CORO

Understanding the SME Security Workload Crisis in a Changing World

Table of Contents

Executive Summary

A Changing World for Businesses Globally

- An Evolving Threat Landscape
- Reliance on Cloud-Based Data Storage
- Remote and Distributed Work Environments

The Security Challenges SMEs Face

- Lack of Resources
- Misconfigurations
- Tool Overload
- Exhaustion and Alert Fatigue
- Endpoint Management Burdens
- Onboarding and Integration Challenges
- Regulatory Compliance

The Incompatibility of Enterprise-Level Cybersecurity Solutions for SMEs

- Extensive Operational Demands
- Complexity and Fragmentation
- Manual Processes
- Limited Actionable Intelligence
- Integrated Solution

Key Aspects for SMEs to Consider When Choosing A Cybersecurity Solution

- Resource Efficiency
- Platform Authenticity

Conclusion: Moving Forward

About Coro

References

Executive Summary

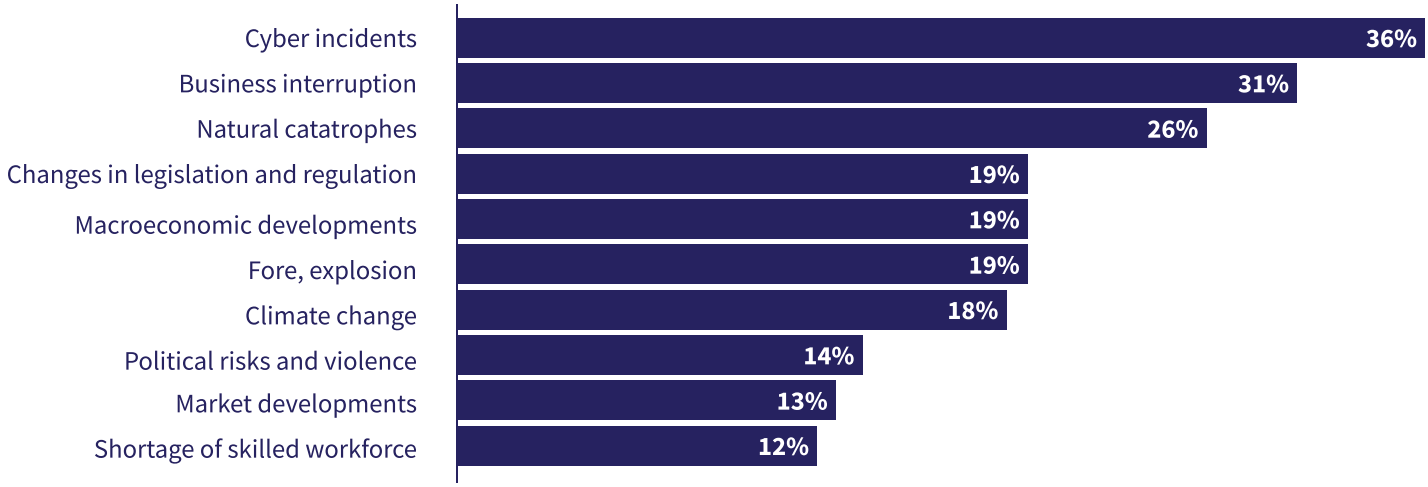
Small and medium-sized enterprises (SMEs) are at a critical juncture in the digital age. With an escalating number of cyber threats, many need more resources and expertise to protect themselves effectively. Findings presented in Coro's 2024 SME Security Workload Impact Report, supported by additional insights from the Coro-sponsored TechTarget Enterprise Strategy Group (ESG) research and other industry research, shed light on the overwhelming burdens SMEs face in managing cybersecurity. This white paper explores these challenges and offers strategic recommendations, emphasizing the need for modular, scalable solutions tailored to the specific needs of SMEs.

A Changing World for Businesses Globally

The Allianz 2024 Risk Barometer Report indicates the rise in cyber threats as a leading cause of destruction for businesses of all sizes. The report lists cyber incidents as the number one risk factor for businesses globally, surpassing disruption to business continuity in parameters such as financial damage, recovery capabilities, and ability to stay in business.

The top 10 global business risks for 2024

The top risks and mjor risers in this year's annual business risk syrvey reflect the big issues facing companies around the world right now - digitalization, climate change and an uncertain geopolitical environment. Many of these risks are already hitting home, with extreme weather, ransomware attacks and regional conflicts expected to test the resilience of supply chains and business models further.



A Changing World for SMEs

According to Accenture cybercrime study, while companies of all sizes have experienced a rise in cyberattacks, 43% of all cyberattacks in recent years have been directed at midmarket organizations (the study sets small businesses at 10-49 employees and medium-sized organizations at 200-499 employees).

Findings presented in the 2024 U.S. Small Business Administration (SBA) Summit confirm the reasons for SMEs' increased exposure to cyber threats. According to data presented at the summit, midmarket organizations endure a particular set of challenges unlike those of larger corporations, primarily:

- added exposure to the evolving threat landscape
- growing reliance on cloud-based data storage
- increased difficulties with the shift to remote and distributed work environments

Data collected from an SBA survey emphasizes that 88% of small business owners felt their business was vulnerable to cyberattacks, yet they lacked the budgets for advanced security solutions, had limited time to devote to cybersecurity, or didn't know where to begin. The Accenture study similarly concurs that only 14% of surveyed SMEs were adequately prepared to defend themselves against a cyberattack.

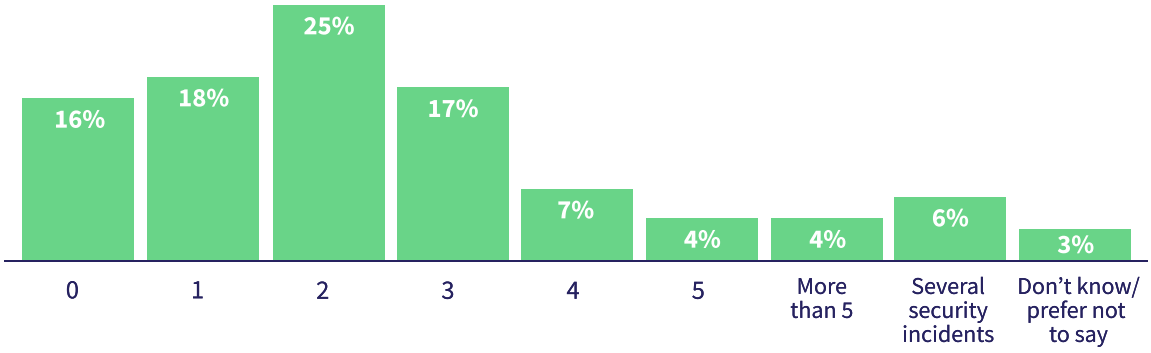
An Evolving Threat Landscape

Many SMEs mistakenly assume their small size makes them invisible or uninteresting to cyber criminals. This couldn't be further from the truth. Data gathered by the Pennyrile Technology Group shows that about half of all cyber-attacks are aimed at small businesses and that 68% of all small businesses experience a cyber attack at least once. Gartner's 2024 report on the evolving cybersecurity threat landscape reveals an uptick in midmarket organizations' exposure to threats. This trend has been on the rise for several years, with a 2021 Verizon report concluding that 46% of all cyber breaches that year targeted businesses with fewer than 1,000 employees. The evolving threat landscape and the rise in attacks can be linked to the growing sophistication of attack tactics employed by cybercriminals, coupled with companies' growing reliance on cloud environments.

The ESG Report similarly indicates that 63% of the businesses surveyed reported experiencing two or more security incidents over the past two years, leading 83% of respondents to increase their investment in security in the next year. The expanding attack surface underscores the need for continuous monitoring and proactive defenses, areas where SMEs often face significant resource constraints.

Approximately how many times has your organization experienced a security incident over the past two years?

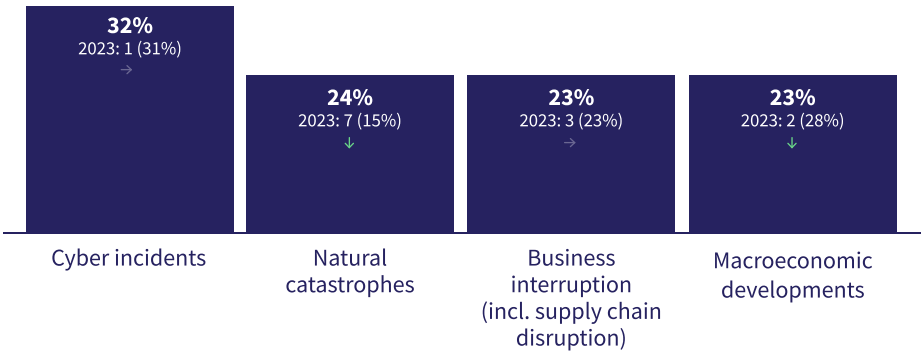
(i.e. system compromise, malware incident, DDoS attack, targeting phishing attack, data breach, etc.)
Percent of respondents, N=379



The Allianz 2024 Risk Barometer Report paints a similar picture by focusing on the cybersecurity risks to SMEs relative to other risks faced by businesses of this size.

Top 4 risks for small companies in 2024

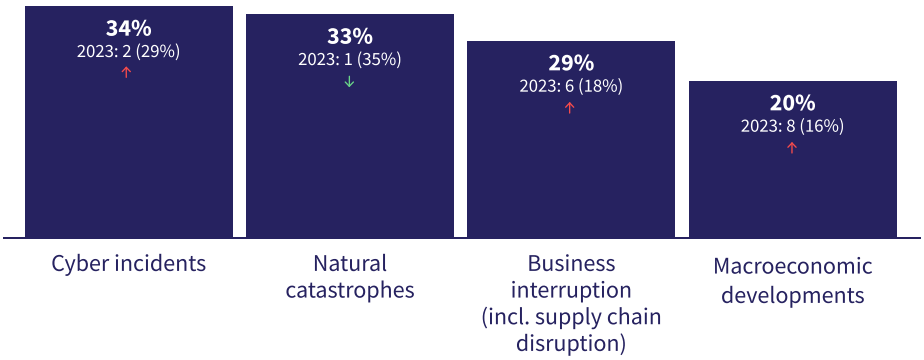
<US$100mn annual revenue



Source: Allianz Risk Barometer 2024. Total number of respondents: 937. Respondents could select more than risk. Top 4 answers.

Top 4 risks for mid-size companies in 2024

<US$100mn + US$500mn annual revenue



Source: Allianz Risk Barometer 2024. Total number of respondents: 937. Respondents could select more than risk. Top 4 answers.

Reliance on Cloud-Based Data Storage

In 2024, a Gartner report revealed a 25% increase in deployed cloud technologies compared to 2023's 50% cloud adoption, bringing the percentage of cloud technologies in deployment to 75% across I&O environments.

According to the ESG Report, 35% of surveyed companies view cloud security as their number one area of focus. 25% of respondents further note that lack of visibility into their cloud environments is one of the top five security issues they face.

Which of the following cybersecurity related topics do you believe are the biggest areas if focus/mindshare for your organization's security team? (Percent of respondents, N=379, three responses accepted)

Remote and Distributed Work Environments

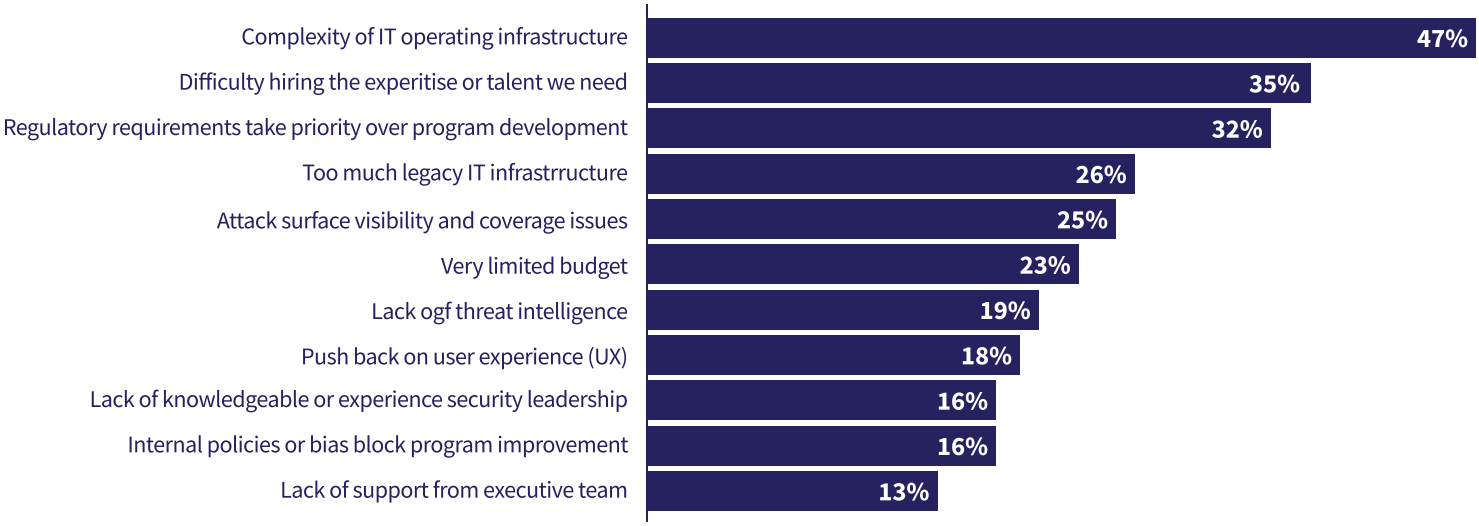
The rise of remote work has introduced new challenges in securing distributed networks and devices. A 2023 Forrester report indicates that shifting to remote and hybrid working models has magnified risk exposure and operational IT challenges.

According to the ESG Report, 61% of organizations indicate that their public cloud services are among their top areas of day-to-day IT involvement. This widespread reliance on cloud services and the expansion of remote work has substantially increased the attack surface that SMEs need to manage. Ensuring secure remote access and protecting endpoints from vulnerabilities have become critical priorities.

The Security Challenges SMEs Face

Recent findings in the SME Security Workload Impact Report, as well as research conducted by the scientific journal IEEE Access, suggest that difficulty managing complex security stacks, talent shortages, and the burden of regulatory compliance are just some of the reasons leading to IT demoralization and high burnout rates in midmarket organizations.

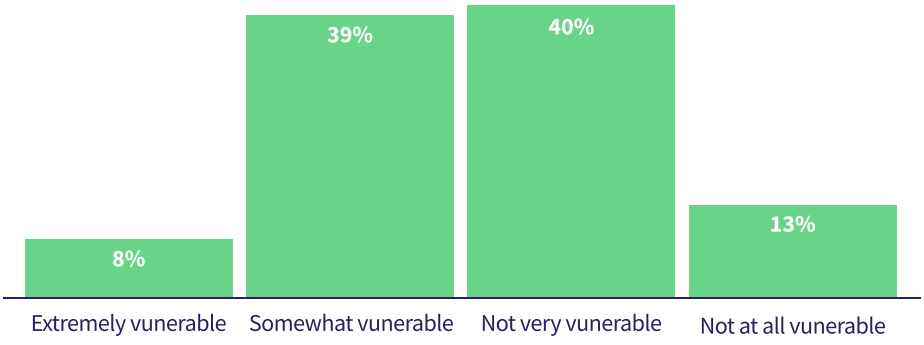
What constraints does your organization deal with as part of the process for building, refining and managing its cybersecurity program? (Percent of respondents, N=379, multiple responses accepted)



Data from the Coro-sponsored ESG Report similarly indicates that while cyber threats do not discriminate based on organizational size, small, understaffed IT teams, lack of security expertise, and high dependency on third-party technology expose SMEs to cyber threats.

The report highlights IT directors' thoughts on their risk exposure, indicating that nearly half of respondents reported feeling either extremely (8%) or somewhat (39%) vulnerable to cyberattacks or data breaches.

In your opinion, how vunerable is your organization to a significant cyberattack or data breach? i.e. one that disrupts business processes or leads to theft of sensitive data? (Percent of respondents, N=379)



These reports jointly paint a picture of, on the one hand, the need for cybersecurity and, on the other hand, the particular set of challenges faced by midmarket organizations in acquiring the cybercity they need.

Lack of Resources

Many midmarket businesses and SMEs need more budgets, small IT teams, and access to advanced cybersecurity tools. This lack of resources makes implementing and maintaining adequate security measures difficult.

The ESG Report reinforces these findings, noting that 35% of organizations need help hiring the expertise or talent they need for their cybersecurity programs.

Misconfigurations

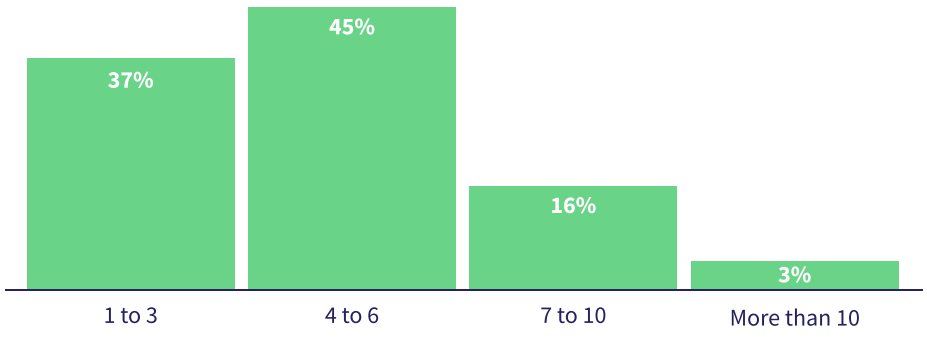
According to the World Economic Forum, human error is the leading cause of cybersecurity breaches, accounting for 95% of incidents. Human error is a significant risk for midmarket businesses, particularly in security settings. Misconfigurations often arise from a lack of expertise, leading to critical vulnerabilities that cybercriminals can exploit.

Additionally, the ESG Report highlights that 47% of organizations find the complexity of their IT operating infrastructure a significant constraint, which can exacerbate the risk of misconfigurations.

Tool Overload

SMEs frequently manage many cybersecurity tools, leading to fragmented security efforts and alert fatigue. The Coro report found that the average SME uses over ten different tools, which can overwhelm IT teams and result in missed alerts. The ESG Report adds that 45% of organizations purchase security products and services multiple providers, further complicating integration and management.

In your estimation, from how many different cybersecurity technology solutions and/or service providers does your organization currently buy security products, subscriptions, and/or managed services?
(Percent of respondents, N=379)



Exhaustion and Alert Fatigue

With 73% of SME IT teams missing security alerts due to the sheer volume of notifications, alert fatigue is a severe issue. This fatigue can delay responses to critical incidents, exposing businesses to potential breaches. The data from the ESG Report supports this, showing that 29% of organizations agree that the alerts from their endpoint security solutions are overwhelming.

Endpoint Management Burdens

Managing endpoint devices is a significant challenge for SMEs, particularly given the number of devices that need monitoring and maintenance.

According to the ESG Report, the average SME manages 656 endpoint devices, with many deploying multiple security agents per device. This scale of endpoints creates a significant management burden, as 53% of respondents from the ESG Report indicate that their endpoint agents require daily or weekly updates. The frequent need for updates and the complexity of managing these endpoints can overwhelm smaller IT teams, increasing the risk of vulnerabilities if updates are missed.

The ESG Report highlights that 26% of organizations agree they are spending too much time chasing issues related to endpoint security. These insights underscore endpoint management's substantial operational burden on SMEs, particularly when resources are already stretched thin.

How many endpoint devices do you manage?

10%
Less than **200** devices

37%
200–500 devices

32%
501–1000 agents

15%
1001–1500 agents

3%
1501–2000 devices

2%
More than **2000** devices

1%
Don't know

Those surveyed reported an average of **656 endpoint devices to manage**

How many endpoint agents are installed per device?

10%
1 agent

58%
2–3 agents

23%
4–5 agents

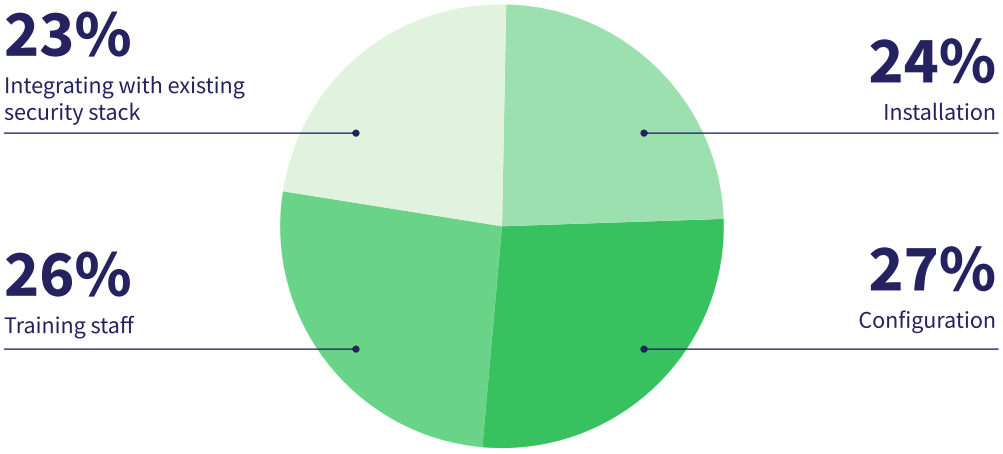
8%
More than **5** agents

1%
Don't know

SMEs average 4 **security endpoint agents per device**

Onboarding and Integration Challenges

Onboarding new cybersecurity tools is another significant challenge for SMEs. The Coro report reveals that a new tool takes an average of 4.2 months to fully operational. The ESG Report complements this by highlighting that 47% of organizations need help keeping up with new or changing IT infrastructure, which can delay the full utilization of new security measures.



Regulatory Compliance

The growing complexity of data security and privacy regulations puts additional strain on SMEs. Without dedicated legal or compliance teams, meeting regulatory requirements can be a daunting task, with significant financial and legal repercussions for non-compliance.

The ESG Report reveals that 41% of organizations are driven by the need to comply with data privacy laws, making this a top priority. Moreover, 21% of organizations highlighted that maintaining compliance and governance capabilities is one of the biggest gaps in their security posture.

The Incompatibility of Enterprise-Level Cybersecurity Solutions for SMEs

While enterprise-grade cybersecurity solutions are robust and comprehensive, they often fall short when applied to the unique needs of small and medium-sized enterprises (SMEs). Data from the Coro-sponsored ESG Report indicates that small, understaffed IT teams, a lack of security expertise, and a high dependency on technology put SMEs at a clear disadvantage when attempting to adopt enterprise-level security solutions.

The challenges most often stem not from the tools but from their adoption and management complexity and the mismatch between these complexities and the operational realities of small IT teams.

Extensive Operational Demands

Enterprise cybersecurity solutions are designed for large, specialized IT teams with abundant resources. However, for SMEs, these tools impose significant operational demands. The intricate processes required for continuous monitoring and maintenance strain the limited time and personnel available, leading to inefficiencies and potential security gaps.

According to the ESG Report, 47% of organizations cite the complexity of IT operating infrastructure as a significant constraint on their cybersecurity programs.

Complexity and Fragmentation

The specialized nature of enterprise tools often results in a segmented approach to security, where different tools are designed to address specific threats or network areas. For SMEs, this creates a complex and fragmented security landscape, making it difficult for smaller teams to maintain a cohesive and effective defense strategy.

The ESG Report supports this by indicating that 34% of organizations struggle with maintaining a consistent security posture across an expanded attack surface.

Manual Processes

Enterprise solutions typically emphasize manual intervention for threat detection and response. While this approach can be effective in environments with extensive human resources, SMEs are often disadvantaged. The lack of automation in these tools means that routine security tasks require constant attention, leading to delays in addressing critical issues and an overall heavier workload for IT teams. The report further reveals that 26% of respondents are pushing for more automation in security operations to address these challenges.

Limited Actionable Intelligence

In large enterprises, security tools are often part of a broader ecosystem that includes teams of analysts and engineers trained to interpret and act on the data generated. SMEs, however, often do not have access to such expertise, limiting their ability to act on security insights. The reality of smaller and less security-experienced IT teams creates gaps between data output and the ability to prioritize and remediate threats based on this data.

The ESG Report highlights that 18% of the surveyed organizations consider threat intelligence a major point to improve on, describing the gap between data and its usage as a primary concern. It is up to solution providers to be mindful of the challenges faced by midmarket organizations and develop their solutions to support SMEs' team size and expertise level. It is also up to SMEs to recognize their limitations and search for security software that supports them in executing on security alerts rather than merely providing detailed, comprehensive threat intelligence, which they do not have the bandwidth to act on.

Integrated Solution

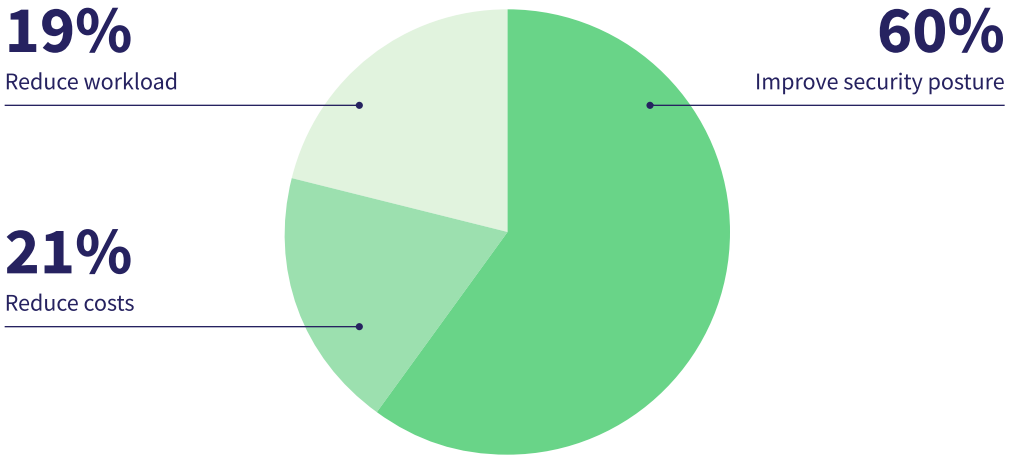
Many tools today call themselves "security platforms" with little regard for what makes a genuine platform. The term "platform" is often used interchangeably with "solution" and "tool," requiring that companies be extremely vigilant in deciphering genuine platforms from other solutions. While large enterprises have the budgets, manpower, and expertise to handle non-centralized security solutions and to manage diverse security stacks, SMEs' are the primary beneficiaries of integrated platform solutions.

A true security platform will include elements of modular architecture that support scalability. It will be centered around a unified management interface that allows real-time visibility into the organization's entire network. It should also use advanced automation and AI capabilities that replace the human touch, taking the workload of routine ticket management off IT teams.

Key Aspects for SMEs to Consider When Choosing A Cybersecurity Solution

To address SMEs' particular set of challenges, it is crucial small businesses consider these points when selecting cybersecurity solutions:

Why do you want to consolidate your cybersecurity?



Resource Efficiency

A cybersecurity solution for SMEs must be designed with resource constraints in mind. Automation should play a central role, enabling the solution to save time and reduce workload. It should be robust, flexible, and scalable, capable of adapting to the organization's evolving needs without imposing excessive costs.

Platform Authenticity

The term "platform" should be more than a marketing buzzword. A genuine integrated security platform should include the following:

- Integrated Approach: A unified solution that offers comprehensive protection without requiring complex integrations of multiple tools. An integrated approach reduces the risk of missing critical alerts, streamlines operations, and alleviates the burden on IT teams.
- Modular Architecture: The ability to customize security by selecting specific modules that meet the business's unique needs.
- A Single Source of Truth: A unified management interface that provides real-time visibility and control over the organization's security posture.
- Scalability: A platform that can grow with the business, supported by flexible pricing models that align with budgetary realities.
- Simplified Compliance Management: Tools that automate compliance checks and reporting, making it easier for SMEs to adhere to regulatory requirements.

Advanced Automation and AI: Features that automate routine tasks and provide smart prioritization and remediation, reducing the workload on IT teams and enabling quicker, more effective responses to threats.

Conclusion: Moving Forward

SMEs urgently need cybersecurity solutions that are effective and manageable within their resource constraints. the road to best supporting SMEs is a joint effort for small businesses and security software developers. Firstly, SMEs must recognize their operational challenges and realize that enterprise-level solutions may not be the best for them. They must require that the security industry develop solutions fit for their particualr needs. Secondly, security solutions must recognize that cybersecurity is not a 'one size fits all', and properly market themselves to the segments they best serve.

By focusing on true platforms that streamline security through modularity, scalability, integrated resources, advanced automation, and AI, SMEs can alleviate their security workload and better protect their businesses in an increasingly complex threat landscape.

About Coro

Coro is the top-tier workspace security platform for small and medium-sized businesses. It provides automated protection for cloud, email, devices, and networks, shielding organizations from various threats without burdening IT teams. The Coro platform offers scalable, easy-to-manage security without unnecessary complexity or high costs. Coro has been named a leader in G2-Grid for EDR/MDR, and has received Triple A grading (AAA) from the testing institute SE LABS. We have also won awards for Best Performer by customer reviews. In early 2024 Coro was named a Global InfoSec Award Winner during the RSA Conference. Most recently, the company was ranked in the top 5 security products by G2.

References

2023 Report: State of Cybersecurity Relisince | Accenture

2024 Report: Risk Barometer | Allianz

“America’s small Businesses Aren’t Ready for a Cyberattack” | CNBC

2023 Report: Mastering Endpoint Security in a Hybrid World | Forrester

2024 Report: How to Respond to the Threat Landscape in a Volatile, Complex, and Ambiguous World | Gartner

2022 Survey: Cybersecurity of SMBs: Challenges, Research Focus, and Recommendations | IEEE Access

“How Much Do SMBs Really Spend on Cybersecurity?” | Pennyrile Technologies

2024 U.S. Small Business Administration Summitt | SBA

“Protect Your Small Business from Cybersecurity Attacks” | SBA

“43 Percent of Cyber Attacks Target Small Business” | Small Business Trends

2022 Data Breach Investigations Report | Verizon

2021 SMB Data Breach Statistics | Verizon

2022 Global Risk Report | World Economic Forum