Overview
Symantec™ Cyber Security Services: Managed Security Services minimize the potential business impact of increasingly sophisticated and targeted attacks by reducing the time it takes to detect, assess and respond to security incidents.

MSS provides proven security expertise, log retention, and real-time monitoring of network security devices and endpoint protection solutions. Partnering with Symantec—an industry leader in managed security services for over twelve years—you can build on existing investments in security technologies to create an effective, scalable information security program to improve your security posture.

Leverage Global Threat Intelligence
MSS integrates threat intelligence from Symantec’s industry leading Global Intelligence Network (GIN) to provide unparalleled visibility of the evolving threat landscape to identify and block new and emerging threats. With more than 64.6 million sensors monitoring worldwide attack activity, the GIN provides timely, relevant, actionable intelligence about emerging threats, threat sources and vulnerabilities.

Actionable alerts, prioritized by business risk
Faced with a continuous deluge of security log and alert data, it can be difficult to cut through the noise to focus on the threats that matter most to your organization. MSS helps assess the business impact of threats by consolidating log and alert data from across your enterprise, then incorporating business context data such as asset value, organization, system function, and compliance restrictions to provide a prioritized list of actionable security incidents.

Security experts to protect your enterprise
Detecting known and emerging threats not only requires advanced technology, it also requires highly specialized security expertise to decipher complex attack patterns associated with malicious activity. Symantec offers quick time-to-value by providing in-region GIAC certified analysts who deeply engage with your team to understand your environment and internal processes as well as provide guidance regarding incident response. Your local team is backed by over 1000 security analysts and research professionals in five Security Operations Centers and 11 Security Response Centers around the world.

Device Classes Monitored
- Behavioral Analysis Sensor
- Data Loss Prevention
- Endpoint Protection
- Host Intrusion Detection/Protection
- Network Firewall
- Network Intrusion Detection/Protection
- Operating System
- Router/Switch
- Unified Threat Management System
- VPN Concentrator
- Web Application Firewall
- Web Proxy

Improved threat visibility with "edge to endpoint" coverage
Your IT environment is continually evolving with new devices and applications— and each new technology represents a separate avenue of attack. Our comprehensive “edge to endpoint” approach identifies and correlates threats for not only network devices, but also includes servers, endpoints, and other IT assets. This enterprise-wide perspective gives us unique insight into your network and allows us to quickly identify emerging threats.
Flexible, Scalable Security Monitoring
Whether you're just beginning to identify requirements or are outsourcing security monitoring for a multi-national organization, Symantec Managed Security Services offer the scalability needed to meet your current requirements—and grow with your security program over time.

Symantec offers two pricing models:

- Our device-based option provides the flexibility to mix-and-match device monitoring to meet your initial requirements, then extend to additional technologies as your security program evolves.
- Our enterprise-wide option is based on enterprise size to help ensure predictable, fixed costs.

We also provide three levels of service to help ensure the right solution for your needs.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise-wide support for the collection, monitoring, and storage of logs</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Reporting to provide documentation for compliance</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>24x7 coverage from global network SOCs</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Real-time monitoring of security event data</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Access to GIAC-certified analysts</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Integration of Global Intelligence Network (GIN) data in security analysis</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Anomalous traffic detection</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Advanced threat protection</td>
<td>•</td>
<td></td>
<td>•</td>
</tr>
</tbody>
</table>

Symantec Hosted Log Retention

Symantec Hosted Log Retention Service provides enterprise-wide log collection, storage, reporting, and querying delivered through a hosted, resilient, and secure environment. Features include:

- Enterprise-wide log collection.
- Hosted log storage in a secure and highly available facility.
- Log collection and retention reporting to help support regulatory compliance requirements.
- Association of logs with security incidents to provide supporting context for incident analysis.
- In-the-cloud online storage for 3 months, offline storage for one year.
- A secure web portal to enable flexible and real-time online log queries.

Symantec Essential Security Monitoring

Symantec Essential Security Monitoring Service provides enterprise-wide security analysis to identify threats. It includes all the features of Log Retention Service, plus:

- Real-time security incident monitoring to detect threats and enable an effective response.
- Association of asset information with incident details to provide context and enable prioritized response.
- Analysis incorporates Symantec™ Global Intelligence Network threat intelligence to identify new and emerging threats.
- Association of asset information with incident details to provide context and enable prioritized response.
- Round the clock coverage from a global network of Symantec SOCs.
- Access to GIAC-certified security analysts to assist with incident remediation.
- A single view of all incidents and reports through a secure web portal.
- Security incident reporting to support regulatory compliance requirements.
- Anomalous traffic detection utilizes powerful data mining and statistical analysis to identify hard-to-find malicious traffic.

Symantec Advanced Threat Protection

Symantec Advanced Security Monitoring Service provides enterprise-wide, intelligence-driven security analysis to identify known and emerging threats to critical infrastructure. It works seamlessly with Hosted Log Retention and includes all the features of Essential Security Monitoring, plus:

- Advanced Threat Protection to automatically correlate network and endpoint security detections with external threat intelligence to detect, assess and respond to unknown and zero day malware.
Summary

Security Monitoring Services reduces overall security and business risk through real-time log management and security monitoring at a predictable cost structure that facilitates operational planning. With our unique “edge to endpoint” coverage to improve your security visibility, our enterprise-wide pricing model to easily adjust to changes in your infrastructure, and our flexible mix and match service portfolio, you can design a security monitoring solution to meet both your security and financial goals. As new threats emerge, you can be confident you are protected with Symantec Managed Security Services.

Complementary Services:

Symantec™ Cyber Security: MSS-Advanced Threat Protection provides bi-directional integration between endpoint security and network security vendors enabling users to rapidly and effectively contain, investigate and remediate unknown and zero day attacks that evade traditional security technologies.

Symantec™ Cyber Security: Intrusion Detection/Prevention Solution with Sourcefire® provides a complete, managed IDP solution combining both hardware and software, fully supported by Symantec Managed Security Services.

Symantec™ Cyber Security: DeepSight™ Intelligence employs one of the industry’s largest threat collection networks to deliver a comprehensive range of timely threat intelligence through a customizable portal or datafeeds, enabling proactive actions and effective incident response. DeepSight™ covers topics including threat actors, tools, techniques, and processes, campaigns, and vulnerabilities, and the managed adversary and threat intelligence delivers insight into the actions of actors, enabling focus on threats of the greatest importance.

Symantec™ Cyber Security: Incident Response provides on-site investigation support to help organizations mitigate the impact of an attack or outbreak and restore business as usual. Symantec draws from deep skills and years of experience to help you resolve incidents, return to normal operations, and prevent incident recurrence while minimizing the impact on your organization.

For More Information:

Visit our website
http://enterprise.symantec.com
http://go.symantec.com/mss

To speak with a Product Specialist in the U.S.
Call toll-free 1 (800) 466-5875

To speak with a Product Specialist outside the U.S.
For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

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