This document provides a brief analysis of Secure Computing’s Secure Web SWG capabilities. The conclusions detailed in this document are based on tests conducted on the Secure Web product. Since Secure Computing is no longer applicable in its previously public company format (the SafeWord business has been acquired by Aladdin, and the Web and email business by McAfee), this review pertains to the Secure Web product (previously WebWasher). References to Secure Web from this point on in the document will be treated as references to the Secure Computing WebWasher product. The test results detailed in this comparative report shed light on Secure Web’s marketing claims. The results provide a clear view of Secure Web’s current proven Content Security abilities.

1.1 The attack vector

Web attacks are not composed of a single event such as access to a malicious website, or the downloading of an infected file. Attacks move along an attack vector which is the most effective way to infect a victim. Along the vector there are four main stages – accessing a resource on the Web (website), running active content within the website (scripts, “Web 2.0” dynamic content), downloading content (executables – usually a Trojan or a Trojan downloader), and delivering an additional payload as well as reporting back to the attacker (other Trojan, stolen information sent to perpetrator). The attack vector represents the different techniques and access layers which are applied in most of the standard web attacks we face today:

- **Initiation** – happens when a resource is accessed on the Web (a website – usually a legitimate one)
- **Activation** – happens when active content (scripts, Web 2.0 elements) hidden in the HTML code “run” on the victim’s machine. This content is run just like other legitimate active content which the website is composed of.
- **Infection** – occurs when executables (Trojan, Rootkit, Key-logger) are downloaded to the victim’s machine after successful exploitation in the activation stage, and are installed on the system.
- **Attack** – the payload (Trojan) that runs on the system is operational, and downloads additional malicious components, as well as sends out data that will be used to generate revenues for the criminals (financial information, classified documents, personal information, etc.).
1.2 Secure Web in Perspective

Secure Web relies on its proxy in order to scan web content, and is limited to detecting traffic to known malicious URLs (1), that appear in their blacklists. Application filtering is limited and relies on the ability to block communication from applications that send traffic via servers that appear in their blacklists (4).

*Figure 1-1: Secure Computing and eSafe capabilities on the Attack Vector graph*

Secure Web is able to address Layer 1, blocking access to known malicious sites. In Layer 2 it provides proactive detection based on identification of known Web threats. In Layer 3 it can block malicious files, using an optional third party antivirus engine. In Layer 4 it can only block access to known malware servers (which is actually the same as Layer 1). It does not provide spyware and other malware protocol analysis and blocking.

Being a proxy, Secure Web is limited to HTTP and HTTPS inspection.

In summary, among our competitors, Secure Web presented a high level of protection against Web threats of many kinds. Secure Web was the only product who passed our test set with an 80% success rate. The downside of their security performance was a relatively high percentage of false positives. The most crucial elements that Secure Web lacks are application filtering, anti-tunnelling and outbound communication protection.
# Secure Web Claimed Capabilities & Issues

This section describes Secure Computing’s market claims and how they fare when put to the test in a real environment.

## 2.1 Marketing Claims vs. Reality

Table 1-1 provides details on various Secure Computing marketing claims along with the findings of the AIRC tests that address these claims.

### Table 1-1: Secure Computing Marketing Claims vs. Reality

<table>
<thead>
<tr>
<th>Type</th>
<th>Claim</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Security</td>
<td>Combines the strength of multiple anti-virus engines concurrently scanning all Web and email traffic. The Proactive Scanning filtering technology additionally detects and blocks unknown malicious code, not relying on time-delayed virus pattern updates.</td>
<td>True. Secure Web provides a high proactive detection rate but it pays the price with a relatively high rate of false positives. A thousand known legitimate files were downloaded from Microsoft’s website through Secure Web; 15% of these files were falsely diagnosed and blocked as malware.</td>
</tr>
<tr>
<td>Outbound Protection</td>
<td>Performs advanced content filtering, pattern matching, fingerprinting, clustering, adaptive lexical analysis on both words and phrases, and image scanning and analysis.</td>
<td>Secure Web only relies on URL filtering and AV engines. Spyware and Trojan outbound communication tests included 1,000 malicious applications that were activated on the client side. Only 50% of the applications were blocked by Secure Computing using the URL filter.</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Secure Computing’s Web SmartFilter provides a proven database of over 20 million blockable websites in over 91 categories.</td>
<td>True. In a test we attempted to access 5000 malicious websites through Secure Web. Nearly 4,000 sites were blocked.</td>
</tr>
<tr>
<td>Malicious Web Content</td>
<td>Enforce corporate security policies and block the latest versions of malware.</td>
<td>True. Secure Web offers protection against malicious ActiveX, script malware and exploits. In a test we attempted to download 500 known malicious scripts through Secure Computing – 80% of which were blocked.</td>
</tr>
</tbody>
</table>
2.2 Key Issues

In continuation of the previous section, this section summarizes the key issues found in the Secure Web product:

- The high false positive rate overshadows the security capabilities of the solution, and renders it a “high maintenance” product in constant need of tweaking and releasing legitimate content.
- Secure Web’s Application Filtering blocks only a limited number of application communications.
- Secure Web’s spyware “call-home” blocking is merely a blacklist of servers. Secure Computing only blocks URL’s based on HTTP protocol and does not analyze the actual content of the traffic.
- Secure Web provides a limited list-based protection against tunnelling applications while failing to examine the actual content.
- Secure Computing’s SWG solution is complex and requires hours of configuration for reducing false positive detections.

<table>
<thead>
<tr>
<th>Gateway level Inspection Elements</th>
<th>eSafe</th>
<th>Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware &amp; malware outbound communication</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Web applications control</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Tunneling applications</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Transparent bridge mode operation</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Instant Messengers (chat, file transfer)</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>P2P (Skype, BitTorrent, etc.)</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Remote control applications</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Advanced non-caching, non-proxy technology</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Transparent HTTP inspection</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>100% Anonymizer blocking</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Blocks incoming/outgoing net worms and TCP exploits</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

Available Feature ✓
Unavailable Feature ✗
Poor Functionality ✯
3 eSafe Main Advantages

3.1 Application Control

- **SecureWeb – Limited application filtering capabilities**
  The SecureWeb Proxy solution includes the Instant Messaging Filter which is a module that intercepts and filters IM and P2P communication protocols. The filter is not included in the Secure Computing appliance, but installed separately. The filter includes the ability to block incoming or outgoing communication, however, it fails to block communication from unknown malicious applications such as Tunneling, Remote Control Applications, malware sending outbound content, and various vulnerabilities and exploits (Trojan and Spyware information theft, Trojan downloaders).

- **eSafe – AppliFilter™ Technology**
  eSafe covers hundreds of Internet applications with individual rules that enable controlling the way the Internet is used, preventing resource abuse and security gaps. eSafe’s AppliFilter™ secures and controls over 500 Internet application protocols from 20 application families, divided into four categories:
  - **Malicious applications**: Spyware, Trojans, Worms, Key-loggers
  - **Unwanted applications**: Adware and add-supported software, anonymizing tools
  - **Exploits and vulnerabilities**: TCP Exploits, drive-by attacks, browser hijackers
  - **Controlled applications**: Instant Messengers, IP Phone, P2P, streaming, tunneling.

  AppliFilter is the enabling technology behind eSafe’s application control. AppliFilter does not rely on a blacklist of servers the application can communicate with, but rather examines the protocol itself, analyzing and blocking incoming and outgoing content that is either malicious, inappropriate or restricted according to the Internet usage policy in real-time. AppliFilter is “source/destination” agnostic and analyzes traffic based on patterns and malicious behavior.

3.2 Spyware “Call Home” Blocking

- **Secure Web – Relies on blacklists for blocking**
  Secure Computing has a very limited ability to block outgoing spyware communications from infected PCs, what is also known as spyware “call-home”. Although Secure Computing can block access to known spyware and phishing sites, the list must be reactively updated and is therefore regular URL filtering. Furthermore, this capability is further limited to port 80 only since their products are proxy-based. Secure Computing is not capable of identifying the protocols used by spyware, not to mention other malware types, which can communicate with the outside world such as Trojans and key-loggers.

- **eSafe – Provides two layers of protection**
  eSafe includes two layers of protection from spyware like those mentioned above. As the first level of protection, eSafe includes two blocking lists of known spyware/malware sites (for crossblocking), as well as a phishing sites category. In addition, since eSafe uses multiple security layers, it not only blocks access to known spyware and phishing sites but can also block their protocols using AppliFilter – irrelevant of which sites on the Internet they try to communicate with.
### 3.3 Tunnelling and Anonymizers

- **Secure Web** – Can only handle known tunnelling and anonymizing methods by relying on their **blacklists and dictionary based dynamic URL classifications**. Today’s tunnelling and anonymizing applications use new evasion techniques that include the usage of dynamic addressing and content randomisation techniques. Secure Computing does not provide deep protocol and content analysis or pattern matching techniques.

- **eSafe** – Provides **three-layer protection against anonymizers and encrypted content**
  eSafe provides three layers of protection against anonymizers:
  
  - **Access level**: eSafe blocks access to known anonymizer sites, and sites with untrusted SSL certificates.
  
  - **Protocol level**: eSafe identifies and blocks traffic generated by anonymizer sites, and protocols, including “stealth” and “tunneled” network protocols, such as Hamachi, TOR, Tunnelier, etc.
  
  - **Content level**: eSafe Web SSL inspects encrypted HTTPS traffic identifying “unknown” anonymizer sites. eSafe Web SSL allows policy based decryption of encrypted Web content over secured protocol. It also plays a key role in enforcing policy over anonymizers that are blocked by protocol, certificate and URL, and by AppliFilter.