ARCTIC WOLF

BRIEF

No Business Is Too Small a Target

How small to midsize enterprises can secure data and infrastructure

The cybercrime economy is worth **$1.5 trillion**

Approximately **58 percent of victims** staff fewer than **1,000 employees**

66 percent of SMEs say threats evade intrusion detection systems

81 percent of SMEs say threats evade their anti-virus solutions

44 percent of security alerts that do get flagged never get investigated.

The rapid pace of digitization in the past two decades has affected every business. Enterprises of all sizes and from all industries—healthcare, finance, retail, transportation, education, etc.—have leveraged data and ubiquitous internet connectivity to automate otherwise time-consuming processes, optimize business workflows, and deliver unparalleled value and convenience to customers.

However, no opportunity is without obstacles. With near universal digitization comes the ever-worsening scourge of cybercrime. Hackers have substantial incentive to target organizations' infrastructure and data, and a single successful phishing scam can quickly escalate into a full-blown data breach. And private information and stolen account credentials can be sold on the dark web to fraudsters. Plus, corporate data can be encrypted with ransomware and leveraged against businesses to extort funds. These are only some of the underground profit centers currently fueling a $1.5 trillion cybercrime economy.[1]

✓ The Threat to Small and Midsize Enterprises

Large-scale data breaches such as the Equifax, Target and Sony incidents generate the greatest media attention, but cybercriminals are equal-opportunity attackers. When it comes to making profits, they don't discriminate against small and midsize enterprises (SMEs). In fact, there's a case to be made that SMEs are a preferred target among cybercriminals. Fifty-eight percent of data breach victims[2] were categorized as SMEs by the Verizon Data Breach Investigations Report, and most received little to no media coverage.

Hackers target SMEs for several reasons. Just like larger enterprises, SMEs possess valuable data, which can be commoditized to an underground market. And now that many cyberattack tools have gone mainstream and are readily available on the dark

[1] Bromium independent study

[2] Verizon 2018 Data Breach Investigations Report, 11th Edition

web, cybercriminals can launch attacks quickly and cheaply, which makes SMEs without a strong cybersecurity posture easy pickings. Also, hackers often seek to infiltrate SMEs as conveniently vulnerable entry points to much larger organizations for whom they are vendors.

These would be non-issues if SME cybersecurity could effectively protect against phishing scams, malware intrusions, data breaches and other pernicious threats. This, of course, is not the case. Which then raises the question:

Why Do SMEs Struggle to Secure Their Data and Infrastructure?

Three primary circumstances inhibit SMEs' efforts to secure data and infrastructure adequately:

1. **Too many tools:** Many SMEs invest in the "latest and greatest" point solutions and think they're secure. Yet exploits and malware evade most SMEs' intrusion detection systems (66 percent of respondents) and anti-virus solutions (81 percent).[3]
2. **Too much noise:** More security tools means more security alerts, many of which are false positives. In fact, 44 percent of alerts[4] are never investigated. SMEs that attempt to implement security information and event management (SIEM) for better event correlation are often defeated by the cost, complexity and time required to deploy, manage and fine-tune it.
3. **Too few security experts:** Security expertise is prohibitively expensive due to the global shortage of qualified cybersecurity talent. Many SMEs lack the budgets to retain enough cybersecurity personnel for round-the-clock protection. This gives hackers an advantage since they can launch attacks at a fraction of the cost it would take to defend them.

A Revitalized Security Strategy: Getting Ahead of Threats and Attackers

International cybercriminals are highly aware of smaller business' security shortfalls, which gives them the incentive to devise SME attack strategies. Consequently, SMEs must revisit their security strategies. To start, they should consider the following:

1. **Outsource security operations:** SMEs can supplement their lack of in-house cybersecurity expertise with assistance from third-party organizations; this method requires minimal internal training and little to no disruption to existing IT infrastructure.
2. **Evaluate service providers based on business requirements:** Many businesses struggle to evaluate the high volume of security service providers. Make sure that the managed security service you choose aligns with your business objectives, that it has a low total cost of ownership, and that it properly addresses advanced threats.
3. **Consider SOC-as-a-service:** SMEs can access the same security benefits large enterprises take for granted in the form of a managed security operations center (SOC). Arctic Wolf's SOC-as-a-service, the AWN CyberSOC™, extends your IT team or augments your security team with security engineers and analysts that have experience and expertise combating sophisticated attacks.

A revitalized security strategy built on SOC-as-a-service can keep employees, suppliers, and partners safely connected, your customers engaged, and your investors confident. For more, read Arctic Wolf's white paper on how to combat the top five attack vectors with managed detection and response.

[3] Ponemon Institute 2017 State of Cybersecurity in Small and Medium-Sized Businesses
[4] Cisco 2017 Annual Cybersecurity Report

ARCTIC WOLF

AICPA SOC

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com