

Ehrlich, Wesen & Dauer, LLC

Software Asset Description

Sentinel Privacy Products

Ehrlich, Wesen & Dauer is a leading provider of technologies and services for internet privacy and security. Whether you are engaged in e-commerce, financial services, or healthcare, or are concerned with international and children's privacy initiatives, Ehrlich, Wesen & Dauer has the right solution to meet your needs. Our comprehensive array of applications and expert professional services can provide you with the protection to navigate safely through the increasingly unsafe channels of the connected world.

<http://www.ewdlc.com>

401 Shady Avenue, Suite D-103 Pittsburgh, PA 15206

t: 412-661-1002

f: 412-661-1008

Ehrlich, Wesen & Dauer (EWD) has done everything to supply you with the most up-to-date information. EWD makes no representations or warranties with respect to the information provided in this publication and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, EWD reserves the right to revise the publication and to make changes from time to time to the content hereof without obligation to notify any person of such revisions or changes. Therefore, please contact us or visit our website for the latest information available.

Should you have any questions regarding this notice, please contact EWD and info@EWDLLC.com.

Executive Summary

This document will briefly define the fundamental privacy problem resulting from the design and the structure of the Internet, describe the ramifications of that problem to businesses and individual users, and detail the technologies developed to mitigate those effects as embodied in the Sentinel line of products. The Sentinel products include the following:

- Personal Sentinel
- Network Sentinel
- Message Sentinel
- Site Sentinel

Each of the product descriptions will follow a similar format by answering the following questions:

- What is the product?
- How is it used?
- How does it work?
- How does it differ from other solutions?
- What are alternative uses of this technology?

Because the primary purpose of this document is to provide factual information, as opposed to marketing hyperbole, it will focus on the description of the Sentinel line of products rather than on any specific marketing and business strategies. In addition, since the product line described covers a wide range of privacy related business applications, a broad spectrum of strategic initiatives may be accommodated through the selective use of the existing products or through minor modifications of the products to meet specific operational objectives. Some of these possibilities are outlined in the “Alternative uses of technology” sections.

NOTE: Ehrlich, Wesen & Dauer, LLC (EWD) is a technology and consulting company that has acquired various intellectual properties from Intelytics, Inc., including all technology and supporting materials related to the Sentinel line of products. Subsequent to that acquisition, EWD has continued to develop and improve certain aspects of the products. *EWD is completely separate from, and has no affiliation with Intelytics Inc.*

Fundamental Problem and Effects

Understanding the nature of web-based privacy violations requires knowledge of a single basic problem: due to the nature of the HTTP protocol, a user can be tracked by 3rd-parties without the user's permission.

Figure 1 below illustrates the problem. A user requests a document from a trusted source (Site 1). In turn, this request triggers other obligatory requests for embedded content, such as images, JavaScript files, and ActiveX controls. A privacy violation occurs when these additional requests are made to 3rd-parties (like Site 2), which record the user's request and add it to a growing database about that particular user. Other mechanisms provided by the HTTP protocol make it possible for sensitive data, such as credit card numbers, user id's, purchase amounts, etc. to be sent to the 3rd-party as well.

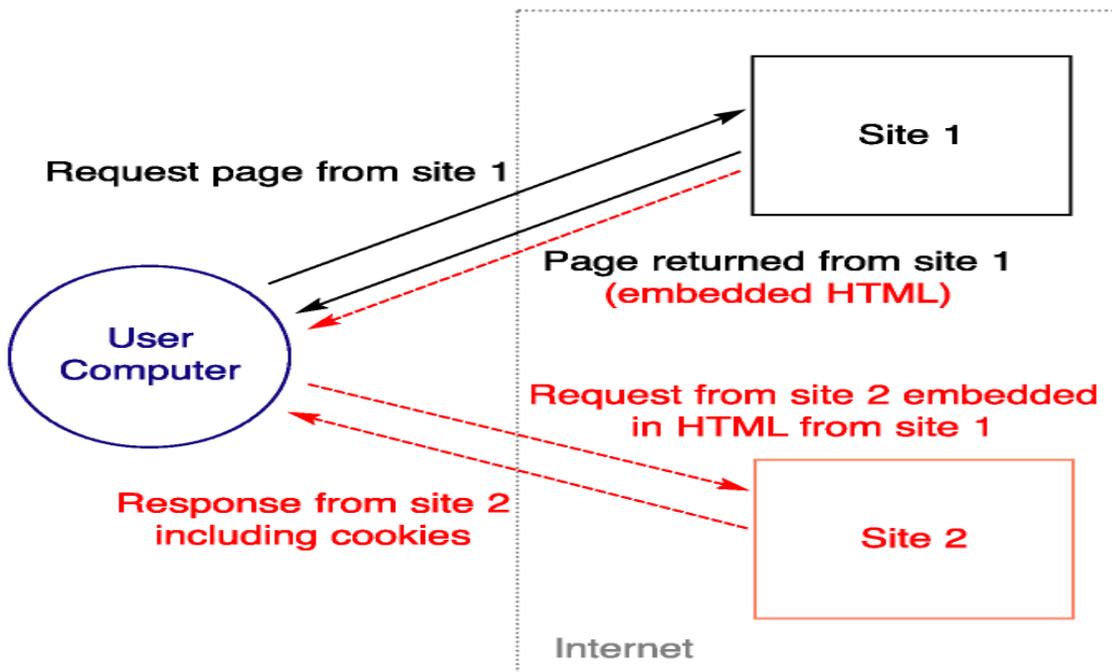


Figure 1.

The problem from the perspective of the consumer or end-user is obvious. Most users would prefer that their actions be anonymous or recorded only by the party originally contacted. They would also prefer that their private information remain private. The Personal Sentinel product (introduced later) addresses this need.

Web interactions are not unique to the web browser. E-mail is often sent as HTML, and the same privacy violations can occur here as well. Message Sentinel (introduced later) was designed with this in mind.

The problem from the organization's perspective is more complicated. Companies with hundreds or thousands of employees have a compounded problem with respect to privacy. Not only is it possible for a company's individual employees to be tracked through corporate firewalls, it is also possible for the company itself, by virtue of aggregate tracking, to have its privacy violated. Tracking entities, in some cases, have more access to information about what a company's employees are pursuing or working on than management of the company itself. Protecting the privacy of the employee or student, as well as the organization itself is the job of Network Sentinel (also introduced later.)

Additionally, companies run websites themselves. Many commercial sites have 3rd-party tracking devices throughout and management is not aware of them. In these cases, the company has an organizational problem that is putting at risk its image and the relationships with its customers. In other cases, sites intentionally track users as part of their business strategy, but have implemented tracking in a reckless and possibly dangerous fashion. In all these cases, Site Sentinel (also introduced later) can help an organization better understand the privacy situation of its web presences and potentially protect it from violations of US and European privacy laws.

The Products

Personal Sentinel

What is Personal Sentinel?

Personal Sentinel is a program designed to protect privacy while users are online. Personal Sentinel works by blocking tracking mechanisms commonly used on the web through embedded content as well as software products. The program offers:

- System-wide protection with additional protection for browsers.
- Low-level integration with Windows to provide real-time analysis and protection.
- Access to multiple data sources such as network data, file systems and other applications allowing better access to contextual information.
- The program and installer compatible with Windows 98, Windows ME, Windows NT 4.0 Service Pack 6, Windows 2000 & Windows XP.

How is it used?

Personal Sentinel continuously monitors the computer installation for potential privacy violations. The program looks for applications trying to access the network, cookies sent to third parties as well as third party servers.

Personal Sentinel provides a network access control feature. The program supports MD5 signatures for executables for greater security as well as permission-based access. The program will prevent persistent data from being sent to third parties through popular browsers or related applications. Personal Sentinel also prevents user specified websites from ever being accessed. The access control mechanism

supports blocking based on domain names, sub-directories and wildcarding. This facilitates a greater degree of control with minimal effort.

The program displays an intuitive interface based on the real time analysis of network traffic to alert the user of connections to third parties, and potential privacy violations that are encountered and blocked based on the user's preferences. Personal Sentinel caters to novice users with easy installation and use while providing power users the ability to customize the product.

How does it work?

Personal Sentinel along with other Windows based products in the Intelytics suite works in collaboration with the Microsoft® Windows networking layer (see Figure 2 below). This enables the application to have access to resources such as real time network traffic belonging to all applications, files stored on the hard disk and other applications that are running. The ability to access and analyze information from multiple sources allows the product to identify and block privacy violations.

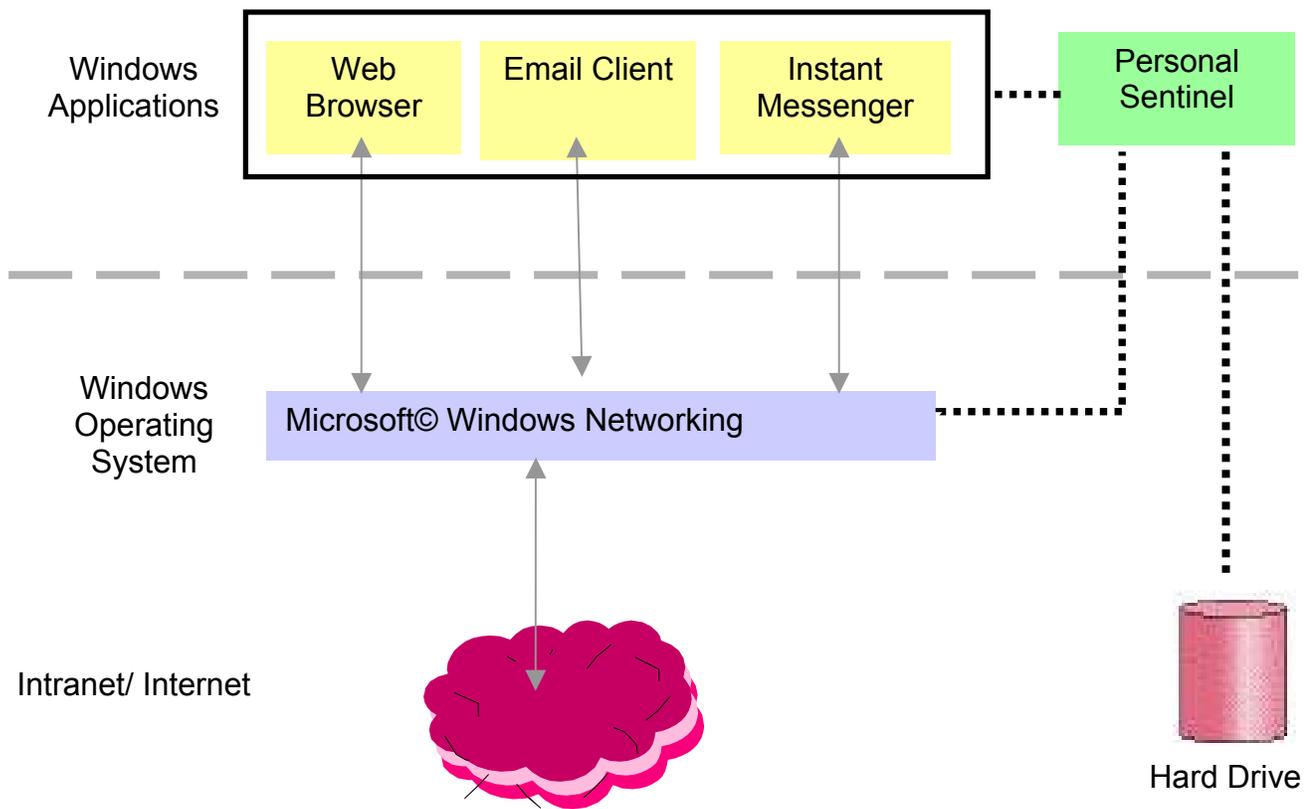


Figure 2: Intelytics Windows Application architecture

Personal Sentinel intercepts and examines outbound network traffic to identify privacy violations. The product then either blocks the violations or transparently

services the request through an internal cache. The product also uses the file system where other violations might be stored.

How does it differ from other products/solutions?

Personal Sentinel is a product focused on protecting user privacy. Whereas personal firewall products do a good job of blocking potential hackers, they do not provide the set of privacy related features that Personal Sentinel does.

Most popular ad blocking software applications use browser specific plugins or proxies to block advertisements and popups but are unable to prevent users from being tracked or alert users to privacy threats. Personal Sentinel automatically works for all applications and requires no additional configuration.

What are alternative uses for this technology?

Personal Sentinel is an easily configurable program designed to help users protect their privacy while they are online. The program is built using versatile technology that can be suitably modified for other purposes. Other potential applications include:

Expand beyond HTTP

Personal Sentinel could be extended to examine other protocols such as NetBIOS in addition to the HTTP protocol. Features such as blocking based on addresses could be extended to these protocols.

Logging

The product could be enhanced to perform logging. Parents concerned with their children's online activities could later examine these logs. The logging preferences would be set by the parents based on parameters such as application used or time of day.

Transparent encryption (Virtual VPN)

This feature would allow all communication between Network Sentinel enabled clients to be encrypted by default. This would allow secure communications without having to change the applications that run on the desktop.

Network Sentinel

What is Network Sentinel?

Network Sentinel is a software system designed to help companies control the flow of corporate information, save corporate bandwidth, and protect their employee's privacy. Network Sentinel consists of a server component and client components that are installed on computers within the network. The product works by allowing an administrator to control the privacy preferences of computers within a network from a single point. The product offers:

- Superior access to contextual data via access to multiple data sources such as network data, file systems and other applications.
- Single point of control for system-wide privacy preferences. End user privacy is protected transparently.
- Periodic reports from client computers on privacy related activity within the network including both summary as well as detailed information.
- Reduced network traffic both within the intranet and to the Internet.
- Low-level integration with Windows to provide real-time analysis and protection.
- Distributed processing eliminates need for expensive servers to perform filtering.
- The client application works on Windows 98, Windows ME, Windows NT 4.0 Service Pack 6, Windows 2000 & Windows XP while the server component is designed to work on Windows NT server & Windows 2000 server.

How is it used?

Installing Network Sentinel is simple. The server software requires an installation of Microsoft® Internet Information Server (IIS) and Microsoft® SQL Server. The client can be installed onto multiple clients using Systems Management Server (SMS) 2.0 and the installer supports using text files to configure the installation.

An administrator can use the administrative console to configure the privacy preferences for users within a network. The preferences that can be configured include blocking web servers as well as blocking cookies. Servers can be blocked based on domain names, directories and through the use of wildcards. These preferences are then served to the client component through the IIS web server.

The client component runs transparently on computers without user interaction. The program will load the administrator specified preferences from the web server and configure itself. It will also periodically check the server for new preferences as well as report information to the server periodically.

The administrator can specify the reporting interval based on time as well as traffic. The interval between successive checks for new permissions can also be specified. The client component reports key information to the administrator to gauge the success of the preference set being used. The numbers include information about the computer, user, cookies, network enabled applications and http traffic.

How does it work?

As shown in Figure 3 below, the Network Sentinel system consists of a server and client components. The server component allows an administrator to control a set of privacy preferences to apply throughout an organization. The system

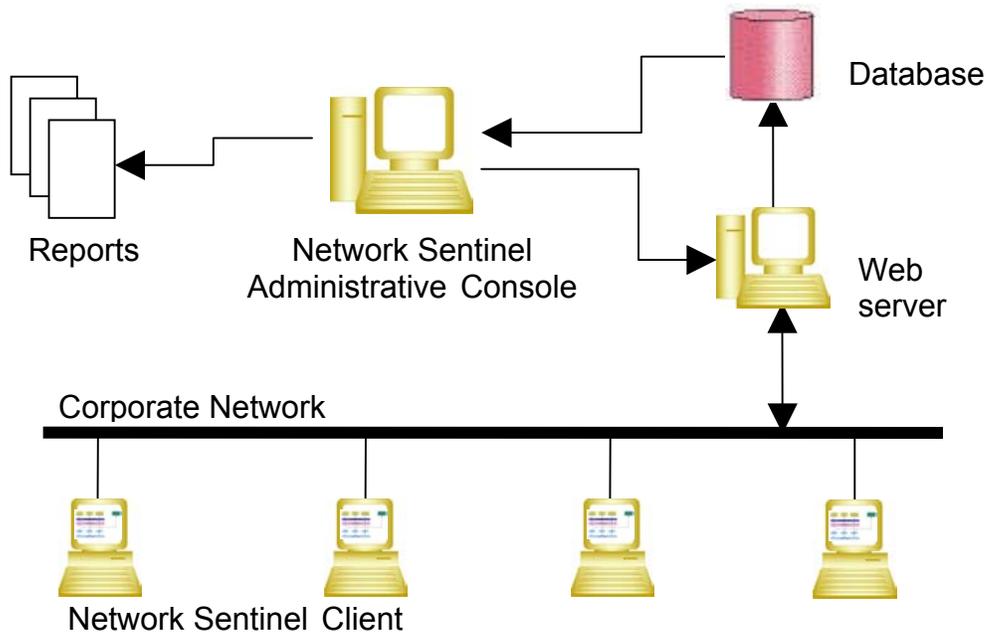


Figure 3: Network Sentinel Architecture

uses Internet Information Server (IIS) to share these privacy preferences with clients within the network.

Clients are installed on each desktop within the network. The clients fetch the privacy preferences from the server and apply those preferences to the desktop computer. The communication between the client and server uses standard HTTP.

The clients also report privacy information back to the server. The server component stores this information in a database. This information can be viewed as a report on a daily, weekly or monthly basis or can be emailed to administrators or managers.

How does it differ from other products/solutions?

Network Sentinel is a privacy product for the corporate network. It allows a single set of privacy preferences to be applied throughout the network in a distributed manner. As a

result, running a Network Sentinel system is scalable and does not require expensive hardware.

Firewall products work in a complimentary fashion to Network Sentinel and can do an effective job of blocking outside hackers and blocking specific ports. However, their effectiveness in controlling privacy violations is limited since they do not operate at the desktop level where most of the privacy violations occur. Network Sentinel is able to block these privacy violations by detecting & blocking them at the desktop itself.

What are alternative uses for this technology?

Network Sentinel is built using flexible technologies that can be applied in different areas. Several applications for this technology have been outlined below:

Application access control

The product could provide network access control capabilities. This would enable a set of functions allowing central administrative discovery and control of applications at the individual client level. This would require support for MD5 signatures to be added on the server side as well as a system for creating and maintaining these signatures.

Expand beyond HTTP

Network Sentinel could be extended to examine other protocols such as NetBIOS in addition to the HTTP protocol. Features such as blocking based on addresses could be extended to these protocols.

Logging

The product could be enhanced to perform logging for legislative compliance. The logging feature could be based on IP addresses or could be integrated with Application access control to log traffic from certain applications only.

Scanning for tags

A new product could be created to scan documents for tags and allow access based on permissions. This would involve the creation of a file system driver that would intercept all calls to access files. In combination with the existing network layer, it would enable an organization to exercise more control over data and documents.

Transparent encryption (Virtual VPN)

This feature would allow all communication between Network Sentinel enabled clients to be encrypted by default. This would allow secure communications without having to change the applications that run on the desktop.

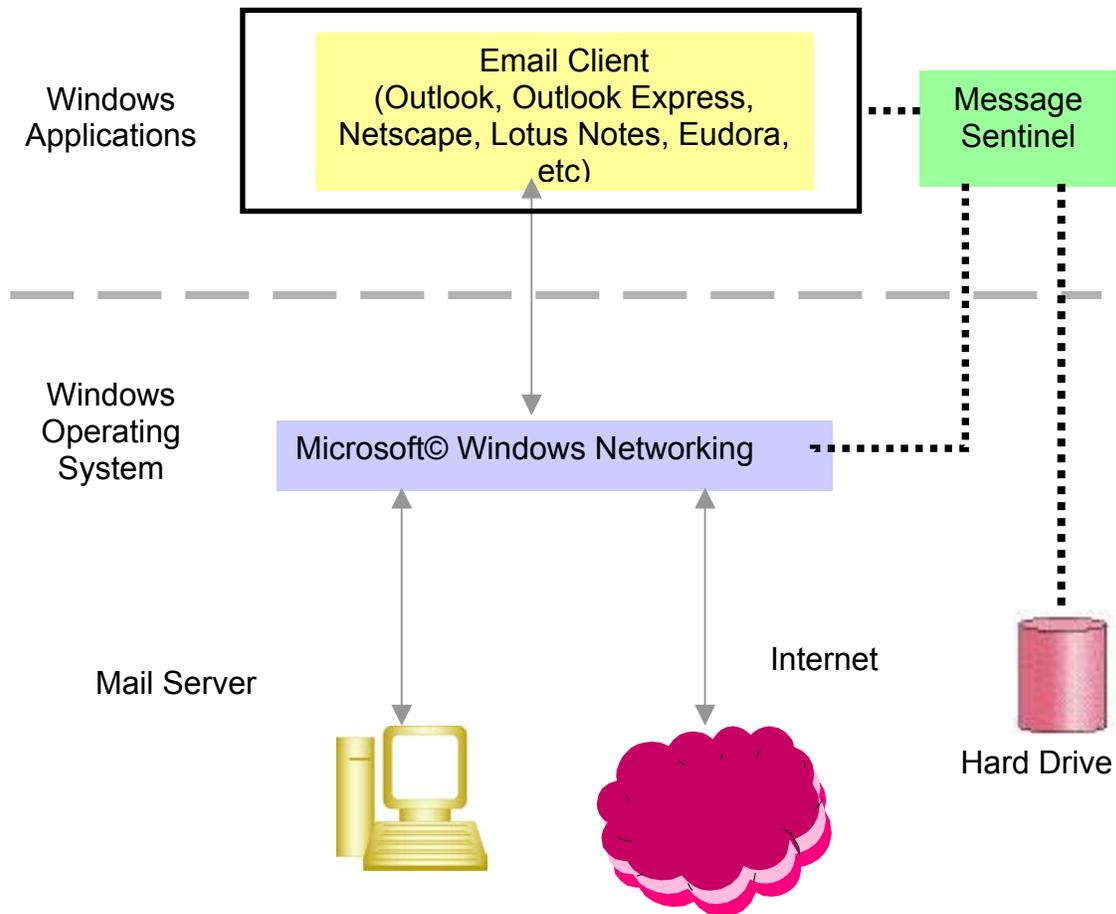


Figure 4: Message Sentinel architecture

Message Sentinel

What is Message Sentinel?

Message Sentinel is a program focused on protecting a user's privacy while checking and viewing email. Message Sentinel monitors email traffic in real time and alerts the user whenever a potential privacy violation is detected. The product offers:

- Real time email scanning, threat detection and alert system.
- Privacy protection via access blocking or text message viewer.
- Simple interface for easy control and configuration.
- POP3 and IMAP email protocol support.
- Support for the popular email clients including Microsoft® Outlook, Microsoft® Outlook Express, Netscape Messenger, Mulberry, Eudora, and Lotus Notes.
- The program works on Windows 98, Windows ME, Windows NT 4.0 Service Pack 6, Windows 2000 & Windows XP.

How is it used?

Message Sentinel ensures the user's privacy through several levels of protection. Message Sentinel is an unobtrusive application that operates in the background to automatically scan all new emails for privacy violations while the user is downloading them. Whenever a potential privacy threat is detected in an email, Message Sentinel will warn the user of the existence of the threat.

After initial threat detection, Message Sentinel provides several options to manage the threat. The user has the option to delete the email, open it in a regular text mode, or have Message Sentinel block the email application from making an HTML request. Although a default set of configuration settings is provided, the product also allows custom configuration settings to allow trusted domains such as newsgroups or mailing lists. Message Sentinel users are in total control of their privacy through each of these steps.

How does it work?

As shown in Figure 4 below, Message Sentinel works with the Microsoft® Windows networking layer to analyze email traffic. The architecture of Message Sentinel is similar to the Personal Sentinel architecture. This architecture allows Message Sentinel access to network traffic, files on the hard drive, and information about applications that access the network. Message Sentinel monitors email traffic that is using either POP3 or IMAP email protocols. This protocol based monitoring allows Message Sentinel to work without any configuration of the email client.

Message Sentinel scans the new email messages being downloaded and identifies potential threats in them. Once a threat is identified, Message Sentinel will alert the user of the threat. Message Sentinel can identify supported email applications on the user's machine and block those applications from accessing the Internet.

How does it differ from other products/solutions?

Message Sentinel works in conjunction with anti-virus products and provides users with additional privacy protection. Whereas anti-virus products are focused on eliminating malicious viruses, they are unable to provide privacy protection.

Unlike SPAM filtering products, Message Sentinel does not obstruct any of the user's email from being downloaded. Message Sentinel scans the email being downloaded and gives a warning to the user after the download is finished. Users can safely download their email because Message Sentinel prevents any HTML embedded content in the email from leaking information. Since Message Sentinel is a client-based product, it does not put any additional load on the email server.

What are alternative uses for this technology?

Message Sentinel is built on a robust and versatile architecture that allows easy expansion or modification to introduce new features and functionalities.

Enterprise email application

Currently, Message Sentinel works independently of the email application. Integration to an email application will unlock new usage and features for the product. While the current version of Message Sentinel does not block incoming email, the product could be easily adapted to filter email messages or to identify certain keywords in messages.

Corporate product

Message Sentinel functionality could be offered along with Network Sentinel to monitor and block privacy violations from email. This would allow companies to protect their email users transparently and unobtrusively using a single point of administration.

Site Sentinel

What is Site Sentinel?

Site Sentinel is a tool that remotely audits a website's privacy performance. It accomplishes this by crawling through the specified website, analyzing the results, and producing reports concerning potential privacy violations.

The Site Sentinel system evaluates the privacy performance of a target website, makes it accessible to non-technical auditors and executives, and then automates it into a recurring process.

It has been designed for use in service companies, but can be easily extended to support a self-service interface. (See "Other Possibilities" below)

Site Sentinel features:

- Data-center operation, running hundreds of simultaneous scans on a recurring, automated basis with little, if any, administration
- A distributed, fault-tolerant crawler engine that actively repairs itself as system failures are detected
- Comprehensive scalability, from data-center all the way down to a laptop, allowing consultants to go behind client firewalls and scan corporate intranets

How is it used?

Although many of the tasks that the system performs are technical and complex, the interface can be used by practically anyone with a vested interest in the privacy characteristics of their websites. That being said, there are three major roles performed which map to three categories of use cases. These are:

- (1) Managing users and permissions;
- (2) Creating and managing scans; and
- (3) Viewing reports

Site Sentinel is a secure system, and as such, requires user management and permission maintenance. In order to protect the resulting reports, an administrator can create, edit, suspend, and remove users and give read and execute permissions on groups of scans to those authorized. The administrator can revoke permissions as well.

In order to crawl a website for privacy performance, a scan must be created. The user can specify that the crawl be generated immediately, or by a specified schedule. The user can monitor a crawl's progress, stop a running crawl, or request additional crawls. The scan parameters and schedule can be modified as well. Scans can be deleted when no longer needed.

Once the crawl has completed, the user can view PDF reports for an executive summary of the privacy performance of the website and HTML reports that provide a consultant enough detail to make specific changes, if desired. Reports are created

that cover low-level privacy issues (such as 3rd-party cookies, web beacons, and data spills), P3P compliance and integration, and legislative compliance.

How does it work?

As shown in Figure 5 below, the Site Sentinel system consists of two major subsystems. These are:

- (1) A distributed crawler engine that simulates a user's journey through a website; and
- (2) A web-based front-end that manages users, creates scans, and delivers reports to the investigator

The crawler engine is composed of several interlocking modules that can be combined together in different quantities at run-time to optimize crawl performance and reliability. This occurs without user intervention or even knowledge, behind the scenes.

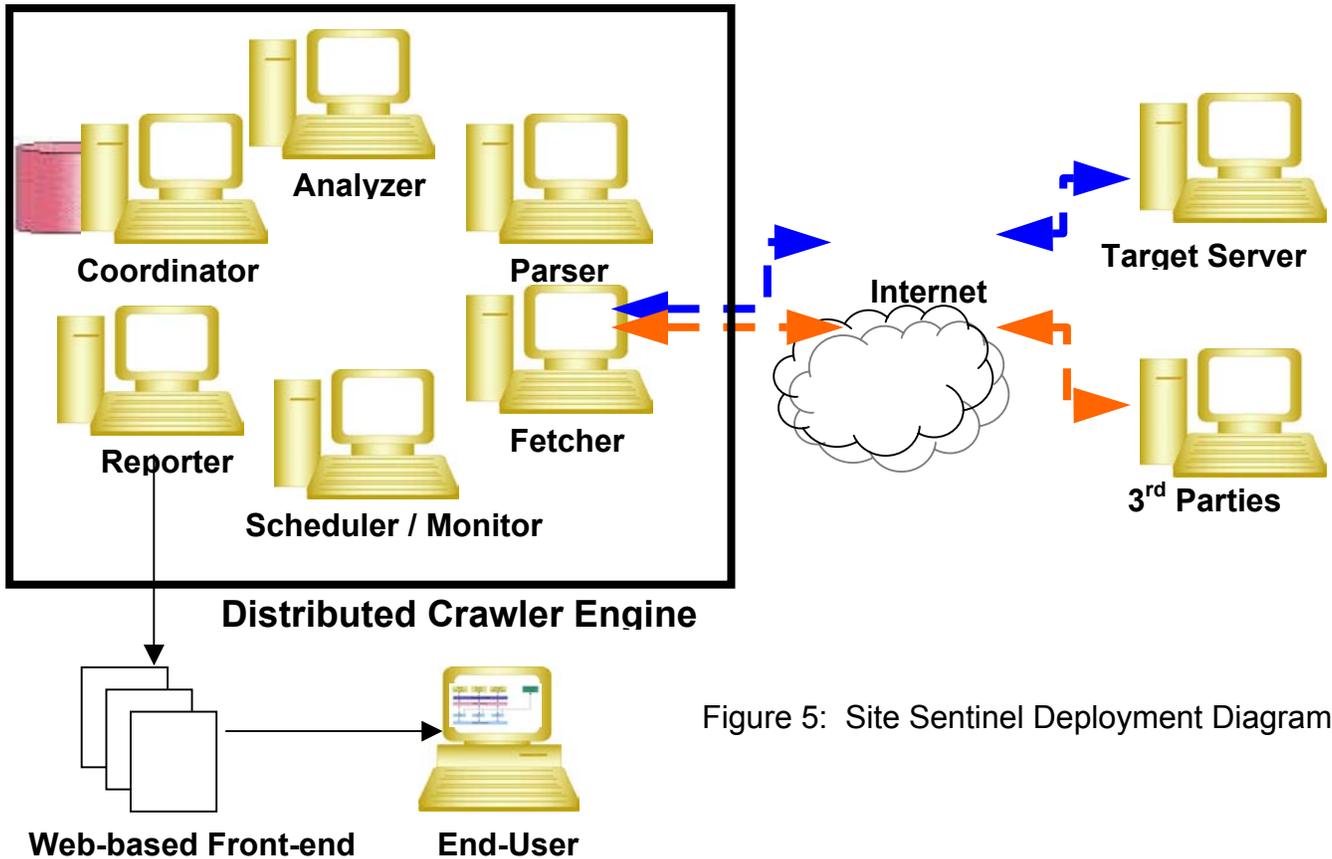


Figure 5: Site Sentinel Deployment Diagram

The front-end consists of a web-based interface that can be accessed by any other machine on the network. From this interface, the user can manage users, scans, and reports.

How does it differ from other products / solutions?

Site Sentinel is the only solution focused on privacy that is built for the data-center. Other products focus mostly on security or website usability, or are designed for use on the desktop as a stand-alone application.

In the security space, firewalls are effective means of preventing unauthorized access to corporate web servers, but are useless in filtering for potential privacy violations. Because privacy violations begin at the desktop, they are not prevented by firewalls protecting the website visited.

Many products exist that scan websites for usability and correctness issues. These utilities produce reports that evaluate the effectiveness and performance of a corporation's website as a marketing and/or e-commerce tool. However, few offer privacy functionality. Those that do, offer it as a plug-in that provides a limited subset of Site Sentinel's features.

Another product offers website scanning functionality in the form of a desktop application. This format precludes the ability to schedule and automate recurring scans, and to provide multiple users appropriate access to the results. It also limits the performance of the system by tying it to a single, PC workstation.

What are alternative uses for this technology?

The product as described above represents a valuable technical asset for a services company. As a general-purpose technology, Site Sentinel represents additional value. Much of the distributed crawler framework can be repurposed to support other related services. Some possibilities include:

Website performance and standards compliance

A variety of content management functions could be realized by adding to the existing product or through the creation of a new product based on the core Site Sentinel technology. This would include things like availability analysis, broken link reporting, embedded objects, etc.

Corporate research, marketing, and other statistical data

The crawler could be repurposed to search for organize and report on a variety of corporate information. The tool could assist in building customer and competitor lists, gathering pricing information, and compiling benchmarking statistics on marketing methods and expenditures. One could even use the tool to measure the success of a consumer marketing campaign by crawling web logs ("blogs") to look for references to a particular product or service.

Crawling alternative protocols

With modification, the technology could be repurposed to crawl alternative protocols. This would be useful for identifying and categorizing content found on networks other than those accessed via browser.