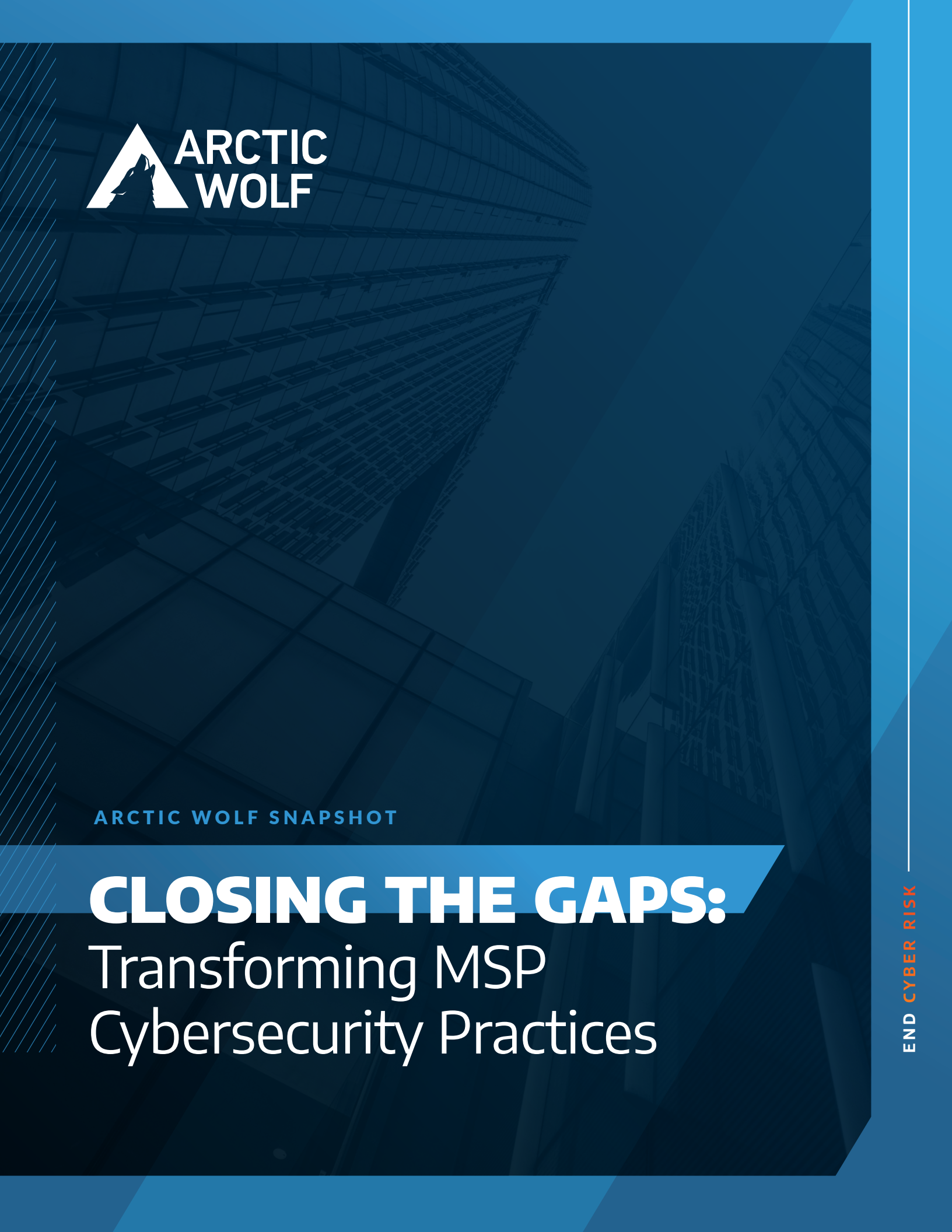


ARCTIC WOLF SNAPSHOT

CLOSING THE GAPS:
Transforming MSP Cybersecurity Practices

END CYBER RISK

CLOSING THE GAPS:

Transforming MSP Cybersecurity Practices

As managed service providers (MSPs) look to expand their strategic footprint and scale their business, one segment that presents a huge growth opportunity is the small and medium business (SMB) market. SMB customers often lack the right resources and infrastructure to adequately manage their own IT services, creating a gap that can be addressed with the in-depth expertise and breadth of services offered by MSPs.

But this opportunity is not without challenges. From an evolving threat landscape to a growing attack surface, MSPs need more than tools to deliver the positive security outcomes expected of them as their customers' trusted security advisors.

Offering a single security solution — or focusing resources only on siloed aspects of the IT environment — puts both your business and your clients at risk. Organizations need effective cybersecurity practices, and with the skills gap only increasing, MSPs are poised to make a significant impact.

What Is an Effective Cybersecurity Practice?

An effective cybersecurity practice is one that looks at security holistically, utilizing proactive and reactive measures to cover the entire security environment with an eye toward continuous security posture improvements.

It includes the following:

- 24x7 monitoring
- Fast threat detection, response, and remediation
- Security training
- Vulnerability management
- Incident response services
- Compliance management
- Staff and security skills on hand (either internally or through a third-party vendor)

Methodology

Arctic Wolf surveyed business leaders from mature, established MSPs and MSSPs to understand the challenges, themes, and blueprints of their cybersecurity practices.

Our methodology included surveying 47 MSP/MSSPs with the following breakdown:

58% of MSPs/MSSPs surveyed have 100 or more customers

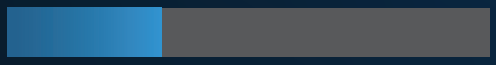
A large majority of MSP/MSSPs have been in business for more than 10 years

Nearly 6 out of 10 MSPs/MSSPs surveyed report their cybersecurity clients have more than $5 million in revenue

MSP and MSSP Clients Generate Hundreds of Cybersecurity Tickets Per Month

On average, survey respondents report over 100 hours (or 12.5 business days) a month per client dedicated to managing ticket volume.

32%



32% of MSPs receive more than 100 tickets per month for their average client.

47%

47% of MSPs/MSSPs report an average of 100+ monthly billable hours dedicated to cybersecurity per client.

500+

At least one in five MSPs/MSSPs surveyed generate **500+ cybersecurity tickets** per month per client for their busiest clients.

While MSP/MSSPs are providing more cybersecurity solutions to their clients, the sheer volume of tickets and hands-on support required show that their work is lacking strategic efficiency.

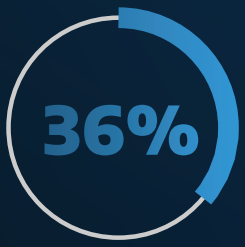
Here are two key takeaways from these results:

01 When the ticket volume is that high, it can create alert fatigue. That has quantifiable impacts on an MSP's finances, staffing (the average tenure for the majority of MSP/MSSPs cybersecurity employees is only three to five years) and the overall security posture of the clients they serve. It means analysts are working through significant noise and are stuck in a cycle of reacting to tickets, which limits their ability to prioritize focus on proactive measures and complete high-value tasks. More volume also means more risk, as critical alerts can get lost in the static.

02 Clients are typically watchful of billable hours, especially those with a high variance month-to-month. While it may be termed a "billable hour," experienced MSPs know that not all time spent on behalf of customers is successfully billed. Combine this data with the high head count required to support a dedicated cybersecurity function, and it becomes a sign that MSPs' cybersecurity practices need more discipline and focus.

This means shifting strategy to long-term planning to reduce noise and the quantity of tickets, focusing more on high-value client needs.

The Largest Shares of MSPs/MSSPs Are Challenged to Effectively Use the Many Tools and Vendors They Juggle



36% of MSP/MSSPs use more than 10 cybersecurity tools.

30% of MSP/MSSPs use 4-5 cybersecurity vendors to deliver services to clients.

Tools can enhance protection and visibility. However, they can also create a massive volume of events and alerts as evidenced above.

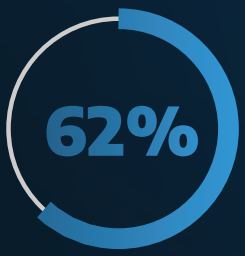
Cybersecurity doesn't have a tools problem, it has an operations problem, meaning MSPs can't reduce their clients' attack surfaces solely by adding more technology.

MSPs need to shift from a tool-focused mindset to an operations mindset. A consolidated approach can help MSPs better serve clients by utilizing a smaller number of security operations-focused tools that will reduce complexity and risk while increasing efficiency.

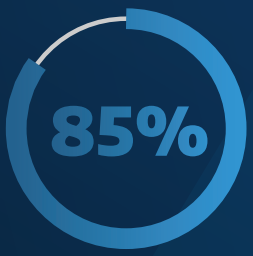
What is a Security Operations Platform?

A security operations platform operates more holistically compared to point solutions that work in isolation because these platforms collect, enrich, and analyze security data at scale, reducing noise and increasing response effectiveness.

MSP/MSSPs' Clients Are Consistently Targeted by Phishing



62% of clients are experiencing phishing/ spear phishing attacks frequently.



85% of MSP/MSSPs currently offer security awareness training.

The prevalence of phishing is not a problem limited to the clients of MSPs. It continues to be a top attack vector and for good reason: it works. Without proper security training, users are falling for phishing attempts en masse, unintentionally opening the door for threat actors to launch or perpetuate a cyber attack. The grim reality with phishing is that an organization often won't know the attempt was successful until it's too late.

While MSP/MSSPs are offering security training to their clients, the sheer frequency of phishing attacks highlights a lack of effectiveness in these trainings.

Effective security training includes:

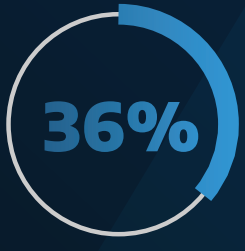
Up-to-date, relevant content for users

Microlearning that allows users to absorb nuggets of information frequently

A regular cadence that is more frequent than annually or semi-annually

Phishing simulations to help users understand what real-world attacks could look like

MSPs should take the time to re-evaluate their security training vendors to see how they are serving their clients and assess client satisfaction around the effectiveness of the security awareness training currently in use.



36% of SMBs consider lack of cybersecurity knowledge/training among employees to be a top operational challenge.

Learn more about SMBs cybersecurity challenge with "Closing the Gaps: Solving Security for SMBs."

MSPs Are Starting to Provide More Holistic Security Solutions

The security landscape is changing — MSPs are rapidly recognizing the value of MDR services.

Surveyed MSPs currently offer (or plan to) these services:

The threat landscape is not the same as it was even a few years ago. With the rise of ransomware-as-a-service (RaaS), ransomware gangs, business email compromise (BEC) attacks, and vulnerability exploits, organizations need to think beyond the firewall.

While once the tried-and-true standard, EDR tools don't address the entirety of customers' environments, and when used alone, leave a large portion of customers' environments insecure. Clients now expect a managed service that will make up for the widening skill gap and increase visibility across the network and cloud environment. In addition, with the sheer volume of cyber attacks ticking up year after year, organizations know that not planning for the worst will end poorly should an incident occur.

As clients are seeking out MSP services to assist with compliance, resource gaps, and a lack of 24x7 monitoring, MSPs need to offer more, and do so in a way that creates depth and breadth while reducing alert fatigue and reliance on siloed tools. As noted earlier, allocating all billable hours to reacting to alerts means analysts don't have time to practice proactive measures like vulnerability management. MSPs need to work with their clients to cover more of the environment and further reduce risk.

Traits of a Strong Incident Response Provider

- **Fast response time**
- **Rapid remediation**
- **In-depth analysis that identifies the root cause of an incident**
- **Parallel investigation and business restoration**
- **Technical breadth and depth**

Cybersecurity Services Increase MSP/MSSPs' Revenue

MSPs/MSSPs surveyed report their 2022 cybersecurity services revenue increased more than 10% compared to 2021.

MSPs surveyed indicate that more than 50% of their total services revenue in 2022 was from cybersecurity services.

> **It should be noted that bundled/tiered pricing is the most common cybersecurity pricing structure for MSP/MSSPs at 45%. While offering more solutions can be more cost-effective for customers, it's important both vendor and client be wary of falling into the "too many tools" trap which can increase resource needs and reduce ROI.**

For MSPs, cybersecurity services translate into profits. Even MSPs that don't specialize in security are seeing it in their revenue — making cybersecurity top of mind for every MSP. Now is the time to have conversations with clients about their needs and how to better help them reach desired security outcomes. If MSPs provide in-demand security solutions that cater to the needs and budgets of their SMB clients, they will be better positioned to achieve healthy revenue growth.

Information is power when it comes to better serving clients.

Learn more about the security needs of SMBs as shared by decision makers from SMBs that currently utilize MSP partners for security services in "Closing the Gaps: Solving Security for SMBs."

MSPs and Arctic Wolf

As more organizations turn to MSPs to proactively and remotely manage their IT infrastructure and end-user systems, they gain a degree of protection. However, while MSPs typically provide remote device configurations, network monitoring, and resell endpoint and perimeter defense tools, they often lack the in-depth security expertise and capacity required to hunt down threats, perform forensics analysis, and mitigate and contain any potential impact.

That's why savvy MSPs, those who seek new ways to bring value to, and engage with, new and existing customers, team with a managed security operations provider. This allows them to provide 24×7 eyes-on-glass coverage by a team of experts, rapidly deliver in-depth security services focused on managed detection and response (MDR), and address the advanced cyber threats impacting their clients

By partnering with Arctic Wolf, MSPs can generate turnkey recurring revenue with industry-leading solutions for MSP security practices, including risk management, cloud monitoring, and managed detection and response.

Learn how Arctic Wolf partners with MSPs to deliver security outcomes to their customers. Become an MSP partner today.

END CYBER RISK