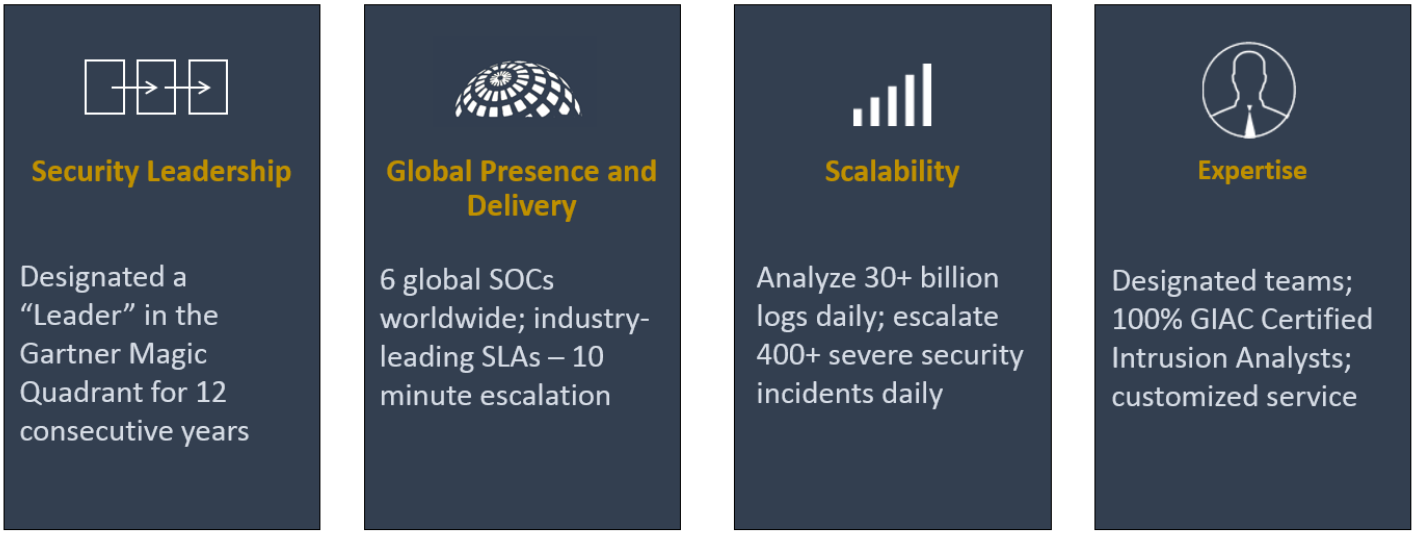
Symantec™ Managed Security Services

Harness the largest human network of cyber experts armed with advanced analytics to defeat attacks

Data Sheet: Symantec Cyber Security Services



Escalating threats have made cyber security a key priority for organizations of every size and across every industry sector. Companies lack the resources, skillsets, expertise, and time to address the growing sophistication of threats and attackers. Symantec has the largest human network of cyber experts armed with advanced analytics to extend an organization's security team and help make timely and proactive information security decisions.

Symantec Managed Security Services

Through our Managed Security Services (MSS), companies receive 24 x 7 x 365 security monitoring and real-time security analytics, equipping them with the strategic insights needed to prioritize and respond to the most critical incidents and build strategies to protect the assets, reputations and viability of their organizations.

Symantec MSS is a comprehensive, advanced threat detection service that is built on a close partnership between our MSS analyst teams and each customer. Together, they build the security monitoring program that is tailored to your organization's security issues and business goals.

Our Teams

MSS leverages a high-touch, delivery model that is unique to the industry. It is centered on the high-value goals and targets that are critical to your business. This approach is executed through our designated teams including a service manager, principal analyst, incident handlers, and engineers who become an extension of your security operation. They learn your network, understand your environment, your industry, your business goals, and your processes. Based on this knowledge, they focus on the issues that are most important to you. They complement the infrastructure you already have in place and help you better manage your security posture before, during, and after a cyberattack.

Our teams are a group of more than 1,000 cyber security professionals. They gather intelligence on malicious activity and threat actors, implement custom detection, and provide individualized counsel on how to address specific threats in your

organization. They also work with you to help you better understand patterns and trends in your company's threat activity. Their efforts support your security planning process, helping to close gaps, and strengthen your security profile.

They are analysts, scientists, researchers, and practitioners, dedicated to every stage of the threat lifecycle. They are 100% SANS-certified intrusion analysts (GCIA), incident handlers (GCIH), Offensive Security Certified Professionals (SDCP), and Security Systems Professionals (CISSP), among other certification security-certified professionals. In addition, they undergo comprehensive Symantec incident-handling training and assessments prior to beginning work with customers.

Our Global Intelligence Network

Symantec MSS has unique visibility into the global threat landscape through its Global Intelligence Network (GIN), a **massive archive of security data of more than 10 trillion security events per year worldwide**. The GIN offers visibility into empirical, real-world customer data from enterprises and consumers, Symantec.cloud, Web Gateway metadata, other third-party sources as well as data from hacker forums, automated monitoring of adversaries and vendors. The GIN also receives raw threat datafeeds from Symantec's extensive network of end-point sensors.

Our Analytics Engines

Big data available from our GIN are correlated with your log data, identifying signs of compromise and providing a high level of detection and prioritization of threats, based on frequency and severity of risk to your organization. Our analysts further review the outputs from this analysis for relevancy and context and bring only the most critical incidents to your attention. Their efforts are further informed by our adversary intelligence reports (MATI), which are prepared by a separate group of highly specialized Symantec analysts who are focused on deeply researching motivations and behaviors of malicious actors.

Our Log Collection

MSS provides 360-degree visibility across all of your monitored security devices, with a collection platform and analytic engines that process large volumes of log traffic – 30 billion logs daily -- looking for patterns relating to malicious activity. While other vendors filter their clients' logs to exclude authorized users and activities from their analyses, MSS purposefully analyzes ALL logs. Here's the reason: Authorized users and activities make up 99 percent of logs, and those logs can contain valuable information that aid in detecting malicious activity. For example, malware most often attempts to behave like an authorized user/activity to prevent identification. Having historic information on true authorized users can help to identify anomalous behavior.

Our log collection platform assists with compliance reporting and can lighten the load associated with annual audit preparation. Through our secure web portal, customers have complete visibility into threat activity, trouble tickets and other published notifications. They also can do ad hoc queries or conduct a 90-day retrospective analysis of their log traffic. Symantec uses best practices to securely manage information and meets regulatory and legislative requirements in accordance with ISO 27001/2, plus national and international law.

Symantec MSS is a PCI-compliant Managed Services Provider. This includes securing customer log data and retaining those logs for the online and offline durations required by the PCI DSS. Additionally, Symantec may manage security devices on behalf of customers, such as NIDS, which may help govern the security of the customer's PCI environment. Upon request, Symantec MSS will provide a copy of its PCI Attestation of Compliance (AOC) report.

How Managed Security Services Can Help

Symantec MSS works with you to understand your business goals and priorities. Our delivery model is personalized and focused so you can make progress toward the goals that are at the top of your agenda. Symantec MSS helps you to:

Reduce Operational Costs – MSS can support your operational planning goals with flexible, scalable solutions that grow with you over time. Our Enterprise-wide pricing model enables predictable budgeting for measurable service level agreements. For a fixed price, you can move, add or change security devices at will, without contract changes. You also benefit from the significant investment Symantec has made in its infrastructure and tools which accelerate deployment of the service within hours. In the meantime, you eliminate the on-going, high cost of hiring, training, and retaining security professionals.

Extend your Security Team – With MSS, you access highly-skilled, GIAC-certified security professionals, automated monitoring and correlation tools, 24 x 7 x 375. You are able to free up staff from this time-consuming, error-prone effort and can redeploy your security staff to more strategic priorities. Meanwhile, MSS analysts, who are informed by Symantec's GIN, ensure your staff has the information it needs to respond quickly to emerging threats.

Accelerate Detection & Response – With access to trillions of MSS customer logs annually, advanced analytics and retroactive log analysis, as well as insights from the Symantec GIN and DeepSight Intelligence, MSS can help you to detect advanced threats faster and to respond to them more quickly.

Report on Compliance – With MSS you can demonstrate the adequate deployment of your security controls. MSS assists with compliance reporting, helping to reduce annual audit preparation effort. Through a secure, easy-to-navigate Web portal, you can access to all security incidents and events tracked throughout the year. You can take advantage of complete visibility into threat activity, trouble tickets, and other published notifications, as well as a monthly report with events and incidents analyses along with the actions taken. With these resources, in addition to our pre-built compliance templates, your compliance process is streamlined and simplified.

Retain Security Logs and Monitor Devices -- MSS offers monitoring and log retention for 90 days -- not only for network devices but also for servers, endpoints, and other IT assets. With this visibility, Symantec provides unique insight across your environment. This is possible because every alert passes through thorough human inspection. MSS analysts apply their deep expertise to the threats that are escalated and help eliminate false positives and add context based on your business and your industry.

Leverage a Fully Integrated Solution

A successful cybersecurity program requires a comprehensive strategy and integration across technology and people. Each offering in Symantec's Cyber Security Services portfolio—**Managed Security Services** for advanced threat monitoring; **DeepSight™ Intelligence** for actionable technical and strategic threat intelligence; **Incident Response** for fast containment and eradication of a threat; and **Cyber Skills Development** for strengthening an entire organization's ability to recognize and prevent advanced attacks—is designed to work together and improve the speed and effectiveness of a security program.

More Information

Visit our website

go.symantec.com/mss

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

21042033-5 05/16