Zero Trust Security - with an Immediate ROI

MSSP Case Study

Seceon's zero trust model, combined with the SonicWall next-generation firewall (NGFW) security services provides a powerful breach detection and mitigation solution. The combined solution enables a breakthrough in reducing operation cost, which allows for extremely profitable MSSP service offerings.

Cyber breaches are growing in both frequency and severity. Despite the vast amounts being spent on today's state of the art cybersecurity solutions - data breaches are happening at an increasing rate with over 600 detected and reported in the U.S. alone by August 2016, and greater severity with over 20 million exposed records, a 20% increase over record-breaking years 2014 and 2015, according to the ITRC.

Most organizations are unable to properly deal with cyber threats because: they are too slow to identify them and too slow to stop them from inflicting damage once the organization is breached. The challenge is most cybersecurity solutions require human intervention – smart humans that are specifically trained in how to use an array of complicated tools to identify a threat and then figure out how to stop it. The problem, as the 2016 Verizon Data Breach Report exposes, is that 95% of attacks exfiltrate and/or corrupt data within a few hours of a breach. This is not enough time for even the smartest humans to react. Worse yet, analysts at 451 Research estimate that fewer than 4% of enterprises and government organizations have dedicated security staff in a security operations center (SoC) to monitor all these products for possible breaches.

Small and medium sized organizations are the most impacted by these security threats and are increasingly asking their Managed Security Service Providers (MSSPs) and service provider partners to help support their security challenges. No longer are MSSPs driven to advocate for the need to invest in security software and services; recent high profile breaches at Yahoo, Eddie Bauer, Oracle's MICROS system, Anthem and the IRS have done all that is necessary to fuel the demand. The mission for today's MSSP is to provide security offerings that can lower a customer's security risk at an acceptable price point. [1] In fact, according to a recent Kaseya Ltd.

MSP Global Pricing Survey[2], which polled owners and operators from nearly 400 MSSPs, over a quarter of all respondents identified "heightened security risk" as the number one IT problem or service MSPs expect their clients to face in 2016.

The combination of Seceon OTM and SonicWall NGFW, breaches can be shut down as they occur, not weeks or months after the data is stolen. It's the ideal solution to be used by MSSPs who are only profitable if they can deal with threats quickly and distribute their staff costs across 10s to 100s of customers.

Consider the following example

- A given customer's managed firewall generates events, for North-South traffic, but demands deeper human analysis for comprehensive threat detection and analysis
- Events for East-West traffic are usually understood by looking at the server logs and network flows, which also demand deeper human analysis and many times require a lot more time even with a good automation
- The volume of events can stack up to more than even a dedicated, trained staff can handle, which no MSSP can manage or afford.
- Our survey indicates at least 3 relevant threats occur daily in a F5000 mid-size company. Each incident troubleshooting requires weeding through the firewall and server logs and many times even looking into network traffic or packets to determine the exact analysis of threat.

Flows/Logs Troubleshooting	Activity Type	Flow/Log Instances	Analysts Comments
Next-generation firewall (NGFW) (SonicWall) generates events/logs around an instance of an infected device attempting to connect to a bad web site.	North-South Activity	444	NGFW is resetting connections from the device over time. Watch this device for other non-critical flagged messages
Device is also performing IP Sweeps	East- West Activity	135	Few separate instances across the internal network
Device is also performing IP Port scans	East- West Activity	92	Few separate instances across the internal network
Device needs to be identified	Internal Activity	1	What device is it? Who or what group it belongs to?
	Total Activity	**672**	instances to investigate

- Costs of Junior and Senior SOC Analysts are approximately as follows:

Jr. SOC Analyst	Sr. SOC Analyst	Costs

$75,000	$250,000.00	SOC Analyst Burdened rate per year
$1,442.31	$4,807.69	cost per week
$36.06	$120.19	cost/hour
$0.60	**$2.00**	cost/minute

The cost of troubleshooting just one incident by a junior analyst is $600 over the course of 2-3 days, the report of which must then be reviewed and analyzed by a more senior analyst over the course of another 1-2 days. **Over time, the cost in time and resources is approximately $1800/day, adding up to $450K/year!**

Minutes per instance investigation	1.5
Total minutes of effort per incident	1006.5
Cost/minute or $ /minute	$0.60
Total cost to correlate one incident	**$603.90**
Typical incidents per business day investigated at a mid-sized F5000 (As per Ponemon/Verizon Reports)	3
Total cost per business day	$1,811.70
Total cost per year	**$452,925.00**

Automating this process would save most of this cost and most importantly, the variable cost of data breaches. Cost of data breaches mostly depends on the industry and the value or criticality of the information being breached; for example, for healthcare industry the approximate cost of losing one patient's PHI record is $355. So a firm that deals with 100,000 patients in this industry is at **risk of $35M if a data breach happens** stealing all of these patients' records.

Seceon + SonicWall Zero Trust approach is a comprehensive real-time prevention method, as well as detection and response for both North-South and East-West traffic. Using SonicWall next generation firewalls we offer perimeter-based defenses for monitoring North-South traffic and blocking unauthorized access. Simultaneously, using Seceon's OTM for threat detection and elimination, Seceon is able to monitor, detect and take action for East-West traffic that would normally go undetected in traditional security designs. Seceon integrates easily with SonicWall NGFW and any source of East-West traffic, including routers, switches, servers, POS. directories and applications to provide a single, comprehensive view of all facets of a customer's environment, including prioritized threat alerts and specific actions to contain the threat.

This solution not only detects threats in minutes it provides complete analysis and it automates remediation steps to a click of a button. The average time spent per threat can be a few

minutes per customer per incident to detect and stop the problem.

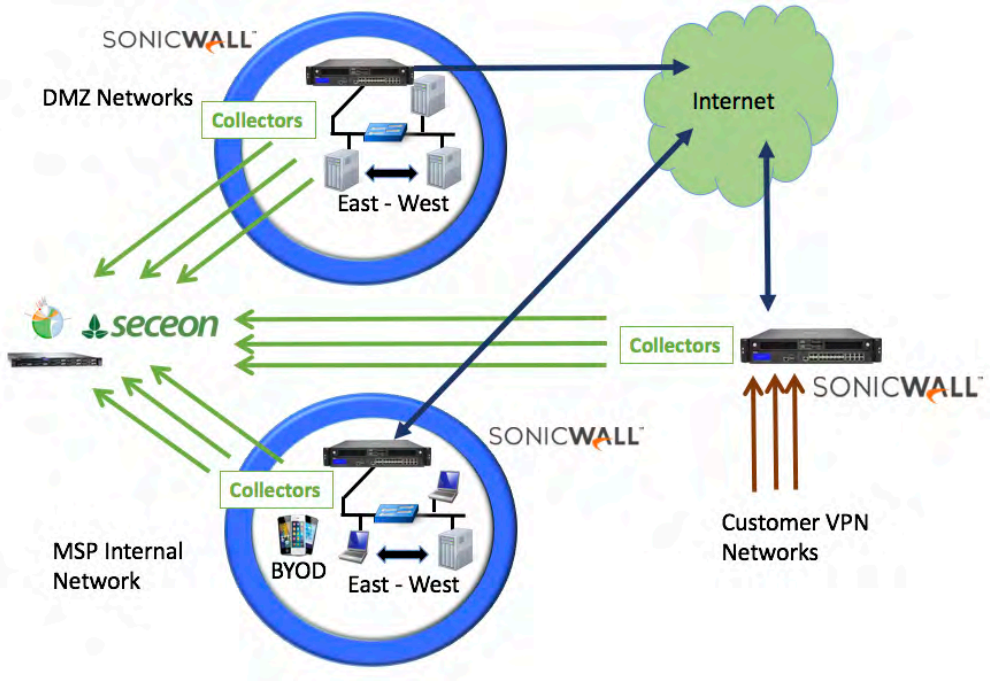
Using our Example:

3 threats per customer per day – Time spent: 5 minutes per threat = yields a cost of $8 per day

This allows an MSSP to offer a superior service and charge a premium while keeping costs to operate down to a few dollars per customer per day.

Reference Architecture

Consider the following reference architecture on how most Managed Security Service Providers (MSSPs) can deploy the combined solution of SonicWall NGFW and OTM.

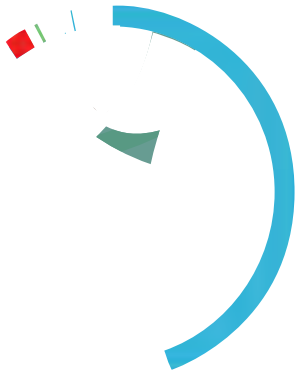


MSSP Reference Architecture with SonicWall

Visibility

The first step in automating incident analysis and response is to provide visibility into all traffic and then correlate any abnormalities with anomalies in behavior.

Seceon, the only threat detection and Management Company to visualize, detect, and eliminate cyber threats in real-time, offers its Open Threat Management (OTM) platform for automated threat detection and elimination. Seceon OTM correlates all of these events from SonicWall



NGFW, network flows and server logs together, using dynamic threat models that leverage machine learning to derive threats that are posted in priority order, and/or sent by email notification. Moreover, by leveraging machine learning, policies and threat models update automatically, continuously "learning" and requiring no intervention for updates. These same learnings can be applied across multiple customer environments, ensuring the communication of valuable threat information to all of the MSSP's customers.

OTM enables MSSP to maintain a comprehensive view of all customers through a single pane of glass--seeing each customer's threat status in one screen while allowing protected portal access to each individual customer environment.

Real-time detection

When it comes to effective breach detection and response, we also know time is of the essence. Recent industry data shows that credentials are compromised in minutes and most of an organization's critical data or intellectual property is lost within the first hour. Specifically, according to Verizon's 2016 Data Breach Investigation Report[3], 81.9 percent of organizations surveyed reported that a compromise took only minutes to infiltrate company systems with 67.8 percent of respondents showing that associated data was "breached" within days of the initial compromise. Therefore, any threat detection solution that cannot detect and remediate threats in near real-time is not much use. Valuable assets could already be stolen and sold on the Dark Web before an organization knows they are even missing!

The cost of losing these assets can mean more than loss of data. The Poneman 2016 report [4] concludes that on an average each data breach costs $4M for the 383 organizations that participated in 2016 data breach cost study. The costs are exacted in terms of financial loss, reputational impact, exposure of personal information and potential customer reimbursement. Average data breach cost per capita is highest is USA ($221) and Germany ($213). This is across all of the industries, but certain industries like healthcare and financials have much higher cost per data breach per capita. Real-time threat detection and elimination can be the difference in stemming significant losses in spite of the inevitable breach.

Seceon OTM and SonicWall NGFW solutions provide the ability to stop threats in real-time[i] by:

- Threats detected by the SonicWall NGFW are forward to the Seceon OTM for analysis and with combined enriched data from other sources, Seceon OTM creates FW policies
- Pushing policies to the SonicWall NGFW to block communication from addresses outside the network, such as those involved with DDoS, Brute force, APTs and Malware CNCs.
- Pushing the policies to isolate any systems (end points or servers) that insiders have used to capture high value data, so that they cannot exfiltrate it out over the network. As well as preventing malware infected from doing harm to other devices
- Disabling of credentials in case of compromised credentials (data breach), or insiders who are attempting to access off limits systems.
- Preventing lateral propagation of threats, such as ransomware, botnets, etc.
- Helping organizations see and stop threats as they become active in minutes, not in weeks, which is today's norm

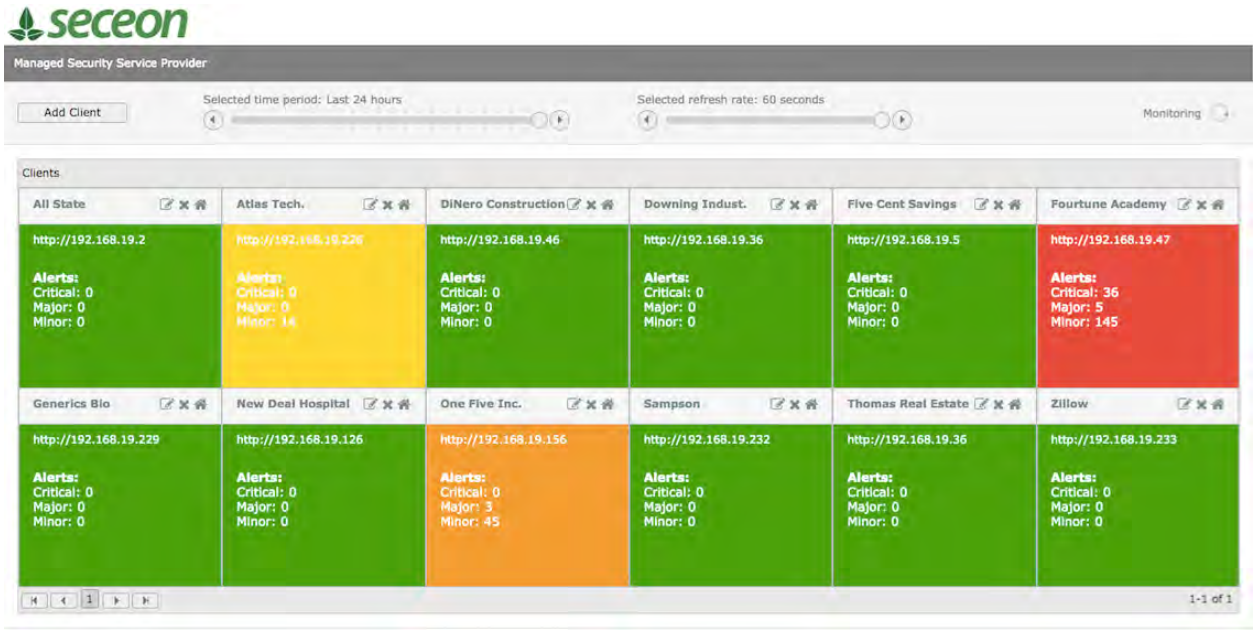
Multi-Tenancy Support to empower MSSP partners with a SOC-in-a-box solution.

Powered by advanced data collection and analysis, machine learning and patent-pending predictive and behavioral analytics, Seceon's OTM provides customers with a proverbial "SOC-in-a-Box™," automating human and time intensive analysis and decision-making and significantly speeding the time to detection and remediation. Anticipating attackers' behavior choices, the solution enables MSSPs to see *and* stop the threats as they happen, preventing risk, damage or loss of valuable information.

Immediately upon deployment, Seceon's solution begins to surface a concise list of threats in plain language. It uses behavioral analytics generated by an extensive set of dynamic threat models, aided by machine learning techniques to detect both known and unknown zero-day attacks. Seceon's OTM is purpose-built to be operationally efficient and installation friendly, allowing easy-to-scale and effective deployment with minimal training.

Seceon's OTM provides MSSPs with a single screen for viewing multiple tenants with each tenant or customer only able to see its own assets. With OTM deployed in a multi-tenancy environment, all customers can benefit from the platform's machine learning capabilities. Any new threats are captured, reported and fed back into the system's threat models, ensuring the continuous sharing of threat intelligence across all customers.

- Single view for MSSP for multiple tenants with each customer seeing only its own assets.
- Easy to apply learned security lessons from one customer to another



Immediate ROI

Today Threats are typically found using SIEM solutions. Typically, most security solutions like SIEM platforms can generate many alerts that can be overwhelming for team of security analysts to process. Seceon OTM not only processes them through their feed, but also correlates them with other feeds and surfaces the real handful of alerts that need attention. *The results of combining feeds to an event saves the security analyst from combing through hundreds of alerts from different systems and hand correlating those that can be found to be related.* The security analyst only needs to review major or critical alerts to decide upon the course of action – and/or follow the systems recommended remediation steps improving their operational efficiency and lowering operational costs. OTM helps MSSPs by improving the efficiency of senior security analysts, who are very hard to find and whose time is a costly MSSP resource that needs to be spent wisely on cyber security issues that really matter rather than on many manual tasks that can be taken care of by automation.

Also the SIEM platforms typically require a higher initial investment since most SIEMs require a perpetual license with higher upfront cost. Most SIEMS can't be shared across multiple customers without comingling their information. Therefore SIEM solutions do not lend themselves to allowing a single operator to easily monitor tens to 100s of customers from a single screen. Seceon OTM is priced on a number of protected devices SAAS model allowing a 'Pay as you go' model ideal for MSSPs looking to offer a monthly service to end-customer organizations of any size. As the example above shows - it immediately provides cost savings through operational efficiency vs. SIEMs other threat detection tools on the market. The joint

Seceon- SonicWall NGFW solution helps MSSPs to easily scale the security services with low initial investment that can be increased incrementally with growth in their customer base.

Seceon's zero trust model, combined with the efficacy of SonicWall NGFW security services, breach detection and mitigation is controlled in a swift, cost effective manner. The end result is a safer network for your company assets, personnel, and financial success.

About Seceon:

Seceon and its OTM Advanced Threat Detection and Remediation Platform is the industry's most highly awarded platform during 2016. Its novel approach at focusing on detecting and stopping threats automatically before data is compromised has redefined the work of today's analysts - freeing them from the difficult work of detecting threats and deciding how to stop them and allowing them to focus on how prevent them from happening in the first place. The OTM solution with it recently added MSSP multitenant capabilities has finally made it operationally profitable for MSSPs to move beyond only offering managed firewall services and offer customers of any size an ability to add advanced threat detection and remediation service – solving today's most vexing problem how to make threat analysis and remediation a task that takes minutes to perform when an incident arises by minimally trained staff.

About SonicWall:

Over 25 years, SonicWall has been the industry's trusted security partner, protecting millions of networks worldwide. From network security to access security to email security, we have continuously evolved our product portfolio to fit in quickly and seamlessly, enabling organizations to innovate, accelerate and grow. Our customers know it takes strong security to say yes. We are the trusted partner that allows them to say yes to the future without fear.

SonicWall security solutions are the preferred choice for distributed enterprise, government, education, retail, healthcare and financial deployments. SonicWall products have been hailed by industry publications such as Network World, InfoWorld, PC Magazine and SC Magazine for easy-to-use, high-efficacy and high-performance appliances and services. In 2016, SonicWall earned the highest rating of "Recommended" in the latest version of the NSS Labs Next-Generation Firewall Security Value Map for the fourth year in a row, and was rated as one of the top products for security effectiveness.

SonicWall. Your partner in cybersecurity.

References:

1. Techspective, Cyber Security Threat Detection - The Case for Automation, September 2016 http://techspective.net/2016/09/21/cyber-security-threat-detection-case-automation/

2. Kaseya Ltd. MSP Global Pricing Survey https://www.channele2e.com/2017/01/09/msp-global-pricing-survey-kaseya-2017-findings/

3. Verizon's 2016 Data Breach Investigation Report *http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/*

4. The Poneman 2016 Cost of Cyber Crime report http://www.ponemon.org/library/2016-cost-of-cyber-crime-study-the-risk-of-business-innovation

[i] The statements contained in this case study regarding the performance of Seceon products and services and SonicWall products and services are attributable only to each company, respectively, and should not be deemed to be the statements or representations of the other company.