FORRESTER®

Attackers Don’t Sleep, But Your Employees Need To

Engage Partners To Fill Skill Gaps And Enable 24/7 Coverage

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY PONDURANCE | JULY 2022

Same Threats, Same Attacks — Way Fewer Resources

The cybersecurity threat landscape is growing so rapidly, it's tough for any organization to keep pace. And, while all companies struggle to acquire and retain talent, small and medium-size businesses (SMBs) are acutely challenged due to limited resources and advancement opportunities. Therefore, many exist in a reactive state and, when things go bump in the night, detection and response efforts are often delayed.

Pondurance commissioned Forrester Consulting to explore how SMBs are evolving their cybersecurity operations practices to protect their organizations and the people they serve.

Key Findings

While the threat landscape is evolving and bad actors never sleep, most SMBs lack 24/7 coverage.

In this already hypercompetitive market, SMBs struggle to fill internal resource gaps, leaving them with serious resource constraints throughout the threat management lifecycle.

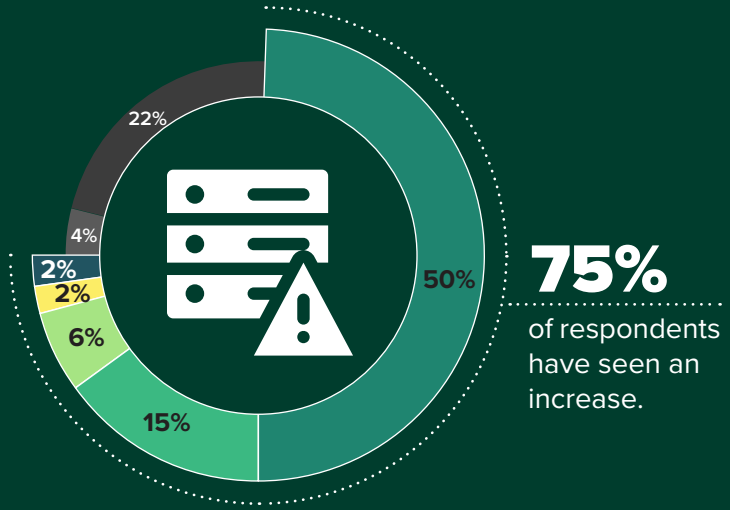
Moving forward, SMBs are relying on external partners for both platforms and services to close their people, process, and technology gaps, resulting in minimized risk and increased bandwidth for SMBs to focus on high-value work that drives their businesses forward.

SMBs Haven't Been Left Out Of The Cyberattack Party

Cyberattack-related news relentlessly bombards the world. Business leaders should no longer ask, "Could this happen to our organization?" because yes — it most certainly can. Everyone is a potential target. Although SMBs aren't sitting on mountains of cash (relative to enterprises), their money spends the same and their data is just as valuable. On top of that, system vulnerabilities and lack of comprehensive monitoring, detection, response, and remediation capabilities leave them tasty targets. Sixty-nine percent of respondents in this study agree, saying their organizations face critical and expanding cybersecurity threats, and 75% say cyberattacks have increased in the past three years.

"How has the number of attempted cyberattacks to your organization changed in the past three years?"

- 1% to 50% decrease
- No change
- 1% to 50% increase
- 51% to 100% increase
- 101% to 200% increase
- 201% to 300% increase
- More than 300% increase



75% of respondents have seen an increase.

69%

"Our organization faces critical and expanding cybersecurity threats."

(Showing "Agree" and "Strongly agree")

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY PONDURANCE | JULY 2022

Base: 232 IT and security operation strategy decision-makers in the US
Note: Showing seven responses; percentages may not total due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Pondurance, May 2022

SMBs Have Limited Internal Cybersecurity Resources, And Most Rely On Partners

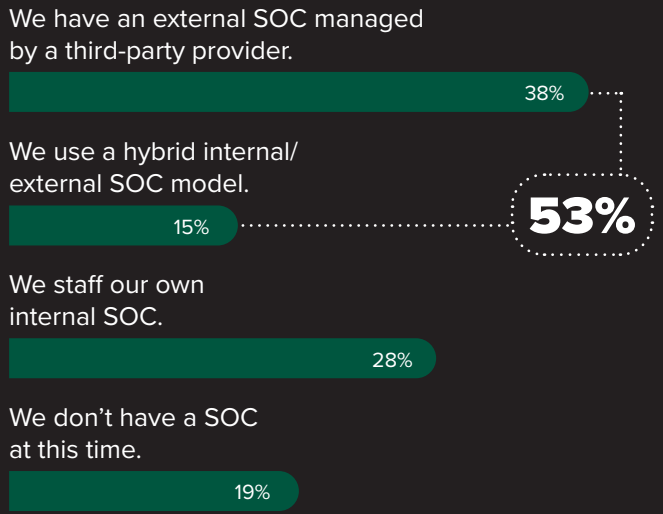
A sound cybersecurity strategy requires executive buy-in and dedicated security leadership. Executing on that strategy requires the tools and manpower to continuously monitor and respond to threats. Most SMBs lack the internal headcount to do this well. Sixty-seven percent of respondents report having 10 or fewer full-time employees solely dedicated to cybersecurity.

Enter external partners. Most SMBs (53%) rely on external partners to keep their security operations centers (SOCs) afloat.

For the purposes of this study, a SOC is defined as a centralized function consisting of an information security team monitoring, detecting, analyzing, and responding to cybersecurity incidents.

67% **of respondents' organizations have one to 10 FTEs solely dedicated to cybersecurity.**

"If applicable, which of the following best describes the current state of your security operations center (SOC)?"



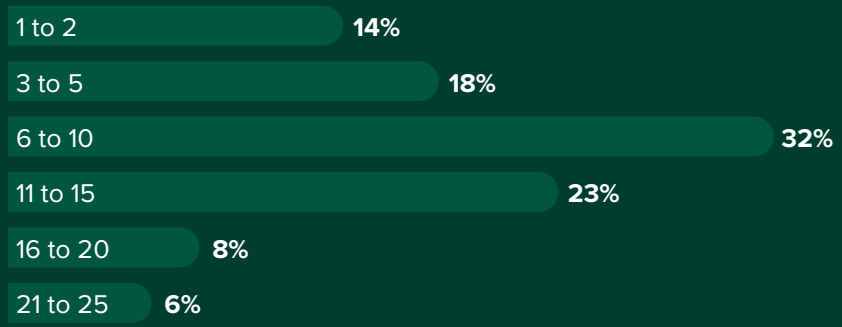
Base: 232 IT and security operation strategy decision-makers in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Pondurance, May 2022

Naptime For SMBs Is Playtime For Bad Actors

Threat actors work around the clock with attacks originating from all corners of the world. This requires businesses to always stay alert for new threats and vulnerabilities and respond rapidly to an incident at any moment. Yet this is not the reality for most SMBs today. For those who have a SOC, 57% of respondents report their organizations lack 24/7 coverage. Of those operating a purely internal SOC, 64% have 10 or fewer employees (and almost one-third have five or fewer). These are not enough resources to run a 24/7 SOC without exhausting employees.

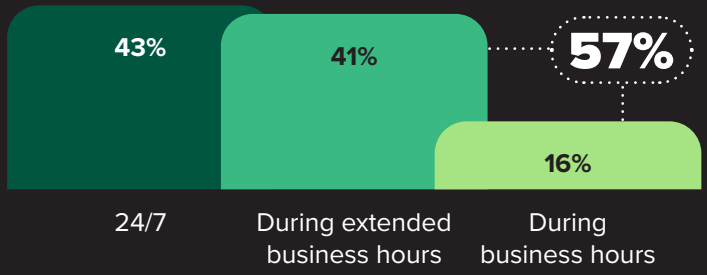
Cybercriminals will typically find the most inconvenient times for your business to launch their attacks, so detecting and responding to them at all hours is imperative.

"How many employees work for your internal SOC?"



Base: 66 IT and security operation strategy decision-makers in the US whose companies operate a purely internal SOC
Source: A commissioned study conducted by Forrester Consulting on behalf of Pondurance, May 2022

"When does your SOC operate?"

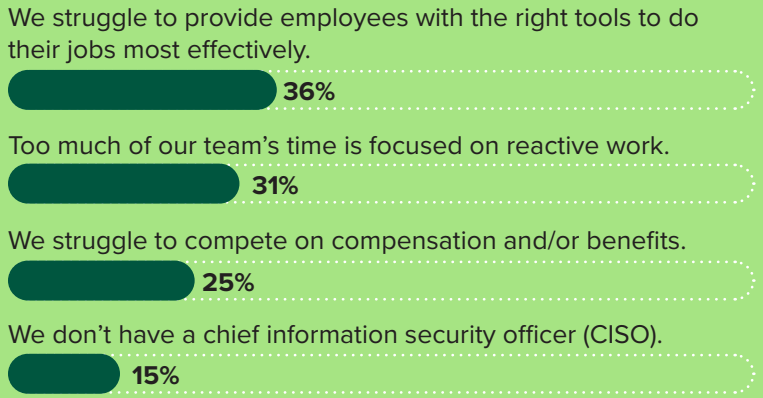


Base: 188 IT and security operation strategy decision-makers in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Pondurance, May 2022

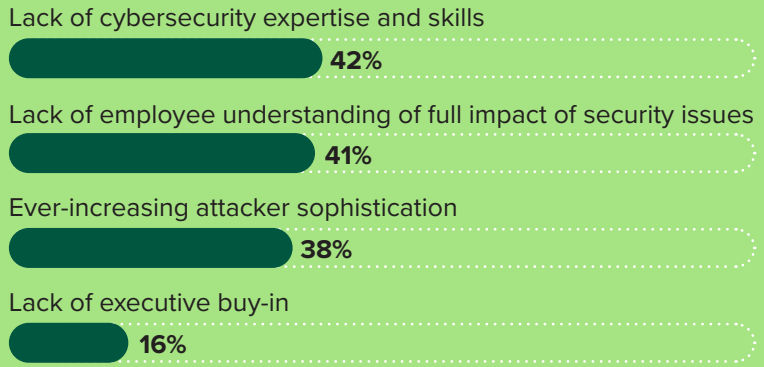
Cybersecurity Operators Lack Sufficient Tooling And Training

Executive leadership should be hyperaware of the perils of underinvesting in cybersecurity capabilities by now. While very few respondents in this study report struggling with a lack of executive leadership (15%) and buy-in (16%), it appears there is a disconnect in the level of prioritization and resources dedicated to giving employees the tools they need to do their jobs effectively. Respondents report lacking the right tools (36%), bandwidth to work proactively (31%), cyber skills (42%), and employee awareness (41%).

"Which of the following makes it challenging for your company to hire and/or retain cybersecurity talent?"



"Which of the following hinder your security operations team from protecting your organization from all cyberattacks?"

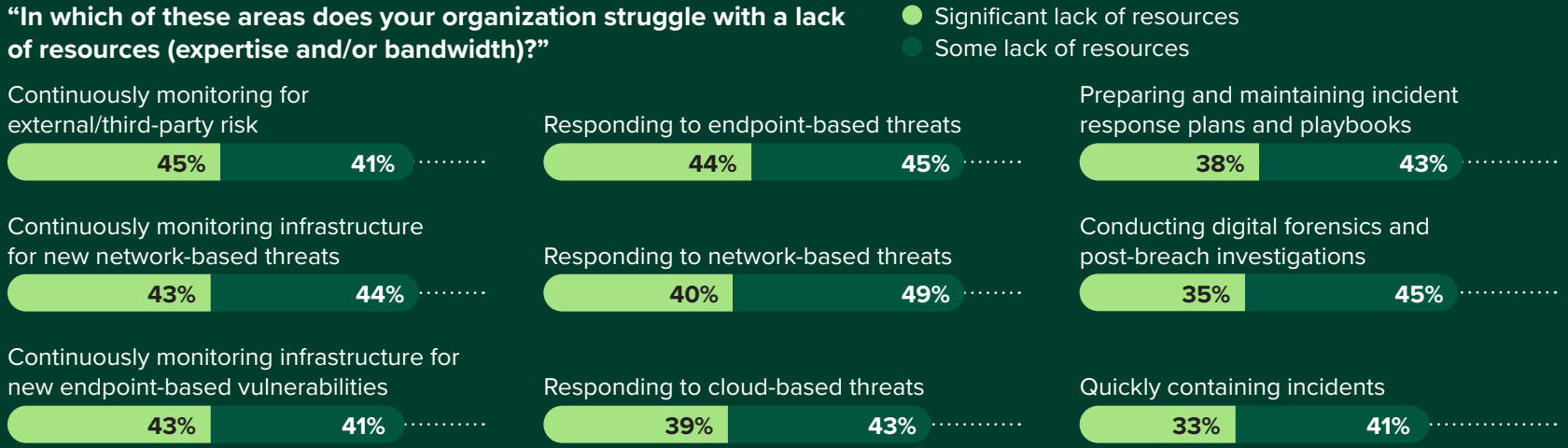


Base: 232 IT and security operation strategy decision-makers in the US
Note: Showing four responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Pondurance, May 2022

SMBs Are In The Early Stages Of Their Security Operations Maturity Journeys

Resource constraints continue to be a top challenge for SMBs, which hinders them from maturing their security operations practices. For example, while Forrester finds that applications are a common entry point today, SMBs still struggle detecting and responding to endpoint- and network-based threats and vulnerabilities. They also struggle to monitor for external risk and respond to cloud-based threats. Given the significant lack of resources across these environments, it comes as no surprise that SMBs exist in a reactive state. Being underwater, they also lack bandwidth to focus on strategic activities like developing plans and playbooks and conducting thorough postbreach investigations.

"In which of these areas does your organization struggle with a lack of resources (expertise and/or bandwidth)?"



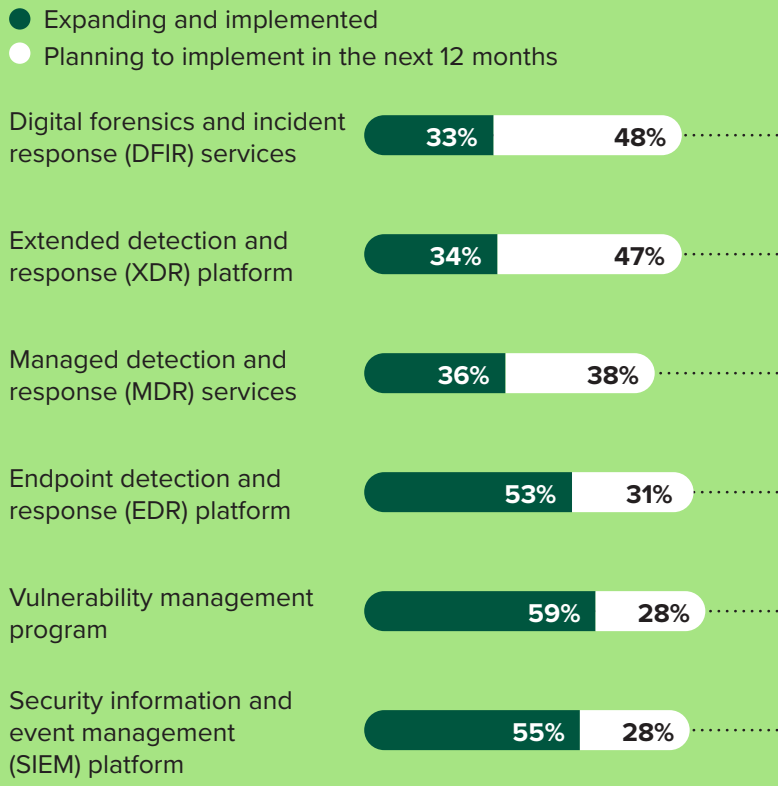
Base: 232 IT and security operation strategy decision-makers in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Pondurance, May 2022

Investments In Detection And Response Services And Tools Are Growing To Address Rising Threats

SMBs need a release valve, especially in the areas they struggle most. As such, they're turning to external partners to elevate their detection and response capabilities. The top services and tools SMBs plan to implement in the next 12 months are managed detection and response (MDR) (38%), extended detection and response (XDR) (47%), and digital forensics and incident response (DFIR) (48%).

They are also not looking for technology alone to address their needs. When asked about their cybersecurity operations' budget allocation, respondents report spending 40% on technology/ platforms and 60% on managed and consulting services. The combination of technology and service is important with technology streamlining the work of existing employees and support services expanding team bandwidth and expertise.

"In which of the following areas is your organization interested in engaging an external security operations partner?"



Base: 232 IT and security operation strategy decision-makers in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Pondurance, May 2022

Collaboration With Partners Helps Mitigate Risk

SMBs see their external partners as extensions of their own teams, relying on them for close collaboration during incidents (52%) and to fill internal skill gaps (47%).

External partners' abilities to round out SMB cybersecurity capabilities not only mitigates risk to the businesses but also satisfies cyber insurance requirements (42%). In the wake of increasing ransomware attacks, supply chain incidents, etc., cyber insurance carriers continue to raise premiums and elevate the requirements of policy holders and applicants.

Having a sound cybersecurity practice, in part by engaging the right external partners, will help SMBs mitigate overall risk and obtain cyber insurance policies.

"What are the most important drivers of engaging an external security operations partner?"

Base: 232 IT and security operation strategy decision-makers in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Pondurance, May 2022

Engaging The Right Partners Stimulates Growth

Security program maturity is necessary to both mitigate risk and support business resiliency and growth. Sixty-seven percent of SMB respondents report that engaging external security operations partners is crucial to maturing their security operations practices.

By engaging the right security operations partners, respondents expect to see increased customer trust (49%), reduced risk (47%), increased revenue (45%), improved efficiencies (44%), and increased employee engagement (44%). Better security and privacy measures give customers a reason to prefer a firm over others; better security in products and services may warrant premium pricing; and empowering security employees with the right tools enables them to be more proactive and engaged.

"Engaging external security operations partners is crucial to maturing our security operations practice."

(Showing "Agree" and "Strongly agree")

"Which of the following benefits have you seen/ expect to see from engaging the right external security operations partner(s)?"

Base: 232 IT and security operation strategy decision-makers in the US
Note: Showing top responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Pondurance, May 2022

Conclusion

SMBs face the same threat landscape as larger companies, but with more limited people, budgets, and skill sets. Countering these threats requires an external partner to:

- **Detect and respond based on adversaries' schedules.** Staffing a 24/7 SOC is unrealistic for most SMBs, but attackers don't care when they operate. An external partner brings real — and affordable — 24/7 support.
- **Gain the required security stack expertise.** If SMBs find talent, it's often hard to retain as they end up talent development pipelines for larger employers or security vendors. External partners find and retain talent in ways SMBs can't, offsetting these conditions.
- **Spend more time growing your business.** Using external support allows your organization's leaders and employees to focus on customer-facing activities and enable business growth. Having external partners bolster your security operations also shows your company cares about security, resulting in increased customer trust.

Project Team

Mandy Polacek,
Market Impact Consultant

Emily Stutzman,
Associate Market Impact Consultant

Contributing Research:

Forrester's Security and Risk research group

Methodology

This Opportunity Snapshot was commissioned by Pondurance. To create this profile, Forrester Consulting conducted an online survey of 232 US-based cybersecurity operations leaders. The custom survey began and was completed in May 2022.

Demographics

COMPANY SIZE	
100 to 499 employees	**29%**
500 to 999 employees	**34%**
1,000 to 2,499 employees	**37%**

RESPONDENT LEVEL	
Director	**54%**
Vice president	**41%**
C-level executive	**5%**

GEOGRAPHY	
United States	**100%**

TOP 10 INDUSTRIES	
Manufacturing and materials	**9%**
Consumer services	**8%**
Consumer product goods and/or manufacturing	**8%**
Retail	**8%**
Healthcare	**7%**
Electronics	**7%**
Financial services and/or insurance	**7%**
Business or professional services	**6%**
Education and/or nonprofits	**5%**
Technology and/or technology services	**5%**

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.


FORRESTER®