

# SYMANTEC.CLOUD SKEPTIC™ TECHNOLOGY

## Stopping Malware Other Systems Can Miss

---

### **The Growing Internet Threat Landscape**

Internet-based threats are evolving. The high profile, large volume virus outbreaks of the past have been replaced by sophisticated, targeted attacks perpetrated by cyber-criminals. Driven by financial gain, these groups are constantly developing new ways to deceive users, steal sensitive data and infiltrate networks. Malware, targeted trojans, spyware, spam, blended threats and drive-by website infections are just a few tools of the trade used by attackers to compromise systems.

The cost of failure is high. Data loss caused by a malware infection can damage a company's reputation, lead to a loss of confidential information and even cause a breach of compliance or adherence to government regulations. What you don't know can hurt you, so ensuring that your business is protected against all these threats is essential. An effective defense should provide protection that can keep you one step ahead of the bad guys.

### **Introducing Skeptic™ : A Unique Defense**

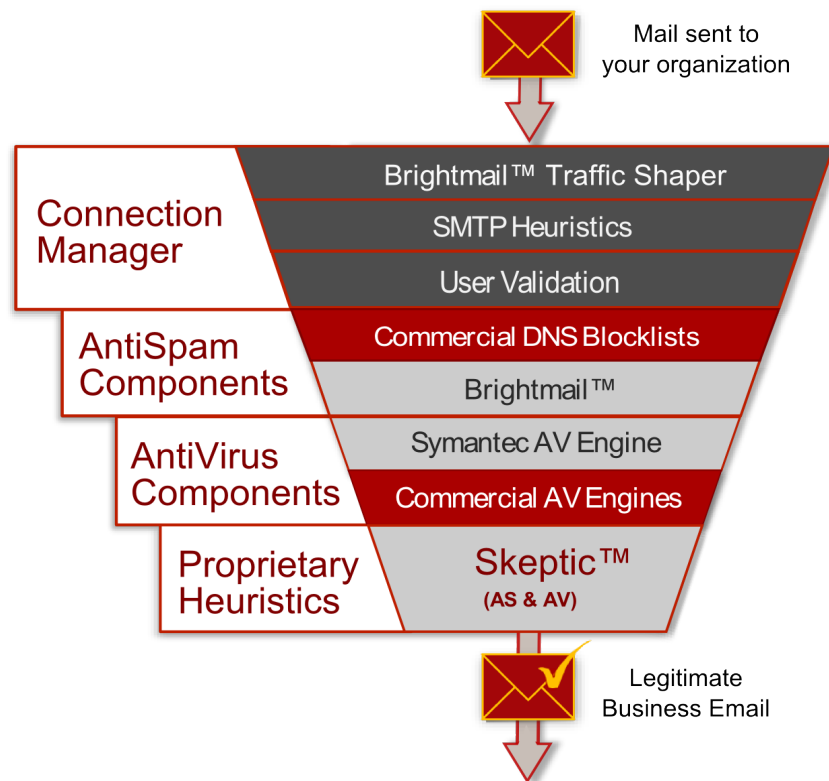
In the face of this growing threat landscape, protection reliant upon signature-based scanners alone can be an incomplete strategy. The sheer volume of new viruses and variants emerging each year is stretching the ability of security vendors with signature-based scanners to quickly identify, analyze, produce and distribute signatures to protect clients. The most targeted and sophisticated threats can also evade signature-based scanners. This is where Symantec.cloud proprietary Skeptic technology can help.

Skeptic is a heuristic technology that does not rely on signatures to detect new, emerging or even variations of older malware. Using thousands of rules and dozens of advanced techniques, Skeptic detects new and emerging malware through techniques such as: application reputation, junk code analysis, and "link-following" which offers protection against positively-identified viral URL links within emails. Skeptic then looks at all the evidence before reaching a conclusion and taking the appropriate actions. Delivered as a cloud-based service, Skeptic is made more powerful and accurate because it continually learns based on the volume of threats it sees and identifies.

Skeptic contains unique and patent-protected technology which allows Symantec.cloud to offer a Service Level Agreement (SLA) with performance levels covering 100% protection against known and unknown email viruses, a 99% spam capture rate (95% for email with Asian characters) with very low virus and spam false positives. And, because Skeptic operates in Symantec.cloud secure global data centers, it is not available publicly for cyber-criminals to test their malware against.

### Part of a Multi-layered Approach

Skeptic is the last line of defense in a series of technologies called upon by Symantec.cloud to detect new and emerging threats. Using multiple layers of technologies, our services begin by deploying Connection and Traffic Management defenses to turn away incoming traffic from known malicious origins. We then use several industry leading signature-based filters to stop known, and previously identified malware and spam. Skeptic then goes to work by detecting and blocking previously unseen (or “zero-hour” ) threats. This provides a unique, intelligent, extra line of defense to protect against threats that signature-based systems may miss. In fact, this extra line of defense detects up to 20% of all the malware stopped by Symantec.cloud services. These are threats that other vendors, without Skeptic technology, might easily let through or allow a window of vulnerability to their customers.



### Extensive Experience, Intelligent Protection

Not all heuristic security is created equal. While many companies claim ‘zero-hour’ protection against new and unknown threats, this is often reliant on blunt methods such as blocking executable files (which can also stop legitimate mail) or outdated techniques designed to stop mass virus outbreaks.

Skeptic on the other hand, has been in continuous development for more than ten years and can draw on a huge base of knowledge accumulated in that time. Further, it is backed by 19 patents granted or pending and a team of 70 antimalware and antispam experts. Because Skeptic learns as it observes traffic, its intelligence is directly related to the traffic volume of the Symantec.cloud infrastructure.

As the industry leader in SaaS, (Software-as-a-Service) Symantec.cloud views huge volumes of email and Web traffic globally and therefore, more threats than other vendors. Our infrastructure processes over 7 billion email connections per month and over 15 billion Web traffic requests. It is also globally distributed, load-balanced, and operates using 15 data centers spanning 5 continents that are located at strategic Internet exchange points. Skeptic also is supplied with threat intelligence from Symantec.cloud Web, Email and IM services to create a unique view into converging threats (threats which leverage more than one protocol). Together, these strengths create a highly available infrastructure for Skeptic to reside within and constantly updated global threat intelligence to call upon to create comprehensive defenses for your business.

Lastly, because Skeptic also examines 'Virus DNA' which stores specific parts of malware when it is identified, it is able to recognize the same malicious code if it appears later. This historical knowledge is particularly useful for the rapid detection of threats in which a malware author has reused another writer's code.

---

### Unique Security & Business Value

Skeptic offers considerable advantages when compared to traditional security measures:

#### Powerful

- Skeptic goes beyond signature-based antivirus scanners by stopping new and targeted threats as soon as they appear.
- Threat data collected by Skeptic is then shared globally across our network in real time ensuring the same level of protection wherever you are located.

#### Accurate

- Skeptic resides in our data centers and can draw on a large amount of processing power to analyze threats in detail, resulting in greater accuracy.
- Possesses intelligent analysis techniques that result in very low levels of false positives helping to ensure that legitimate email is not stopped.
- Continuous and automatic updates are performed across the network through the Symantec.cloud global database replication architecture, providing zero-hour protection.

#### Secure

- Skeptic isn't available publicly, so spammers and virus writers can't test their code against it.
- Resides in highly secure Symantec.cloud global data centers.

#### Proven

- Backed by a Service Level Agreement with performance levels for 100% protection against known and unknown email viruses and a 99% spam capture rate.
- Includes patented technology and is supported by a global team of experts working around the clock.
- Draws on more than a decade's worth of experience and accumulated knowledge.

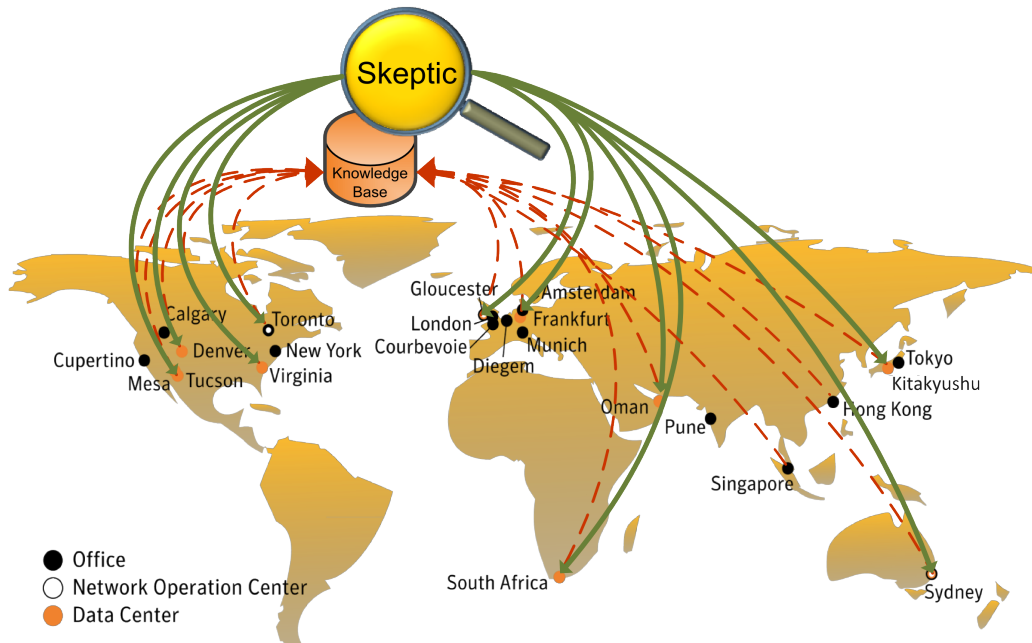
#### Comprehensive

- Skeptic works across email, Web and IM protocols and is able to deliver converged threat protection as a result. (Examples include phishing attempts and malicious URL links in emails.)

### A Proven Track Record

Since Skeptic was deployed in 1999; it has consistently protected our customers from major and targeted virus outbreaks. Threats made famous in the media such as Lovebug, Melissa, Mydoom, Kournikova, BadTrans, Klez Bredolab, Sasfis, Zbot, Hydraq and imsolk.b which caused havoc in the business world – did not reach Symantec.cloud customers.

We continue to protect our customers against the next generation of converged threats that distribute malware through email, Web, and IM, and are very targeted in nature. When Skeptic detects a threat in one protocol, it can rapidly defend customers against the same threat in all the others. This provides protection to Symantec.cloud customers regardless of the form of initial delivery or ensuing forms of delivery the threat may use.



The large size of our customer base (over 32,000 customers and over 10 million users at the time of writing) is a huge asset for Symantec.cloud and advances the accuracy of Skeptic. This is evidenced by the amount of threats that are uniquely detected by Skeptic. Out of the over 8 million pieces of malware captured by Symantec.cloud each month, over 220 thousand are uniquely detected by Skeptic. Simply put, If there is an outbreak or a new trend in attacks, Skeptic is more likely to see it first. This translates into more effective protection for our clients, from the smallest business to the Fortune 500 level.

Skeptic's accuracy is also increasingly important as the threat landscape continues to shift toward smaller, more targeted attacks which appear and disappear quickly to evade detection.

To defend against the dangerous windows of vulnerability left by traditional signature-based methods, organizations need the extra reassurance of Symantec.cloud services and, in particular, our proactive Skeptic technology. Our clients enjoy a unique extra line of defense, protection from potentially dangerous or disruptive threats, reduced administrative management challenges, and peace of mind from a proven service backed by an aggressive Service Level Agreement.

### Next Steps

Visit our website: ([www.symanteccloud.com](http://www.symanteccloud.com)) to begin a free trial of our services and leave the security of your organization to the experts.