NIGHTDRAGON

MARKET REPORT:

SMALL AND MEDIUM BUSINESS

September 2024

www.nightdragon.com

Foreword

Small and medium businesses (SMBs) are the core of our economy. The local dentist's office you visit for a checkup, the regional hospital saving lives, the corner store you go to for a snack, the local restaurant or bar – all of these are meaningful pieces of our daily lives and our local communities.

The impact of SMBs on society is extensive, from being responsible for nearly half of all employment to creating local economic resilience and growth. When SMBs hire locally and then circulate the money back into the community, they stimulate jobs, opportunities, creativity, entrepreneurship, and enterprises. All these not only allow a community to prosper but also protect it from external economic instability.

Unfortunately, they are also a group at risk. Cyberattacks increasingly target SMBs, who are, in many cases, less able or prepared to defend themselves due to limited budgets and staff. While SMBs may have thought they were too small to be targeted for attack, that is increasingly proving not to be the case. In fact, it's very much the opposite. The majority – 78% - of SMBs report worrying that a serious attack could put them out of business.

As a result, we are seeing a growing market emerge around SMB security. While previously a smaller market, it has grown significantly, accounting for nearly half of all spending on technology and billions of dollars of investment into cybersecurity. We are also seeing new innovators and technology emerge explicitly targeted to help mitigate risk for this sector.

In this NightDragon Special Market report, we'll explore the growing market for SMB cybersecurity, including examining the challenges facing these organizations, overall market growth, and a map of current technology players innovating in this space.

Table of Contents

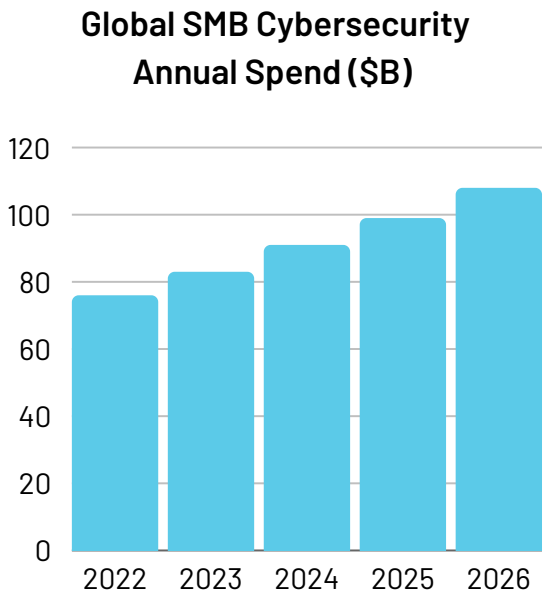
The Market

What is an SMB?

There are several ways to categorize if a company falls into the small and medium business category versus being a midsize or large enterprise. One common metric to quantify is the number of employees, with an SMB typically having 1000 employees or less, with fewer than 100 employees signifying a small business. Another way to characterize them is by annual revenue, with SMBs typically defined as having less than $50 million in annual revenue. These are just some select metrics, though the definition varies greatly and is loosely defined overall depending on who you ask.

Market Size

Globally, SMBs make up 90% of all companies, while in the U.S. that figure jumps to 99.9%. SMBs create over 1.5 million jobs in the U.S. each year, contributing to 64% of the country's annual job growth. In the U.S., SMBs account for 45.9% of the workforce, a figure that grows to 60-70% when you look worldwide.



It's no surprise, then, that SMBs account for about half of the $370 billion spent on technology. The market for SMB cybersecurity spending is also growing significantly, from $76 billion in 2022 to $91 billion estimated this year. That market is expected to reach $108 billion by 2026 at a CAGR of 9.2%. The market is significantly varied, with many technology innovators, platform companies, and service vendors supporting SMBs' unique and important needs in mitigating cybersecurity risk. We will explore this market further in subsequent sections.

The Challenge

SMB organizations face security challenges that affect them to a greater degree than larger enterprises. Some examples include:

RISING CYBER THREATS

64% of SMBs report experiencing a malware attack in the last 12 months, and 40% say they are likely to experience a cyberattack in the near term. There was also a 37% rise in ransomware attacks in 2023, with the average cost of these attacks reaching $1.85 million. While larger companies often have the resources to meet these demands and recover, SMBs typically lack the same financial and technical means to pay ransoms or recover from the damages, leading to many going out of business.

LACK OF BUDGET

SMB budgets are typically significantly smaller than those of a larger enterprise. The median SMB cybersecurity budget was $150,000 in FY22 and about half of companies that have fewer than 50 employees have no cybersecurity budget, making SMBs an easier target. What's more, amidst inflation and a lack of talent to hire, many SMBs plan to cut their technology budget to prepare for economic uncertainty. These technology budget cuts range from 25-30% within the next two years.

TALENT SHORTAGE

50% of SMBs report difficulty filling their open positions with 90% saying they have difficulty finding qualified candidates. For SMBs, it can be harder to recruit top talent as they must compete with larger, more established organizations with more resources. Many SMBs also don't have the financial resources to compete with larger corporations' attractive offers and positions, and struggle to reach candidates with the talent and experience they are searching for.

THIRD PARTY RISKS

Due to a lack of flexibility and resources, SMBs are deeply impacted by supply chain issues, such as natural disasters, financial instability, or geopolitical events. Third-party risk also extends to software supply chain, which can introduce new risks through software vulnerabilities or even an outsourced IT provider, like a Managed Security Provider (MSP). SMBs have less personnel, technological expertise, and time to allocate for effective inventory management, and can't predict and prepare for demands as easily as larger businesses. What's more, SMBs are often frequent users of open source software, which could be another vector of attack or vulnerability.

REGULATION

Data privacy laws and similar regulations dictate how organizations can share, use, and collect personal information. Ensuring compliance with these regulations, from HIPAA, to PCI, to GDPR and more, can be very cost prohibitive for an SMB, or they may not even be aware of which regulations they must be compliant with and face the risk of a fine.

HIGHER STAKES

If a cyber incident occurs, an SMB's stakes are much higher. The average global cost of a single incident is estimated at $3.62 million, a sum out of reach for many small or medium businesses. As a result, according to one estimate, 60% of small companies will go out of business within six months of experiencing a cyberattack.

Threats that Impact SMBs

In 2020 alone, over 700,000 attacks hit small businesses, totaling $2.8 billion in damages. The nature of SMB activity exposes them to a subset of cybersecurity threats that they are particularly concerned about:

PHISHING

Year after year, phishing remains one of the most common vectors of attack. SMBs are no exception, with phishing potentially resulting in stolen passwords, installation of malware, ransomware and more.

SOCIAL ENGINEERING

Social engineering is a tactic for attack where a user is manipulated or duped through impersonation into revealing information or downloading malicious content. SMBs face these types of attacks in high percentages, with some estimates finding that SMBs face 350% more social engineering attacks than their peers.

RANSOMWARE

Ransomware attacks, where systems are infected with malware and held hostage with encryption until the victim pays a ransom, affect businesses of all sizes. Nearly half of all SMBs report being the victim of ransomware, which can put their operations or reputation at risk, and 75% of SMBs say they could not continue operating if hit with an attack.

SUPPLY CHAIN ATTACKS

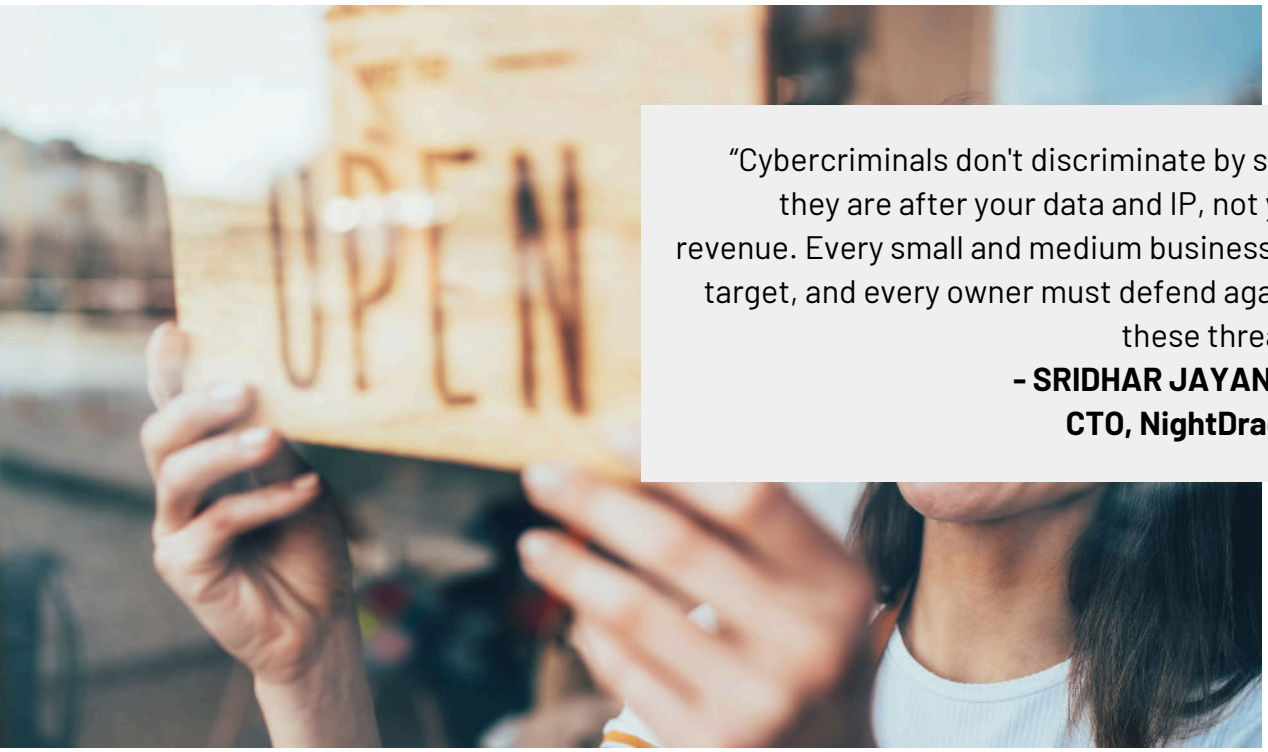
An SMB's supply chain can also put them at risk, including vulnerabilities in the third-party software they use or relationships with partners. What's more, they are often reliant on open-source software or software from their IT providers, which can add further vulnerability through third parties.

BOTNETS

Botnet attacks hit businesses of all sizes, but reports find that SMBs are often hit the hardest in terms of impact due to drain on email servers and network resources.

REMOTE WORK

Remote and hybrid work models in the post-Covid world have expanded the attack surface for SMBs, with insecure home networks and devices becoming new vectors for cybercriminals.



"Cybercriminals don't discriminate by size - they are after your data and IP, not your revenue. Every small and medium business is a target, and every owner must defend against these threats."

- SRIDHAR JAYANTHI
CTO, NightDragon

SMB Hospitals Under Attack

In H1 2024 alone, the healthcare sector reported 280 cyber incidents — with the biggest being attacks on Change Health Care, Kaiser Permanente, and Ascension, together accounting for 24% of all US cyber events in 2024. Each attack cost hospitals significantly, putting lives at risk and facing an average staggering cost of $10.93M.

While large healthcare systems often make headlines when hit by cyberattacks, SMB hospitals are also increasingly becoming targets. America's 1,800 rural hospitals (which serve more than 60 million Americans) are among the most vulnerable, often with older IT infrastructure, smaller budgets and inadequate IT staffing. A recent examples of an attack includes Group Health Cooperative of South Central Wisconsin (April 2024, affecting ~500k people), Otolaryngology Associates of Carmel, IN (February 2024, affecting ~316k people), Ernest Health Hospitals in 13 states (January 2024, affecting ~101k people), and Logan Health in Kalispell, MO (March 2022, affecting ~130k people).

Hospitals and healthcare institutions, small and large, have become prime targets for cyber-attacks in recent years. There are several reasons for this:

- Valuable data: Hospitals hold large amounts of sensitive personal and medical data, which is valuable to cybercriminals for identity theft, fraud, or ransom. Medical records also have long-term value for various malicious purposes, making them attractive to hackers
- Critical operations: Hospitals provide essential, life-saving services. This makes them more likely to pay ransoms quickly to restore operations and protect patient safety.
- Vulnerable systems: Many hospitals have focused more on patient care than cybersecurity, often using outdated systems or lacking robust security measures.
- Financial motivation: Cybercriminals perceive hospitals as having significant financial resources and being more likely to pay ransoms.
- Supply chain vulnerabilities: The complex nature of the healthcare industry makes supply chain attacks a popular vector for cybercriminals.
- Emotional leverage: Ransomware threats to healthcare carry a heavy emotional burden as attackers exploit the life-or-death nature of hospital operations.

The Market

Cybersecurity for SMBs is a dynamic and evolving market, currently valued at $76 billion. This figure is only growing, with SMBs becoming an increasingly attractive target for threat actors, the market is expected to reach up to $108B over the next four years, accounting for 60% of the total spending on cyber security worldwide. With 43% of cyber-attacks targeting SMBs and 61% of SMBs failing to get adequate cybersecurity insurance, the demand for solutions tailored to the needs of SMBs is stronger than ever.

At the same time, SMBs recognize the challenge posed by cybersecurity and the need to invest in increased protection. In fact, 83% of SMBs expressed an intention to increase their security posture over the next year. Overall, SMBs are expected to spend $90 billion on cyber security in 2025, up from $57 billion in 2020.

$76B

Market Size for
SMB Cybersecurity

Investment and M&A

We've seen an increase in funding for IT security among high-growth SMBs. Recent attacks in the sector have drawn greater attention to the need for safeguards against threat actors, leading to investment in companies solving this issue. Examples of recent funding include Todyl ($50M Series B),Guardz ($18M Series A), Coro ($100M Series D), Huntress ($150M Series D), and Ostra Cybersecurity ($4M Series A).

Larger cybersecurity companies have recently acquired other companies to bolster their offerings for SMBs. For example, Palo Alto Networks recently acquired Cortex XSOAR ($670M), Cisco recently acquired Kenna Security (undisclosed), and Crowdstrike acquired Humio ($400M). These acquisitions by cyber titans may set the tone for other, smaller organizations to focus on the needs of SMBs.

Advancing Innovation

The SMB market covers a wide variety of types of technologies, gearing many of the technologies that you might see in use at the enterprise for a smaller scale and budget. For example, features important for this sector can include:

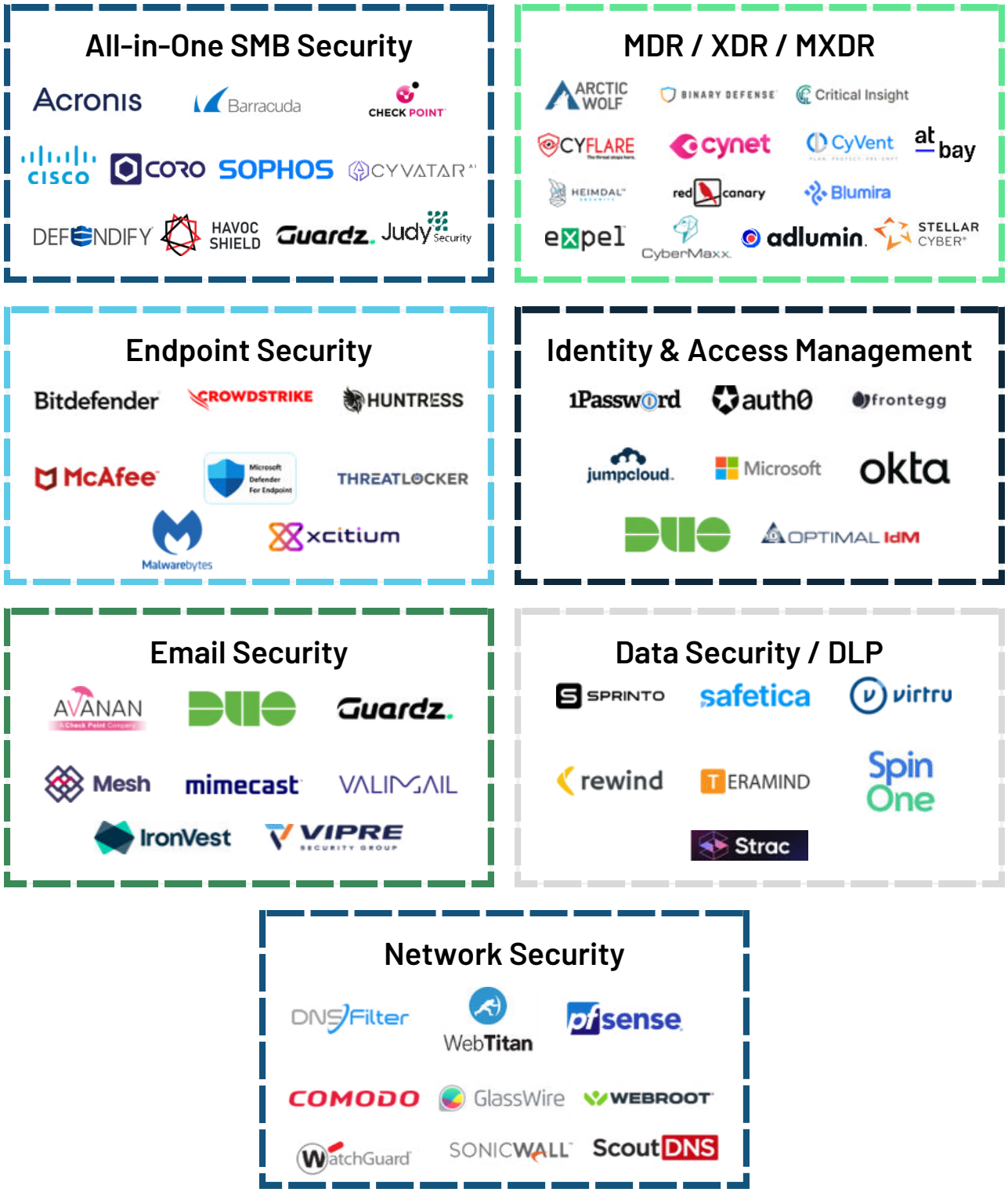
- User management
- Multi-factor Authentication
- Password Management
- Endpoint protection (including Cloud)
- Email/Phishing Protection
- DNS/URL filtering
- Network (firewall management)
- Detection and Response (across endpoint, email and network vectors)
- Compliance
- Awareness/Training

Although these look like a typical enterprise set of functionalities, the difference is often in how these features are offered, in tiers with the ability to upgrade with additional features. Many vendors will also emphasize ease of deployment and management through features like a single pane of glass dashboard, overall simplicity of use, a focus on awareness and education, or AI-based automation to support smaller team sizes. Additionally, many vendors recognize the importance of MSPs and MSSPs to the SMB ecosystem and have built their tools accordingly. This starts leveling the playing field for SMBs in terms of security technology sophistication with enterprises.

"There is a huge opportunity for a security platform that can provide a full stack of security tooling to small businesses that can't afford to buy best in class of everything like their enterprise counterparts."

- MATTHEW MARTIN
Founder, Two Candlesticks; NightDragon Advisor

SMB Market Map



Rise of Managed Service Providers

Managed Service Providers (MSPs) help businesses by delivering services around network, application, infrastructure and security implementation, as well as ongoing support and maintenance of a customer's technology environment. In essence, acting as an outsourced IT arm for a company.

The SMB segment is the fastest growing in the managed security services market. Heading into 2025, SMBs are forecasted to spend $29.8 billion on managed security services, as 82% of SMB leaders report increasing budgets.

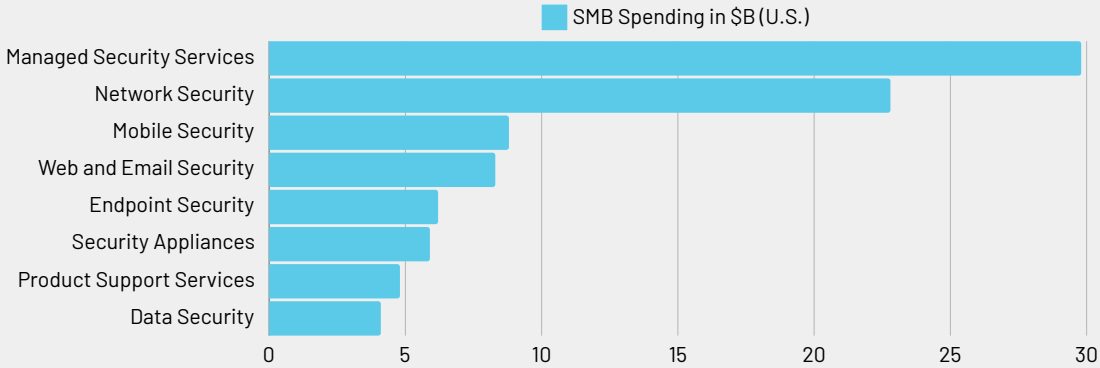
Why is this? Small and medium businesses often do not have the budget to build a security team to focus on security operations. What's more, it is costly to maintain a team big enough to handle ongoing cybersecurity updates, such as ensuring anti-malware software is updated regularly, establishing email policies to protect the company from spam or phishing, backup activity, user/password/access management and reviewing security alerts coming from the various security products to protect the company are a basic necessity that requires resources across all shifts 24/7.

"We see a growing opportunity for the MSP community to deliver security outcomes to these underserved businesses and at the same time drive business growth for themselves," said Raja Patel, Chief Product Officer at Sophos and NightDragon Advisor.

Rise of Managed Service Providers (cont'd)

"SMBs aren't capable of building and managing 24/7 Security operations, however, can benefit from a scaled out 24/7 Managed Detect and Response service, delivered by either a trusted partner or cybersecurity vendor, which is flexible to evolve with them as they grow with economics that they can afford," Patel said.

As a result, most SMBs turn to cost-effective MSPs or Managed Security Service Providers (MSSPs) to keep them safe. It is estimated that roughly 70% of U.S. small to medium enterprises plan to fully or partially outsource security to an MSSP or MSP by 2025. The figure is likely to be closer to 90% in less than a decade. These service providers come in various shapes and sizes, typically called MSSP, MSP, or MDR, depending on the security services they offer. Since most SMBs do not have a dedicated member of the team to handle security measures, any available spend is typically allocated to MSPs or Network Security (see chart below).



Source: Statista

This dynamic is now, in turn, evolving the vendor landscape. To further capitalize on this opportunity, security vendors in the SMB space have designed multi-tenant architectures that allow for a "manager of managers" approach, enabling a "master" MSSP to fully or partially manage security for customers of other MSPs and MSSPs. This type of innovation has allowed a larger number of SMBs to improve their security posture in what is becoming an increasingly complex threat landscape, all while working with their existing MSPs.

NightDragon Perspective

SMBs represent enormous market potential – one that only increases each year. This market has been historically underserved for various reasons, the most significant being a lack of resources and easy access to talent to manage security for this segment. The new growth in this market can be attributed to:

- Growth in Threats — Each year, security threats impact more SMBs, and the severity of these threats can be catastrophic to such businesses with limited resources. As a result, SMBs are looking for innovative ways to protect themselves from these attacks.
- Understanding of Need for Security – With 60% of SMBs going out of business following a cyberattack, it's clear the stakes are high. As a result, SMBs are quickly maturing in their outlook on security, becoming more security-literate and seeking out the best possible solutions.
- Managed Security Market Growth—As SMBs' security demand increases, most MSPs are turning into MSSPs and offering sophisticated security services that are bite-sized and easily understood by SMBs. This presents a secondary market opportunity for innovation and technology growth.
- New Categories of Technology - After a slow start from enterprise vendors trying to address the SMB market, a new category of specialized SMB security technology vendors has arisen over the last few years to provide easy-to-understand and manage security products that limit their features and capabilities to only what's needed for SMBs.
- Significant Future Market Size— The underserved SMB security market that is visible today is only the tip of the iceberg and has the potential to overtake the enterprise security market. For instance, McKinsey estimates a $2 trillion opportunity in the SMB cybersecurity market.

Many enterprise businesses try to move into the SMB market with a few changes to the product, but not always successfully. The dissimilarities in the market can be attributed to differences in requirements across product, SaaS deployment, go-to-market, billing and even how protection, alerts and remediation are managed. The market encompasses a wide variety of channels such as telecom service providers, consulting companies, and a variety of MSSP

NightDragon Perspective

types. For the foreseeable future, we do not believe products meant for the enterprise market can be successful in the SMB market and vice versa.

As a new crop of startups focus solely on the needs of the SMB market, the innovation has gathered pace, and the channels of sales and services have risen to meet the opportunity. NightDragon looks for qualities such as tiered offerings for SMB purchasing flexibility, transparent billing, and optimization for security concepts including single-agent feature set, ease of deployment, simplicity, AI-based automation, dashboards, customer reporting and awareness/education options.

Contact Us

If you're building interesting technology in this sector or have a perspective on disinformation, please reach out to the members on our team following this market:

Sridhar Jayanthi
Chief Technology Officer
sridhar@nightdragon.com

Alec Kiang
Associate
alec@nightdragon.com

NIGHTDRAGON