Symantec Insight™ and SONAR

It takes combined strength to defeat malware effectively. It's all in the numbers.

We keep track of **over 3.1 billion executable files**

We gather intelligence from **over 210 million machines**

We deliver **70 per cent faster[1] scans**

What Is Symantec Insight™ and SONAR

Symantec Insight™ is a security technology that identifies new, mutating threats as soon as they appear. It uses the file's age, frequency, location, and anonymous telemetry data to look for rapidly changing encryption and mutating codes. Insight is able to detect threats rapidly and accurately.

Symantec Online Network for Advanced Response (SONAR) proactively detects new threats based on their behaviours. Enhancing detection for zero-day threats, it complements Insight by working together to monitor and stop previously unknown malware.

Symantec Insight™ and SONAR offer an intelligent and innovative security approach that can detect malware as soon as it appears. Powering Symantec™ Endpoint Protection 12, these technologies work together with traditional endpoint security technologies to create a fast and effective endpoint security solution – built for both physical and virtual environments – to stop malware from compromising your network.

[1] *Source: Internal testing – comparison between Symantec Endpoint Protection 11 and Symantec Endpoint Protection 12 with Insight technology. This metric relies on the number of files considered "trusted" by Insight that will not be scanned.*

For more information, contact an Enterprise Security Specialised Partner.

Symantec

Symantec Insight™ and SONAR

It takes combined strength to defeat malware effectively. It's all in the numbers.

Why signature-based security is not enough for today's organisations

Mutating malware

Due to vast improvements in technology and greater access to malware toolkits, malware is mutating rapidly, finding new ways to encroach on organisations' security. Signature-based antivirus solutions are only as effective as their latest signature definitions. Hence, organisations require a solution that can detect and block new malware as soon as it appears, based on age, security rating, and how they can be associated with threats.

Advanced Persistent Threats (APTs)

Targeted cyber attacks have also become more sophisticated and extensive. The most significant element is the emergence of highly targeted, long-term attack campaigns known as Advanced Persistent Threats (APTs). They use tactics including drive-by downloads, malware, spyware and phishing. Some characteristics of APTs are:

- **Distribution via social engineering:** They induce unsuspecting employees to download or open links that appear to be from trusted partners or colleagues
- **Customised attacks:** They exploit security loopholes and tailor their tools, such as zero-day vulnerability exploits, viruses, worms and rootkits
- **Long-term campaigns:** They avoid detection by attacking slowly over long periods of time, remaining undetected as they continue towards their objective
- **Focused and targeted:** They're aimed at organisations with valuable technology or intellectual property, targeting distinct individual systems instead of the "spray and pray" methods of phishing scams
- **Higher aspirations:** APT attackers are often well-funded, analysing information to look for greater opportunities instead of simply selling that information quickly

Symantec

Symantec Insight™ and SONAR

It takes combined strength to defeat malware effectively. It's all in the numbers.

How to define a good intelligent security solution

A powerful intelligent security solution can anticipate and prevent APTs and mutating malware. It utilises the following features:

- Automatically assigns ratings for any software files based on contextual dimensions, such as file prevalence, age, and domain reputation
- Ratings for both good and bad files
    - **Bad files**: Display suspicious or malicious behaviour
    - **Good files**: Trusted files that do not show suspicious or malicious behaviour
- Covers billions of files to ensure most files have a rating
- Ratings for files downloaded globally
- Quickly identifies new malicious files via malicious behaviour, even if they are seen by only a few endpoints
- Supports millions of endpoints by providing real-time file reputation lookups

For more information, contact an Enterprise Security Specialised Partner.

Symantec

Symantec Insight™ and SONAR

It takes combined strength to defeat malware effectively. It's all in the numbers.

Why Symantec's intelligent security solutions are more effective than other technologies

Insight and SONAR can identify rare and unknown files based on age, security rating, and how they can be associated with threats. Insight and SONAR are different from other technologies because they:

- **Allocate ratings based on multiple factors**: Based on anonymous data, the popularity and age of the file, and the reputation of the domain
- **Rate both good and bad files**: Provide safety rating on every known executable file, be it good or bad
- **Utilise a large database and extensive knowledge**: More than 210 million machines have contributed data to Insight since 2007
- **Have a wide reach**: Track about 3.1 billion executable files and close to 100 billion associations
- **Deliver increased performance**: Eliminate up to 70 per cent of scan volumes to boost network performance[1]
- **Enhance detection of zero-day threats**: Pick up on the malicious behaviour of even previously unknown threats

Symantec technologies are designed to be more comprehensive, intelligent and experienced

Many Internet security solution suppliers claim to incorporate similar intelligent security features into their solutions.

However we believe our approach is demonstrably more comprehensive, intelligent and experienced.

[1] *Source: Internal testing – comparison between Symantec Endpoint Protection 11 and Symantec Endpoint Protection 12 with Insight technology. This metric relies on the number of files considered "trusted" by Insight that will not be scanned.*

For more information, contact an Enterprise Security Specialised Partner.

Symantec

Symantec Insight™ and SONAR

It takes combined strength to defeat malware effectively. It's all in the numbers.

- **Reputation versus in-the-cloud virus definition lookup**: "In-the-cloud" virus definition lookup is a technology that relies on traditional virus sample collection but signatures are maintained on a server in the cloud instead of on the computer. This increases the rate of malware detection as the user does not have to download the new signature definitions file. Despite this, it still relies on a collection of virus samples. Hence, it is unable to defend against new threats that have not been analysed in a lab. In addition, only malicious applications are identified rather than both good and bad files. It does not offer true zero-day protection and does not block unknown files. Conversely, Insight tracks the reputation of all executable files and assigns a rating based on multiple criteria. Hence, "in-the-cloud" virus definition lookup is only one part of a complete solution that Insight can offer.
- **Collective intelligence**: Symantec is a market share leader in endpoint security[2]. This gives us the opportunity to leverage a massive, globally installed base to collect anonymous data, which is in turn analysed by the Symantec™ Global Intelligent Network (GIN). Such data provides global intelligence with a local perspective. With this global reach, Symantec is able to:
    - Effectively track sets of files and associations comprehensively
    - Detect the prevalence and age of files
    - Offer true zero-day protection and block unknown files
- **Extensive experience:** Symantec has led the way with reputation technologies and first deployed Insight technology in 2007. Since then, Insight has been protecting our users and providing crucial intelligence on threats as they emerge:
    - **We keep track of over 3.1 billion executable files**
    - **We gather intelligence from over 210 million machines**
    - **We deliver 70 per cent faster[1] scans**

[1] *Source: Internal testing – comparison between Symantec Endpoint Protection 11 and Symantec Endpoint Protection 12 with Insight technology. This metric relies on the number of files considered "trusted" by Insight that will not be scanned.*

[2] *IDC Worldwide Endpoint Security 2011 – 2015 Forecast and 2010 Vendor Shares # 231307, published November 2011*

For more information, contact an Enterprise Security Specialised Partner.