Overview

Protection from Advanced Threats with Symantec™ Insight™ and SONAR™

Unique technologies that detect unknown, polymorphic, and zero-day threats.

Symantec™

With targeted attacks and unknown threats continuing to grow, it's easy to feel overwhelmed and unsure about whether you've taken the right steps to protect your business. Connecting to the Internet and sharing information both inside and outside of your company network is imperative to nearly every business today, but how can you be confident that you're protecting vital business assets and customer information from advanced threats?

As part of Symantec™ Endpoint Protection, Symantec Insight™ and Symantec Online Network for Advanced Response (SONAR™) technologies provide real-time monitoring and analysis of behavior and reputation to help you close the gaps in your defenses and protect against today's advanced threats:

- **New malware:** In 2014 alone, 317 million new malware variants were released into the wild. That's nearly 1 million variants per day.[1] In August 2015 alone, there were 46.6 million new pieces of malware created, well above the monthly average of 41.5 million for the previous 12 months.[2] This includes many ransomware and crypto-ransomware variants designed to encrypt the data on victims' hard drives.
- **Targeted polymorphic attacks:** Attackers increasingly modify existing malware to avoid detection by traditional antivirus solutions. These so-called polymorphic threats are more advanced and often focused on specific targets and can remain undetected in your environment. Polymorphic malware is more widespread than you think. In 2014, 60 percent of all targeted attacks struck small- and medium-sized organizations.[3]
- **Zero-day exploits:** Vulnerabilities that hackers attempt to exploit before developers can fix them were at an all-time high of 24 in 2014, as recorded by Symantec. The news gets worse: It took 204 days, 22 days, and 53 days, respectively, for vendors to provide a patch for the top three most exploited zero-day vulnerabilities. Even after a patch is available, attackers continue to exploit known vulnerabilities through mass attacks that look for unpatched targets.

Sophisticated defense against advanced threats

To protect your organization against unknown and zero-day threats, you need a solution that

- Uses real-time reputation lookups, ratings, and file analysis to evaluate the safety of software files
- Offers intelligence on billions of files globally, with ratings for both good and bad files
- Monitors file behavior to quickly identify new malicious files
- Blocks suspicious files before they execute and do damage

Current threat landscape

- **317 million** new malware variants in one year
- **10 zero-day vulnerabilities** disclosed during September 2015 alone
- **8.8 million** ransomware attacks
- **60 percent** of all targeted attacks against small- and medium-sized organizations

Sources
"Symantec Internet Security Threat Report, Volume 20," April 2015.

"Symantec Intelligence Report: September 2015," www.symantec.com/security_response/publications/monthlythreatreport.jsp.

1 "Symantec Internet Security Threat Report, Volume 20," April 2015.
2 "Symantec Intelligence Report: August 2015."
3 Ibid.

Symantec provides a comprehensive set of solutions that work together to deliver maximum protection against even the most sophisticated and elusive advanced threats. Offering reputation-based security for more than five years, Symantec is the industry pioneer in using its vast amount of global intelligence to improve protection.

Included as part of Symantec Endpoint Protection, Insight blocks rapidly mutating malware and enables faster scan times, while SONAR stops zero-day threats by monitoring file behavior and blocking suspicious files while they execute. Together, these technologies strengthen the entire security stack, decreasing security gaps and increasing the efficiency and effectiveness of your security team.

Symantec Insight for reputation-based security

By analyzing key file attributes, Insight can accurately identify whether a file is good and assign a reputation score to each file, effectively protecting against targeted attacks while significantly reducing scan overhead and false positives by using context. This unique Symantec technology correlates tens of billions of linkages between users, files, and websites to detect rapidly mutating threats and block files judged to have a bad or unknown reputation. It examines the characteristics of the file and its context, including

- Source of the file
- Newness of the file
- How common the file is (e.g., how often it has been downloaded)
- Other security metrics such as whether the file is associated with malware

This information allows Endpoint Protection to block more threats and defend against new mutating malware, while mitigating false positives through contextual analysis and comparing reputation data from more than 3 billion files. Insight technology accurately identifies file reputation so only at-risk files are scanned, effectively eliminating up to 70 percent of scan overhead compared to traditional solutions.

Symantec SONAR for behavior-based detection

SONAR uses machine-learning heuristics as well as reputation data from Insight to detect, monitor, and block emerging and unknown threats. It effectively stops new threats by monitoring nearly 1,400 file behaviors and identifying suspicious activities while they execute in real time before they can do harm. SONAR protects against zero-day threats by detecting them before traditional virus and spyware definitions can be created to address them. With almost 1 million new variants of malware each day, it has never been more critical to have proactive protection at your endpoints.

Symantec Insight by the numbers, to date

- Directly blocked more than **8.7 million** attacks
- Assisted in blocking more than **31 million** attacks
- Tracked more than **3.1 billion** files
- Served **4.1 billion** Insight file ratings each day

Because SONAR monitors and blocks process behaviors in real time, it provides a final line of defense against threats like these:

- **Unknown files:** SONAR determines if an unknown file behaves suspiciously and whether it represents a high or low risk, using reputation data from Insight to help determine risk.
- **System changes:** SONAR detects applications or files that try to modify Domain Name System (DNS) settings or a host file on a client computer.
- **Trusted applications that exhibit bad behavior:** Some trusted files might be associated with suspicious behavior. SONAR detects these files as suspicious behavior events.

Symantec Global Intelligence Network

Both Insight and SONAR technologies use Symantec Global Intelligence Network, the largest civilian threat intelligence network in the world. Symantec Global Intelligence Network is made up of more than 64.6 million attack sensors and records thousands of events per second. It monitors threat activity in more than 157 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Intelligence, Symantec Managed Security Services, Norton™ consumer products, and other third-party data sources.

Symantec Insight and SONAR for advanced threat protection

Insight and SONAR are part of the fastest and most effective endpoint protection security solution to stop malware from compromising your network:

- **Detect advanced threats fast:** Detect new, unknown, and mutating threats before they cause harm to your business.
- **Deliver great performance:** Insight reduces scan overhead by 70 percent, and Endpoint Protection has been shown to outperform all products in its class in scan speed and total performance impact.[4]
- **Gain more control:** With Insight, you can choose your company's tolerance levels for risk.
- **Focus on what's important:** Insight and SONAR use contextual and heuristic analysis as well as global intelligence to reduce false positives and help you focus on the real threat instead of fighting the wrong fires.

School district saves hundreds of hours with Symantec Endpoint Protection

Indian River School District in Delaware relies on Symantec Endpoint Protection for zero-day protection. Symantec Insight technology scans files using trust ratings from Symantec users all over the world. It also takes advantage of SONAR technology to scan application behavior in real time to identify and stop unknown threats.

"We went from reimaging about two infected systems each week for our 14 locations to a total of just a few in a year that need to be reimaged for the whole district," says Patches Hill, technology systems manager at Indian River School District. "By detecting and blocking threats more effectively, Symantec Endpoint Protection is saving as much as 200 staff hours a year in security remediation time."

Read more at www.symantec.com/resources/customer_success/detail.jsp?cid=indian_river_school_district.

Symantec achieves highest score in independent rating

Symantec Endpoint Protection detects and removes threats more accurately and is the only product to consistently receive the AAA rating **for over 11 quarters**, the highest score possible, from Dennis Labs Real World Antivirus Test.

Source
Dennis Labs: www.dennistechnologylabs.com/reports/s/a-m/2015/.

4 "Enterprise Endpoint Security Performance Benchmarks," PassMark Software, 2014.

Installation and enablement of Symantec Insight and SONAR

For maximum protection against advanced, unknown threats, simply make sure that you've installed and enabled Insight and SONAR using the Endpoint Protection management console. Here's how:

- **Confirm that Insight Advanced Download Protection is installed:** If it's not installed, you will need to install it.
- **Confirm that Insight is enabled:** While enabled by default, you can confirm that Insight has not been disabled by selecting the relevant Virus and Spyware Protection policy for the client group you would like to verify. Then select Edit Policy. Select Download Protection and confirm that there's a check mark next to Enable Download Insight.
- **Check that Insight lookups are enabled:** Go to the Clients page and select the Policies tab in each group where Insight should be enabled. Select External Communications Settings. In the External Communications Settings dialog box, make sure that Allow Insight Lookups for threat detection is enabled.
- **Confirm that SONAR is installed:** If not installed, you must install it as part of the Virus and Spyware Protection policy.
- **Check that SONAR is enabled:** In the Endpoint Protection management console, select the relevant Virus and Spyware Protection policy for the client group you would like to verify and then select Edit Policy. Select SONAR and confirm there is a check mark next to Enable SONAR. In addition to enabling SONAR in the Virus and Spyware Protection policy, you must enable Insight lookups.

For more information about enabling Insight and SONAR, or to ask questions about security settings, check out Symantec Support knowledge-base articles at https://support.symantec.com.

Why Symantec advanced threat solution is more effective than other technologies

- Allocates reputation ratings based on multiple factors
- Tracks more than **3 billion** executable files and **100 billion** associations
- Uses Symantec Global Intelligence Network with more than **64 million** attack sensors in **200 countries**
- Accesses comprehensive database with data from more than **210 million** machines
- Delivers fastest performance by eliminating up to **70 percent** of scan volumes

Source
Passmark report: http://www.symantec.com/content/en/us/enterprise/other_resources/enterprise-endpoint-security-performance-benchmarks-w7-passmark.pdf.