SOLUTION BRIEF

Symantec Managed Security Services

Harness the most experienced human network of cyber experts armed with big data analytics and tools to detect and respond to advanced on-premises and cloud-based attacks.

Symantec™

Introduction

Symantec™ Managed Security Services (MSS) provides round-the-clock security monitoring powered by big data analytics, equipping you with the strategic insights you need to prioritize and respond to critical incidents—as well as build the strategies required to protect your organization's assets, reputation, and viability.

Symantec MSS is a comprehensive, advanced threat detection service that partners closely with you to tailor a security monitoring program to address your organization's specific security issues and business goals.

Symantec's global team of experts

MSS executes its high-touch delivery model through a designated team (including a service manager, onboarding personnel, principal analysts, incident handlers, and engineers). Teams are based on your industry and geography to become an extension of your security operations, enhancing your infrastructure already in place.

To better predict, detect, and respond to cyber threats and attacks, Symantec's designated team learns your network, environment, business goals, and processes, and focuses on the issues most important to your organization. They gather intelligence on malicious activity and threat actors, implement custom detection, and advise you on how to address specific threats to your organization. They make sure you understand threat patterns and trends and support your security planning process to close gaps and strengthen your security profile.

MSS selects your designated team from a group of more than 1,000 global cyber security professionals (analysts, scientists, and researchers dedicated to every stage of the threat lifecycle) with extensive security training and experience. These experts have achieved numerous industry certifications including Global Information Assurance Certification (GIAC) for intrusion analysis; GIAC Certified Incident Handler (GCIH) for incident handling; and Certified Information Systems Security Professional (CISSP) for security systems operation. Prior to working with customers, analysts also undergo Symantec incident-handling training and assessment.

The power of intelligence

The Symantec Global Intelligence Network (GIN), the world's largest civilian threat intelligence database, gives Symantec MSS unique visibility into the global threat landscape. The Symantec GIN compiles empirical, real-world customer (enterprise and consumer) data from Symantec's extensive network of endpoint sensors, as well as from other Symantec solutions, and from third-party sources including hacker forums and automated monitoring.

Symantec correlates big data from our global intelligence network and DeepSight™ Intelligence (technical and adversary threat intelligence) with your log data to identify signs of compromise, enabling MSS to detect threats and prioritize them based on frequency and risk to your organization. MSS analysts review this analytical output, along with intelligence from the DeepSight Managed Adversary Threat

Detect the unknown with MSS analytics

- Go beyond signature logs and rule creation.
- Detect signatureless files.
- Identify anomalies, trends, and associations.
- Analyze logs retroactively.

Intelligence (MATI) research group, to determine the motivations and behaviors of malicious actors and campaigns, and to identify emerging global trends and critical incidents that require your attention.

MSS analytics engines

MSS is vendor agnostic, providing 360-degree visibility across all your monitored security devices. Our security operations center (SOC) technology platform and analytic engines process 160+ billion logs each day, looking for patterns of malicious activity.

While other vendors filter their clients' logs—excluding authorized users and activities from their analyses—MSS purposefully analyzes all logs. Logs of authorized usage and activities comprise 99 percent of all logs, and they contain valuable information that aid in detecting malicious activity. Having this additional data is extremely helpful to SOC analysts because most malware tries to avoid detection by behaving like an authorized user/activity. Historic information on true authorized users is one way that MSS identifies anomalous behavior.

MSS compliance support

The Symantec SOC technology platform supports your compliance reporting and makes audit preparation easier. Our secure web portal gives you complete visibility into threat activity, trouble tickets, and other published notifications. Use it to perform ad hoc queries and conduct 90-day retrospective analyses of your log traffic.

Symantec uses best practices to securely manage your information, and we meet regulatory and legislative requirements in accordance with ISO 27001/2, SOC1, and national and international law.

Symantec MSS is a Payment Card Industry (PCI)-compliant managed services provider. We secure customer log data and retain it as required by the PCI Data Security Standard. Symantec also manages security devices (such as your network intrusion detection systems), which improves PCI environment security.

Symantec is committed to safeguarding your organization's personal data and privacy. Naturally, we consider General Data Protection Regulation (GDPR) readiness a critical initiative. We've strengthened and enhanced our privacy practices for European Union nations and across the globe; we're committed to providing GDPR-compatible products and services; and we are dedicated to transparency every step of the way.

Symantec Integrated Cyber Defense

Symantec's Integrated Cyber Defense (ICD) Platform unifies products, services, and partners to drive down the cost and complexity of cyber security, while protecting enterprises against sophisticated threats. ICD combines information protection, threat protection, identity management, compliance and other advanced services, powered by shared intelligence and automation across endpoints, networks, applications, and clouds.

Symantec MSS is harnessing the power of the ICD Platform to provide more value, including to better protect against targeted attacks on premises and in the cloud.

Improve Threat Detection Capabilities

Consider your team's ability to:

Hunt for emerging IoCs and sophisticated adversary TTPs.

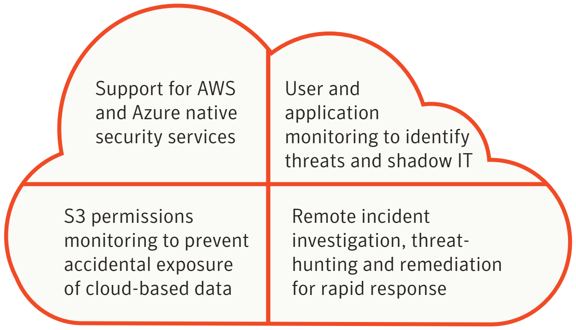
Investigate suspicious threat activity across on-premises and cloud endpoints.

Verify attacks and quickly remediate compromised endpoints 24 hours a day.

Maximize the value of endpoint detection and response tools.

Managed Cloud Defense

Cloud monitoring for full SaaS and IaaS security protection


Support for AWS and Azure native security services
User and application monitoring to identify threats and shadow IT
S3 permissions monitoring to prevent accidental exposure of cloud-based data
Remote incident investigation, threat-hunting and remediation for rapid response

MSS cloud capabilities

Are you moving business-critical assets to the cloud? Symantec Managed Cloud Defense ensures you maintain a consistent and seamless security posture across multiple clouds with the broadest cloud security monitoring services available. Threat monitoring across IaaS and SaaS infrastructures, coupled with dynamic machine learning analytics and threat intelligence correlation, provide a single view into suspicious and confirmed threat activity across your cloud and on-premises environments. Our cloud-trained cyber warriors, available around-the-clock to work with you individually, use this information to enable your SOC teams to detect and respond to cloud-based threats.

Key Managed Cloud Defense features include:

- **Monitoring of cloud platforms via native integrations with Amazon Web Services and Microsoft Azure**—For increased cloud security
- **Cloud user and application monitoring**—For discovering threats and shadow IT
- **Amazon Simple Storage Service (S3) permission monitoring**—For protecting critical cloud-based data storage
- **Remote incident investigation, pre-authorized remediation, and managed threat hunting**—For rapid response

Managed Endpoint Detection and Response capabilities

Even as new tools reduce the time between threat detection and response, organizations with limited in-house skillsets, resources, and time still find it difficult to address threats on their own. Living-off-the-land threats are particularly challenging because they linger in the environment and may go undiscovered by traditional security technologies.

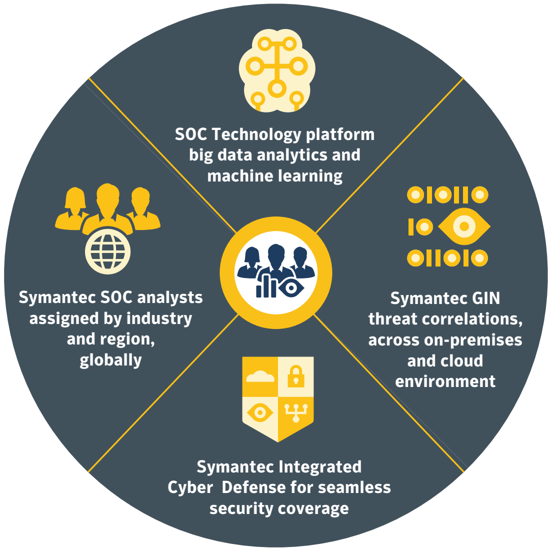
Symantec Managed Endpoint Detection and Response addresses these challenges by arming your dedicated team of Symantec MSS analysts with Symantec Endpoint Detection and Response, a tool that enables them to look beyond security logs that were pushed to the MSS SOC technology platform.

Key Managed Endpoint Detection and Response features include:

- **Managed threat hunting**—Automated and continuous hunting for emerging indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) using the MITRE ATT&CK framework, all enhanced with expert human analysis

- **Remote investigations**—Continual investigations (including memory, disk, and system forensics) of suspicious and confirmed threat activity across on-premises and cloud endpoints

Four key pillars of Symantec Managed Security Services


SOC Technology platform big data analytics and machine learning
Symantec GIN threat correlations, across on-premises and cloud environment
Symantec Integrated Cyber Defense for seamless security coverage
Symantec SOC analysts assigned by industry and region, globally

- **Pre-authorized remediation***—Fast remediation of compromised on-premises and cloud-based endpoints using Symantec Endpoint Detection and Response* via a single agent with Symantec Endpoint Protection

Managed Security Services benefits

Your Symantec MSS team works with you to understand your business goals and priorities. This personalized and focused delivery model ensures you defend your organization against today's most advanced threats. Count on Symantec MSS to:

Reduce Operational Costs—MSS supports your operational planning goals with flexible, scalable solutions that grow with you over time. Our enterprise-wide pricing model enables you to predictably budget for measurable service level agreements. For a fixed price, you can move, add, or change security devices without contract changes. You also benefit from Symantec's investment in its own infrastructure and tools: The service rolls out in hours and eliminates the ongoing (and costly) need for hiring, training, and retaining security professionals.

Extend Your Security Team—When you take advantage of highly skilled, certified security professionals and automated monitoring and correlation tools, you free your security staff from time-consuming, error-prone work and redeploy them to other strategic priorities. Interact with your dedicated Symantec service manager and SOC team around the clock via phone, portal, email, and online chat, ensuring your security staff gets the insights they need when they need them.

Accelerate Detection and Response—Monitoring billions of MSS customer logs annually, and by providing advanced analytics and retroactive log analysis, as well as insights from our global intelligence network and Symantec DeepSight Intelligence, Managed Endpoint Detection and Response gives you advanced capabilities—managed threat hunting, remote investigations, and pre-authorized remediation—to extend threat detection and further mitigate business impacts.

Report on Compliance—MSS enables you to demonstrate the effectiveness of your security controls. MSS assists with compliance reporting, reducing your annual audit preparation effort. Access all your (tracked) year-long security incidents and events through a secure, easy-to-navigate web portal. Take advantage of complete visibility into threat activity and other published notifications, as well as a monthly report with events, incident analyses, and actions taken. Our pre-built compliance templates further streamline and simplify your compliance process.

Retain Security Logs and Monitor Devices—MSS monitors logs and retains them for 90 days, not only for network devices but also for servers, endpoints, and hundreds of cloud and on-premises IT assets.

*Remediation is available to customers with both Symantec Endpoint Protection 14.x and either Symantec Advanced Threat Protection: Endpoint 3.x or Symantec Endpoint Detection and Response 4.x. Remediation support for Symantec Endpoint Protection 15 is expected in the first half of calendar year 2019.

Many companies lack the resources, expertise, budget, and time to address the growing number of increasingly sophisticated cyber threats and attackers. Extend your security team, and make informed cyber security decisions faster, with the most experienced human network of cyber experts armed with advanced analytics, threat intelligence, and tools.

Security Leadership

- Designated a Leader in the Gartner Magic Quadrant for 15 consecutive years.

Global Presence & Delivery

- Six global SOCs worldwide
- Industry's best SLAs (10-minute escalation)

Scalability

- Analyze 160+ billion logs daily
- Escalate 400+ severe incidents daily around the world

Expertise

- Designated teams
- 500+ certified SOC analysts
- Customized service

An MSS analyst inspects every alert, providing tailored insight across your environment. MSS analysts apply their deep expertise to escalated threats, reducing false positives and adding context based on your business and industry.

Take advantage of a fully integrated, managed solution

A successful cyber security program requires a complete strategy, integrating both technology and people. For the most accurate prediction, fastest detection, and most effective response, each Symantec Cyber Security Services offering draws on the depth and breadth of the Symantec Integrated Cyber Defense Platform. Cyber Security Services includes:

- **Managed Security Services** for advanced threat monitoring, hunting, investigation, and response
- **DeepSight Intelligence** for actionable technical and adversary threat intelligence
- **Incident Response** for preventative IR program development and rapid threat containment and eradication

They're all designed to work together and improve the speed and effectiveness of your security program.

Next steps

For more information, visit us at go.symantec.com/mss.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™

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