

Web Tap Security

Keeping Your Data **TOP SECRET**

Web Tap Enterprise Product Information

Contact Email: enterprise@webtapsecurity.com

Website: <http://www.webtapsecurity.com>

Copyright © 2008 Web Tap Security, Inc.

Executive Summary

Web Tap Enterprise is a passive networking monitoring system that detects malware, unwanted applications, and insider leaks. Web Tap uses patent-pending analysis technology to uncover advanced threats that evade firewalls, anti-virus software, and conventional intrusion detection systems.

Web Tap is designed for medium to large enterprises that place a high value on confidentiality. It has been under development since August 2006 and is currently in the Beta testing stage. One primary customer, a medium-sized business, has been using Web Tap for over a year. With the help of Web Tap, the customer has identified and mitigated numerous security threats that slipped past anti-virus and intrusion detection software.

Unlike other network behavioral anomaly detection (NBAD) systems, Web Tap analyzes and maps all network traffic to known applications. Traffic that does not fit a known profile is suspicious, and may be associated with malware or an unwanted application. This allows Web Tap to detect a wider array of security threats than other NBAD systems. Web Tap also uses protocol knowledge to precisely measure outbound information flow. It can detect insider leaks even when they are small, encrypted, and spread out over time, which other NBAD systems cannot do.

The remainder of this document describes the Web Tap technology and summarizes customer experience. It then presents the product specifications and concludes with information about evaluating Web Tap in your network.

Technology

Current IDS and anti-virus systems rely on signatures for known malicious activity. This approach worked well when malware was limited in its diversity and easy to classify. However, malware has become so widespread that keeping up with signatures is increasingly difficult for anti-virus vendors, which, at best can only detect 86% of malware¹.

Web Tap uses a new and alternative strategy. It identifies all network applications and then filters those that match known good profiles. Instead of searching for bad behavior, Web Tap excludes good behavior and considers everything else suspicious. This way, Web Tap can detect a wide variety of both known and unknown threats, including zero-day malware, which would evade traditional security systems.

Web tap uses patent-pending traffic analysis technology to identify network applications. The technology focuses on three aspects of network traffic: *formatting*, *timing*, and *bandwidth*. Web Tap examines the format of protocol headers in every web request. If they do not conform to specifications and match the signature of a known good application, then Web Tap generates an alert. Web Tap also measures request timing to determine which network

¹ Based on research results from “Rethinking Antivirus: Executable Analysis in the Network Cloud” by J. Oberheide, E. Cooke, and F. Jahanian, available at <http://jon.oberheide.org/files/hotsec07-cloud.pdf>.

traffic comes from an automated process. When Web Tap discovers programmatic network access, it checks if the server is a trusted web service endpoint, and, if not, raises an alert.

Finally, Web Tap calculates *unconstrained* outbound network bandwidth. Web applications can send a lot of data to the internet, but most of it is constrained by the application protocol. For example, browsers send out cookies with every request, but cookies are copied from previous messages sent by the server. Even though cookies can be large, they do not contain information from the client. Web Tap performs advanced protocol processing on both client and server traffic to isolate information provided by the client. Examples include file uploads, message board posts, and data that has been surreptitiously inserted by malicious software. Web Tap raises an alert when it detects over 40 KB per day of unconstrained bandwidth.

Web Tap's daily bandwidth limit, 40 KB, is equivalent to about half the size of a ten-page Word document or one fifth the size of a 640 x 480 JPEG image². This hard limit will detect even the most sophisticated hackers if they try to extract information from your network, regardless of data encryption or obfuscation. Web Tap is the only available software that measures unconstrained bandwidth and can provide a high level of protection against network-based information leaks.

Customer Experience

As of February 2008, Web Tap has one primary customer who has been running the software for over a year. The customer's network contains approximately 500 computers that share a 12 Mbps network connection. Web Tap has identified several threats in the customer's network, including:

- "Bot" malware trying to blend in with normal web traffic
- File sharing programs, some of which tunnel their traffic through the Tor anonymous routing network
- Spyware programs
- File uploads and large posts including web mail

The customer's organization has an open network policy; individuals may install any software they like. This type of policy is the most challenging in terms of false positives. After a brief tuning period of less than one day, Web Tap is able to maintain a low false positive rate in this environment (less than ten per day).

Overall, the customer has been happy with Web Tap's ability to detect security threats that were not stopped by anti-virus software, firewalls, or conventional intrusion detection systems.

² 40 Kilobytes is also approximately equivalent to 5100 credit card numbers or 6800 words of plain text.

Product Specifications

Web Tap is in the Beta development stage. As such, these specifications are subject to change and improvement. Please contact us at enterprise@webtapsecurity.com to discuss your specific requirements and we will do our best to accommodate your needs.

Network Placement	Requires passive access to incoming and outgoing traffic prior to address translation. Typically connected to a switch's span port.
Supported Platforms	Windows XP, Vista, Server 2003 Fedora Core 5 and 6 Any as VMWare Appliance <i>Hardware Appliance (Planned)</i>
Maximum Sustained Data Processing Rate (With low-end T2500 2.0 GHz processor)	25 Mbps
Maximum Peak Bandwidth	1 Gbps
Maximum Number of Hosts	Unlimited – See bandwidth limit
Memory Usage	Varies – Usually 50-200 MB
Required Disk Space	2 GB
Required Third-Party Software	PostgreSQL, WinPCap

Trial Information

Web Tap is available free of charge during the Beta testing phase. If you are interested in seeing how Web Tap can improve security in your organization, please contact us at enterprise@webtapsecurity.com. We will be happy to provide you with the latest version of Web Tap Enterprise and assist you with installation. We also give on-site demonstrations subject to location and availability. Send us an e-mail today if you have any questions about Web Tap. We look forward to hearing from you!