The Missing Link in Security: The Evolution of the Modern MSP
Business has never stopped evolving. From the very first Dino-Dentist and Tar Pit Taxidermist, SMBs have been shrinking, growing, re-focusing and changing. And when Ugg the caveman first discovered his competitor trying to steal trade secrets, the security market was born. Yesterday’s wooden club is today’s firewall.

Of course, at some point, there came along a savvy erect-standing, fur-clad business owner who figured out that he had better things to do than manage his growing IT problems. He called his local VAR and the dawn of the Managed Service Provider had come and it’s never stopped evolving.

In this paper we follow the evolution of the security market, walking in the footsteps of MSPs as they journey from product sales and basic services and advance into a comprehensive security provider.
The 2015 security market has expanded to nearly $77 billion at the end of 2015.

History books tell us that in the beginning, the cybercrime situation kept getting worse and worse with security incidents increasing with double-digit growth year after year.¹ So the VAR community said unto the end-user, “We’re going to flood your back office, endpoints and perimeter with security solutions. When the threat changes, we’re going to sell you more stuff, too!” Of course the vendor community kept developing more and more solutions for the threat du jour. The result: the cybersecurity market has grown to nearly $77 billion (2015).² And now the security market is fully-laden with point products promising to be the “silver bullet” in cyber-threat detection.

Eager and well-meaning sales people continue to push their products and solutions onto IT Managers who are desperate to protect their proprietary data and company bank accounts. But the result is a growing collection of products that increase cost, complexity and management burden. In the SMB segment where expertise and resources are in short supply, the proliferation of point products can introduce even more risk because the administrator can’t properly manage and respond to the events those products are uncovering.³
2.0 The Big Bang

According to Alex Stamos, CISO of Yahoo!, “The explosion of security needs means the median security engineer in 2015 is less experienced than their counterpart in 2005. Security companies need to recognize that most of their addressable market cannot properly consume their products.”

Why can the market not “properly consume” today’s multitude of point products? There are several reasons. First, IT Administrators often don’t fully understand the threats. Threats come from numerous vectors, in numerous forms and they’ve become increasingly complex - combining ingenious forms and non-traditional vectors in targeted attacks. Without an understanding of the threat, its origin and its target, the right security strategy cannot be developed. And without the right strategy, security tools are ineffective.

Second, multiple tools require multiple consoles and multiple configurations, necessitating training that eats into the limited time and budget of an IT Administrator. Lack of training results in misconfigured devices and, ultimately, contributes to inadequate protection.

Finally, even with proper configuration, someone with the expertise to understand what the tools are telling them needs to monitor and manage these solutions on an ongoing basis. Just like a trained nurse watches over a patient’s monitors, someone needs to be watching 24/7, and when an alert occurs, they must know what to do with that alert and how to remediate the incident.
3.0

Enter: The Dark Ages

While security spend continues to increase, data breaches are also increasing. According to the 2014 Verizon Breach Report, 43 percent of companies had experienced a data breach. Sixty percent of those breaches occurred in small and medium-sized businesses - and 60 percent of those organizations will fail within six months of a cyber-attack because they do not have the financial wherewithal to weather such a storm.

Even with all of these point products, attacks are taking longer than ever to uncover. According to the Verizon Report, 83 percent of attacks took more than two weeks to discover. Sixty-seven percent took months. Some went unnoticed for years. Why is this? Cyber criminals have become extremely sophisticated in their approach to attacking organizations, using a combination of phishing, social engineering and malware, taking advantage of common business tools like email, social media and valid business web traffic to launch attacks. Every possible vector is exploited to gain access to valid administrative credentials and systems with proprietary data or company bank accounts. They simply take their time to make sure they’ve reached their target.
Big Data, Big Problems

Just like the contents of a DNA strand, the amount of data produced by systems in a typical network can be massive. Network devices, data/file servers, web servers, storage devices, OSs and applications generate thousands of log entries per day. Buried within those logs is often the evidence of an attack. Log data, particularly when correlated across multiple systems on a network, can provide a very accurate picture of an attack, where it’s coming from and what it’s targeting. This data can be used to remediate the event and provide an identifiable fingerprint to prevent future attacks. Deploying the technology required for watching and understanding the data that these logs provide is daunting, particularly for the SMB IT organization.

Security Information and Event Management (SIEM) technology is used to separate the important alerts from the rest of the noise as it sifts through thousands of logs each second. SIEM products are both expensive and complex, requiring highly trained engineers to configure and manage them. Expertise is also required to correctly read the output of a SIEM tool, understand what the alert is, and know how to respond to the threats that are uncovered. And because most organizations, particularly in the SMB segment, cannot afford 24/7 resources to watch alerts in real-time, threats go un-noticed until the damage is done.
In 2001, Hewlett Packard released a white paper entitled “A Fool with a Tool is Still a Fool,” focused on the HP OpenView product. The overall premise of the document is that the tools being used are only as good as the people, processes and technology in the organization. This is also true of a SIEM product. Unless it is configured with the intelligent rulesets needed to find today’s complex threats, attacks will be missed. Without properly trained security engineers to decipher and understand the data and then apply the proper remediation steps, attacks will be successful, which as we saw earlier, can lead to the demise of the business.

So what is missing from most SIEM implementations and security strategies today? Intelligence and expertise! A tool is only as good as the intelligence used in its configuration/setup and the expertise of the engineer using the data it generates to remediate events and develop strategies to prevent future events.
A SIEM is only as good as the correlation rules that are used to pinpoint malicious activity. Tuning the SIEM over a period of time is essential for determining risk and pinpointing attacks. Turning on thousands of pre-configured, “out-of-the-box” rulesets can create so much noise that real alerts go undetected. Conversely, a configuration with too few rulesets can result in missed events and a false sense of security. As threats grow in both volume and complexity, knowing what to look for is critical, and continuous updating of the rulesets and knowledge base is mandatory. The majority of SMB IT departments do not have the security expertise to properly configure a SIEM to find today’s complex threats and targeted attacks.

Even if you configure your SIEM properly to pinpoint today’s threats, the human element is required on a 24/7 basis to watch, analyze, triage and respond to alerts that are generated in real-time. Many organizations spend tens, even hundreds of thousands of dollars on implementing technology but are hesitant to bring in the expertise and resources needed to triage, respond to and remediate events.
The Managed Security Services (MSS) market is projected to grow 45% over the next 5 years.

Because of this lack of resources and expertise, the SMB market is increasingly outsourcing their security monitoring. According to Infonetics Research, the Managed Security Services (MSS) market is projected to grow 45 percent over the next 5 years. Unfortunately, many MSSP customers are not totally happy – or are dissatisfied with their provider and might even consider leaving early on in the relationship. Why?

MSPs and other IT Solution Providers often suffer from the same lack of resources and security expertise as their customers. When outsourcing, the SMB client expects to completely hand off security to their partner. Unfortunately they end up having to do more work than expected because their partner is not equipped to handle triage and remediation of security events. Dissatisfied with unrealized expectations, customers might not renew and retention numbers will dip.
What options does the MSP have? One solution is to build a 24x7 Security Operations Center (SOC), but that requires capital investments that many partners just don’t have. A robust and redundant infrastructure can run into the high six if not into seven figures. The SOC must then be staffed with highly trained, often hard to find security engineers. Processes and procedures must be built, including Service Level Agreements and Master Service Agreements protecting both the customer and your business. While implementing all of these components won’t take eons, it’s not an overnight fix, either.

The truth is, creation of such a service delivery mechanism is beyond the capability of all but the largest MSP organizations today. But the lack of a 24/7 SOC means partners will be unable to provide the security services that customers are demanding.
We’ve come a long way on our journey to determine who the modern MSP is, and how they’re supposed to survive in this new world. But before we look to the future, let’s turn around briefly to summarize where we are:

- Clients have a bunch of security solutions in place that they can’t manage.
- They need security experts to help them, so they call MSPs.
- The MSP can’t provide comprehensive help because they don’t have the technology, expertise or threat intelligence.
- The only solution on the market is to spend upwards of $1 million on a 24/7 SOC.

It’s evident that we have a huge gap between customer need and the MSP’s ability to solve it. Let’s call it the missing link. Vijilan Security was created to fill this intelligence and resource gap. Vijilan sells continuous monitoring, threat analysis and response guidance exclusively to and through Solution Providers and MSPs. This enables MSPs to provide security services without having to invest in infrastructure, 24/7 resources or the cyber-intelligence required to detect and remediate today’s complex threats.
Vijilan has invested millions in building a robust, redundant, 24/7 Security Operations Center so the MSP doesn’t have to. It’s staffed with highly trained security engineers that monitor and remediate in real-time. Most importantly, you can go to market with these services immediately, providing a response to customer demands and improving customer retention.

Vijilan helps reduce your customers’ security risk by collecting real-time logs, performance and configuration data from the devices on their network. We then use our expertise and knowledge-base to identify and remediate cyber-incidents. Our services include:

- Collection and parsing of event logs and device information from the client’s network
- Automated application of correlation rules in our advanced, cloud-based SIEM infrastructure
- Human “eyes on” scrutiny to every event identified by our 24/7 cyber-threat detection engine to eliminate false positives
- Expert, detailed analysis of security alerts from our fully-staffed Security Operations Center (SOC)
- Mitigation and remediation guidance by Vijilan’s advanced Security Engineers
- Access to reporting and monitoring status via an exclusive partner portal

Vijilan is 100 percent channel, which means we will never compete with you for your customer, and we’re committed to make your business more profitable. Our time-to-market is literally over-night as there is no product to purchase, and nothing to install at your site. You can begin selling immediately.
Vijilan helps you fill the gap and evolve into your client’s ideal partner – to solve the missing link – with services and intelligence that truly protects your customer from cyber-crime. Visit us today at www.vijilan.com and see for yourself how Vijilan can add immediate value to your customer base.

9. A FOOL WITH A TOOL IS STILL A FOOL! Lindsay Parker, HP OpenView. 2001