CROWDSTRIKE

REPORT

The State of SMB Cybersecurity Survey

Table of Contents

SMBs at the Center of a Changing Threat Landscape

Small and medium-sized businesses (SMBs) are no longer flying under the radar of cybercriminals. Once considered too small to be worthwhile targets, SMBs are now being hit by increasingly sophisticated adversaries that are leveraging AI and automation to scale their operations to businesses of any size. Despite their growing awareness of cybersecurity threats, many SMBs remain underprepared and caught in a dangerous gap between recognizing cyber risks and implementing effective responses.

To better understand the cybersecurity readiness of SMBs around the globe, CrowdStrike commissioned a comprehensive survey of companies with fewer than 250 employees. The results paint a complex picture: **Though awareness is high, execution often falls short, leaving critical security issues unaddressed.**

This survey explores where SMBs are making progress and where key shortfalls remain. It highlights several findings that reveal hidden gaps and unchallenged assumptions about SMB cybersecurity readiness. It then digs into the details and discusses how small businesses — together with their enterprise partners — can make progress, closing the gap.

Key Takeaways

1. **SMBs understand the risks but struggle to evolve defenses.**
Though 94% of respondents say they're knowledgeable about cybersecurity threats, many fall short on training, tools, and consistent execution of their security strategy.

2. **Business size influences security posture.**
Most SMBs with at least 150 employees (89%) have security plans, compared to just 47% of micro-businesses (fewer than 50 employees). Yet even the more mature organizations struggle with execution gaps and overconfidence.

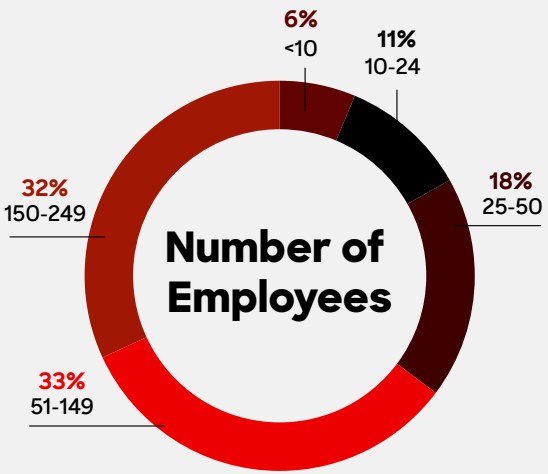
3. **Affordability vs. effectiveness: SMBs shouldn't have to choose.**
Two-thirds of SMBs cite cost as the biggest obstacle preventing them from upgrading to more advanced security tools, and only 7% say their security budget is "definitely sufficient."

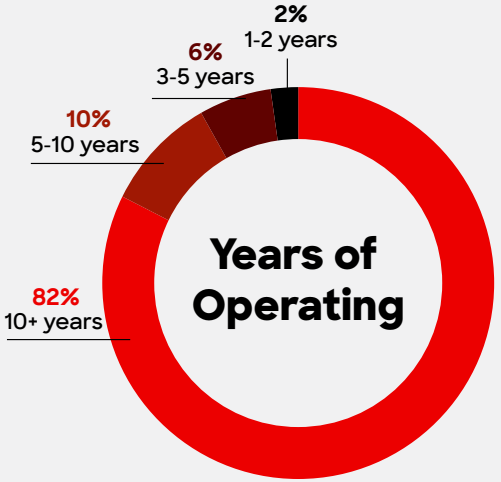
4. **The smallest businesses are ransomware targets.**
Ransomware hits micro-businesses the hardest. Among companies with fewer than 25 employees that suffered a cyber incident, 29% reported a ransomware attack — making this segment of micro-businesses the most affected by successful ransomware campaigns, despite the fact that they ranked it lower as a perceived threat.

5. **SMBs want guidance, not just tools.**
Half of SMBs surveyed feel overwhelmed by the vast selection of security tools available to them. Nearly 70% rely on outside experts for guidance, underscoring the need for clear, practical support beyond just products.

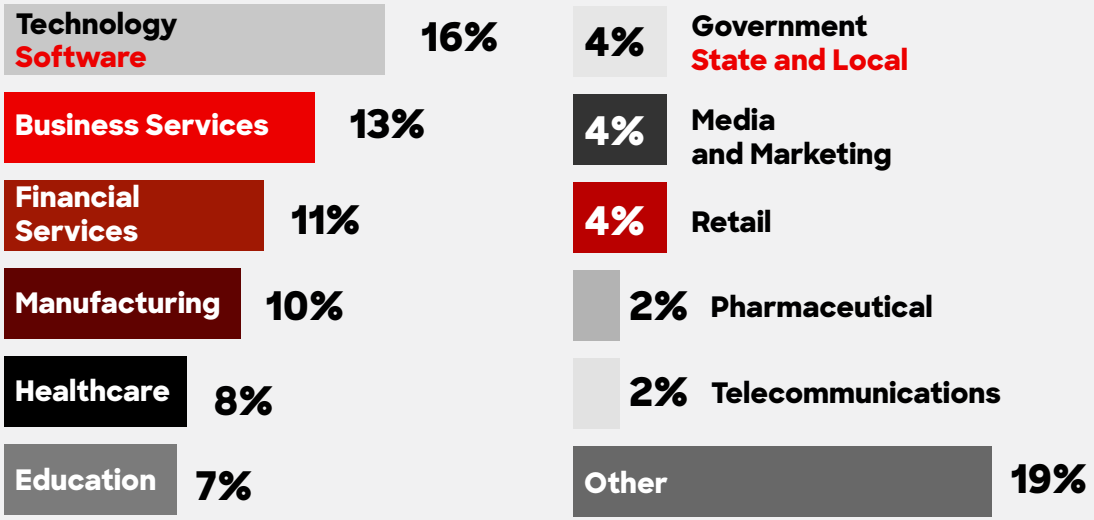
Survey Methodology

CrowdStrike commissioned research firm Virtual Intelligence Briefing to survey the attitudes, challenges, and cybersecurity needs of 291 SMB leaders from companies with fewer than 250 employees. The smallest businesses, sometimes referred to as micro-businesses, have a maximum of 50 employees (34%). Mid-sized SMBs have between 51 and 149 employees (34%), and the largest have between 150 and 249 (32%). Conducted in February and March 2025, the 32-question survey explored cybersecurity strategies, incident response practices, investment priorities, and perceptions of emerging threats. Respondents, who were invited to participate in the survey voluntarily, shared insights on their current toolsets, training practices, and budget constraints as well as where they seek guidance, offering a detailed snapshot of SMB cybersecurity maturity and gaps.





Primary Industry



KEY FINDING 1

SMBs Understand the Risks but Struggle to Evolve Defenses

Awareness is high, but action is uneven

Ninety-four percent of SMB leaders say they're "somewhat" or "very" knowledgeable about cyber threats, but that awareness doesn't consistently translate into action. A large majority (83%) report having a cybersecurity plan in place, yet only 42% provide regular employee training — a key component to cybersecurity literacy and knowledge and mission-critical to an effective cybersecurity strategy.

Unsurprisingly, phishing remains a leading attack vector across businesses of all sizes and industries, as evidenced by a 442% increase in voice phishing between the first and second half of 2024, revealed in the CrowdStrike 2025 Global Threat Report. Without regular education, employees are easy targets.

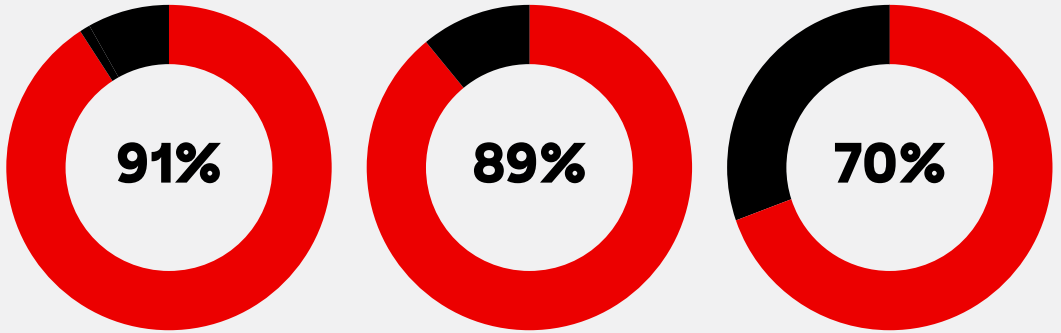
Execution gaps undermine SMB security plans

Businesses with security plans were just as likely to fall victim to breaches (25%) as those without (24%), suggesting many plans are either subpar and underdeveloped or not effectively implemented. This parity reveals the dangerous misconception that having a plan is the same as being prepared.

Legacy tools dominate defenses

Most SMBs continue to rely heavily on outdated tools. Commodity firewalls (91%) and traditional antivirus (70%) remain some of the most common solutions in use, even as modern threats shift toward fileless malware, credential theft, and zero-day exploits. Only 11% of respondents reported using AI-powered tools to defend against today's AI-driven attacks, highlighting a dangerous disconnect between the tools SMBs depend on and the evolving threats targeting them.

SMBs' Most-used Cybersecurity Tools

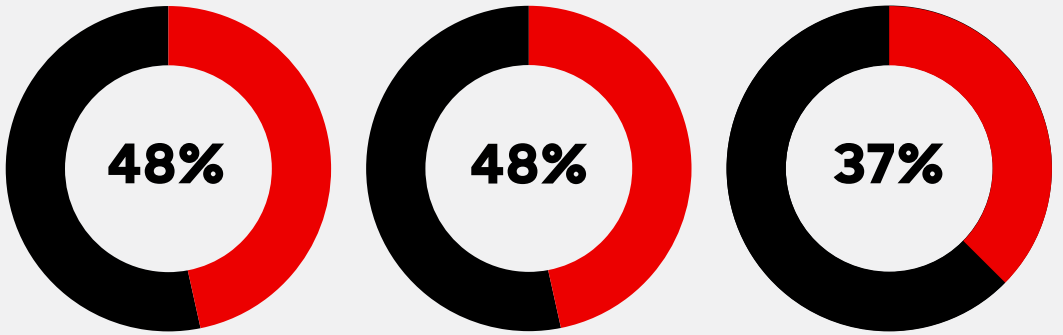


Firewalls

Multifactor authentication

Traditional antivirus

Top Three Emerging Threats that Most Concern SMBs



AI-powered cyberattacks

Deepfake or social engineering scams

Cloud security risks

KEY FINDING 2

Business Size Influences Security Posture

Micro-businesses struggle

Cybersecurity readiness among SMBs is far from uniform, with a significant shift at the 50-employee mark. Below this threshold, most SMBs lack formal plans and investment; above it, readiness begins to scale. The SMB security divide is most evident among micro-businesses with fewer than 10 employees: Only 47% of these businesses have a cybersecurity plan, and more than half spend less than 1% of their total budget on security.

Examining the mid-market maturity gap

Mid-sized SMBs (51-149 employees) are the most likely to say their budget is either “not sufficient” (38%) or that they are “unsure” (18%) about whether it meets their needs, as they’re caught between growing risk and limited internal resources. While over 80% report having security plans, only one in five allocate more than 6% of their budget to cybersecurity. They’re drawing attention from potential adversaries, but they’re not mature enough to scale security effectively.

Bigger budgets lead to better tools

By contrast, larger SMBs (150-249 employees) show stronger, more advanced security postures. Nearly 90% of these businesses have formal security plans, and almost half (45%) allocate more than 6% of their budget to security. They’re more than twice as likely to use AI-powered tools than smaller businesses.

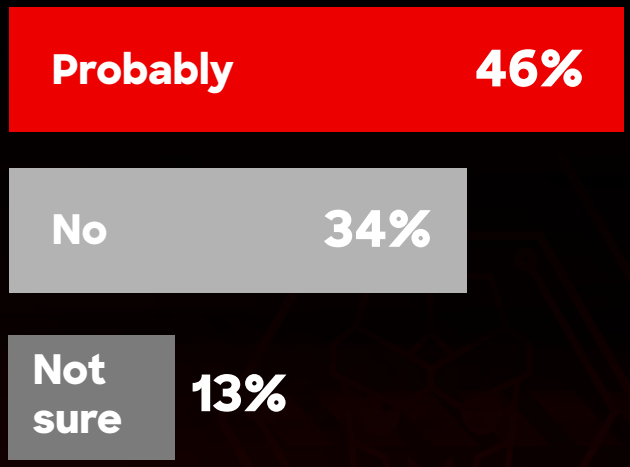
KEY FINDING 3

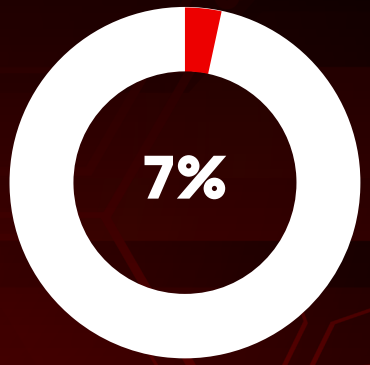
Affordability vs. Effectiveness: SMBs Shouldn't Have to Choose

SMBs are strikingly aware but challenged by costs

For many SMBs, the biggest barrier to stronger cybersecurity isn't a lack of awareness — it's a lack of resources. Cost is the most commonly cited obstacle to adopting advanced security tools, with 66% of SMBs naming it as their top concern. Just 7% of all SMBs say their cybersecurity budget is "definitely sufficient."

Budget Sufficiency





Just 7% of all SMBs say their cybersecurity budget is "definitely sufficient."

Cost-first choices can backfire

Although 67% of SMBs prioritize cost when choosing cybersecurity tools, only 57% focus on protecting against advanced threats. This emphasis on affordability over effectiveness often results in false savings where lower-cost solutions fail to deliver real protection, leaving businesses exposed to expensive breaches.

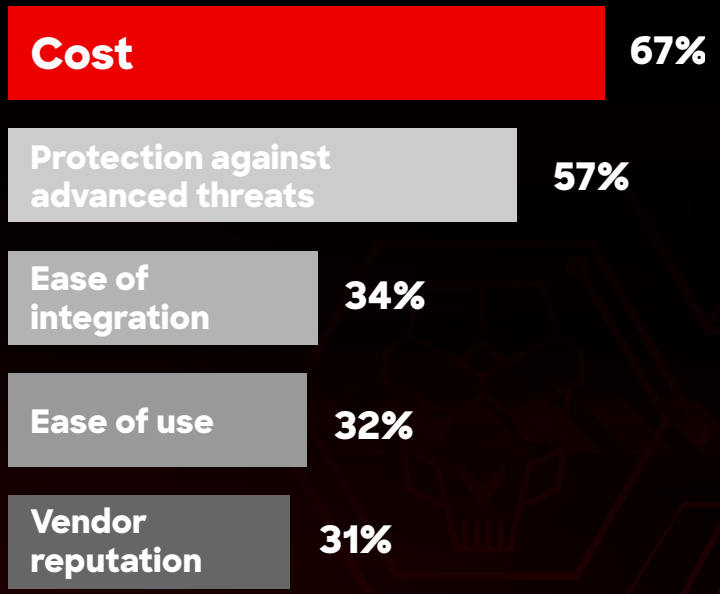
Lean teams, growing threats

Getting the most value from available funds is a challenge for SMBs. Two in five SMBs without a cybersecurity plan say they also lack in-house expertise, and over a quarter of those without a plan still don't view cybersecurity as a top business priority. Even when the intent is there, limited budgets and lack of subject matter expertise lead to hard trade-offs that result in poor decision-making and weak cybersecurity execution, leaving critical systems exposed to fast-moving threats.

Expertise gaps widen exposure

Without dedicated security teams, many SMBs rely heavily on general IT staff (70%) or outsourced providers (21%). As a result, security tools must be easy to use for general IT staff and look and feel like the standard software-as-a-service (SaaS) solutions these teams use to run the rest of the business.

Top 5 Solution Decision Factors



KEY FINDING 4

The Smallest Businesses Are Ransomware Targets

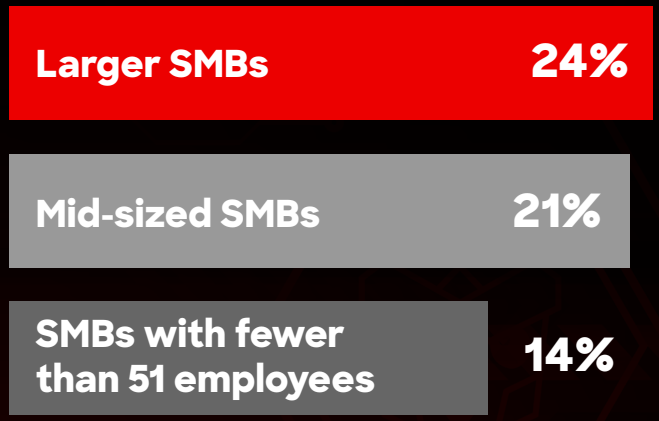
Clash of perception and reality

Ransomware was identified as the greatest cybersecurity concern by 21% of mid-sized SMBs and 24% of larger SMBs but only by 14% of those with 50 employees or fewer. However, among businesses that experienced a cyber incident, ransomware hit the smallest organizations harder: 29% of those with fewer than 25 employees reported a ransomware attack, compared to 19% of businesses with 150-249 employees. These attacks often exploit the weaknesses common among smaller businesses: limited in-house expertise, inadequate security controls, and reactive IT strategies.

Small businesses struggle to recover

Micro-businesses are also the least prepared to recover from an incident. Three-fourths of micro-businesses say a major cyberattack would "likely" or "definitely" put them out of business, compared to less than one-third of mid- and large-sized SMBs. The smallest businesses are especially vulnerable to this kind of disruption because many of them lack the plans, backups, cyber insurance, or vendor partnerships needed for recovery.

Ransomware Identified as the Greatest Cybersecurity Concern by SMBs



Businesses Hit by Ransomware

KEY FINDING 5

SMBs Want Actionable Help, Not Just Tools

Knowledge gaps and complexity stall progress

Many SMBs recognize the importance of improving their cybersecurity posture, but knowing what steps to take next is a challenge. A lack of internal expertise — combined with the complexity of modern security tools — often leaves these organizations unsure where to begin. Half of SMBs report feeling overwhelmed by the number of cybersecurity tools and choices on the market, underscoring the need for clarity and simplified decision-making.

SMBs seek expert guidance and practical insights

Nearly 70% of SMBs turn to recommendations from IT consultants and security experts when selecting cybersecurity solutions. They seek product comparisons, live demos, case studies, and best practices that speak directly to their needs. To move forward with confidence, SMBs need clear, actionable guidance that supports them at every stage of their security journey.

Enterprises have a role to play

Larger organizations — including vendors, partners, and enterprise customers — are in a strong position to help close the gap. Survey respondents say they value vendor education, platform simplicity, and built-in automation to reduce manual workloads and accelerate protection. This presents an opportunity for security providers to lead with enablement, not just technology, and for enterprise partners to invest in raising the security baseline across their ecosystems.

Turning Awareness into Action

Today's adversaries are targeting smaller businesses with enterprise-level tactics, moving faster, striking harder, and exploiting even minor gaps in visibility or response. Though awareness is high across the SMB space, execution lags. The result is a dangerous gap between knowing the risks and being able to stop them.

But that gap doesn't have to persist. With the right support from trusted vendors and strategic and enterprise partners, SMBs are far more likely to reduce their risk exposure. Managed services, AI-powered tools, and integrated platforms that can grow as needed are already helping many smaller businesses improve outcomes without overwhelming their teams.

Enterprises also have a stake in securing the SMBs they rely on. Whether it's a supplier, service provider, or channel partner, every third party represents a potential path into the broader ecosystem. Everyone benefits when enterprises help SMBs improve their security posture through guidance, tooling, or shared intelligence. Risk decreases, resilience improves, and the entire supply chain becomes harder to compromise.

Cybersecurity isn't a solo effort. For SMBs and enterprises alike, partnership is the key to staying ahead.

Working Together to Help SMBs Stop Breaches

CrowdStrike sits at the intersection of enterprise security and SMB resilience, empowering organizations of all sizes to stop breaches. By equipping SMBs with the same AI-native protection, managed services, and expert guidance trusted by the world's largest companies, CrowdStrike helps secure the broader ecosystem. When enterprises partner with their SMB vendors, suppliers, and service providers to extend cybersecurity best practices, everyone benefits. Stronger SMBs mean stronger enterprises and a safer, more resilient digital supply chain.

CrowdStrike's Solutions for SMBs

CrowdStrike offers SMBs flexible cybersecurity options — from CrowdStrike Falcon® Go, an easy-to-use, out-of-the-box solution, to CrowdStrike Falcon® Enterprise for small businesses needing additional endpoint detection and response (EDR) capabilities — all built on the same AI-powered platform. For SMBs seeking fully managed protection, Falcon Complete® Next-Gen MDR delivers 24/7 expert monitoring and threat response, helping eliminate risks before they disrupt business operations — no in-house security team required. In the event of a breach, CrowdStrike's Small Business Incident Response Services deliver fast, expert-led investigation, containment, and recovery — so you can get back to business with confidence.

Resources for SMBs

- **Take CrowdStrike's small and medium business cybersecurity recommendation assessment to discover which solution is best for securing your business.**
- **Sign up for a 15-day free trial and explore the most popular CrowdStrike solutions for your small business.**

Resources for SMB Partners

- **Learn more about the CrowdStrike Enterprise SMB Partnership program to see how you can become a partner and help deliver world-class protection to your SMB customers.**

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.