

STONESOFT

Whitepaper

**Starting Managed Security
Services with the Stonesoft
MSSP Solution**

Contents

Executive Summary	3
Introduction	4
The easy way to service delivery	5
Efficient operation	7
Unique customer experience	9
Cutting edge technology against Advanced Evasion Techniques	10
The economical choice	11

Executive summary

Many small and medium-sized businesses (SMB) are thinking about outsourcing their security operations to a managed security service provider (MSSP). Possible reasons include:

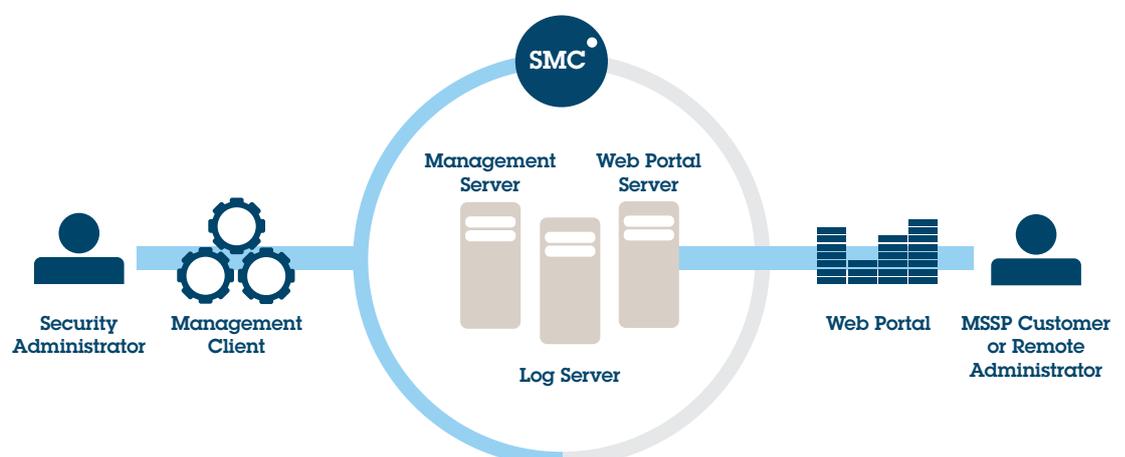
- Security is not their core business.
- SMBs need more protection as hackers have become more sophisticated and thwarting attacks requires more skill, time and effort.
- SMBs want to have greater competency and reduced costs. Good network security people are expensive and it is not cost-effective for small companies to have them on their payroll.
- SMBs want to gain 24/7 coverage. Modern global business requires an always-on mentality which is difficult to provide with limited resources.
- New regulatory requirements mean extensive reporting and continuous auditing of security systems.

It makes sense for SMB customers to outsource their security. With an MSSP, SMB customers can concentrate on their core business while getting high-quality professional security services from a centralized location. Operating costs can also be reduced because MSSPs can replicate similar services for multiple customers, lowering unit costs.

The Stonesoft Managed Security Service Provider solution offers an easy and low-risk approach to starting and maintaining MSSP services. Stonesoft's innovative business model combines cutting edge technology and low total cost of ownership (TCO) to create an outstanding business opportunity.

With the Stonesoft MSSP solution there are several ways to generate additional revenue streams using the different capabilities offered by Stonesoft products. For example, the Stonesoft Web Portal can offer highly customizable real-time visibility of the customer environment including firewall and IPS security policies, logs and reports. Each of these elements can be a separate billable item. Customers can also use the Web Portal to give read-only access to 3rd-party auditors, allowing them to easily audit the security environment remotely.

Stonesoft's Firewall/VPN and IPS make it easy to provide MSSP services with devices on the customer premises or with devices located in a security operation center (SOC). Typically, a customer will outsource a small portion of their security to test the service and see if the MSSP can live up to its Service Level Agreements (SLA). Gradually customers will then move to more comprehensive outsourcing. After a good track record has been established, customers will be ready to choose from several additional service levels and add-on services that an MSSP can offer.



Stonesoft centralized management is the heart of the system and has been designed with an MSSP in mind. Centralized management provides an MSSP with situational awareness of their security service environment and its current state. Automated tasks make service delivery efficient and the infrastructure scales well when an MSSP's business grows. For example, Stonesoft products provide basic SIEM (security information and event management) services for a starting MSSP so that it can avoid investing in an expensive SIEM solution. Virtualization and cloud services offer a cost-efficient way to provide MSSP services.

Introduction

The starting point for a new managed security services provider is to decide how much capital investment to make. There are generally two different types of managed security services: a hosting service or a provisioning service. In a hosting service, the customer owns their devices and decides what kind of devices they are using. The service provider just runs or manages them, which only requires a small capital investment. In the provisioning model the customer only buys managed security services and the service provider owns and decides what kind of equipment will be used. Normally a service provider has a security operations center (SOC) where it runs managed security services for several customers. Naturally, the provisioning approach requires more capital investment than the pure hosting service.

Many new MSSPs start small with a hosting service model and gradually move towards a provisioning model as the number of customers increase. This usually means that both managed security service models are in place within the same service provider during their growth period. Stonesoft products are a good fit for both hosting and provisioning service models.

A managed security service provider also has to decide what kind of Service Level Agreements (SLA) to provide. For example, it can offer either 8-to-5 services or 24/7 services. In addition, the response time to customer requests needs to be defined. Typical response times range anywhere from 1 day to 1 hour. Onsite support might be needed and its response time has to be decided as well. All these decisions affect a managed security service provider's personnel requirements. The general rule is that the tighter the Service Level Agreement is, the more people it requires.

Running managed security services creates costs and these costs can be divided into capital expenses (CAPEX) and operational expenses (OPEX). During an MSSP's early years most costs will be capital expenses. As the number of customers increases, the majority of costs will become operational expenses. Stonesoft is a good choice for a managed security service provider because the Stonesoft MSSP solution reduces both CAPEX and OPEX, enabling MSSPs to maintain higher margins.

The easy way to service delivery

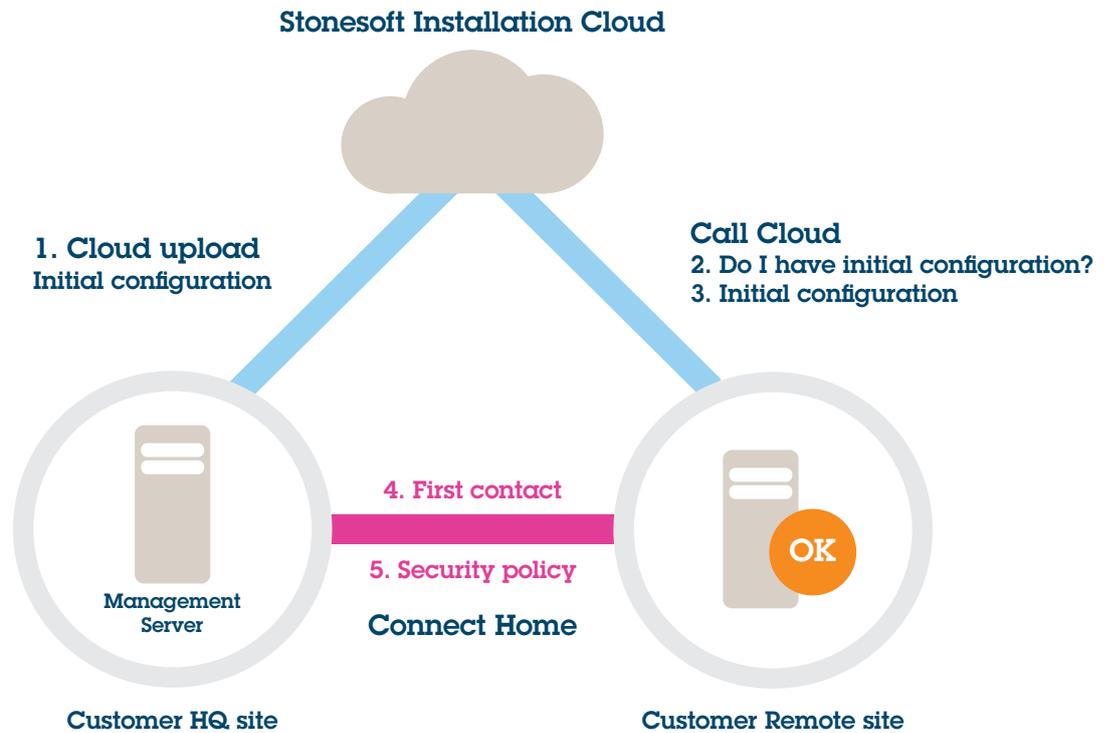
The Stonesoft Management Center makes it easy to start a managed security services business with physical appliances and/or virtual appliances.

The main challenge for MSSPs is that not all customers are alike. They have different service level needs and the MSSP should be able to cater to all them. Stonesoft professional services can help MSSPs to create customer-specific service levels and suitable content for them. The three levels are called **standard**, **advanced** and **premium** service levels.

MSSP SERVICE OFFERING - PROPOSAL		STANDARD	ADVANCED	PREMIUM
Service				
Gen.	Web Portal acces	-	1 account	5 accounts
	Localization	-	+	+
Support	Support level (email)	Basic (8/5)	Premium (24/7)	Premium (24/7)
	Response time	24 hours	6 hours	2 hours
	Hot line support/assistance	-	Basic (8/5)	Premium (24/7)
Logs	Log archive (logs stored in MSSP servers)	3 months	6 months	Year
	Log archive delivery to third party location	-	-	Monthly
Changes	Free policy change requests / month	10	20	100
	Free routing change requests / month	5	10	20
	Cost for additional change requests	100 €	100 €	50 €

Providing different service levels does not have to be difficult, thanks to the Stonesoft Management Center. The basic principle is simple: create once and use it everywhere. Most of the Stonesoft Management Center's elements are reusable. You can decrease your workload per customer by using the same policy templates, report templates, etc. for multiple customers. At the same time you can ensure that customer-specific elements are never mixed up – customer domains mean that all customer-specific information can be isolated from other environments. The domain structure makes management of hundreds of customers with the Stonesoft Management Center easy.

Gartner Research states that 99% of security incidents are the result of configuration mistakes or human error. To avoid this, many of the daily tasks an MSSP needs to undertake are predefined and automated in the Stonesoft Management Center. The Customer Domains feature implicitly separates customer environments from each other and makes each customer simpler to manage. In addition to element reuse, automated routine tasks and numerous security validations help administrators to prevent human errors as far as possible.



From the customer’s point of view, Mass Security deployment is easy and they can start using the service immediately – a good basis for an outstanding customer relationship.

Stonesoft also provides methods to convert existing firewall or IPS implementations from other vendors to a Stonesoft-compatible implementation. This helps to make conversion projects faster and less error prone by reducing manual work. Some 3rd party products can be even kept and monitored centrally through the Stonesoft Management Center’s 3rd party event management features.

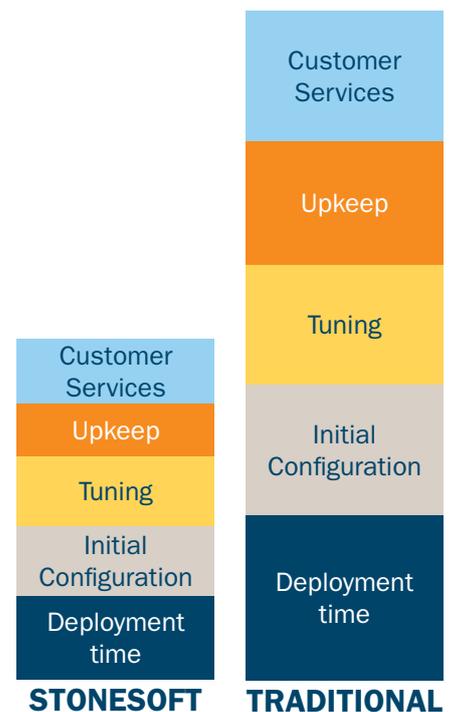
You can learn more about Stonesoft Mass Security at masssecurity.stonesoft.com.

Efficient operation

An effective centralized security management system is one of the most important tools that a managed security service provider needs. Security service provider time is typically divided between the following tasks:

- Deployment time
- Initial configuration
- Tuning
- Upkeep
- Customer services

When the time spent on these tasks is reduced it directly and positively affects a security service provider’s revenue. After all, a large proportion of a managed security service provider costs are operational costs – the manpower needed to run the environment. Simple and monotonous operational tasks should be automated to free resources for use in places where human intelligence is really needed.



Deployment time is the time it takes to actually install a security-enforcing device and get it operational. As mentioned in the previous section, the Stonesoft Mass Security feature significantly reduces deployment time because it automates many of the installation phases. It also removes the need for IT-personnel to do the physical installation of security-enforcing devices.

Initial configuration covers all the tasks that are needed to create a new customer environment or add new security devices or services to the existing customer environment. With the Stonesoft MSSP solution, initial configuration time is reduced because the Stonesoft Management Center can create hundreds of firewall configurations at one go with the help of different configuration wizards and reusable templates. Many common elements can be shared with different domains while keeping the customers separated from each other. There are tools to automatically convert existing elements and security rules to a Stonesoft format in product replacement scenarios. Then elements can then be imported en masse to Stonesoft's centralized management environment.

One example of a replacement scenario is where two merged companies decide to outsource their security management to a managed security service provider. Both companies have their own fragmented internal and external IP address spaces. Normally it would take several days to input all servers, desktops and devices. With the Stonesoft MSSP solution, a simple Excel sheet with all the needed info can be created and imported into the Stonesoft Management Center in a few minutes.

Tuning tasks consist mainly of different kinds of customer change requests. The Stonesoft MSSP solution's "create once and use everywhere" mentality removes the need to create unnecessary copies of redundant information. Administrator workflows have been optimized so that they can do their daily tuning tasks with just a few mouse clicks. The user interface is the result of several years of usability studies that Stonesoft has conducted with our customers.

Customer services are either basic services or value-added services. Basic security services consist of providing support services and status reports to the customer. Value-added security services are more advanced services like providing additional visibility through a web portal or high availability in the customer environment. Value-added services are a great way for a security service provider to differentiate from the competition. The Stonesoft MSSP offering has many value-added services that provide additional revenue possibilities for the service provider.

One example of a value-added service is management of 3rd party log events and reporting. Stonesoft products can provide basic level security information event management (SIEM) services, meaning that a new managed security service provider does not have to spend a lot of money for a full-blown SIEM environment. Using the logs from Stonesoft products enables managed security service providers to get a situational overview of the whole environment – and therefore provide much better preventive maintenance and faster incident response for the customer than having the same information dispersed across several different monitoring systems. This visibility over 3rd party reports and logs can be provided to the customers as a value-added service.

Unique customer experience

A basic managed security service consists of running a security environment with very few customer changes and standard reporting. This is good for customers that are not very security conscious and have a simple and static security environment. Basic managed security services do not create a lot of margin for an MSSP because the competition is heavy and many companies are able to offer similar services. It is therefore important for managed security service providers to create value added services where the margins are better, there is less competition and there are several possibilities to differentiate from the rest of the competition.

Stonesoft provides several possibilities for value added services. All Stonesoft products are created with high availability in mind, enabling MSSPs to offer the following services to customers that require their systems to always be up and running:

- Firewall and IPS clustering
- Internet service provider clustering (patented feature)
- Global redundancy for the management server
- Additional log servers close to log creation points
- Load balancing for web services

Stonesoft has been doing high availability for the last 20 years, meaning the technology is mature and works in even the most demanding environments. For example, one way to lower managed security service provider fixed costs is to combine several low price network connections into one pipe instead of using an expensive MPLS (Multiprotocol Label Switching) pipe. Stonesoft's patented Internet Service Provider (ISP) clustering creates a high bandwidth and high availability Internet connection using several low cost connections. Internet Service Provider clustering is also scalable and allows a managed security service provider to mix and match several ISPs. It creates independence from ISPs and makes it possible to negotiate the lowest possible fees for Internet connections. Network outage in one single ISP does not affect the availability of customer connections because they are automatically load balanced to the remaining providers. You can get more information about ISP clustering at avpn.stonesoft.com.

Another interesting area for additional revenue is authentication services. Many companies would like to use cloud services but they are worried about putting user and password information in the hands of a cloud service provider. There have been several high-profile hacking cases where username and password information have been stolen from a cloud service provider. This poses a big security risk because many people use the same username and password across multiple services, giving hackers more possibilities to break into other systems. Stonesoft provides a way to keep the authentication data in the customer's hands and still use cloud services. This service is based on federated authentication and is a great value-added service for the managed security service customer who wants to use cloud services in a secure way. You can find more information at a2cloud.stonesoft.com.

The Stonesoft Web Portal is an easy way to provide value added services like:

- Access to reports, security policies and logs
- Localization support
- Look and feel customization to match different customers
- Highly granular user profiles and access rights
- Mobile device support

Even though customers are outsourcing their security management they still would like to have some control or at least good visibility over it. The Stonesoft Web Portal is a useful way to provide customers with additional visibility over their own managed security environment.

For example, a medium-sized MSSP was providing managed security services to car rental firms across the globe. They had to perform an external audit of their environment for each of these car rental companies every year. The audit normally took one week for each customer environment when external auditors came and collected all reports and went through all the security rules and audit logs. Audit time was reduced to two days when they started to use the Stonesoft Web Portal, which provided external auditors with direct read-only access to the customer reports, security policies and audit logs. The external auditors were also satisfied because they could do most of the work at their own desk and then just make brief site visit to check that everything else was ok.

The benefits included reduced costs for the managed security service provider because they saved three days of work for each audit. The rental car companies were satisfied because their audits went faster and costs were lower. Third party auditors were happy because they were able to perform audits from their own desk and the quality of the data was better because it came directly from the systems that they were auditing.

The Web Portal is a useful tool for a managed security service provider because it can be used to create several unique service levels for different customers. All changes can be done on the fly so the customer can start using new service levels immediately when they order it. You can find more information at mssp.stonesoft.com.

Cutting edge technology against Advanced Evasion Techniques

One issue that differentiates Stonesoft products from the competition is protection against Advanced Evasion Techniques (AET). An advanced evasion is able to make an exploit “invisible” to network security devices and therefore bypass them.

Stonesoft has the world’s leading AET testing laboratory and has not yet found any network security device that protects against advanced evasions. Stonesoft products, however, perform a special kind of traffic normalization which can detect and block AETs.

Stonesoft’s AET testing laboratory is continuously discovering new advanced evasions using a unique automated test lab environment. When a new working evasion is discovered Stonesoft builds protection against it. Updated protection is then delivered to all Stonesoft products automatically so that they will protect customer systems all over the world. Advanced evasions are a new dynamic threat towards network security and Stonesoft is in the best position to provide protection against it.

A new managed security service provider can use the protection against AETs service as a completely unique differentiator against the competition.

You can get more information about Advanced Evasion Techniques from www.antievation.com.

The economical choice

Stonesoft products provide a lucrative possibility to start a managed security service provider business for the following reasons:

- Low initial costs and low financial risks
- A business model that supports growth
- Low operational costs
- Short time to revenue
- Possibility to upsell new security services

Stonesoft products can be used on three different platforms: normal appliances, pure software products and virtual appliances (running on the VMware platform). Management of all these systems is identical, so managed security service providers can choose the best platform for each customer case.

Stonesoft has generated a business model that supports managed security service providers. It does not require heavy initial investments and reduces financial risk. The Stonesoft Management Center (the core of the system) is free at the beginning so that service providers can start their business with low investments and attract customers by offering a full service package.

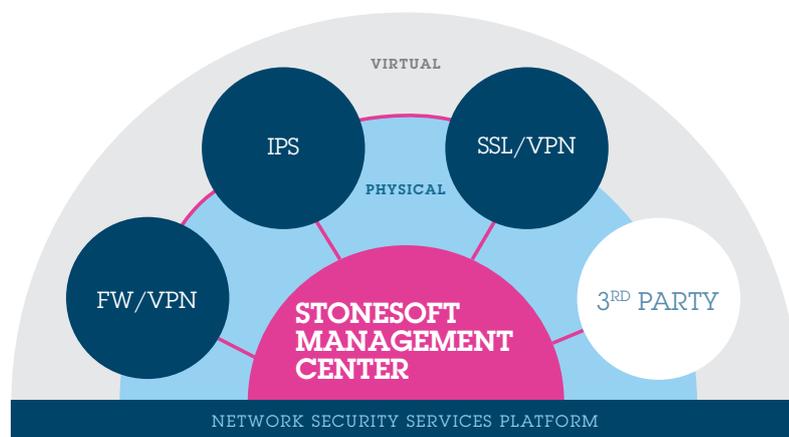
As the service provider grows, Stonesoft Management Center costs are based on active nodes. There are no pricing thresholds so you do not have to buy, for example, a 50 nodes license to get started.

Stonesoft products have been designed with low total cost of ownership (TCO) in mind. There are numerous features and functions that make the management of a large security environment easy and effortless. Many tedious, monotonous and simple tasks have been automated. All routine tasks can be scheduled and their results delivered automatically to customers.

Stonesoft has conducted numerous usability studies with different security system administrators to see how they perform daily routines. The studies showed that a graphical user interface and drag-and-drop tasks were the most efficient ways to manage the environment. All this data was used to make the workflow as smooth and effective as possible.

Stonesoft products reduce the possibility for human error and make any anomalies visible quickly. The human brain is very efficient at pattern matching and that shows when people are handling graphical information from a complex security system.

Network Security Services Platform



Because of the small initial investment and very low total cost of ownership, a starting managed security service provider will experience short time to revenue. Customers will experience excellent enterprise-level services and they have many options to enhance their service level.

Starting a managed security service gives many possibilities to create a unique offering that resonates well in their target customer segment. Different high availability, Web Portal, application control, security inspection, Web filtering, antispam, antivirus, report and log handling features and their customization possibilities offer numerous variations for additional revenue generation.

STONESOFT

Stonesoft Corporate

Itälahdenkatu 22 A
FI-00210 Helsinki
Finland
tel. +358 9 476 711
fax. +358 9 476 713 49

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338, USA
tel. +1 866 869 4075
fax. +1 770 6681 131

Copyright 2012 Stonesoft Corp. All rights reserved. Registered or unregistered trademarks in this document are property of their respective owners. The products described in this document are protected by one or more of U.S. patents and European patents: U.S. Patent No. 6,650,621, European Patents No. 1065844, 1289202, and may be protected by other U.S. patents, foreign patents, or pending applications. Specifications subject to change without notice.