# Symantec™ Cyber Security Services: DeepSight™ Intelligence

Actionable intelligence to get ahead of emerging threats

## Overview: Security Intelligence

Companies face a rapidly evolving threat environment with frequent high profile breaches putting pressure on executive teams to invest in their security programs. Traditional security solutions, although effective against known threats when kept current, are still being bypassed by attacks that morph or utilize zero-day exploits. Due to the increasing number of alerts, most security teams lack the time to look outside their environments to identify emerging threats and implement appropriate protective measures. This results in a security posture that is predominantly reactive and ineffective against persistent adversaries.

Organizations have found that integrating cyber threat intelligence into their security program not only provides an edge against these threats, but also provides the additional context to prioritize the large volume of alerts typically generated. This allows a smaller security team to better secure and react to critical threats than a larger team without intelligence.


**Symantec™ Cyber Security Services: DeepSight™ Intelligence** is a cloud-hosted cyber threat intelligence platform that provides that edge. DeepSight provides you access to technical and adversary intelligence collected by Symantec through its end-points and other security products and aggregated through its big data warehouse. The data is enriched, verified and analyzed to provide attribution and to connect seemingly disparate indicators into campaigns with known actors and motivations behind them.

Powered by two newly released cyber threat intelligence services, Managed Adversary and Threat Intelligence (MATI) and Directed Threat Research, DeepSight enables organizations to shift from always being one step behind the attackers to being informed, prepared and to having the right measures in place to mitigate risks.

| Feature | Standard | Enterprise | Advanced Enterprise | Advanced Enterprise + DTR Option |
|---|---|---|---|---|
| User Count | 2 Users | Unlimited | Unlimited | Unlimited |
| Administrator Users | 2 Admin | 5 Admin | 5 Admin | 5 Admin |
| Search File, Network, and Vulnerability indicators | ● | ● | ● | ● |
| Analyst Journal | ● | ● | ● | ● |
| Alert Creation | ● | ● | ● | ● |
| Security Risk, Malcode, and Vulnerability Intelligence | ● | ● | ● | ● |
| Receive Email Alerts: HTML/PDF | ● | ● | ● | ● |
| Receive Email Alerts: XML | | ● | ● | ● |
| Event Statistics | | ● | ● | ● |
| Create Custom Reports | | ● | ● | ● |
| Managed Adversary & Threat Intelligence (MATI)* | | | ● | ● |
| Directed Threat Research (DTR)* | | | | ● |

**DeepSight™ Intelligence Portal is available at a number of different service levels and contract lengths; you can select the level that fits your needs and requirements. (*) Asterisks denote that these offerings are available in specific countries around the globe.**

---

*DeepSight™ Intelligence Portal (Standard and Enterprise)*

The DeepSight™ Intelligence Portal is a cloud-hosted web portal that provides customers access to technical intelligence that has been derived by analyzing billions of events stored in the Symantec™ Global Intelligence Network (GIN). By customizing DeepSight alerts, customers are able set up an automated way to receive technical intelligence reports on Symantec detected threats.

DeepSight™ Intelligence Portal content includes:

**Vulnerability Intelligence:** Symantec DeepSight™ Intelligence services provide comprehensive vulnerability coverage across over 60,000 technologies from more than 19,000 vendors, powered by a dedicated in-house vulnerability analyst team that ensures access to the most comprehensive Vulnerability Intelligence available for both emerging and historic threats. DeepSight allows customers to set up a technology list to receive vulnerability reports on new or updated vulnerabilities in technologies in their network. Received reports contain details on the vulnerability, available patches and threat information regarding exploitation of the vulnerability in the wild.

**Network Information:** DeepSight maintains ownership, reputation, and event data on IPs, Domains, and URLs that have been observed by its global collection network to be connected to malicious activity. The data is used by analysts to speed up investigation of suspicious network activity and provides a service which is complementary to internal security devices that detect malicious behavior within your network. The event information in DeepSight provides an outside-in view of detected malicious behavior and can potentially detect threats that have avoided detection by traditional security devices.


**Security Risk / Malcode:** DeepSight contains detailed write-ups on viruses, worm, trojans, adware, spyware, and other potentially harmful files and applications. This near real-time updated security risk and malcode data is an invaluable reference when trying to stay ahead of polymorphic malware. Supplemented with information from the DeepSight Intelligence team who acquires malware from cybercrime forums and other sources where hacker tools are sold

before being used in attacks, DeepSight is able to provide the best source for known and unknown security risks to your network.

*DeepSight™ Intelligence Portal (Advanced Enterprise)*

The DeepSight™ Intelligence Portal Advanced Enterprise subscription gives customers access to Managed Adversary and Threat Intelligence (MATI) reports. These cyber threat intelligence reports, produced by the DeepSight Intelligence team, provide additional context regarding attribution and motivation behind cyber-attacks. Our analysts and researchers have extensive experience working in the Intelligence Community and security industry, bringing rigor to our analytical process to ensure that DeepSight intelligence meets analytical standards and is:

- **Timely:** the intelligence is sourced by monitoring adversaries, researching the Dark Web, and by observing attack infrastructures to be able to produce intelligence prior to or in conjunction with an attack
- **Relevant:** our analysts focus on providing information and insights on threats that are pertinent to DeepSight customers, and explicitly address the direct or near-term implications of the threats
- **Context-rich:** the service provides information on who is behind an attack, why, how victims were targeted, and the best way to mitigate the threat
- **Accurate:** all indicators and attribution to known adversaries are verified and peer reviewed before publication to exclude false positives and to ensure the quality of our intelligence

**Managed Adversary and Threat Intelligence (MATI)**

To help your security teams and executives better assess the impact and risk from known and unknown threats, Symantec's DeepSight Intelligence team tracks hundreds of thousands of adversaries at any given time. Our team of global researchers is dedicated to understanding the adversary ecosystem and providing insightful reports about their tactics, techniques, and procedures, attacks, and campaigns in order to help our customers to take action to disrupt their activities.

MATI reports apply to all industries around the globe but our teams have a unique focus on industries such as finance, insurance, manufacturing, and professional and technical services. Focusing on specific industries ensures that our reports are relevant, actionable, and context-rich, with unique insights and indicators.

**Directed Threat Research Add-on**

When you want to ask specific questions directly to our research team, DeepSight™ Intelligence Directed Research takes our adversary intelligence one step further; providing tailored cyber threat intelligence reports built just for you. Common Directed Threat Research questions may include:

- "Do you have information regarding the Anthem breach? We think we might have been targeted too?"
- "Can you keep us informed regarding activity related to #OpPetrol?"
- "We have an upcoming online meeting and have been targeted in the past. This is a high-risk event; can you provide intelligence on any threats that we should be aware of?"
- "Does Symantec have a list of indicators associated with actors belonging to the Middle East Cyber Army?"

DeepSight MATI and Directed Threat Research reports provide a single unique source for cyber threat intelligence for both security operations teams to help them detect and mitigate threats, and for executives to understand their organization's threat landscape and risk profile.

*DeepSight™ Intelligence Web Services (Datafeeds)*

DeepSight™ Intelligence Web Services is an expanding set of services that enable customers to export and integrate Symantec's technical intelligence directly into security, risk, and management systems (e.g. SIEM, Network Security, GRC, Vulnerability Management, Security Dashboards) to provide visibility into emerging and current threats.

**DeepSight™ Intelligence Reputation Datafeeds**

DeepSight reputation datafeeds are systematically generated intelligence feeds for customers that wish to perform automatic blocking or monitoring of connections to known bad sources, making the reputation datafeeds excellent for automating the application of intelligence and increasing the effectiveness of existing security devices through integration of intelligence.

The entities included in the datafeeds have been observed by Symantec or our partners participating in specific categories of malicious behavior. By analyzing the nature of the observed activity, volume of misbehavior and duration, Symantec is able to provide summary scores which simplify development of rules for operationalizing the intelligence.

The reputation datafeeds provide IP addresses and Domains/URLs exhibiting malicious activity such as malware distribution and botnet command and control server communication. The reputation datafeeds are derived from observed activity on the Internet. A reputation score along with additional contextual attributes are provided for each of the IP address and Domains/URLs, which allows enterprises to customize the data set to better suit the needs of their application and use-cases. The DeepSight Reputation datafeeds are available in multiple formats (CSV, XML, and CEF) as well as in basic (minimal set of contextual attributes) and advanced (complete set of contextual attributes) datasets for IP's and Domains/URLs.

| ATTRIBUTES INCLUDED | DeepSight Intelligence Reputation Feeds | | | |
|---|---|---|---|---|
| | Reputation | | Advanced Reputation | |
| | IP | Domain/URL | IP | Domain/URL |
| IP | ● | | ● | |
| Domain | | ● | | ● |
| URL | | ● | | ● |
| Reputation | ● | ● | ● | ● |
| History | ● | ● | ● | ● |
| Prevalence, Confidence | ● | ● | ● | ● |
| Geolocation* | | | ● | ● |
| Industry* | | | ● | ● |
| Ownership* | | | ● | ● |
| Behavior Details | | | ● | ● |

**(*) Asterisks denote attribute intelligence is available in specific countries around the globe.**

**DeepSight™ Intelligence Security Risk Datafeed:** The security risk datafeed provides visibility into malicious code, adware/spyware and other security risks. Combining prevalence, risk, and urgency ratings with disinfection techniques and mitigation strategies ensures that you can protect against both known and emerging threats in an effective and timely manner. The security risk datafeed provides unique threat data from Symantec which, when integrated with governance, risk and compliance systems, offers improved capabilities for these technologies.

**DeepSight™ Intelligence Vulnerability Datafeed:** The Vulnerability Datafeed provides an easy to consume source of vulnerability intelligence that is best used when integrated into an existing vulnerability management tool that contains asset inventory. These systems correlate the CPE information in the Datafeed to assets in your environment enabling you to automate the identification, analysis, prioritization and response to emerging threats important to your particular environment.

---

*Complementary Services*

Symantec™ Cyber Security Services (CSS) provides a wide range of other complimentary services. Consider the benefits of leveraging additional Cyber Security Services:

**Symantec Cyber Security Services: Incident Response** provides onsite 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.

**Symantec Cyber Security Services: Managed Security Services** delivers 24/7 security monitoring services by expert security staff, providing broad visibility of activity and potential threats across your organization's infrastructure. The Managed Security Services team reduces the time it takes to detect and prioritize security incidents and can improve response times by providing detailed analysis of your log data to your incident responder including vertical-specific and customer-specific context and incident history.

**Symantec Cyber Security Services: Security Simulation** provides hands-on live-fire exercises based on real life scenarios and threat modeling to assess and train your security teams to combat the latest attacker techniques.

---

## More Information

### *Visit our website*

http://enterprise.symantec.com

### *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 an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 19,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2015, it recorded revenues of $6.5 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

***Symantec World Headquarters***

350 Ellis St.

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com



21359350-2 10/15