A security gap exists between the advice of security experts and the capabilities provided by security point products.

Executive Overview
The complexity of cybercrime is overwhelming the ability of in-house IT teams to protect critical resources and data using traditional tools and approaches. This is particularly true for mid-market companies that don’t have the luxury of big enterprise staffs and budgets at their disposal.

Amplified by a diminishing perimeter, mobile endpoints and cloud computing applications, cybercrime can leverage social profile information for custom lures that play into human curiosity with increasing effectiveness. The stakes are high as one out of two people are employed by small to midsize U.S. companies that rely on the Internet to conduct business – 60 percent of which experts predict would cease operations within six months of a cyberattack.

A security gap exists between the advice of security experts and the capabilities provided by security point products.
Experts advise IT staffs to inventory their devices, software and applications and to provide continuous monitoring for vulnerabilities and anomalies. Meanwhile, security point products are focused primarily on malware defenses. We seem to know our enemy better than ourselves, and yet an estimated 80-90 percent of attacks could be mitigated with security controls on our own people, processes and technology. The truth is that no company can ignore external or internal threats, either of which can compromise sensitive data and destroy a business.

Bridging this security gap is a challenge that mid-market companies have not had the time or resources to tackle, until now. A new generation of security operations center (SOC) services has emerged to provide mid-market companies with people, process, and technology to combat cybercrime and achieve their cybersecurity goals, at a cost they can easily afford.

**Cyber threats are moving targets**

Advanced threats, theft of competitive information and intellectual property, and compromised assets are all indicators of the changing threat landscape. The days of high-profile attacks directed at a broad audience to gain notoriety, have given way to threats that are timed and targeted with the precision of a sniper, often for financial or political gain. The threat kill chain today often starts with a spear phishing email to specific individuals leading to compromised legitimate websites hosting the latest exploit kits to detect open vulnerabilities in targeted systems. Once found, open vulnerabilities often lead to malware infection, call-home communications and eventually data theft.

Traditional network defenses are becoming less effective against targeted attacks that are relatively slow and persistent threats served from compromised legitimate sites using dropper files and tested for obscurity. Combine simple human curiosity with social cons designed to lure the user into controlled web links and you have a perfect runway for cybercrime. Most networks are also run like an airport security force, with defenses on inbound traffic akin to passing security checkpoints and boarding the plane. When departing a plane, however, you have the opportunity to grab the wrong bag and exit with little to no security checks. Likewise, there are no security checks on data leaving the network.

IT departments are also facing a changing endpoint that was once homogenous, controlled and using known internal applications. Today, the endpoint can be personal, on networks you do not control and using cloud-based applications at the user’s discretion. Personal and work environments are blending, especially with millennial employees whose social media profiles tend to be ripe with information that can be used in targeted attacks. IT must now cover a larger, more complex and unpredictable playing field in order to protect company assets and meet compliance requirements.

**Security expert recommendations**

Over the past several decades, security solutions have focused on the enemy, resulting in a situation where many of us do not know our own security exposure. Security recommendations from the United States and United Kingdom are bringing this to light in an age of advanced threats that impact our businesses, economies and future. Even so, few security vendors are addressing this problem. To be successful in the battle for cybersecurity we need to know both our enemies and ourselves.

“If you know the enemy and know yourself, you need not fear the results of a hundred battles.”

— Sun Tzu
This is very visible in the first four critical security controls from the SANS.org list of the Top 20 Critical Security Controls developed over several years by both government and private sector security experts.

**Top Four Critical Security Controls**

1. **Inventory of Authorized and Unauthorized Devices**
2. **Inventory of Authorized and Unauthorized Software**
3. **Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
4. **Continuous Vulnerability Assessment and Monitoring**

The fifth critical security control is Malware Defenses. While the entire list of 20 security controls is a challenging project for most small to midsize companies to address, the first four critical security controls are rated “very high” for attack mitigation followed by a “high” rating on two other controls.

The first of these two is Application Software Security (#6), which addresses the need to neutralize vulnerabilities in web-based and other application software. The second is Wireless Device Control (#7), which serves to protect the security perimeter from unauthorized wireless device access.

The United Kingdom’s GCHQ office published a 2012 guide with “Ten Steps to Cyber Security.” The introduction by Iain Lobban, Director GCHQ, notes that about 80 percent of known attacks would be defeated by embedding basic security practices for people, processes and technology. Concurring with this perspective, the Center for Strategic and International Studies in 2013 stated that 90 percent of small and medium business breaches could have been avoided with the most basic techniques such as patching and restricting administrative privileges.

When it comes to reducing risk, chasing all security vulnerabilities is futile as scans can produce a large number of results that are well beyond available resources to mitigate. Another strategy of just focusing on top-rated vulnerabilities may result in missing a medium vulnerability that is publicly exposed for a valuable asset. Some security experts estimate that 80–90 percent of vulnerabilities are not high risk. This brings to light that most IT staffs are drowning in an ocean of data when what is needed is actionable security intelligence.

**Recommendations common to these guidance reports can be summarized:**

- Establish a baseline for hardware, software and applications
- Know who and what should be on your network and the web
- Continuously monitor for vulnerabilities and anomalies
- Deploy malware protection and infected system detection
- Monitor risk profile reporting, plus remediation and recovery processes

Knowing what you have is the first step to risk assessment and management. Simply put, risk equals the threat times the vulnerability times the asset cost \((R = T \times V \times C)\).
Security vendor solutions and tools
The lure of shiny new tools to solve security challenges has been around for decades with antivirus, firewalls and URL filtering being primary examples. Transparent security has also been heavily favored for deployments so users are not interrupted and workflows process smoothly. For mid-market companies, traditional security defenses are often the mainstay of threat protection, prevention and remediation. As traditional defenses continue to become less and less effective against targeted and timed threats, new concepts emerge on the horizon as the next silver bullet. The net result is another deployment with a console, dashboard and more reports to analyze with limited resources and time to do it effectively.

A common vendor strategy is a product security suite for mid-market companies, where multiple solutions are bundled together at an attractive price with varying degrees of integration and unification. The challenge with suites is that you are forced to deploy all of the components even when only certain core features are desired. While suites provide lower price points per component, the expense of deployment, configuration and administration remains the same.

Once you have multiple security and network-monitoring tools deployed, then the strategy of aggregating all the logs, alerts and forensic information makes sense. Security information and event management (SIEM) solutions seek to fill this role, but there are known issues. They can be hard to use, often lack standardization for inputs that may cross political boundaries, and require skilled analysts and resources to scale. The concept of big data is very attractive, though it is not a magic bullet to solve security issues.

When it comes to new releases and features, there are two main strategies in the industry for products. Waterfall development cycles create larger releases that complete all engineering and test processes step by step until general availability. These releases normally have significant release numbers and show up, at best, once per year and more likely every two years or longer. Between these major releases are minor releases and patches. From a customer perspective, this means you often have to wait on annual or longer release cycles to see new desired features if they are prioritized and make a release cut. Waterfall releases tend to have longer product roadmaps that customers are advised to monitor.

The end goal is to meet the objectives from security experts to reduce risk and mitigate attacks using the most effective vendor solutions.
The second strategy for product releases is an agile development cycle using sprints to create small feature releases in the range of five to nine times per year. Agile development works very well with cloud-based solutions where deploying new software updates to customers is minimized and often avoided. New features show up with minimal effort to upgrade by customers. However, paying attention to release notices, change impact notices and service availability is strongly advised. For major functionality updates, a longer time period is required but it is often divided into small deliverables to stay true to the methodology.

For both waterfall and agile environments, functionality is generally controlled by the user interface or user experience (UX). Customers can complete tasks and processes provided within the interface and hopefully in a logical layout with meaningful steps. This is one of the most constricting design elements for a security solution as the functionality often lies beneath the interface, while controls have not surfaced due to release cycles and feature prioritization.

There are several ways that security vendors enable customers to accelerate ad hoc and custom feature requests. One method is to create a scripting language to enable customers to build their own desired outcomes for policy controls, reporting, etc. Another method is Application Programming Interfaces (APIs) that enable development-minded customers or vendor partners to augment the core product with additional capabilities. Online communities allow users to share ideas, discuss concepts and benefit from a multiplier effect of shared intelligence and improved serving of scripting languages and APIs.

In summary, the end goal is to meet the objectives from the security experts above to reduce risk and mitigate attacks using the most effective vendor solutions with available resources. This can be a challenge for mid-market companies relying on traditional security defenses with limited resources and time. Adding another product solution with more output for a growing haystack of security data may not improve the ability to gain actionable security intelligence to reduce risk.

**Businesses face the security gap**

Cloud, social and mobile technologies have changed the playing field and will continue to provide new leverage points for mid-market companies. They also blur a once well-defined perimeter of homogenous systems and internal applications. As the changing threat landscape makes security more complex, businesses face a security gap, which includes:

- Security vendor solutions defined by release cycles and user interfaces
- Security expert advice on fundamental controls to reduce attacks by an estimated 80–90 percent
- Continuously changing threat landscape focused on espionage of competitive information
- Numerous security vulnerability and threat tracking sources lacking normalization
- Limited IT resources overwhelmed by malware infections and remediation efforts
- Security training and certifications for staff, plus managing retention and turnover
- Balancing an IT budget against risk goals of the business
Doing everything is not possible. Prioritizing and focusing with available resources, security skills and existing infrastructure is critical. While most traditional security defenses have ‘set and forget’ controls with report monitoring on a weekly or monthly basis, newer solutions are raising the bar on security skills to mine larger amounts of data. Traditional defenses mainly focus on the enemy or cyberattack while security experts today are advising us to know ourselves and implement continuous monitoring on our inventory of devices, software and applications.

The security gap that mid-market companies face is even more of an issue given a lack of specialization in duties that large enterprises have in their organizations, plus outsourcing to system integrators with specialized skills. For the most part, these companies rely on themselves and local resellers for security skills, training and advice. The same food chain that enables larger customers to acquire the best resources, often results in small businesses on the phone with a sub-par call center resource, depending on their service plan.

Overwhelmed, the IT staffs of mid-market companies generally resort to a combination of two strategies. The first is applying controls they have heard about and can afford, and the second is dismissing threats as things that happen to other people.

Not making a decision is still a response to risk as the three generally accepted options are: acceptance (live with it), mitigation (controls), or transfer (insurance). Consciously or not, every business decides on one of the options above. In summary, what mid-market companies need is security and risk assessment with evaluation and recommendations that they can manage and afford.

The impact of security incidents
The National Cyber Security Alliance completed a National Small Business Study in 2012. To no one’s surprise, mid-market companies surface the strategies above in their responses for the study. First, 90 percent of mid-market companies do not have professional IT managers on staff. This results in a part-time security focus which favors set and forget solutions to minimize the impact on resources. Next, 50 percent do not consider cyberattacks a serious threat to their companies because they believe they are too small to be targets. Additionally, 47 percent believe they are not targets for cyberattacks because they feel that they protect themselves well enough.

Conversely, the Verizon Data Breach Investigation Report for 2012 states that 72 percent of mid-market companies reported a data breach in the last year. So believing security through obscurity or that you are well defended is dismissing the reality of the situation. More bluntly, the Wall Street Journal reported recently that most small businesses do not recover from cybercrime, noting nearly 60 percent will close operations within six months of experiencing a cybercrime. The WSJ article also notes that 20 percent of all cyberattacks hit businesses with 250 or less employees and that the average cost of a data breach is $214 per compromised customer record, which can send these businesses into bankruptcy.

The National Cyber Security Alliance report for 2012 also brings to light that mid-market companies are the backbone of the US economy, with 1 out of 2 workers being employed at a small business. Of the 15 million net new jobs created from 1993 to 2009, 65 percent were within mid-market companies. From an online perspective, 73 percent

Security is now reaching a state of complexity and overwhelming data that most mid-market companies cannot address.
say a safe and protected Internet is critical to their business success with 87 percent having at least one or more employees working daily on the Internet. 55 percent noted that not having Internet access for 48 hours straight during business operations would be disruptive and 38 percent noted that it would be very disruptive.

In summary, the Internet is the backbone for modern business communications and processes to drive commerce, even more so for mid-market companies looking for leverage.

Managing your business
Focus is key to business success, providing a unique and valued service or product to customers. Most people have visited businesses that show a lack of focus, poor attention to detail, questionable customer service or poor product quality. To keep focus, mid-market companies often must rely on the expertise of other businesses for success. Examples include: banking services, legal advice, shipping goods, suppliers, local advertising, website development and online resources, and perhaps even a daily lunch service for employees to save time out of office.

Security has been an in-house topic since antivirus solutions surfaced on desktops and file servers with the wide use of the Internet. Firewalls and web filtering came along as widespread viral threats and denial-of-service attacks also showed the vulnerability of online communications. Security vendors have kept their product focus with high-end services available from large consulting firms for the largest of customers. Mid-market companies have been stuck in a packaged security product environment for decades, resulting in limited focus on security and risk management skills internally and practicing security through obscurity alongside traditional defenses.
In an era of targeted attacks leveraging online social profile information with exploit kits automating the search for open vulnerabilities, the odds of hiding behind obscurity are running out. We are in an era where keeping your business focus is critical for success and leveraging security expertise for actionable security intelligence is required. D-I-Y with a growing stack of security products producing a haystack of security data is overwhelming and puts a strain on resources that should focus on primary business objectives and projects.

The simple test of sending a phishing email to employees highlights the frailty of human curiosity and the ineffectiveness of traditional defenses. In most of these tests it is common to see nearly 80 percent of employees opening a phishing email to read it and 50–60 percent clicking on embedded web links and providing their credentials to review more information. This is an eye-opening test with several online tools available at phishline.com or phishingbox.com. Also note that most large data breaches start with a phishing attack, or a more focused spear-phishing attack to specific individuals. While most malware and virus attacks stay close to desktop environments, the social con knows no boundaries, making mobile devices and tablets open targets.

In summary, security has been an in-house product-driven environment for years and is now reaching a state of complexity and overwhelming data that most mid-market companies cannot address. As these businesses leverage other firms for products and services to remain focused, they will find the solutions they need in a new generation of security operations center services.

Recommendations

Following the security experts' advice is prudent; know yourself and your enemy. However, addressing the critical security controls with traditional defenses is a challenge and adding more security products with more data to analyze only strains already overwhelmed IT resources.

For companies with limited security resources, a security operations center is what’s needed to provide visibility into their security posture. SOC delivered as a turnkey service such as AWN CyberSOC can provide companies with the expertise, people, process, and technology to manage their security operations without having to invest in additional infrastructure or staff.
AWN CyberSOC is the industry’s easiest to deploy SOC service and can be up and running in less than 60 minutes. It is based on a monthly subscription model that lets companies use only a fraction of their security budget to have a full SOC capability. AWN CyberSOC augments existing prevention/network/security tools and does not change or need any additional hardware, software, or security experts. It is anchored through a dedicated security engineer who acts as an extension of a company’s internal IT team and conducts both real-time and hunting tasks to protect the company against known and future threats. AWN CyberSOC addresses the complete security value chain of threat detection and response at a price that’s affordable for mid-market companies.

AWN CyberSOC combines best of breed technologies to analyze millions of security events in real-time through different tools. Strong algorithms, correlation rules, machine learning, real-time threat intelligence, and analytics tools help detect new threats exploiting zero-day vulnerabilities. As a distributed SOC model, AWN CyberSOC has machine learning capabilities that share anonymized threat intelligence between teams to proactively hunt for threats known or detected by other teams.

The combination of human and machine intelligence analyzes millions of events in real-time for 24x7 threat detection. The machine learning, threat intelligence feeds, and big data security analytics tools collect and correlate security events from all of a company’s infrastructure, security devises and applications, delivering events to a dedicated Security Engineer to review and respond to in seconds. The SE then notifies the company with relevant details along with forensic analysis and recommended remediation as incident response. For mid-market companies with limited resources, AWN CyberSOC saves valuable time for internal IT and security teams while helping to mitigate the risks of a data breach.