What are Web Bugs?

Privacy threats have been created that are specific to the tools and techniques of the Internet. One particularly widespread and damaging form of Internet privacy threat is the web bug, which is a third party tracking device used to monitor and record the activity of an online user. Web bugs follow online users and may report their every move back to the web bug host, opening a new window of surveillance on a traditionally private sphere of communications. To date, Intelytics has identified and categorized four different types of web bugs.

Types of Web Bugs:

Type 1 Web Bug

Type 1 is the "classic" web bug, based entirely on the steps taken in the parsing of HTML.

Type 1 web bugs were originally designed to help match site page requests with a particular user session. The implementation is an object, typically an image, which is fetched by a browser via an HTTP GET query, with additional information sometimes included in the request that is relative to the particular page. In the HTTP response, this object sets a cookie on the user's machine that is sent back along with all subsequent HTTP requests to the same domain. For the web bugs that concern us, the foreign object is on a third party server.

The dominant form of a Type 1 web bug is the image tag, which is typically a 1x1 transparent GIF image. In principle, a Type 1 web bug can be any image in any format that is sufficiently unobtrusive. The source of the image tag contains the filename and an additional query string with information about the page. The cookie sent and received by the HTTP request for the image identifies the user session, and possibly the user. This form of web bug requires cooperation of the website because it resides in the HTML created, stored, and sent by the website to the user. This also requires passive cooperation of the user because the user must enable their browser to accept and agree to send cookies. However, as this is the default setting for browsers, active action on the part of the user may be required to avoid this situation.

The image tag is the most common, but not the only manner in which Type 1 web bugs can be created. Web bugs can also be created in body, link, table, and layer tags, among others.

Type 2 Web Bug

The second major type of web bug is a Type 2, or network resident, web bug. This type of bug lies at the operating system level, infecting a user's computer via an executable application that has access to implant the web bug on the system. The application can monitor network traffic, cache the information, and then relay it to a central repository in batches. The site that is being monitored is not cooperative because it has no knowledge of or control over the monitoring. Type 2 web bugs fall into three categories, namely Types 2a, 2b, and 2c.

Type 2a

Type 2a web bugs require the explicit cooperation, but not knowledge, of the user. The user must perform some action such as executing a program or installing an ActiveX component. However, the user is not normally aware that this action allows for the installation of a web bug on their machine. This may be thought of as a Trojan horse because the monitoring and reporting function is not a stated or known purpose of the software the user executed.

Type 2b

Type 2b web bugs are perhaps the most insidious of all of the web bugs because they require neither the cooperation of the user nor the website being monitored to be

effective. Through only normal browsing, these web bugs can become installed on a user's system if, in the course of browsing, the user unknowingly opens an executable application.

Type 2c

Type 2c web bugs require the cooperation of the user, as well as inform the user of their operation. The activity of the web bug is a stated functionality of the software that the user is asked to install. In behavior, these are identical to Type 2a web bugs, but differ in the key point that they inform the user.

Type 3 Web Bug

The third type of web bug is the browser, or application resident, web bug. These web bugs are installed into and directly affect the Web browser or other application used to generate and receive HTTP requests. The fundamental difference between Type 3 and Type 2 web bugs is that the latter are installed on the user's operating system. Like Type 2 web bugs, Type 3 web bugs result from something that the user has downloaded in the course of their Web browsing, they may not require the cooperation of the site that is being monitored to be effective, and they store their information and relay it in batches to a central place. Type 3 web bugs are differentiated into three classes based on the user's knowledge and cooperation, namely Types 3a, 3b, and 3c.

Type 3a

Type 3a web bugs require the cooperation, but not knowledge of the user. An example of a Type 3a web bug would be a browser plug-in that monitors and reports a user's browsing information.

Type 3b

Type 3b web bugs require neither the cooperation nor the knowledge of the user. An example of a Type 3b web bug would be JavaScript that exists in part of a frameset or another window that collects information about browsing. Another example would be using JavaScript to implant a Type 1 web bug or to set a cookie circumventing browser controls on whether cookies can be set. Please note the second example does require cooperation of the originating site.

Type 3c

Type 3c web bugs require the cooperation of the user, but give full disclosure. That is, this activity of the web bug is a stated functionality of the application that the user downloads. A Type 3c web bug is identical to a Type 3a web bug in functionality, but discloses to the user its web bug nature.

Type 4 Web Bug

The Type 4 web bugs are document-tracking devices that use HTML-enhanced e-mail as their delivery mechanism. Searching the Internet with a Web browser is not the only way an online user can access HTML. For example, HTML can be delivered to a user the instant that individual opens an e-mail message that contains instructions to display a graphic file. His or her computer will then automatically fetch the image from a specified location on the Internet. By adding a unique identifying code to those

instructions, a sender can record when a particular recipient retrieves the image, and thus when the e-mail message was opened.

Why Should I Care About the Privacy Threat Posed by Web Bugs?

Although users may like to think so, they are not anonymous when they surf the Web. Privacy concerns are an issue for a vast majority of the nearly 350 million connected users of the Internet. There is mounting concern that the once freewheeling world of the Web is being transformed into Orwellian cyberspace.

According to a study conducted by the Boston Consulting Group, over 70% of 9,300 users responded in an online survey that they were "more concerned about privacy on the Internet" than they were about privacy threats from any other medium. When a web bug is encountered by an online user, the following information can be sent to the server on which the monitoring website resides:

- Demographic and personally identifiable information about the user
- The user's operating system
- Previously set cookie values
- The IP address of the computer that fetched the web bug
- The time at which the web bug was viewed
- The type of browser that fetched the web bug image
- The URL of the page on which the web bug is located
- The URL of the web bug image
- The user's Web surfing history

Online advertising networks that pay to place advertisements on websites include a link from a host's webpage to the advertising network's URL. When a user navigates to a webpage that contains an advertisement, web bugs can send cookies to the user's system not only from the requested website, but also from the online ad network involved. The ad network can then retrieve the cookie from the user's system and use the information that it acquires about that user in marketing advertisements targeted to the specific buying habits and personal tastes of that user. This allows the ad network to maximize their advertising dollar. For example, the user's personal profile, which is stored in a database server belonging to the ad network, can be used to determine what banner add to show to that particular user. Web bugs can also be used to transfer demographic and personally identifiable information about the visitors of an e-Business website to an ad network.

An ad network can also acquire information about a user from cookies retrieved from other websites the user has visited if the network advertises on those other sites. This search string information can be combined and cross-referenced to construct, broaden, and refine the marketing profile of the user's online activities. Furthermore, law enforcement agencies, insurance companies, employers, and other third parties could also pay to consult the linked databases. In doing so, they would only require a user's e-mail address to access the record of an individual's online behavior.

Web bugs provide a mechanism for the independent accounting of how many users have navigated to a particular website, as well as have the ability to collect statistical data about Web browser usage at different places in the Internet. This information is typically used in aggregate to determine the type and format of content to place on a website to maximize viewers. Furthermore, the information security threat posed by web bugs is not simply a consumer issue, as Intelytics has identified two types of web bugs that can remain resident on user systems and track activities and data behind corporate firewalls.

Type 4 web bugs that use e-mail as a delivery mechanism pose an additional privacy threat to online users. These web bugs can be used to find out if a particular e-mail message has

been read, and if so, when that message was read. They can be used to test if an e-mail address is valid, if someone is using an e-mail reader application that understands HTML-enhanced messages, and if a user has JavaScript, Java, and ActiveX capability in their e-mail reader. Within an organization, a web bug can provide a gauge as to how often a message is being forwarded and read. Type 4 web bugs are particularly valuable to advertising agencies that send out "junk" e-mail because they allow them to determine how many people have viewed the same e-mail message in a marketing campaign. People that do not view a message can be removed from the list for future mailings. Type 4 web bugs can also be used to track how often press releases are read by reporters and if they are passed to people within or outside of their organization, to detect potential newsletter copyright infringement, and to count the number of times an ad is viewed in a Usenet newsgroup message.

If you are a consumer in the global e-market, you are likely concerned with information privacy. When you provide biographic or personal financial information to an e-Business, you probably expect that information will be handled confidentially and solely by the company with which you conduct business. An e-Business is only legally required to handle personally identifiable information and other consumer data that they collect online in accordance with the guidelines disclosed in their privacy policy. Privacy policies are legal user agreements that detail how an e-Business handles your personal information upon receipt. By using the company's website, you consent automatically to the collection and use of this information as detailed in their privacy policy. However, information may be collected immediately when you navigate to a website before you even have the chance to link to and read the privacy policy. Topics considered in typical privacy policies include information collection and use, information sharing and disclosure, cookies, security, ability of customers to edit or delete collected information, and third party websites.

Web bugs pose a direct threat to the information privacy of the online consumer because they provide third parties, and perhaps even the company website itself, with a means of surreptitiously collecting personal information beyond the regulations outlined in the privacy policy of an e-Business.

Where can I learn more about web bugs and Internet privacy issues?

For detailed information about how online privacy and security threats may affect you, please visit http://www.intelytics.com.

What is Intelytics Personal Sentinel Pro?

Intelytics Personal Sentinel Pro is downloadable software that protects your privacy by monitoring and displaying Internet surfing activity for privacy threats, allowing you to filter undesirable content, online advertisements, and Internet cookies, updating your system with the latest privacy threat patterns, and removing privacy threats from your system. Personal Sentinel Pro also offers security protection through a personal firewall that controls Internet and network connections from your computer and alerts you to attempted connections and potential intrusions.

Personal Sentinel Pro provides the complete solution for Internet users and online consumers interested in managing their own Internet privacy and security concerns.

How does Personal Sentinel protect my privacy?

Personal Sentinel Pro protects your privacy and security by:

- Filtering undesirable content, online advertisements, and Internet cookies
- Graphically displaying your real time privacy risk
- Removing unfiltered privacy threats
- Reporting on your Internet traffic
- Updating your system with the latest privacy threat patterns
- Controlling Internet and network connections to and from your computer
- Alerting you to attempted connections

The Information Center

Access the Information Center by right clicking on the Personal Sentinel icon in the taskbar and selecting **Show Information Center**.

The Information Center displays a graphical representation of your real time privacy risk, as well as a per session listing of the number of:

- Web bugs encountered
- Internet requests blocked
- Cookies residing on your system
- Cookies blocked

Click **Menu** to:

- View the Information Center in Float On mode
- Access the Control Center
- Clean web bugs
- Exit the Information Center
- Access the help files
- Access information about Personal Sentinel

Click **Clean Bugs** to update your system with the latest privacy threat patterns and remove all known privacy threats.

Float On/Float Off

By clicking **Float On**, the Information Center will shrink and display only the number of web bugs encountered, the number of cookies residing on your system, and the Privacy Risk Meter. To restore the Information Center, right-click on the interface and select **Float Off**.

The Privacy Risk Meter

Found on the left side of the Information Center interface, the Privacy Risk Meter provides a real time indication of the privacy threat level to which your system is exposed as you navigate the Web.

The Internet Requests Section

The Internet Requests section displays the number of web bugs encountered and Internet requests blocked by Personal Sentinel in the current session.

The Cookies Section

The Cookies section displays the number of cookies residing on your system, as well as the number of cookies blocked by Personal Sentinel in the current session.

The Control Center

Access the Control Center by right clicking on the Personal Sentinel icon in the taskbar and selecting **Show Control Center**. From the Control Center, you can view your privacy threat information and make changes to your user preferences.

General Tab

Available in Basic and Advanced Modes, the General tab allows you to:

- Enable cookie filtering
- Enable content filtering
- Switch between Basic and Advanced Modes
- Enable privacy protection

Enable Cookie Filtering

Select **Enable Cookie Filtering** to:

- Add cookies to the cookie filter
- Delete cookies
- View cookies
- View cookies blocked by Personal Sentinel

Enable Content Filtering

Select **Enable Content Filtering** to view and block unwanted content and online advertisements from the domains in the Content Filter list. Personal Sentinel is supplied with a list of content and advertisement sources to block. In Advanced Mode, you may add your own desired domains, subdomains, or subdirectory names to the Content Filter list.

Advanced Mode

Select **Advanced Mode** to access the advanced features of Personal Sentinel including all functions in the Cookie Filter, Content Filter, History, and Filter Manager tabs. Press **Apply** when complete.

Operating in Advanced Mode allows you to:

- Conduct advanced filter management
- Enable and edit the Cookie Filter
- Personalize the Content Filter
- View detailed reporting and history
- View and edit your personal firewall

If you do not select the Advanced Mode option, you will operate in Basic Mode. In Basic Mode, you will only have access to the General tab, which enables Personal Sentinel to filter content and advertisements, as well as protect your privacy, using the default settings and filter lists. You will be unable to configure Personal Sentinel while in Basic Mode.

Enable Privacy Protection

Select **Enable Privacy Protection** to block or mask outgoing third party cookies. Privacy

Protection is available in Basic and Advanced Modes.

The Cookie Filter Tab

Available only in Advanced Mode, the Cookie Filter tab allows you to:

- View cookies
- Delete cookies
- Add cookies to the Cookie Filter
- View the Cookie Filter
- View cookies blocked by Personal Sentinel

View Current Cookies

Click **View Current Cookies** to view all cookies on your system. Available information includes:

- Cookie domain
- Browser used
- Cookie name
- Information contained within each cookie (e.g. password or username),
- Cookie path
- Whether or not the cookie is secure
- Cookie expiration date

In addition to viewing this information, you can also remove cookies from your system by placing a checkmark next to the desired cookie and clicking **Delete Selected Cookies**.

To remove cookies and add them to the Cookie Filter List, click **Delete Cookies and Add to Filter** after making your selections.

To remove all cookies from your system or remove all cookies and add them to your Cookie Filter list, click **Select All** and then click **Delete Selected Cookies** or **Delete Cookies and Add to Filter**, respectively.

To update the list of entries, click the Refresh icon.

View Cookie Filter

Click **View Cookie Filter** to view all the cookies in the Cookie Filter list including those you have added.

In addition to viewing the information, you can also remove cookies from the Cookie Filter list by placing a checkmark next to the desired cookie and clicking **Delete Selected**.

To update the list of entries, click the Refresh icon.

View Blocked Cookies

Click **View Blocked Cookies** to view the last 50 third party cookies blocked by Personal Sentinel. You can view the following information on each cookie:

- Cookie domain

- Cookie host
- Request referrer
- Object being requested
- Actual cookie string

To update the list of entries, click the Refresh icon.

The Content Filter Tab

Available only in Advanced Mode, the Content Filter tab allows you to:

- View the Content Filter
- Add entries to the Content Filter
- Delete entries from the Content Filter
- View content blocked by Personal Sentinel

View Content Filter

Click on **View Content Filter** to view all the domains in the Content Filter list.

To add entries to the Content Filter list, enter the desired domains, subdomains, or subdirectory names in the space provided inside the Add to Content Filter box and click **Add**. Click **Apply** to submit your changes. Note: To filter based on subdomains, subdirectories, or specific topics, you must define the data with wild cards (*) so that the filter will screen based on a collection of the pre-defined characters. For example, a filter of *xxx* would filter out all URLs containing the phrase "xxx." A filter of ad* would filter out all URLs beginning with the phrase "ad." Simply entering "xxx" or "ad" without the wild cards will not work, as no URL is solely comprised of the phrase "xxx" or "ad."

Remove entries from the Content Filter list by placing a checkmark next to the desired entry and clicking **Delete Selected**.

To update the list of entries, click the Refresh icon.

View Blocked Content

Click the **View Blocked Content** button to view the last 50 requests blocked by Personal Sentinel. You can view the following information on each request:

- Content domain
- Application used
- Request host
- Request referrer
- Object being requested
- Actual cookie string (if a cookie is within the request)

To update the list of entries, click the Refresh icon.

The History Tab

Available only in Advanced Mode, use the History tab to view and edit your session's 200 most recent HTTP requests. You can view the following information for each request:

- Domain name
- Application used
- Request host
- Request referrer
- Object being requested
- Actual cookie string (if a cookie is within the request)

To add an entry from your history to the Content Filter list, place a checkmark next to the desired domain and click **Add to Content Filter**.

To add an entry from your history to the Cookie Filter list, place a checkmark next to the desired domain and click **Add to Cookie Filter**.

To update the list of entries, click the Refresh icon.

The Filter Manager Tab

Available only in Advanced Mode, use the Filter Manager tab to import, export, and merge content and cookie filter lists.

To manage your Cookie Filter list, select **Manage Cookie Filter**.

To manage your Content Filter list, select **Manage Content Filter**.

Import Cookie/Content Filter

To import a cookie or content filter list, click **Import Cookie Filter** or **Import Content Filter** and select the desired list, clicking **Open** when complete.

Export Cookie/Content Filter

To export a cookie or content filter list, click **Export Cookie Filter** or **Export Content Filter** and select the desired list, clicking **Save** when complete.

Merge Cookie/Content Filter

To merge two or more content or cookie filter lists, click **Merge Cookie Filter** or **Merge Content Filter** and select the desired lists, clicking **Open** when complete.

Firewall Tab

Available only in Advanced Mode, use the Firewall tab to view and edit the Internet and network connections made to and from your computer.

For each connection, you can view the following information:

- Application used
- Application description
- Application path
- Level of permission for each application

To make changes to the permission levels associated with each application, click the application and select the desired permission level. For each application, you can assign

the following permission levels: “Always allow program to connect”, “Always ask before allowing connection”, and “Never allow program to connect”. The default permission level is “Always ask before allowing connection”.

To update the list of entries, click the **Refresh** icon.

Exiting Personal Sentinel

You can exit Personal Sentinel Pro by right clicking on the Personal Sentinel Pro icon in the taskbar and selecting **Exit**.

Uninstallation Instructions:

To uninstall Personal Sentinel Pro, select **Uninstall Personal Sentinel** in the Personal Sentinel folder located in **Start** > **Programs** > **Intelytics** > **Personal Sentinel**. Click **Yes** when asked if you are sure you want to remove Personal Sentinel Pro and all of its components.

Frequently Asked Questions

How can I limit the collection of personally identifiable information by third party cookies?
Basic Mode blocks third party requests to your system using a Cookie Filter list automatically supplied and updated by your IT administrator. You do not need to make further changes in Basic Mode to block third party requests.

Use Advanced Mode to make changes to the Cookie Filter list including adding and deleting cookies. To begin, set Personal Sentinel to Advanced Mode by placing a checkmark in the box next to Advanced Mode in the General tab, clicking Apply when complete. Select Enable Cookie Filtering by placing a checkmark in its box, clicking Apply when complete. You can now make all changes from the Cookie Filter tab. Read "The Cookie Filter Tab" section in these help files for information on viewing and editing the Cookie Filter list.

How do I prevent my system from displaying unwanted content?
Personal Sentinel Basic Mode blocks content requests to your system using a default Content Filter list. You do not need to make further changes in Basic Mode to block third party requests.

Use Advanced Mode to make changes to the default Content Filter list including adding and deleting entries. To begin, set Personal Sentinel to Advanced Mode by placing a checkmark in the box next to **Advanced Mode** in the General tab, clicking **Apply** when complete. You can now make all changes from the Content Filter tab. Read the "The Content Filter Tab" section in these help files for information on viewing and editing the Content Filter list.

How do I clean web bugs from my system?
To remove all known threats from your system, click **Clean Bugs** inside the Information Center.

How do I receive the latest privacy threat pattern updates?
Click Clean Bugs inside the Information Center to receive the latest pattern updates.

What is a Content Filter list?
The Content Filter list is the list of domains, subdomains, and subdirectories blocked by Personal Sentinel. It includes the list supplied by your IT administrator and any entries made by the user.

What is a Cookie Filter list?
The Cookie Filter list is the list of cookies blocked by Personal Sentinel. It includes the list supplied by your IT administrator and any entries made by the user.

What is the Control Center?
The Control Center provides the user with a view of all privacy threats and allows the user to configure Personal Sentinel.

How do I access the Control Center?
Access the Control Center by right clicking on the Personal Sentinel icon in the taskbar and selecting **Show Control Center**

What is the Information Center?
The Information Center presents privacy threat information to the user in a graphical format.

How do I access the Information Center?
Access the Information Center by right clicking on the Personal Sentinel icon in the taskbar and selecting **Show Information Center**.

What is the Privacy Risk Meter?
Found in the Information Center, the Privacy Risk Meter provides a real time indication of the privacy threats to your system encounters in the current session.

What is the Internet Requests section?
Found in the Information Center, the Internet Requests section displays the number of web bugs encountered and requests blocked by Personal Sentinel in the current session.

What is the Cookies section?

Found in the Information Center, the Cookies section displays the number of cookies residing on your system, as well as the number of cookies blocked by Personal Sentinel in the current session.

What are wild cards?
Symbols used to represent any value when selecting specific files. The asterisk (*) represents any collection of characters, and the question mark (?) represents one single character. (e.g. *.doc would be interpreted by the computer to mean all files ending with the .doc extension)

What does it mean to Enable Privacy Protection?
Enabling Privacy Protection blocks or masks all outgoing requests from third party cookies.

What is the difference between Basic and Advanced Modes?
While in Basic Mode, the user will be unable to configure Personal Sentinel and will only have access to the General tab.

Advanced Mode allows the user to access the advanced features of Personal Sentinel including all functions in the General, Cookie Filter, Content Filter, History, and Filter Manager tabs.

What is the difference between Floating On Mode and Regular or Floating Off Mode for the Information Center?
Floating Off or Regular Mode allows the user to view all the features of the Information Center including the Privacy Risk Meter, the number of cookies, the number of privacy threats, the number of cookies blocked or masked, and the number of HTTP requests blocked.

Floating On Mode reduces the size of the Information Center and displays only the Privacy Risk Meter, the number of cookies residing on your system, and the number of web bugs encountered.

How do I acquire new content and cookie filter lists?
You can find and download filter lists from many online privacy education websites.

How do I delete cookies from my system?
You must operate Personal Sentinel in Advanced Mode to delete cookies from your system.

To remove a cookie from your system, click on the **Cookie Filter** tab and then select **View Current Cookies**. To delete a specific cookie from your system, place a checkmark next to the desired cookie(s) and click **Delete Selected Cookies**.

How can I add a cookie to my Cookie Filter list?
You must operate Personal Sentinel in Advanced Mode to add cookies to your system.

To add a cookie to your Cookie Filter list, click on the **Cookie Filter** tab and then **View Current Cookies**. To delete a specific cookie from your system and block future requests, place a checkmark next to the desired cookie(s) and click **Delete Cookies and Add to Filter**.

How can I delete cookies from my Cookie Filter list?
You must operate Personal Sentinel in Advanced Mode to delete cookies from your Cookie Filter list.

To make changes to your Cookie Filter list, click on the **Cookie Filter** tab and then **View Cookie Filter**. To delete a specific cookie from the Cookie Filter list, place a checkmark next to the desired cookie(s) and click **Delete Selected Cookies**.

How can I view which cookies are being blocked by Personal Sentinel?
You must operate Personal Sentinel in Advanced Mode to view the cookies blocked by Personal Sentinel.

To view the cookies blocked by Personal Sentinel, click on the **Cookie Filter** tab and then **View Blocked Cookies**.

How can I add an entry to my Content Filter list?
You must operate Personal Sentinel in Advanced Mode to add entries to your Content Filter list.

To add an entry to your Content Filter list, click on the **Content Filter** tab and then **View Content Filter**. Enter the desired domains, subdomains, or subdirectory name in the space provided inside the Add to Content Filter box, clicking **Add** when complete. Click **Apply** to submit your changes.

How can I delete entries from my Content Filter list?
You must operate Personal Sentinel in Advanced Mode to delete entries from your Content Filter list.

To make changes to your Content Filter list, click on the **Content Filter** tab. Once there, press **View Content Filter**. To delete a specific entry from the Content Filter list, place a checkmark next to the desired entry and click **Delete Selected**.

How can I view what content is blocked by Personal Sentinel?
You must operate Personal Sentinel in Advanced Mode to view the content blocked by Personal Sentinel.

To view the content blocked by Personal Sentinel, click on the **Content Filter** tab and then **View Blocked Content**.

What is a cookie domain?
The cookie domain is the Internet address from where the cookie originated (e.g. http://www.cookiesareus.com)

What is a cookie name?
The cookie name is the distinct word or phrase used to designate the cookie.

What is the cookie path?
The cookie path is the exact location within the domain where the cookie originated. (e.g. /cookie/home)

What does the expiration date mean?
The expiration date is the date and time the cookie will stop functioning.

Who is the cookie host?
The cookie host is the original source of the cookie.

Who is the request referrer?
The request referrer is the entity that directs the request to a different location, possibly a third party.

What is a cookie string?
A cookie string is a set of alphanumeric characters that comprise the cookie (e.g. a login name)

What does it mean if a cookie is secure?
A secure cookie is received through a secure connection or SSL.

What platforms are compatible with Personal Sentinel?
Windows 98, ME, NT 4.0 SP 4.0 and above, 2000.

What is a personal firewall?
A personal firewall is a software application used to protect a single Internet-connected computer from intruders. Personal firewalls work in the background to protect the integrity of your system from malicious attacks. They control Internet and network connections to and from your computer and alert you to attempted connections and potential intrusions. The Personal Sentinel firewall works by allowing you control over the applications that access the Internet to either send or receive information.

How do I make changes to my personal firewall?
Within Personal Sentinel Pro, you can make changes to the permission levels within your personal firewall by clicking on the Firewall tab within the Control Center. Select the application to which you would like to make the change and choose the desired permission level.

What is the application path?
The application path is the route to a specific application on a disk. The full path to a file will include the drive, folder, and file name. For example, the application path "C:\Program Files\ABCProgram.exe" is the route to the application "ABCProgram" within the "Program Files" folder on the hard disk "C:". In this example, "C:" is the drive, "Program Files" is the folder, and "ABCProgram.exe" is the file.

What are the permission levels I can assign to connecting applications?
For each application, you can assign the following permission levels: "Always allow program to connect", "Always ask before allowing connection", and "Never allow program to connect".

About Personal Sentinel

Personal Sentinel Pro is a licensed product of Intelytics Inc., an iventurelab partner company specializing in software and services for Internet security, privacy, intelligence gathering, and data mining. Whether you are engaged in e-Commerce, financial services, or healthcare, or you are concerned with international and children's privacy initiatives, Intelytics has the right solution to meet your needs. Our comprehensive array of software platforms and expert professional services can provide you with protection necessary to navigate safely through the increasingly unsafe channels of the connected world.

For more information, please contact:

Intelytics Inc.
461 Melwood Avenue
Pittsburgh, Pa 15213
info@intelytics.com