Symantec Cyber Security Services

The World's Best Cyber Warriors at Your Service

Executive Folio

Symantec

Executive Folio

A cyber attack puts everything at risk: Your brand, your reputation, your intellectual property—your very existence.

Symantec™ Cyber Security Services bolsters your in-house security program with an integrated services portfolio no other vendor can match—powered by Symantec global threat intelligence, advanced analytics, machine learning, and the unequaled human expertise of our cyber security warrior network.

Symantec™

End-to-End Cyber Security

The integration of our Cyber Security Services offerings ensures you'll accurately predict, quickly detect, and effectively respond to threats across your entire security program.

DETECTING ATTACKS: Know when your enterprise is under attack from targeted and advanced persistent threats and campaigns.

Symantec Managed Security Services extends your security program with a dedicated team of SOC experts providing always-on threat monitoring, hunting, investigation, and response.

PREDICTING ATTACKS: Use global intelligence to track and analyze adversary groups, key trends, and threats worldwide.

Symantec DeepSight™ Intelligence delivers technical and strategic intelligence, providing insights that mitigate your cyber security risk by promoting faster, better informed, and more decisive actions.

RESPONDING TO ATTACKS: Be prepared for attacks, and quickly contain and eradicate incidents.

Symantec Incident Response Services forensics experts prepare and test your response plan and stand ready to destroy threats, both remotely and onsite.

Symantec

Take Charge

Key security questions

As you examine your organization's ability to predict, detect, and respond to cyber threats and attacks, consider these key security questions.

Does your threat intelligence program enable faster, more definitive decisions?

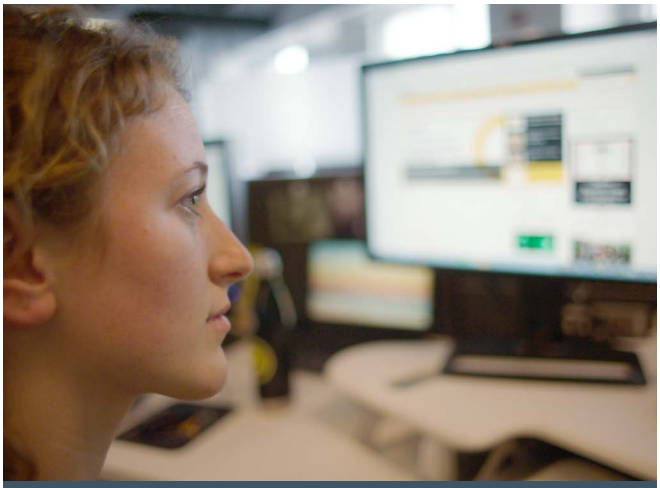
- See threats on the horizon with enough time and detail to understand the risk and deflect the attack.
- DeepSight Intelligence supports fast action with technical and adversary threat intelligence for understanding the nature and impact of threats, as well as who's attacking, why, and with what.

Can you diagnose critical threats in real time?

- Extend and amplify your cyber security program across the entire attack chain.
- Symantec Managed Security Services deploys one of the largest global networks of cyber experts—in six security operations centers (SOCs) and nine security research centers—who continuously monitor and actively defend your organization.

How quickly and effectively do your teams respond to an incident?

- Keep incidents from becoming breaches—and stop data exfiltration—with forensics investigations and expert threat eradication.
- Symantec Incident Response Services experts oversee your IR plan; collect, analyze, and preserve attack-related evidence; and enable in-house security leaders to quickly make the appropriate business decisions.



Your Security Experts

1,000+
certified cyber security warriors

15+
years' advanced threat monitoring

12+
years' (average) active investigation

Experience and Expertise

Partner with a world-class security team

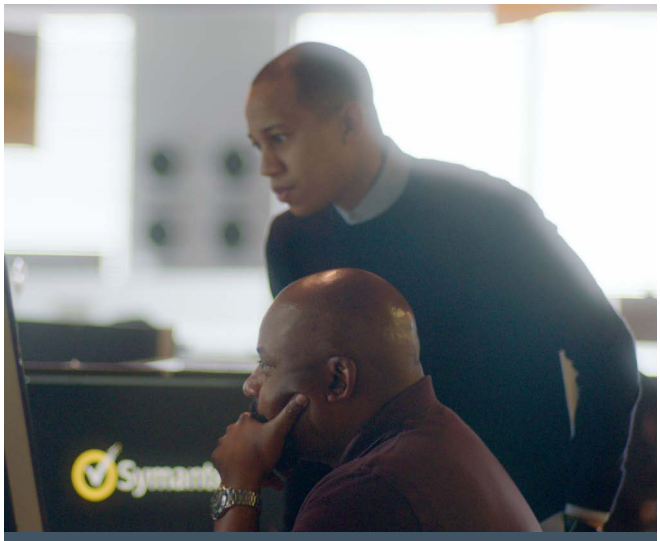
Does your organization lack sufficient staff, threat intelligence, or analytical tools to accurately predict, detect, and effectively respond to cyber attacks? You're not alone.[1]

Imagine what you could do with a world-class team of skilled security experts running a precision security program.

Symantec Cyber Security Services handpicks certified security professionals from top private and public institutions around the world. They comprise a cyber warrior network experienced with all threat actors, threat vectors, and types of attacks.

Then we dedicate a team to your organization, based on your specific industry and region.

In addition to its own experience and expertise, your team of Symantec SOC experts employs powerful Symantec resources as they monitor, hunt, investigate, and respond to stealthy threats. These resources include the SOC Technology Platform with big-data analytics and machine learning algorithms, as well as telemetry from the Symantec Global Intelligence Network (GIN)—the world's largest civilian threat database. Equipped with these tools, your Symantec SOC team defends against more threats because they detect more.



66%

of security leaders say their organization's ability to detect and respond to threats is limited by a lack of security staff, security analytics, or incident response skills.

Source: ESG Research *Threat Detection and Response Survey*, December, 2018

[1] The number of organizations reporting a shortage of cyber security skills increased from 42 percent in 2015 to 53 percent in 2019. Source: ESG Research Report, *2019 Technology Spending Intentions Survey*, February 2019

Symantec

The Symantec Cyber Security Services Incident Response team has been guiding customers through cyber attacks since 2013. The following figures summarize the incidents it has triaged, investigated, and contained since January 2018, by vertical and incident type.

Incidents by Vertical

- 27% Healthcare
- 14% Manufacturing
- 14% Retail
- 13% Financial Services
- 13% Accounting
- 6% Communications
- 5% Education
- 3% Software
- 2% Telco
- 2% Other (not indicated)
- 1% Gaming

Incidents by Type

- 27% Malware Outbreak Known
- 21% Malware Outbreak Previously Unknown
- 21% Advanced Persistent Threat
- 17% Virus
- 10% Web Application Attack
- 2% DDoS
- 2% Application Exploitation

Actionable Intelligence

Symantec DeepSight Intelligence

Anticipate threats and mitigate risks with actionable threat intelligence

Effective cyber security requires a clear understanding of the threat landscape. Stay ahead of the bad actors with DeepSight Intelligence, a cloud-based platform that delivers a steady stream of technical and adversary threat intelligence via a customizable portal and APIs.

DeepSight insights are

- **Timely**—Intelligence is continually sourced and analyzed in real time.
- **Relevant**—Analysts focus on the direct or near-term implications of threats.
- **Context rich**—Numerous sources contribute rich contextual data on threats, adversaries, and their methods. Includes suggested mitigation.
- **Accurate**—Analysts and algorithms continually examine the reliability, variety, and quality of sources.

Managed Adversary and Threat Intelligence team tracks adversaries for valuable insights

The DeepSight Managed Adversary and Threat Intelligence (MATI) research team informs you of emerging threats and their indicators, who's involved, and why. The service:

- Tracks global adversaries, threats, and campaigns
- Maps the dynamic threat ecosystem
- Assesses impacts and risks from known and emerging threats
- Issues timely reports that detail global campaigns

DeepSight customers get unparalleled global threat information, accessible via reports or APIs, that includes:

- **Vulnerabilities**: Discover weaknesses among 60,000+ technologies and 19,000+ vendors; includes rich data on risk scores, impacted products, patch availability and exploits, and more.
- **Malicious Network Indicators**: Receive alerts for—and block inbound and outbound communications to and from—malicious IPs, domains, and URLs.
- **Security Risks and Malware**: Use detailed analyses about infection targets, symptoms, disinfection techniques, and more, protecting against rapidly-changing malware variants.
- **Malicious Files**: Accelerate investigations and connect the dots with other malicious indicators, as well as campaigns and attackers.

MATI provides a range of intelligence deliverables, including:

- **Intelligence Reports**—In-depth analyses of campaigns, actors, and tactics, techniques, and procedures (TTPs)
- **Intelligence Flashes**—Condensed, timely information on evolving threats
- **Open Source Intelligence Insights**—A weekly summary prioritizing reports in the public domain about current cyber threats
- **Quarterly Retrospective**—A review of larger threat movements
- **Malware Configuration Updates**—Current indicators associated with important malware

Level up all your security disciplines

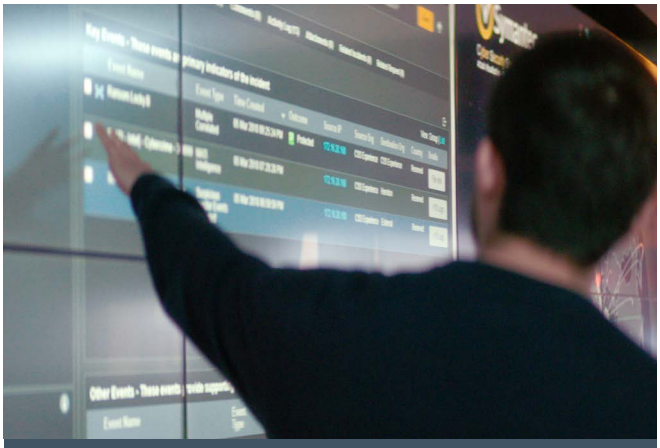
DeepSight Intelligence enhances every security team.

- **Threat and vulnerability teams**—Put controls in place before broadly targeted attacks occur.
- **Security operations teams**—Detect advanced attacks faster.
- **Incident response teams**— Understand, surveil, and eradicate threats before they become breaches.

Executives also use DeepSight Intelligence to understand how threats affect risk and how to align resources when planning budgets and investments.

Make your security technologies smarter

APIs and data feeds integrate DeepSight technical and adversary intelligence with your security stack, improving detections and response. DeepSight connects with a broad range of security technologies including Security Information and Event Management systems, Technical Intelligence Platforms, Security Orchestration and Response platforms, and many others.



DeepSight MATI team members average 10 years' of experience.

Areas of expertise include:

- Intelligence analysis
- Cyber espionage and nation-state cyber threats
- Cyber crime including point-of-sale malware
- Industrial controls systems security
- Advanced penetration testing
- Computer forensics
- Incident response
- Malware reverse engineering and fuzzing
- Botnet emulation and tracking
- Vulnerability research and discovery

Vigilance and Defense

Symantec Managed Security Services

Fortify your internal security program with an expert SOC team providing continual threat detection and response

Challenged by limited security resources, time, and budgets? Symantec Managed Security Services provides:

- **A dedicated SOC team**—Your Symantec team of experts works closely with you to meet your specific and evolving needs and goals. Your team includes
  - Service manager: Your advocate and main point of contact
  - Onboarding: White-glove service to get you up and running fast
  - Technical services: Ongoing technical support
  - Cyber analysts: Day-to-day threat prioritization, hunting, investigations, containment, and remediation recommendations
- **Direct, round-the-clock access to experts**—Via the portal, email, phone, and online chat
- **Continuous enrichment**—Customized monthly reports, monthly threat webinars, regular business review meetings, and emerging threat reports

Improve visibility across cloud and on-premises environments

A shift to cloud apps and infrastructure decreases visibility across your full environment. Take charge of your cloud security with a panoramic view across your hybrid environment and correlated threat intelligence across all your clouds. Symantec Managed Cloud Defense provides the most complete and tightly integrated security monitoring services for SaaS and IaaS apps and infrastructures.

Boost threat detection and speed your response

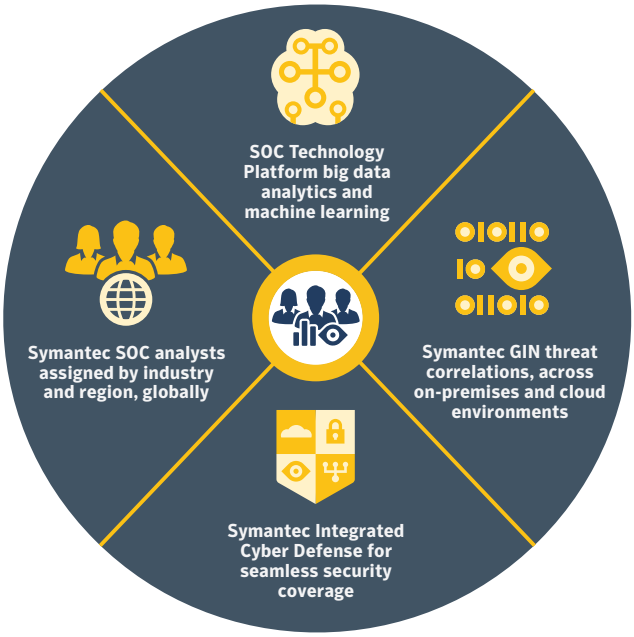
Symantec Managed Endpoint Detection and Response experts quickly find, investigate, validate, and neutralize advanced threats and suspicious activity often missed by traditional detection systems.

Your Managed Security Services analysts use Symantec Endpoint Detection and Response to outsmart threats with:

- **Managed threat hunting**—Automated threat hunting based on indicators of compromise (IoCs) and TTPs using the MITRE ATT&CK framework and DeepSight MATI intelligence
- **Remote investigation**—Rapid assessment of suspicious activity across your on-premises and cloud endpoint environments
- **Pre-authorized remediation**—Fast remediation of compromised endpoints

Symantec Managed Network Forensics lets you see deep into network packet-capture data and traffic logs to monitor hostile activity, track lateral movement, and prevent data exfiltration.

Managed Endpoint Detection and Response and Managed Network Forensics analyze security logs and alerts, hunt threats, and conduct in-depth investigations to quickly identify and respond to emerging threats and suspicious activity.



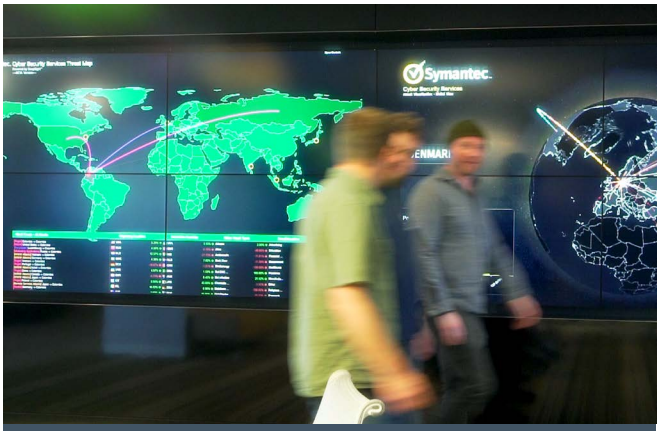
The four pillars of Symantec Managed Security Services

Detect emerging threats through advanced analytics

Our proprietary Managed Security Services SOC technology platform tames the dense noise of alerts and data that makes you miss the forest for the trees. Its array of analysis techniques—from machine learning to clustering and statistical analysis—identifies anomalies, trends, and associations so you quickly perceive threats.

A key feature of the detection platform is its correlation with integrated threat intelligence from the Symantec GIN, the world's largest civilian threat database. This unparalleled data lake gives our analysts unmatched ability to deeply analyze and correlate malicious activity—from campaigns and malware to phishing and spam.

Managed Security Services analysts are made even more effective with adversary intelligence insights from DeepSight MATI.



The Symantec Global Intelligence Network

comprises nine trillion rows of security data, monitoring threat activities in 157 countries and territories through a combination of Symantec products, technologies, and services, and other third-party data sources.

Improve SOC Services

Your Managed Security Services team provides SOC services that perfectly align with your business goals. Given your specific needs, these may include scaling and improving SOC capabilities, reducing operational costs, educating on improvements in security posture, and reporting on compliance.

Reduce operational costs

- Predictable expense
- Budgetable cost
- Measurable SLAs

Extend your security team

- Dedicated, certified analysts
- Continuous access to security experts
- Automated monitoring
- On premises and in the cloud

Accelerate detection and response

- Insights from the Symantec GIN
- Context on adversaries and campaigns
- Analytics/retroactive log analysis
- Managed threat hunting and investigations
- Pre-authorized remediation

Enhance compliance

- Assistance with compliance documentation
- Access to all security incidents and events
- Monthly reports on analysis and actions

Respond and Resolve

Symantec Incident Response Services

Create an effective IR program to quickly neutralize incidents

After an attack, your security and response teams face immense pressure to assess and resolve, all while engaging concerned stakeholders. How prepared are your teams?

When conducting cyber security and forensics investigations, it's imperative you work with a trusted partner who's staffed with experienced, senior investigators providing critical onsite and remote services from start to finish.

Symantec Incident Response works with you, providing incident triage and validation, containment, and threat eradication. In addition to incident response, our preemptive services prepare and improve your security and response teams' readiness and threat hunting capabilities.

Key Incident Response Services include:

Emergency response

- Services whenever you need them

Retainer

- Readiness, investigation, and response services by subscription
- Pre-negotiated terms and service-level agreements

Readiness

- **Incident Response Plan Assessment**—Assesses your IR plan's ability to accommodate current and future needs.
- **Incident Response Tabletop Exercise**—Tests and refines your response plan and processes in an onsite exercise.
- **Advanced Threat Hunting**—Continually searches your environment for previously unidentified IoCs.
- **Incident Readiness Assessment**—Assesses your response capabilities and recommends improvements.

> **"The skills, professionalism, and recommendations provided by Symantec's IR team were instrumental in our ability to respond effectively and were the best we have ever received."**
>
> —VP of Information Systems, Insurance Group

> **"From the first discovery call, our IR manager had a clear understanding of what was happening in our environment and made recommendations that allowed us to contain the incident before the team even made it onsite."**
>
> —IT Manager of Enterprise Resiliency, IT Solutions Partner

Integration

Symantec Integrated Cyber Defense Platform

Symantec's Integrated Cyber Defense (ICD) Platform unifies products, services, and partners, driving down cyber security cost and complexity 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.

Our platform is powered by the world's largest civilian threat intelligence network, deep security research and operations expertise, and a broad technology ecosystem—all working in concert to enhance security controls, improve visibility, and reduce cost and complexity.

As an open platform, ICD coordinates efforts and outputs between Symantec products, third parties, and customers. This integration promotes broad and deep visibility, expediting real-time incident detection and response. As ICD's benefits expand, CSS customers reap the benefits across all control points.

Some examples include:

Endpoint Security

- **Advanced detection and response**
  - Symantec Managed Security Services takes advantage of Symantec Endpoint Protection (SEP) and Symantec Endpoint Detection and Response, pulling in a wider data source for more powerful machine learning and big data analytics. The Endpoint Detection and Response technology integration is the basis for the Managed Endpoint Detection and Response offering.
- **Mobile monitoring**
  - Managed Security Services monitors Symantec Endpoint Protection Mobile (SEP Mobile), extending threat detection to mobile devices.
- **Deception monitoring**
  - Symantec Managed Security Services monitors SEP Deception, a tool that quickly reveals attackers and reduces dwell time. Our analysts provide contextual information that details the attacker's activity on your network.
  - Managed Security Services advises you on configuring and running Deception.

Network Security

- Managed Security Services takes advantage of network monitoring and forensics technologies to quickly detect threats across your network. Analysts also provide Symantec Managed Network Forensics through its integration with Symantec Security Analytics.
- Managed Security Services monitors Symantec ProxySG, Symantec EDR Sensor, and Data Loss Prevention, providing visibility into internal suspicious activity of lateral movement or data exfiltration within your organization.

Email Security

- Symantec Email Security.cloud provides key contextual data, which our teams use to track threat vectors and identify the 'patient zero' of advanced threats.
- Managed Security Services provides summaries of collected events potentially requiring action, such as phishing alerts, so you better understand threat activity and trends.

Cloud Security

- **Cloud visibility**
  - Symantec Managed Cloud Defense, the most complete and tightly integrated security monitoring services available for SaaS and IaaS apps and infrastructures, integrates with Symantec Cloud Workload Protection, giving you deep visibility into cloud platforms and infrastructure, and cloud native services (such as Amazon Web Services and Microsoft Azure).
- **Cloud user behavior**
  - Managed Cloud Defense integrates with Symantec CloudSOC, as well as various user and entity behavior analytics (UEBA) security products, offering insights into both internal threats and unauthorized activities by trusted insiders.
- **Threat hunting, remote investigations, and remediation**
  - Managed Cloud Defense capabilities include managed threat hunting, remote investigation of suspicious threat activity in Amazon Web Services EC2 and Azure VM environments, and pre-authorized remediation via SEP and Symantec Endpoint Detection and Response.

Take the Next Steps

Accurately predict, quickly detect, and effectively respond to threats and attacks. To learn more about—

Cyber Security Services—please visit
Go.symantec.com/CSS

DeepSight Intelligence—please visit
Go.symantec.com/DeepSight

Managed Security Services—please visit
Go.symantec.com/MSS

Incident Response Services—please visit
Go.symantec.com/IncidentResponse

If you are experiencing an incident, contact the Incident Response Services team directly.

Email:

incidentresponse@symantec.com

Phone:

United States: +1 855-378-0073

United Kingdom: +44 0800-917-2793

Singapore: +65 800-120-6718

Australia: +61 1-800-481-774

Japan: +81 0066-33-813303

Symantec™