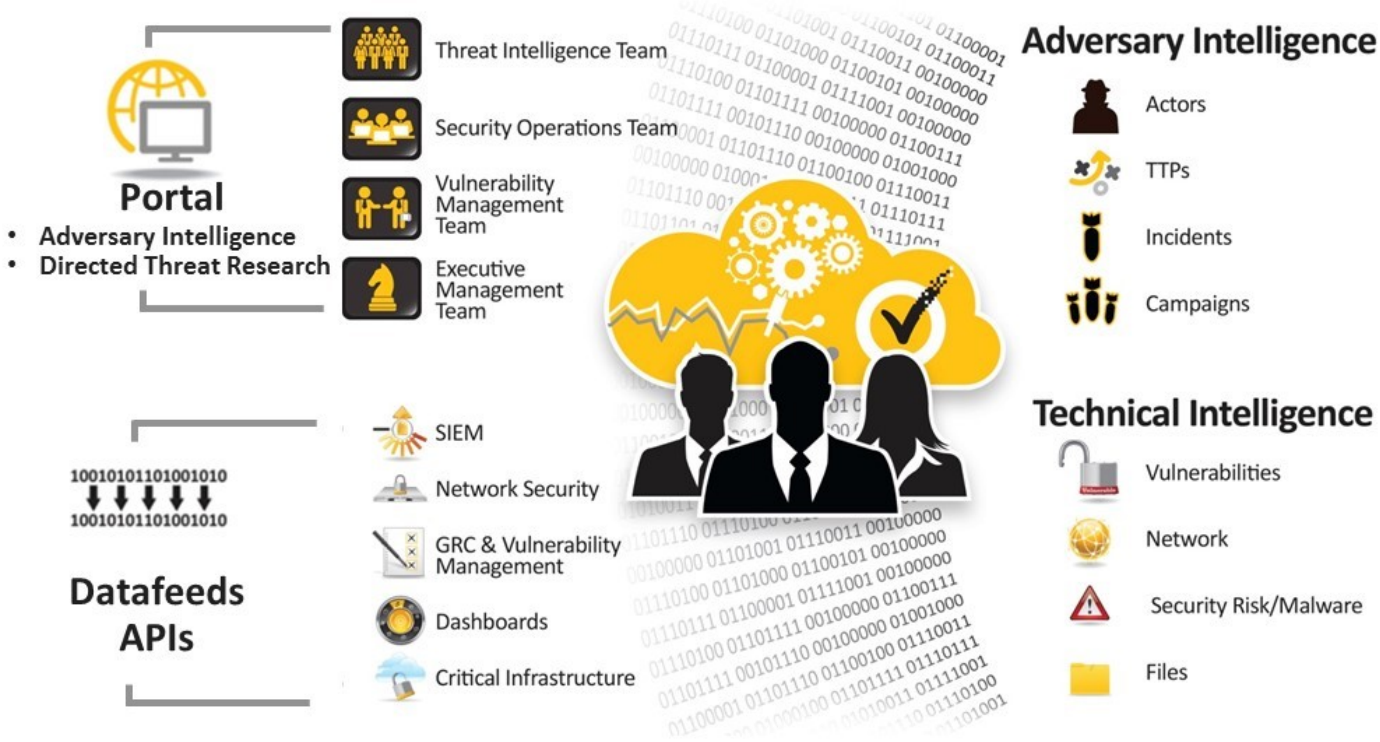
Symantec™ DeepSight™ Intelligence

Actionable intelligence to get ahead of emerging threats

Data Sheet: Symantec Cyber Security Services

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 programs not only provides an edge against these threats, but also provides the additional context to prioritize the large volume of alerts typically generated. Small and large teams that need to better secure and react to critical threats can benefit equally from threat intelligence.



Symantec™ Cyber Security Services: DeepSight™ Intelligence is a cloud-hosted cyber threat intelligence platform that provides that edge. DeepSight provides you access to both *Adversary Intelligence* and *Technical Intelligence*. The intelligence is drawn from Symantec's broad portfolio of security products, as well as its adversary intelligence operations, which include security research and analysis teams positioned across the globe. DeepSight Intelligence data is enriched, verified and analyzed to provide attribution and to connect seemingly disparate indicators into campaigns with known actors and motivations behind them. The finished intelligence product is actionable and is made available via a web portal, datafeeds or restful APIs.

DeepSight™ Adversary Intelligence

Our analysts and researchers have extensive experience working in the intelligence community and security industry. They bring rigor to our analytical process and ensure that DeepSight intelligence meets analytical standards and is timely, relevant, context-rich and accurate. DeepSight™ Intelligence Directed Threat Research (DTR), provides an option to directly engage our analyst team in relation to very specific questions pertaining to attacks or incidents faced by your organization. The DTR option provides you with cyber threat intelligence reports built just for you.

DeepSight MATI and DTR reports support security leaders in elevating security issues to the top of their organizations. Together, they represent a robust, analyst-finished package that can be highly effective for communicating with executives on the organization's risk profile as well as the threat landscape. DeepSight Adversary intelligence enables organizations to shift from being one step behind to being several steps ahead of the attackers.

DeepSight™ Technical Intelligence

Vulnerability Intelligence:

DeepSight provides comprehensive vulnerability coverage across 60,000+ technologies from more than 19,000 vendors. Available for both emerging and historic threats, DeepSight vulnerability intelligence includes a rich set of contextual attributes including risk scores, impacted products, patch availability and exploits, among others.

Network Reputation:

Cybercriminals have an immense number of exploits and attack vectors available, and they use numerous techniques to hide their identities and activities such as encrypted communications, DNS cache poisoning, URL redirection and hyperlink obfuscation. However, disabling inbound and outbound communications from malicious IPs and Domains/URL's is a highly effective way to keep networks secure. DeepSight maintains ownership, reputation, and event data on IPs, Domains/URLs that have been observed by its global collection network as malicious. The intelligence can be used by your analysts to speed up investigation of suspicious network activity and to defend your network against malicious behavior.

Security Risk / Malcode:

DeepSight provides detailed analysis on viruses, worms, trojans, adware, spyware and other potentially harmful files and applications. This near real-time security risk and malcode intelligence is an invaluable reference when trying to stay ahead of malware variants, the behavior of which is not documented. This content provides key behavioral characteristics of these challenging threats so you can determine how to take corrective action.

File Reputation:

Modern malware has a way of entering your internal environment through malicious files. DeepSight dynamic file intelligence can help to effectively identify, analyze and stop the distribution of these emerging threats. DeepSight provides file reputation intelligence for billions of files that have been observed by its global information network, helping your analysts accelerate investigations as well as connect the dots with other malicious indicators, such as campaigns or attackers.

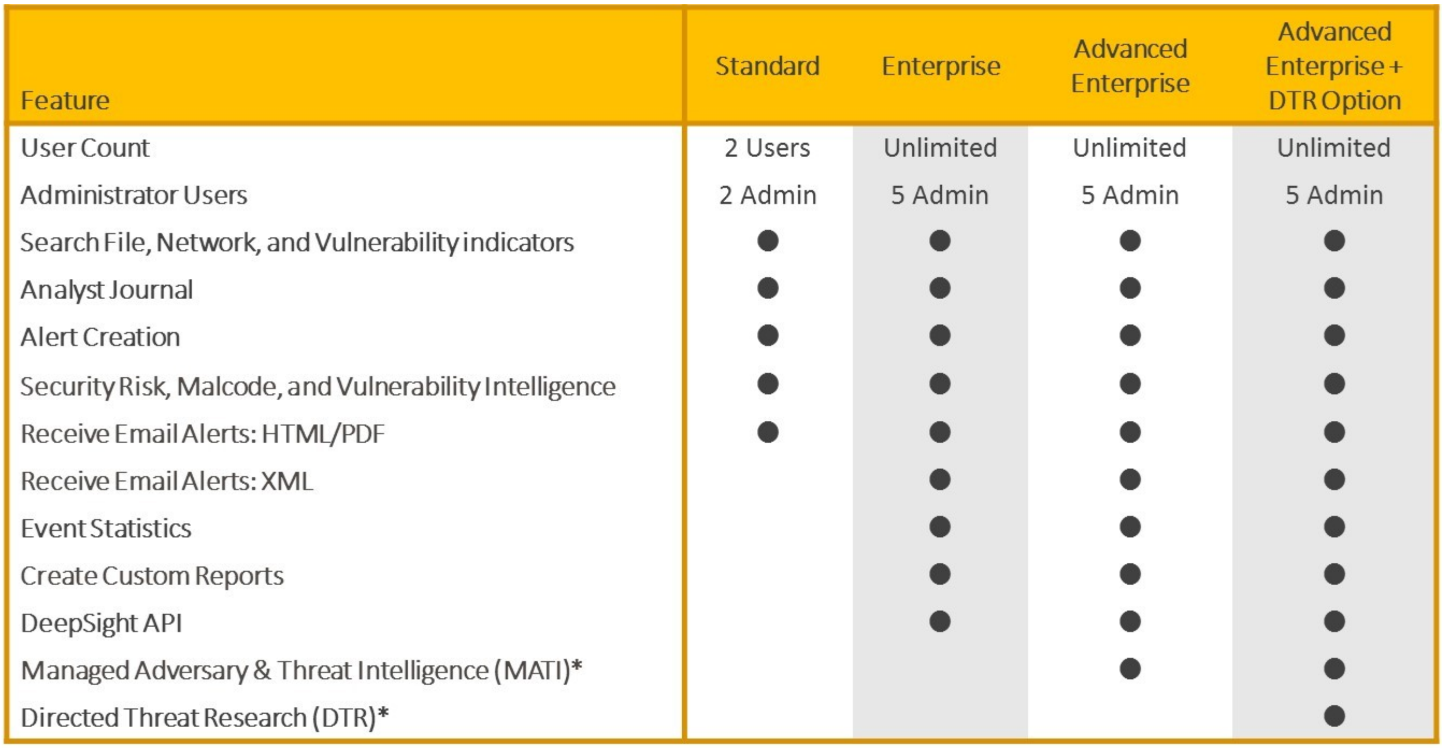
DeepSight™ Intelligence Delivery Methods

DeepSight™ offers multiple options for delivering security intelligence, including portal, datafeeds and APIs for automation. The table below details the types of intelligence and the corresponding delivery mechanisms available.

	Intelligence Type	Portal			DataFeeds			API
		Standard	Enterprise	Advanced Enterprise	Advanced Reputation		Vulnerability	
					IP	Domain/ URL		
Technical Intelligence	Vulnerability	●	●	●			●	
	Network Reputation (IP)	●	●	●	●			●
	Network Reputation (Domain/URL)	●	●	●		●		●
	Security Risk	●	●	●			●	
Adversary Intelligence	Actor Profiles			●				●
	TTP's			●				●
	Campaigns			●				●
	Incidents			●				●
				Data Format	XML CSV CEF	XML CSV CEF	XML	JSON

The DeepSight^{TM} Portal and DataFeeds are available as a subscription service with flexible terms of 1, 2 or 3 years. Subscription to the DeepSight Intelligence Portal or DataFeeds entitles users to a fixed number of DeepSight Intelligence API calls per day, based on usage needs, and additional calls can be added at any time. Intelligence content delivered via the API is based on the appropriate subscription entitlement.

The DeepSight^{TM} Portal offers additional features that address specific user needs. The table below contains key features available on the portal.



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		●	●	●
DeepSight API		●	●	●
Managed Adversary & Threat Intelligence (MATI)*			●	●
Directed Threat Research (DTR)*				●

(*) Asterisks denote that these offerings are available in specific countries around the globe

Complementary Services

Symantec™ Cyber Security Services (CSS) provides a wide range of other complimentary services. Consider the benefits of leveraging additional 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 resolve incidents, return to normal operations, minimize impact and prevent incident recurrence.

Managed Security Services delivers 24/7 security monitoring by expert security staff, providing broad visibility of potential threats across an 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 vertical- and customer-specific context, incident history and detailed analysis of your log data to your incident response teams.

Cyber Security Skills Development provides hands-on, live-fire exercises based on real life scenarios and threat modeling, helping to mature your security posture and train your security teams to combat the latest attacker techniques.

More Information

Visit our website

www.symantec.com/deepsight-products

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