# Build or Buy? Security Operations Center Strategies for Midmarket Companies

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper

February 2017

PREPARED FOR: ARCTIC WOLF

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

## Table of Contents

## Building Enterprise-grade Cyber Security in Midmarket Companies: Challenges and Opportunities

The midmarket is becoming an increasingly hot spot for cyber-attacks. Companies with revenues between $50 million and $1 billion accounted for nearly half of all cyber claims last year, according to the NetDilligence/McGladrey 2015 Annual Cyber Claims study. Weak midmarket defenses create not only the opportunity for attackers to extort resources from the business itself, but also the ability to use them as gateways to hack their enterprise partners (as evidenced by the Target data breach in 2014).

For their part, midmarket companies are aware of the increasing threat – investments in strengthening cyber security posture rank amongst their top priorities in 2017.[1] Yet there is dissonance in this segment on exactly what makes a security program "strong."

Weak midmarket defenses create not only the opportunity for attackers to extort resources from the business itself, but also the ability to use them as gateways to hack their enterprise partners.

Companies seem to operate under the viewpoint that security only needs to be as comprehensive as budgets will allow, something evident in a recent Vanson Bourne survey[2] of IT decision makers at 200 companies with between 500 and 3,000 employees. Some 95% of those organizations said that their security programs were above average to great, but pressed further, a majority admit to being overwhelmed with day-to-day tasks, bogged down by false positives, and unable to respond to security alerts within a week, if at all. [3]

What's more, even those with resources to hire dedicated security staff are facing intense competition to find, afford, and retain individuals with specialized skills. In 2016, EMA research identified that 76% of organizations are impacted by security staffing shortages, which is an increase of eight percentage points over 2015.[4]

It's why forward-thinking midmarket companies, cognizant of their budgetary constraints, security vulnerabilities, and the difficulties of finding and retaining people to fix them, are maximizing ROI and effectiveness from security spend by turning to managed security services providers (MSSPs). In 2016, 54% of organizations EMA surveyed identified that they were using an MSSP for more than 50% of their security operations and 55% indicated they would increase spending in this area.

One MSSP service that is gaining popularity is the managed security operations center (SOC), such as those provided by Arctic Wolf Networks (AWN). The managed SOC is a premium service and more than managed security incident and event monitoring (SIEM). Managed SOC ensures organizations that face the dilemma of a lack of qualified staff have 24/7 monitoring, investigation, and remediation of threats, freeing the company to focus on their core competencies.

## Crucial Challenges in Managing Security Internally

Enterprises combat the complex and evolving threat environment with sophisticated 24/7 SOCs. These are a concert of technology, people, and processes that do nothing but eat, sleep, and breathe security. SOCs constantly analyze threats within the context of business and adapt security to align with business strategy. For midmarket companies, however, building these programs internally is extremely challenging.

[1] SMB Group's 2017 Top 10 SMB Technology Trends

[2] The State of Mid-Market Cybersecurity: Findings and Implications

[3] Ibid

[4] EMA Data-driven Security Unleashed

The chief obstacle is the competition for security talent. *The unemployment rate for cyber security professionals currently sits at 0%*, according to a report by Cybersecurity Ventures, and there are approximately two job openings for every qualified candidate.

Furthermore, tasking an individual security engineer with the lion's share of day-to-day security operations means this person has little time to document repeatable, sustainable security processes that align with strategic business objectives. In the very real event that the individual is lured away by a more attractive job offer, the organization finds itself more vulnerable than it was at the outset.

Many midmarket organizations cannot find or afford dedicated security personnel so the people who are good at infrastructure management are tasked with breach monitoring, remediation, and log analysis. These people struggle to identify credible threats in a sea of alerts, including false positives, while performing their daily operations duties. Predictably, with so much to do, security becomes an exercise in simply ensuring compliance, not reducing risk. More than 70% of respondents in the Vanson Bourne survey reported that they couldn't spend as much time on security as they should and almost 90% said that reducing the number of false positives would help them spend more time on more important security issues.

The result is that midmarket companies open their doors to hacks. Less than 25% of respondents in the Vanson Bourne survey reported that they had the ability to investigate security alerts within the hour. A total of 30% were not investigated for a week or more or not at all, creating longer attacker dwell time and, according to the Ponemon Institute, more costly consequences and remediation.

The security posture at Hornblower, one of the largest and most established charter yacht and dining cruise lines in the United States, mirrors many businesses of its size. Budgetary constraints meant that its perimeter and endpoint defenses were monitored by an extremely lean IT staff whose expertise in networking and telecom more than ensured day-to-day operations ran smoothly, but left gaps in its security defenses. Phishing attacks persisted despite investments in content and spam filters, and Hornblower lacked end-to-end visibility into its security posture notwithstanding implementing market-leading tools. To alleviate this problem, they engaged Arctic Wolf Networks.

> Budgetary constraints meant that its perimeter and endpoint defenses were monitored by an extremely lean IT staff whose expertise in networking and telecom more than ensured day-to-day operations ran smoothly, but left gaps in its security defenses.

## The Advantages of Managed Security Operations Centers

Recognizing this reality, forward-thinking companies like Hornblower seek the advantages of engaging an SOC as a service, which offers cloud-based security incident and event management (SIEM) partnered with a team of expert security engineers to provide both operations support, incident analysis, and response. Some of the benefits Arctic Wolf Networks' managed SOC service provides include:

**Rapid time to value.** In implementing security operations as a service, a company realizes value from day one of the purchase and has the advantage of itemizing the service as a monthly cost rather than financing a capital technology project. In many cases, the cost of outsourcing is less than the yearly salary of a full-time security engineer.

**Scalability.** With cloud-based technology and access to a global talent pool, a partner can help quickly scale operations as your business grows to gain end-to-end visibility into your company's security posture and defend against and prevent breaches. Organizations gain capabilities in vulnerability assessment, threat hunting, and security data triage.

**Easy upgrades, reduced complexity.** With security operations technology based in the cloud, businesses avoid costly maintenance and infrastructure, disruptive upgrades required of on-premises software, and reduce the complexity of managing a SIEM support infrastructure internally. The SOC and threat intelligence is always updated and current so customers can focus on their core business.

**Focus on strategic priorities.** The SOC as a service engineers, operators, and analysts weed through thousands of alerts, tuning the systems to reduce noise volumes from false alerts. They only engage client resources to events that require attention, providing the IT department time to focus on the business's strategic priorities.

## EMA Perspective

As customers examine an MSSP market growing at nearly 20 percent each year,[5] finding the right partner can be overwhelming. In navigating this landscape, customers must be mindful that security operations success is driven as much or more by people than it is by technology. As HP's recent assessment of the state of security operations centers shows, some 82% of organizations are still under target maturity levels[6] and vulnerable to attack because of their tendency to "chase new processes and technologies" while failing to look at the "bigger picture."

The operations team is a huge part of what differentiates Arctic Wolf Networks (AWN) CyberSOC from other providers. The AWN CyberSOC marries a cloud-based security incident and event management (SIEM) platform with a team of expert security engineers, who become intimately familiar with a company's security and operational requirements. Arctic Wolf's engineers are offered ample professional development opportunities and boast impressive certifications and security specializations that keep them on the cutting-edge of their field.

> The AWN CyberSOC marries a cloud-based security incident and event management (SIEM) platform with a team of expert security engineers, who become intimately familiar with a company's security and operational requirements.

As part of the service customers are assigned a Concierge Security Engineer, a designated point of contact who becomes an invaluable extension of the internal team. Regular vulnerability assessments are conducted by the Concierge Security Engineer to assess the security posture and identification of any security gaps. At Hornblower, the Concierge Security Engineer detected a malware-infected server and encrypted traffic being sent to a malicious website, something that previously went undetected by Hornblower's internal firewall and antivirus software.

[5] Business Wire: Research and Markets Report

[6] Credit Union Times: Security Operations Centers Leaving Firms Open to Attack

Other notable features of AWN CyberSOC include:

**AWN cloud-based SIEM** service powered by a proprietary platform that leverages Web 2.0 technologies such as big data, Elasticsearch, and machine learning to analyze security logs and data to improve efficiency, effectiveness, and speed of threat detection. Threat intelligence subscriptions are integrated automatically and included as part of the service.

**Advanced breach detection** leveraging entity behavioral analysis to detect and alert on suspicious activity.

**AWN customer portal** providing customers with real-time visibility into the security of their networks, applications, and data, including access to unlimited data collection and storage for analysis.

Unlike MSSPs that primarily serve large enterprises, AWN CyberSOC is purpose-built for midmarket companies in terms of capabilities and pricing. Arctic Wolf's service can provide a fully operational, extremely robust security operations center to mid-market companies at a fraction of what it would cost to build a security operations center internally, freeing businesses to efficiently and effectively manage security while focusing on their core competencies.

## About Arctic Wolf Networks

Arctic Wolf redefines the economics of security with a turnkey SOC as a service that deploys in less than sixty minutes. Concierge Security Engineers use the AWN Platform to provide tactical and strategic insights into your security to answer the question, "Am I safe?" It leads the industry in making security simple, actionable, and affordable for mid-market companies.

### About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

**Corporate Headquarters:**
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3520.020617