ZERO-DAY, ZERO TRUST SECURITY WITH IMMEDIATE ROI

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 cyber-security 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 business (SMB) customers are increasingly asking Managed Security Service Providers (MSSPs) to handle their security challenges.

> 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.

The following example demonstrates the high cost of deploying current cyber security defenses for the enterprise and illustrates the painful reality that SMBs lack the funding and resources to protect precious digital assets:

- Firewalls generate incidents for North-South traffic, but these events demand deeper human analysis
- Incidents for East-West traffic are usually understood by looking at server logs and network flows, which also demand deeper human analysis, and often, a great deal of time even with a good automation
- The volume of incidents stacks up to more than even a dedicated, trained staff can handle, assuming a company even has dedicated security staff

Flows/Logs Troubleshooting	Activity Type	Flow/Log Instances	Comments
NG FW (Dell SonicWALL) generates events/logs around an instance of an infected device attempting to connect to a bad web site.	North-South Activity	444	NG FW is resetting connections from the device over time and is not correlating these "non-critical flagged" incidents
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? Which group it belongs to?
	Total Activity	**672**	**Instances to investigate**

- Research suggests that at least three relevant threats occur daily in a Fortune 5,000 mid-size company. Troubleshooting each incident requires weeding through the firewall and server logs and frequently demands looking into network traffic or packets to determine the exact analysis of threat

The analysis is conducted most often by a human analyst. The costs of these analysts are approximately as follows:

Jr. SOC Analyst	Sr. SOC Analyst	Costs
$75,000.00	$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.

Faced with insurmountable costs and demand for talent they just can't access, SMBs turn to MSSPs for help in addressing their technical, resource and budget challenges.

New Offering from Leading MSSP Secure Designs, Inc. (SDI)

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

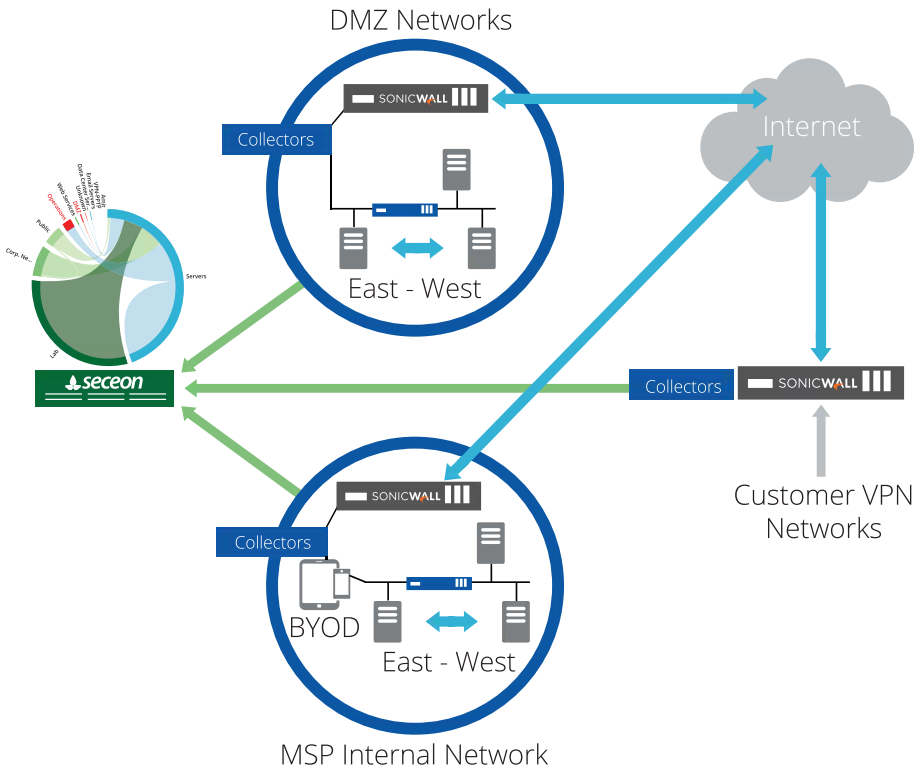
firewalls, SDI offers perimeter-based defenses for monitoring North-South traffic and blocking unauthorized access. Simultaneously, using Seceon's OTM for threat detection and elimination, SDI is able to monitor, detect and take action for East-West traffic that would normally go undetected in traditional 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 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



Most SMBs and MSSPs are unable to properly deal with cyber threats because they are too slow to identify and stop them from inflicting damage once the organization is breached. Moreover, most SMBs don't have the resources to spend on investigating every security incident and thus, are more vulnerable to cyber security attacks. Automating this process would reduce this expense and,most importantly, dramatically reduce the variable cost of data breaches, which can be tens of millions of dollars depending on the value or criticality of the information being breached. By correlating events and prioritizing legitimate threats, Seceon automates tedious, but necessary, manual tasks, improving the efficiency of MSSP security consultants and keeping them focused on addressing cyber security issues critical to SMB success.

Consider the reference architecture on how Secure Designs, or other MSSP, can deploy the combined solution of SonicWALL and Seceon OTM. The Seceon OTM platform can scale across multiple customers while maintaining the sanctity of customer information, as well as for MSSP's internal network and other service protections.. Multi-tenancy is supported through a single Seceon OTM platform, which provides separate dashboard views for multiple customers, distributing the cost of the platform.

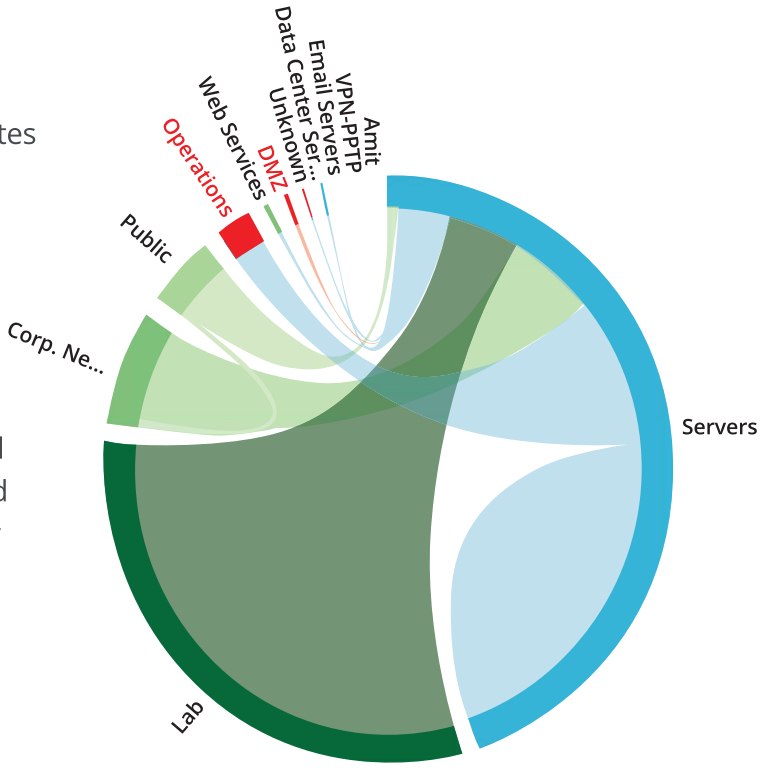
Visibility

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 OTM enables Secure Designs 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 and Elimination

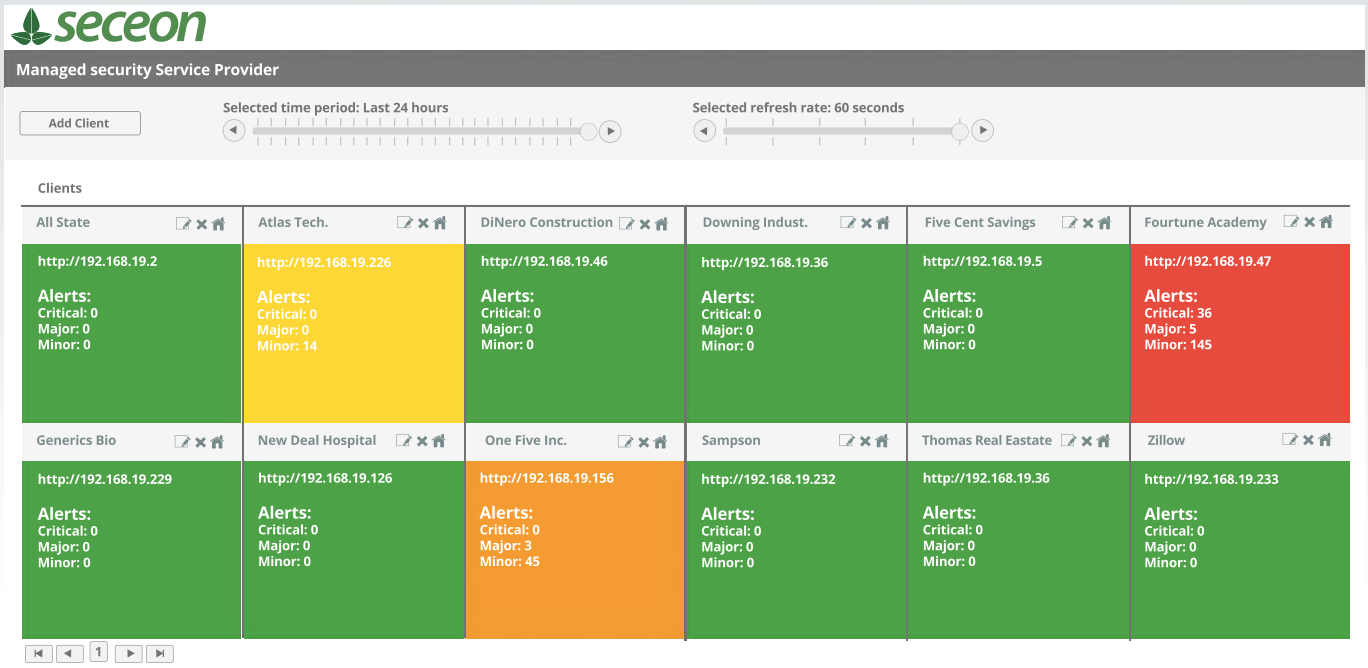
When credentials are compromised within minutes and most of an organization's critical data or intellectual property is lost within the first hour, time is of the essence. Secure Design offers a fully integrated Seceon OTM and SonicWALL solution that provides automated, real-time threat detection and elimination by:

- Pushing policies to isolate any systems (end points or servers) that are malware-infected or to prevent an external IP from doing any harm (data breach)
- Disabling of credentials in the case of compromised credentials or insider threats
- Preventing lateral propagation of threats



Multi-Tenancy Support

Seceon OTM provides Secure Designs 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, Seceon enables Secure Designs to see and stop the threats as they happen and surfaces a concise list of threats in plain language. 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 Secure Designs with a single screen for viewing multiple tenants while enabling each tenant or customer to only see its own assets. With Seceon OTM deployed, all Secure Designs 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.

> 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.

Affordable Investment, Immediate ROI

Seceon OTM's subscription-based offering is an affordable model for organizations of any size, providing immediate cost savings through operational efficiency. The protected assets-based subscription model allows MSSPs, including Secure Designs, to deploy Seceon OTM with a smaller initial investment and operational costs than many current alternatives, including SIEMs. This model enables MSSPs to easily scale their security services with low initial investment that can be increased as its customer base grows.