybersecurity Training

All employees need ongoing cybersecurity training — but especially remote workers who can sometimes let their guard down. In the previous section, we highlighted fundamental cybersecurity topics that SMBs should cover (whether they are delivering training themselves or using a third-party training consultant or firm). In addition, SMBs should:

- Warn remote workers against over-sharing on social media, since such activity can draw the attention of hackers.
- Remind remote workers to always keep their devices with them, and never leave them unattended. In public spaces such as coffee shops, malls, airports, hotels and so on, thieves will carefully observe a victim for prolonged periods of time, and then rapidly spring into action the moment they see an opportunity. All they need is a few seconds.

## Switch to Cloud-Based Storage

Storing data in the cloud not only is more convenient for remote workers, but also enhances protection from cyberthreats with protections such as enforcing conditional access, DRM, UEBA, DLP, encryption, and more. If a device is stolen, then access to cloud-based data can be instantly revoked.

# 9

SMBs must get four core benefits from their remote access tools: improved security, efficiency, governance, and affordability.

The survey revealed that the surge in remote work is creating challenges for SMBs in four core areas: security, efficiency, governance, and affordability (cost).

To address these challenges and concerns, below we provide a checklist to help SMBs choose the right remote access tools — and steer clear of the wrong ones:

## Addressing Security Challenges

Focus on remote access tools that feature the following:

- **Strong encryption:** All passwords stored in the data sources should be encrypted using a strong encryption algorithm, so that if an end user attempts to access the data directly in the database, it will be rendered unreadable.
- **Account brokering:** Credentials can be brokered on behalf of an end user when launching a connection, therefore preventing them from ever knowing the credentials.
- **Role-Based Access Control (RBAC):** All restrictions can be predefined and enforced by granular-level permissions.
- **Two-Factor Authentication (2FA):** Enforce two consecutive authentication steps before granting access to a data source.
- **User Vaults:** User-specific vaults give unique end users access to specific privileged accounts.

## Addressing Efficiency Challenges

Focus on remote access tools that feature the following:

- **Centralized Password Vault:** Store all passwords and credentials in a secure vault, and log in from anywhere via a secure browser plug-in.
- **Mobile Access:** Launch sessions, manage desktops and servers, and retrieve passwords on-the-go with a secure, easy-to-use mobile app.
- **Offline Access:** Launch sessions without internet connectivity by accessing an offline editable copy of the database that is as secure as the online version.
- **Automatic Connections:** Launch secure and direct connections to privileged sessions, including remote servers, virtual machines, and other critical assets.
- **Support for Multiple Tools and Technologies:** The list of integrations should include RDP, SSH, VPNs, Web, VNC, Telnet, ICA/HDX, ARD, etc.
- **Support for Multiple Data Sources:** Easily share databases, including SQL Server and more.
- **Session Sharing:** Easily and securely share all remote sessions across the entire team.
- **Multiple Vaults:** Store and organize entries in an unlimited number of vaults to easily manage massive numbers of entries, documents, and other sensitive data.

## Addressing Governance Challenges

Focus on remote access tools that feature the following:

- **Audit Trail:** Monitor, verify, and analyze time spent by an end user on a specific client or a machine for audit purposes.
- **Activity Log:** Record when, what, and who performed an action on a session, and monitor all opened sessions for all users.
- **Real-Time Connection:** Know exactly who is connected in real-time for several types of sessions and verify if an end user has connected despite receiving a warning.
- **Integrated Console:** Get a quick overview of machine state and facilitate management tasks through integrated virtualization consoles, such as Hyper-V, Terminal Server, and XenServer.

## Addressing Affordability Challenges

Focus on remote access tools that feature the following:

- **Free Trial:** Evaluate the tool in your own environment to verify security, functionality, usability, and other requirements before you commit to purchasing.
- **Per User vs. Per Installation Licensing:** Ensure that licensing is per user and not per installation. This gives SMBs much more flexibility and control over their budget.
- **Multiple Licensing Options:** SMBs should have the freedom to choose from a variety of licensing options, such as: Site up to a maximum number of users; Site for an unlimited number of users; and Multi-Site for unlimited number of users across multiple sites. This flexibility helps ensure that SMBs only pay for the access they need — and nothing more.
- **Demonstrated ROI:** The total cost of ownership (TCO) should not exceed the ROI for risk reduction and productivity gains.

# RECOMMENDATIONS FOR SMBs TO ENHANCE IT SECURITY MANAGEMENT

# 10

To get more IT security budget, IT professionals should ensure that any pitch, proposal, or presentation focuses on five elements: trust, compliance, insurance, employees, and ethics.

For many IT professionals in SMBs, it is a familiar and frustrating story: they repeatedly attempt to get more IT security budget — not for their own enjoyment or glory, but to protect the company from risks, threats, compliance violations, and reputation damage — yet they are either outright denied, or they are given a fraction of what they need.

Indeed, this scenario is so common that many IT professionals are forced to conclude that their boss (or possibly, multiple bosses) simply do not care about strong IT security and fail to see it as a fundamental requirement. What is going on here?

Devolutions has engaged thousands of non-IT executives and decision-makers in SMBs around the world, and we have reached a clear conclusion: the root problem is not (contrary to what many IT professionals believe!) that their colleagues do not care about strong IT security.

Rather, it is because their colleagues without an extensive IT background — which includes many business owners, CEOs, CFOs, VP of Operations, etc. — can mistakenly believe that their company is already investing in strong IT security; especially if they haven't yet experienced a severe and scary breach. As such, they believe that there is no need to increase the IT security budget, or give their IT professionals more authority to decide, in terms of access, who in the company can do what (and where, when, how, and why).

Furthermore, IT professionals who repeatedly sound the “WE NEED STRONGER I.T. SECURITY AROUND HERE!” alarm bells in conversations, memos, and meetings can be seen as alarmists — when in truth they are realists.

So what can IT professionals who lack the resources they need to thwart bad hackers — and mitigate the damage and chaos triggered by rogue and negligent end users — do to finally convince their colleagues that investing in strong IT security is strategic instead of superficial?

To answer this pivotal question, we recommend that IT professionals focus on five core factors in any informal or formal pitch, proposal, or presentation:

## 1. Strong IT Security Helps Earn and Maintain Customer Trust

Billionaire Warren Buffet has said that “it takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.” Consider that:

- [More than 80% of consumers](#) view trust as a deciding factor in their buying decisions.
- [88% of consumers](#) say that trust is more important in times of change (and we are definitely experiencing that now!).
- [70% of consumers](#) want to know that data protection is considered a top priority by the companies that they do business with.

The message for IT professionals to convey is that allocating more resources towards IT security is not just a *technical* issue. It is fundamental to earning and maintaining customer trust, which makes it a *business* issue.

Indeed, companies that are viewed as untrustworthy because they neglected to invest in strong IT security are forced to spend an enormous amount of money to try to recover. Obviously, this expense is far greater than what it would have cost to strengthen IT security in the first place.



## 2. Strong IT Security is Necessary for Compliance

We just finished noting that many customers will stop doing business with a company that failed to proactively strengthen its IT security (even if those customers, themselves, were not directly or materially affected by an attack).

However, there are also some customers that will outright refuse to do business with a company that has not had its IT security infrastructure, governance, and controls evaluated and verified by a third-party. There are several credible compliance standards and programs, such as:

- [SOC 2](#)
- [ISO 27001:2013](#)
- [PCI DSS](#)
- [HIPAA](#)

Since the one thing that keeps executives awake at night is leaving revenues and profits on the table, conveying this message in practical terms can go a long way towards creating a paradigm-changing “aha” moment: one where IT security stops being perceived as an unavoidable expense, and starts being seen as a profitable investment. Strong IT security expands the marketplace to include more customers, while weak IT security shrinks the marketplace and puts companies at a major disadvantage vs. the competition.

## 3. Strong IT Security May be Necessary for Insurance

This is a trend that we have been seeing accelerate greatly in the last couple of years: companies that have purchased cybersecurity insurance are discovering, upon renewal of their policy, that their insurer is demanding stronger IT security controls — especially with respect to privileged access management (PAM).

And what about IT professionals whose company does not have cybersecurity insurance, or whose insurer (at the moment) is not demanding stronger IT security? They can still cite this trend to bolster their case. For example, they can say: “If a growing number of insurance companies — which are exceedingly pragmatic — are so worried of covering the costs of a data breach or leak, then shouldn’t we be just as concerned?”

## 4. Strong IT Security Sends the Right Message to Employees

Whether they are [falling for phishing scams](#), insecurely and/or improperly sharing passwords, losing laptops — and the list goes on — end users have always been, and will always be, [the weakest link in the IT security chain](#).

An SMB that makes responsible and appropriate IT security investments sends a clear, confident message to their workforce: “We take strong IT security very seriously around here, and we expect you to do the same.”

Conversely, an SMB that neglects to pay attention to strong IT security will face resistance and pushback when telling end users to practice good IT security hygiene — because those users will see the gap between what the company is preaching vs. practicing.

## 5. Strong IT Security is Ethical

IT professionals should strive to help executives and decision-makers appreciate that supporting strong IT security is not just the *smart* thing to do, but also doing the *right* thing to do. It is not just about avoiding costs and consequences. It is also about being socially responsible and being a good corporate citizen.

SMBs that lead the way of IT security earn the right to feel great about “living their values” at work — because when good companies win the IT security fight, hackers and rogue users lose!

## Additional Tips

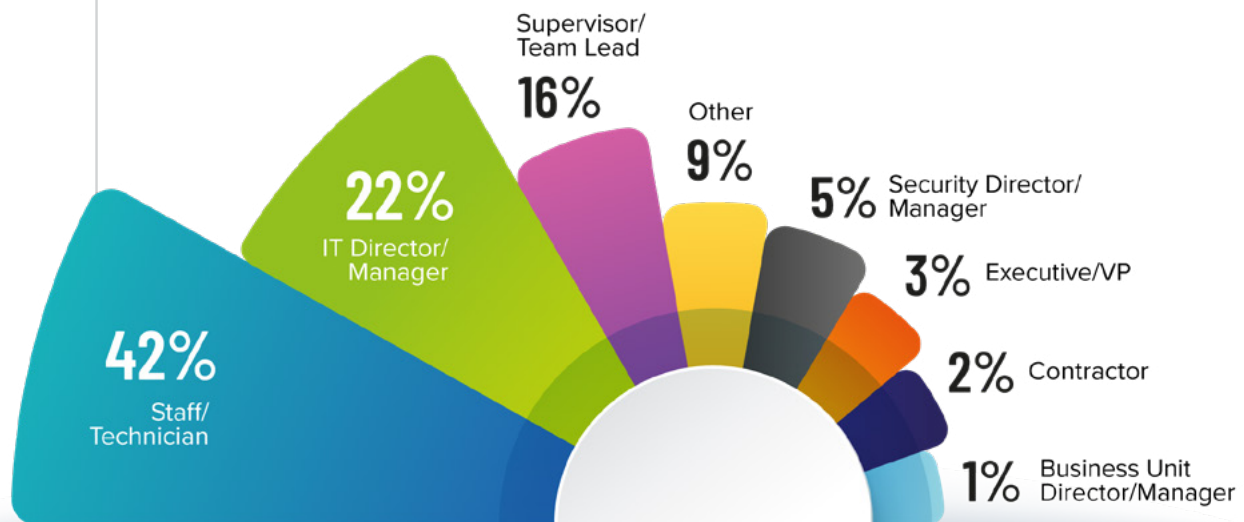
To help get all of these messages across to their colleagues, IT professionals should keep these tips in mind:

- Demonstrate the risks and impact of a breach. For example, a realistic exercise that simulates a ransomware attack can be eye-opening for decision-makers.
- Use plain language and avoid jargon. What is readily familiar to CISOs and CTOs may be quite unfamiliar to CEOs and CFOs.
- Where possible, quantify risks with numbers (e.g., “This type of breach cost a similarly sized company in our marketplace \$1.25 million to investigate and clean-up”) vs. abstract dangers (e.g., “This type of breach involves hackers stealing emails.”)
- Be prepared with a proposed IT security budget that includes a clear list of the recommended new tools, technologies, training, staff, etc.
- When assessing various tools and technologies, take advantage of free trial offers to confirm usability, security, flexibility, scalability, etc.
- Work with vendors that specialize in serving the needs of SMBs and demonstrate the following:
  - Their solutions are affordable and make sound business sense.
  - Their solutions are easy and fast to implement.
  - They provide exceptional technical support.
  - They help SMBs focus on critical priorities vs. “nice-to-have” options.
  - They help SMBs get the most value for the least amount of spending.

# PART 7

## PROFILE OF RESPONDENTS

Which title best describes your position within the organization?

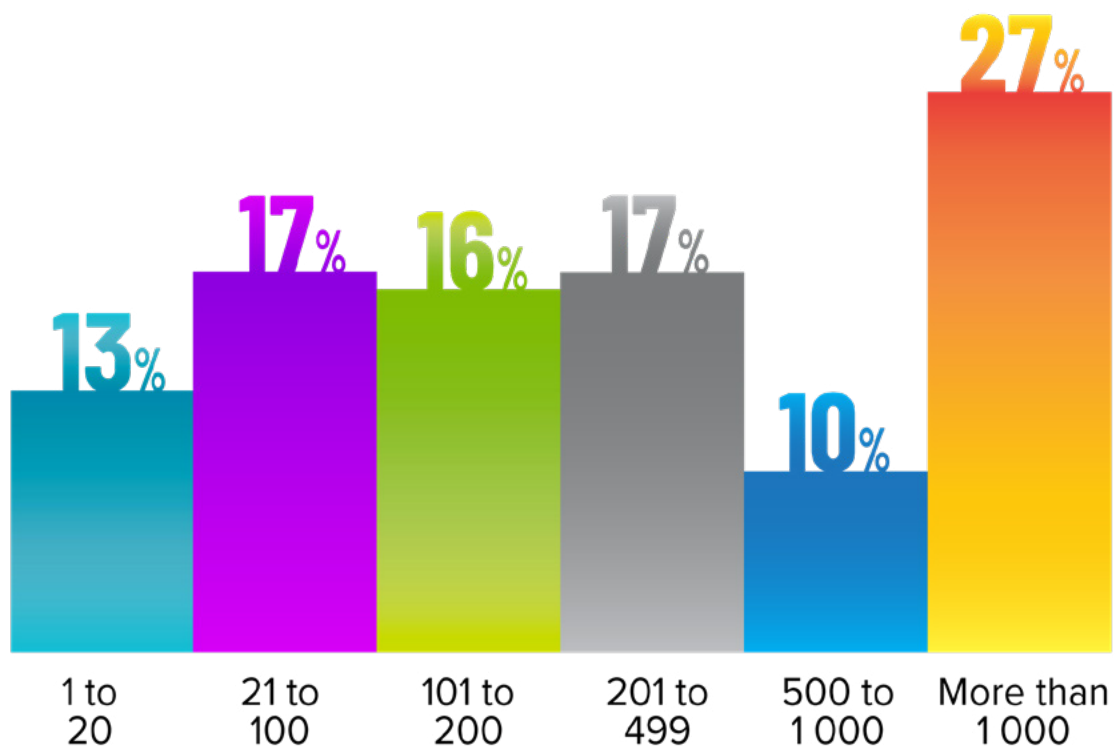


What best describes your organization's sector?

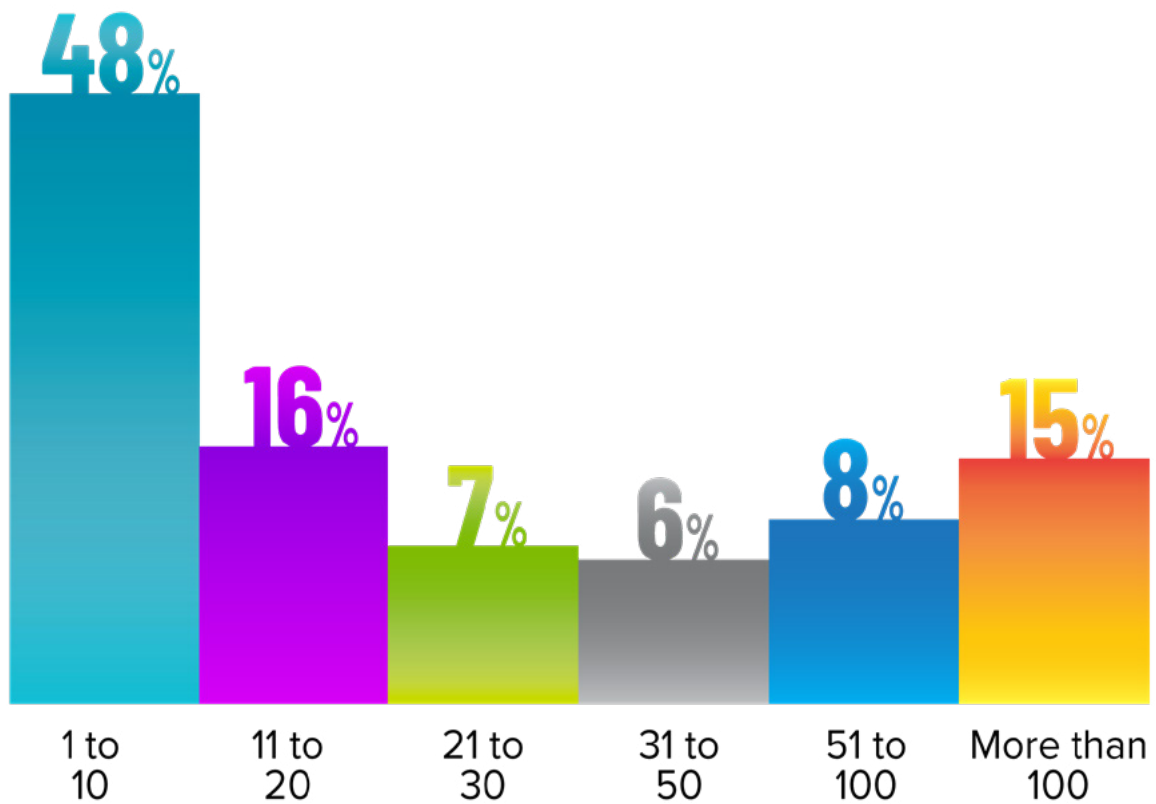


- 29% ● IT services
- 12% ● Manufacturing
- 9% ● Finance and insurance
- 9% ● Technology
- 5% ● Education
- 5% ● Government
- 3% ● General services to business
- 3% ● Health
- 3% ● Oil and energy
- 3% ● Retail
- 3% ● Other (please specify)
- 2% ● Communications
- 2% ● Computer and network security
- 2% ● Construction
- 2% ● Customer service
- 2% ● Entertainment
- 2% ● Security, defense technology and infrastructure
- 2% ● Utilities
- 1% ● Apparel and fashion
- 1% ● Transportation

How many people are employed in your organization across all locations worldwide?



How many of your organization's employees work in the IT department?

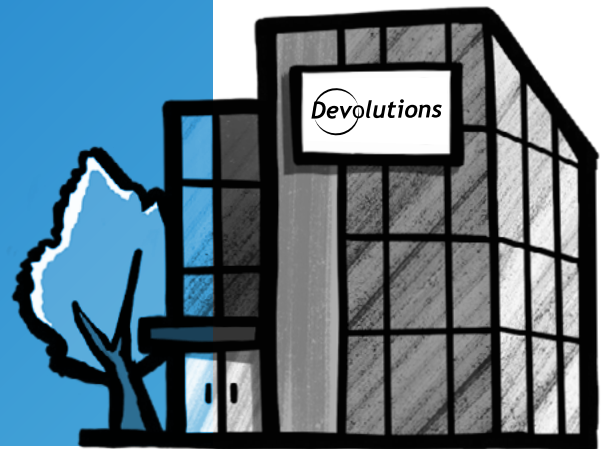


# HELPING SMBs STAY SAFE AND SUCCEED

**Although 99% of organizations are SMBs**, virtually all best-in-class Privileged Access Management, Password Management, and Remote Connection Management solutions are prohibitively expensive and excessively complex for most SMBs. This leaves SMBs vulnerable to security gaps and compliance breaches, reduces their productivity and competitiveness, and risks sending them backward when they need to move forward on the post-pandemic landscape.

At Devolutions, we believe that neglecting SMBs and treating them like “second-class citizens” is wrong and unacceptable. That is why we have built a set of Universal Password and Access Management solutions specifically designed to meet the growing needs of SMBs, and which are:

- Available at affordable price positions and multiple licensing models that make long-term sense.
- Highly secured and safeguarded by enterprise-grade protection, logging, and monitoring.
- Refreshingly simple and fast to deploy either on premises or in the cloud.
- Intuitive and easy-to-use for both technical and non-technical business users.
- Accessible through smartphone apps to support remote working anytime, anywhere.
- Backed by world-class sales engineers and technical support provided by an in-house team of specialists.



We make best-in-class Privileged Access Management, Password Management, and Remote Connection Management solutions available to SMBs. Because all companies — not just large organizations and enterprises — need to control the IT chaos, strengthen security, increase efficiency, and drive results. We call it **“Universal Password and Access Management for the rest of us!”**



# OUR SUITE OF SOLUTIONS

Below is an overview of our suite of solutions.  
**Free trials are available.**



## Devolutions Server

**Devolutions Server (DVLS)** is a full-featured shared account and password management solution with built-in privileged access components to meet the ever-expanding security requirements of SMBs. DVLS also features an integrated PAM component that supports a variety of enhanced functions, including account discovery, account check-out approval, and automatic password rotation.

[Learn more here.](#)

---



## Password Hub Business

**Password Hub Business (PHB)** is a secure and cloud-based password manager for teams. It empowers SMBs to easily and securely vault and manage business-user passwords and other sensitive information through a user-friendly web interface, which can be quickly, easily, and securely accessed via any browser. PHB also features role-based access control, a centralized password vault, a strong password generator and more.

[Learn more here.](#)



**Password Hub Personal** is a safe, easy-to-use and free password manager for individual users who want to store personal passwords in a secure vault, which is only accessible by the user. You can also easily create and access your own Password Hub Personal from your Devolutions Account.

[Learn more here.](#)

---



**Remote Desktop Manager (RDM)** centralizes all remote connections on a single platform that is securely shared between end users and across the entire team. With support for hundreds of integrated technologies — including multiple protocols and VPNs — along with built-in enterprise-grade password management tools, global and granular-level access controls, and robust mobile apps to complement desktop clients for Windows and Mac, RDM is a Swiss Army knife for remote access. RDM also features role-based access control, account brokering, administrative password sharing, session recording, centralized password vaulting, and more.

[Learn more here.](#)



## **CONTACT DEVOLUTIONS**

Based in Lavaltrie, Québec, Canada, Devolutions delivers productivity and security solutions to more than 800,000 IT professionals and business end users in over 140 countries worldwide. Please direct your inquiries and free trial requests to us via the following:

**Email:** [sales@devolutions.net](mailto:sales@devolutions.net)

**Phone:** +1 844 463.0419

**Live Chat via our Website:** <https://devolutions.net/>