

# Technology Infrastructure

## Butler Group Subscription Services

# Security and Services

## TECHNOLOGY AUDIT

### Symantec Corporation

#### Managed Security Service (MSS)

**Abstract** *Managed Security Service (MSS) from Symantec provides mid- and large-sized organisations with an IT security monitoring service. Organisations with large networks often find it a very difficult task to manage the various point solutions that they have for IT security. Also, with increasing regulatory and legislative pressures, improving IT security is often necessary for compliance. MSS provides an ongoing assessment of IT security risk for customers, providing advice on the threat and vulnerability situation in real time. The monitoring is agent based, collecting and assessing the information from the devices on which the agent is installed. Currently MSS can monitor more than 35 products from various vendors, and Butler Group looks forward to seeing an increase in the number of compatible products. The service is very useful for mid- to large-sized organisations that have not yet made their decisions on whether to build or buy their security management framework, as MSS provides a good interim solution.*

#### KEY FINDINGS

- |                                                                                                                                                                                                                              |                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>✓ Rapid assessment of IT security risk for customers.</li> <li>✓ No scalability issues – new devices can be added as and when required.</li> <li>i Agent-based monitoring.</li> </ul> | <ul style="list-style-type: none"> <li>✓ Can feed device criticality into risk assessment.</li> <li>i Currently 35 products are included for monitoring.</li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Key:** ✓ Product Strength ✗ Product Weakness i Point of Information

#### LOOK AHEAD

Symantec is a company with a strong name in IT security solutions, and in Butler Group's opinion it can deliver a well-marketed managed security service to its potential target market, and MSS is expected to continue its success in Europe that it has experienced in the US.

## ► FUNCTIONALITY

All sizes of organisation are struggling with the ability to manage the many point security solutions that they have installed across their networks. Events are reported from all of these solutions on a continuous basis, and it can be difficult to spot the critical alerts from those that are purely informational. Add to this the fact that the threats and vulnerabilities change on an alarmingly regular basis, and managing security events can become extremely problematic for all sizes of organisation.

Many organisations today are also facing increasing legislative and regulatory pressures. In Butler Group's opinion the requirement for information security includes the mechanisms and technologies in place to prevent information from being changed, damaged, or deleted without appropriate reason. Thus, compliance is a big driver for organisations in wanting to improve their IT security.

### Service Delivered

Symantec has a Managed Security Services (MSS) offering, which was originally delivered to support other activities within Symantec. The solution is, however, almost vendor-agnostic, in that around 82% of the products that it monitors are from non-Symantec sources.

Using MSS individual customer organisations have access to 'trusted advisors' at Symantec who will monitor their devices and notify them of any relevant risks that need to be addressed. Thus, rather than actively managing security for the customer, MSS gives the customer the ability for someone else to monitor their current IT security point solutions and then advise them of what needs to be done to manage their security more effectively. Symantec can also deliver a management service. MSS is an agent-based service – agents are installed (remotely) on all devices or single data collection points to be monitored in a customer's network.

In delivering MSS Symantec has 'The 5 C's', shown in the following diagram:

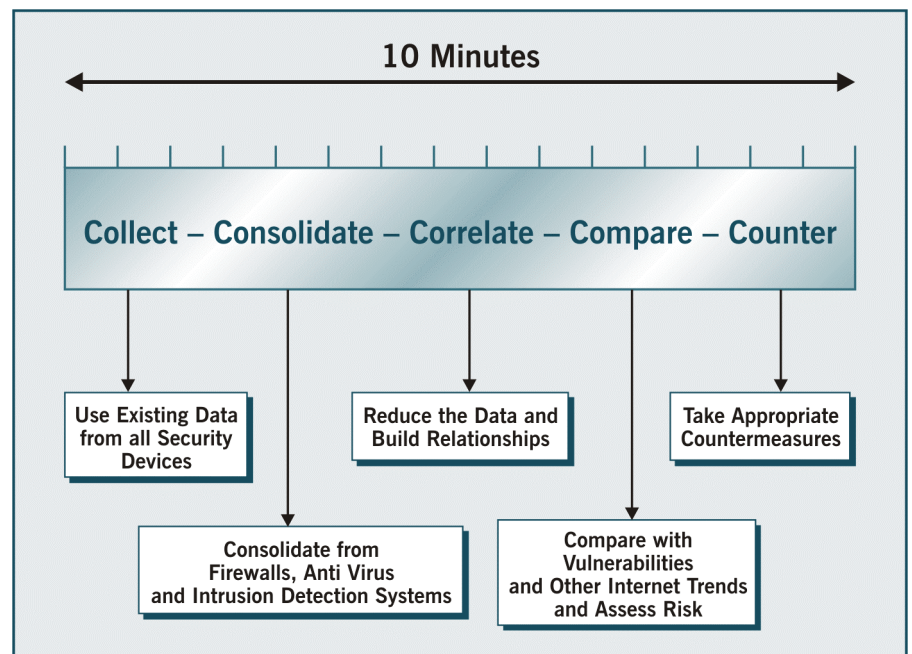


Figure 1: The 5 C's – Customer Measure (source: Symantec)

In explanation of Figure 1, over a typical period of ten minutes, the following events take place for all MSS customers:

1. **Collect:** Data is collected from all of the security devices on which there are agents for each customer. Once captured by the monitored device, the data is encrypted before being sent on to MSS.
2. **Consolidate:** The collected data is consolidated from multiple security sources, into a single data repository. All data is normalised and stored in the same format.
3. **Correlate:** The large volumes of data collected and consolidated is then reduced down to understand what the threats are. Thousands of queries are run against this data in order to build up a picture of the situation.
4. **Compare:** The threats that have been identified are then compared with the vulnerabilities that MSS knows that the customer has. Symantec real-time analysts individually assess the risk of these vulnerabilities being breached.
5. **Counter:** Suggested countermeasures are sent to the customer to mitigate the risks. These could include patching, anti-virus protection, blocking ports, etc.

MSS delivers security event information, including the suggested countermeasures, to the customer in prioritised form primarily through a portal. This is backed up by other escalation procedures that Symantec holds for that individual customer, including telephone, automated message, and e-mail. Symantec assigns dedicated staff to customers at the appropriate Symantec Security Operations Centre (SOC), but can also provide on-site staff through its professional services or partner organisations if required.

Pre-defined, custom reports are available via the portal for customers to produce on their 'currently-held' events. Symantec also produces monthly reports for customers. It is important to be aware that the portal is two-way – as well as information being pushed to customers, customers can also contact MSS.

Customers can choose from the following range of MSS offerings:

- Global notification of emerging threats.
- Managed virus protection service.
- Managed Internet vulnerability service.
- Managed and monitored firewall service.
- Managed and monitored Intrusion Detection System (IDS) service (host IDS and network IDS).
- Managed and monitored integrated security appliance service.
- Managed policy compliance service.
- Deepsight threat management service.
- Deepsight alerting service.

Overall Symantec monitors around 20,000 firewall and IDS sensors, plus 150 million anti-virus desktops reporting on virus threats and anti-spam intelligence. The information that is gathered from the various customer devices is put into the intelligence database.

## Service Analysis

IT security is a moving target. The threats change almost on a daily basis, but one must also remember that the way in which an organisation's IT assets are deployed also changes quite regularly. The ethos of the MSS solution is that by operating the '5 C's' with an alert service level of ten minutes as described previously, Symantec is able to keep track of this moving target for its customers. In Butler Group's opinion this is not something that customers are necessarily able to do themselves, and although there is still a window of vulnerability (i.e. up to 9 minutes 59 seconds), this risk is much lower than not having IT security monitored in this way. There will always be the issue of threat versus risk, and it is possible for organisations to over-insure themselves in terms of IT security, thus in our opinion MSS presents only a small window of vulnerability risk that cannot realistically be improved upon.

As MSS is primarily a monitoring service, the customer organisation needs to have a thorough understanding of its IT security set up and also have the management infrastructure to be able to respond appropriately and in a timely manner to threats and events that are notified by the service. Butler Group would always recommend that when using an outsourced service the customer retains at least some level of expertise in-house. Even if a customer selects the managed service it is still important to retain in-house expertise, although the SOC should also be seen as an extension of a customer's security team.

Essentially the SOC obtains the information about the customer's systems and the threats that are in the wild, analyses and validates those threats, and then raises prioritised incidents with the customer. The customer receives all events through the portal, but the higher priority ones are escalated more rapidly, as one might expect. Every event is prioritised as follows:

- Informational.
- Warning.
- Critical.
- Emergency.

The customer can manage the risk, in that the importance of particular devices can be defined by the customer. For example, Device A being monitored by MSS might be deemed 'crucial' by the customer, and this can be fed into the threat rating from MSS for that customer. In Butler Group's opinion this ability to take the customer's prioritisation into consideration when delivering the threat analysis is another strength of the service.

The portal also lists the latest threats on the Internet, with a rating of one (low) to four (critical). This is a general picture for all users of MSS, and is not tailored specifically to individual customers.

Alongside MSS, Symantec produces the Symantec Threat Report, every six months, which reviews the threats and vulnerabilities that all of Symantec's customers have faced. All customers have access to this information on a continuous basis through the portal described earlier, but this Report is used by many organisations to obtain a view of IT security from the Symantec SOC in the delivery of MSS during the period of the Report.

A huge volume of information goes not only into the production of the Symantec Threat Report, but also in terms of the number of events that are scanned. This has led to the development of the Early Threat Notification system, the process for which is shown in the following diagram:



**Figure 2: Symantec Early Threat Notification Process** (source: Symantec)

In delivering this system Symantec sets a baseline of activity for a particular area of IT security using the information it has collated from customers. If the activity in that area increases an alert is provided, and the Symantec MSS advisors can then begin to build a profile for the customer and recommend what can be done to mitigate the threat.

In terms of scalability there is no issue with Symantec's MSS – further agents are simply added to new devices when they need to go into the service. In Butler Group's opinion this is a strength over other 'black-box'-based MSS solutions.

Analytics and reporting are available to the customer on a monthly basis to compare the customer's situation to an average for specific verticals. This is fed back via Symantec's Threat Management System. According to Symantec after using MSS for between seven and nine months the number of companies with severe events is reduced to 30%, from 100% in months one to three.

### Service Emphasis

In order to fully appreciate the MSS offering organisations need to understand the complete picture of IT security. Monitoring devices across a large network can be an almost impossible task, requiring a large team dedicated to it. Symantec's MSS solution is aimed at organisations that need to protect critical information assets, and must prove monitoring services to conform to data privacy and industry-specific legislation (i.e. compliance).

## ► SERVICE DEPLOYMENT

As MSS is a service, customer involvement in setting up usage of the service is minimal. As stated previously, a remotely installed agent is used for the devices, and Symantec or the customer can undertake this installation. If the customer elects to do this, Symantec provides Rimporter, which is Symantec patented technology that delivers an encrypted file for the customer to install. This file must be stored in a secure location on the server.

The service can generally be up and running within 30 days of being ordered, including the remote installation of agents on all devices that are to be monitored. It is important that escalation procedures are defined at this stage so that when events are reported, they are acted upon as appropriate.

Symantec recommends that the customer organisation has a thorough understanding of its own IT environment, to ensure the recommendations that are derived from the monitoring service can be acted upon (unless the Symantec management service is used).

A security point of contact is required by Symantec who can respond to alerts – this would typically be the IT manager or security officer. In this regard Symantec encourages its customers to have a 'Response Team' that is able to respond directly to events or alerts that are notified via the service. The building of this team can be undertaken directly by the customer or in association with Symantec's professional services option. There is also a four-day course for customers on how to build a security response team, and this can be tailored to MSS if required.

When first deploying MSS, the Symantec Service Operations Centre (SOC) undertakes a vulnerability scan against a customer's network. This delivers information on what the customer has in terms of IT security devices and how these devices are configured, and in this way the SOC can understand the customer's assets and any potential vulnerabilities.

There are five SOCs worldwide, located in the UK, Germany, Japan, Australia, and the US. These SOCs provide a 24x7 service to Symantec's MSS customers.

The following Service Level Agreements (SLAs) are available:

- **10 minutes** – threat identification.
- **30 minutes** – identification of device availability.
- **60 minutes** – emergency changes are notified/made.
- **180 minutes** – standard changes are notified/made.

If customers require alternative SLAs then they are available and negotiable.

## ► SERVICE STRATEGY

MSS is a horizontal solution, although Symantec is focused on its use by mid-market and large-sized enterprises in the financial, power and energy, health, and manufacturing sectors. Around 32% of MSS customers are from the financial services sector. The Small to Medium-sized Enterprise (SME) market place is not currently targeted as MSS is likely to be too costly; however, this is not ruled out as a possible future development for Symantec.

The route to market is through direct and indirect sales, and Symantec has a fairly comprehensive channel strategy. The partners selling MSS are classed as Solution, Services, and reseller partners.

In terms of EMEA activity, Symantec has active MSS service partnerships in many EMEA countries including the UK, Germany, Italy, France, Spain, Turkey, Nordics, The Netherlands, South Africa, and the Middle East.

Symantec has recognised that the managed security market place has not been particularly successful for other organisations, but points to the fact that Symantec is a global company with a very robust sales and marketing capability that should help it achieve success. It also has the ability to continue investing in the service, which will provide customers with the 'comfort factor'. In Butler Group's opinion Symantec can deliver a well-marketed managed security service to its potential target market, and it stands a good chance of continuing its success.

Customers sign up to the service over a period of years, and the average contract length is two years. The cost of the service is entirely dependent upon the customer's infrastructure and requirements, but it can be said that the usual benefits of a service apply, e.g. low-level entry costs and rapid delivery. In terms of Return On Investment (ROI), Symantec states that customers see approximately a 70% reduction in the number of 'severe' incidents that impact their network in the first 6-9 months of service.

A new release of the portal is provided approximately every quarter. Additionally, Symantec is looking to increase the range of devices and products that it covers under MSS. In Butler Group's opinion an increase in the number of solutions supported within the service would be a welcome enhancement.

Symantec believes that organisations are moving away from solely point solutions for IT security, and Butler Group concurs with that opinion. Customers are deciding between the 'build' approach (refresh technology and manage point solutions), the 'buy' approach (end-to-end IT security with a single vendor), or 'consolidate' (through a service provider). By using MSS for two or three years organisations are given the opportunity to decide on 'build-versus-buy' and simultaneously have their IT security monitored effectively.

## ► COMPANY PROFILE

Symantec was founded in 1982, and is headquartered in Cupertino, California, USA. Employing over 5,000 staff across 36 countries, the company has offices in North America, South America, Europe, and Asia-Pacific, including: Argentina, Australia, Brazil, Canada, China, France, Germany, India, Italy, Japan, Russia, South Africa, Spain, UAE, and the UK.

MSS has around 60 staff worldwide dedicated to R&D. Global services and support contains approximately 2,500 staff worldwide.

Symantec is a publicly listed company (NASDAQ:SYMC), and has a corporate mission statement to become the trusted security partner for individuals and enterprises around the world. Currently Symantec provides comprehensive Internet security products, solutions, and services for more than 125 million users worldwide. These range from the largest corporate enterprises, service providers, government agencies, and higher education institutions, to small business users and individuals.

Reported revenues for the last three fiscal years are as follows:

March year-end	2004 (US\$ million)	2003 (US\$ million)	2002 (US\$ million)
Revenues	1,870	1,407	1,071

## ► SUMMARY

Reliable managed security services are few and far between, and the MSS offering from Symantec gives customer organisations the use of an established name in the IT security arena to monitor their network. The '5 C's' is a good way of delivering a complete circle in this monitoring and advice service, and allowing the customer to feed their priorities into the notification system helps tailor the solution.

MSS will be useful for mid- to large-sized organisations that have not yet made their decisions on whether to build or buy their security management framework, as it provides a good interim solution. The expected reduction in the number of severe incidents is not only positive in terms of the corresponding reduction in disruption for dealing with these incidents, but also demonstrates an improvement from a compliance perspective.

## ► CONTACT DETAILS

### **Symantec Corporation**

World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino  
CA 95014  
USA

Tel: +1 408 517 8000

[www.symantec.com](http://www.symantec.com)

### **Symantec United Kingdom Ltd.**

Hines Meadow  
St. Cloud Way  
Maidenhead  
Berkshire, SL6 8XB  
UK

Tel: +44 (0)1628 592222

[www.symantec.co.uk](http://www.symantec.co.uk)

### **Important Notice:**

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.

### **About Butler Group:**

Butler Group is the premier European provider of Information Technology research, analysis, and advice. Founded in 1990 by Martin Butler, the Company is respected throughout the business world for the impartiality and incisiveness of its research and opinion. Butler Group provides a comprehensive portfolio of Research, Events, and Subscription Services, catering for the specialised needs of all levels of executive, from IT professionals to senior managers and board directors.