

Internet Safety Technical Task Force Technology Submission

PureSight Technologies Ltd. / Ouri Azoulay

<http://www.puresight.com>

ABSTRACT

Accepted industry wisdom estimates that 10% of all registered domains are of adult nature. That places at risk today's generation of children growing up on-line. Furthermore, Chat-Rooms, IM-services and Social Networking sites are the favorite media of today's youngsters, but they may also expose them to online predators, identity thieves, hacker attacks, and cyber stalkers. Finally, many kids use public file-sharing Web sites to download files with no respect to copyright issues and despite the danger of infecting the home computers with viruses, worms or Trojan horses.

PureSight PC is a unique platform provided by *PureSight* that not only filters web-content on the fly but also allows parents to enforce filtering and blocking of IM and P2P applications.

Keywords

Parental Controls
Web/IM-Filtering
P2P Blocking

Functional Goals

- Limit harmful contact between adults and minors
- Limit harmful contact between minors
- Limit/prevent minors from accessing inappropriate content on the Internet
- Limit/prevent minors from creating inappropriate content on the Internet
- Limit the availability of illegal content on the Internet
- Prevent minors from accessing particular sites without parental consent
- Prevent harassment, unwanted solicitation, and bullying of minors on the Internet
- Other – please specify

PROBLEM INTRODUCTION

1. Minors are exposed to offensive material on the Web, including pornography, hate, violence, drugs and more. (70% percent of teens have accidentally come across pornography on the Web. [1])
2. Pedophiles use chat-rooms, IM-services and Social Networking sites to trap minors. (61% of parents say their teens participate in chat-rooms and/or instant messaging. [2])

3. Many youngsters down/upload video clips, movies, or program applications with no respect to copyright issues and despite the danger of infecting the home computers with viruses, worms or Trojan horses.

PureSight PC (PSPC) analyses web-content on the fly and classifies it into content categories such as: adult, dating, gambling and sport. It also integrates a URL Database for content classification to the following categories: chat, social networking, weapons, drugs, hate, violence, blogs and forums

PureSight PC incorporates an ApplicationSDK (AppSDK) monitoring, filtering and blocking IM/P2P applications based on signature recognition and deep data analysis. A strong update mechanism makes sure that the product recognizes new applications and new versions of existing applications.

PSPC is client based, works in a Windows environment, can easily be installed and is difficult to circumvent due to an iron like security mechanism.

PROPOSED SOLUTION

1. PureSight's dynamic Web-filter is based on the following multi-layered structure:

Custom black or white lists of domains and URLs - managed by the guardian locally.

PureSight URL Database –URL found in this DB, will return successfully the relevant category to the PureSight PC application.

URL Classification Cache - contains the results of previous categorizations that have been made by the PureSight ACR (Active Content Recognition) real time dynamic categorization engine.

URL Tagging - classification layer identifying content categories via standard content rating systems such as ICRA and SafeSurf, found in the headers of web pages.

Active Content Recognition (ACR) - dynamic categorization engine made of a set of powerful algorithms able to analyze and classify web content as it is requested, in real-time. ACR inspects every web page request, breaks it up into distinct elements and applies an in-depth analysis to map it accurately and identify the nature of its content.

2. PureSight's AppSDK uses signature recognition and deep data analysis to block/filter IM/P2P applications. The AppSDK is not based on port identification since many IM-services use port 80 or 443 to circumvent IM blocking. Following Filtering modes are available for IM-applications

- a. Keywords – list of inappropriate keywords/phrases managed and maintained by the guardians
- b. Contacts – lists of allowed or forbidden contacts managed and maintained by the guardians
- c. Daily Time Quota – Internet access will be denied, once the quota is exceeded
- d. Single Time Quota – Specific IM-sessions will be disrupted, once the single time quota is reached.

In Addition to the Above Description, Please Address Each of the Following:

- Technical Attributes: PSPC Web-filter maintains 12 content categories (e.g. adult, hate, violence, weapons, chat, etc.), customizable URL black/white lists, reporting system, abuse alert systems with instant email notifications, URL override mechanism, and Internet-Usage time scheduling and time quota. PS AppSDK as an integrated part of the PSPC blocks IM/P2P applications and filters IM applications by keywords, contacts, and time quota. It has monitoring, reporting and logging systems, and supports abuse alerts with instant email notification.
 - Use Cases: PureSight has deployed an OEM strategy as a route to market and consequently its technology is often embedded in other authors' solutions. Two high brand equity examples are those of F-Secure and Computer Associates (CA). Both are authors of Internet Security Suites for home PCs. In both cases, the parental control components of these products are predicated on PureSight's ACR and multilayer classification technology. Both these companies OEM their offerings to others in the industry and if one combines their ISP customers and our own direct accounts, over 100 ISPs use PureSight's engine world wide. Road Runner the 4th largest consumer ISP in the USA is another use case. Road Runner provides PSPC to all its customers for free. Also Israeli ISPs provide PSPC to their subscribers as a service, aggregately dominating over 90% of the child protection market.
 - Strength: PSPC Web-filter recognizes 95% of adult content on the web and hardly suffers from over-blocking none-adult related websites. PS AppSDK blocks most IM/P2P applications and is constantly updated to include the latest applications.
 - Weakness: So far, PSPC makes no age differentiation/verification instead parents can select categories suitable for different ages.
- Testing/Evaluation: PureSight developed testing tools that return classification of websites to estimate the filtering accuracy of all PureSight products. In addition, Throughput, Latency and Requests per Second are constantly tested by PureSight to estimate the performance level of PureSight products.
 - Implementation requirements: PC with OS: Windows 2000 Pro, XP Pro, XP Home, Vista, 533 MHz or later Processor, 128 MB RAM, 10 MB free hard-disk space.
 - Technical standards/ Technology's reliance/ use of law and policy: PSPC supports several regional and international standards; the UK IWF, the Australian ACMA list and the AFA regulation by the French government.
 - Viability US and international markets: PSPC is viable for all markets; since PureSight's dynamic Web-filter is not predicated upon keywords and is therefore language independent. In terms of GUI, PSPC UI is available in 9 languages: English, Spanish, French, German, Italian, Russian, Arabic, Turkish, and Hebrew
 - Effectiveness: PureSight's web-filters achieve an accuracy of approx. 95% when it comes to blocking adult content. PSPC is robust and difficult to circumvent. So far, PureSight knows of no case in which one of its products failed or was successfully tampered by intruders.

EXPERTISE

PureSight develops proprietary next-generation, real-time content classification technologies. PureSight Internet content classification technologies prevent individuals and children from accessing inappropriate Internet content through the Internet and mobile networks. PureSight CSDK/AppSDK technologies can be integrated by hardware and software solution vendors for both mobile and wired Internet surfing. PureSight parental control solution, PureSight PC, is available through OEM partners, major Internet Service Providers and software editors. PureSight products are:

PureSight CSDK for Mobile Solutions - Easily embed PureSight Classification Software Development Kit to hardware or software solutions for the mobile industry

PureSight CSDK - Integrate PureSight's Internet content filtering Classification Software Development Kit for security suites, standalone Parental control applications or home gateway appliances.

PureSight AppSDK - Integrate PureSight's Software Development Kit for IM&P2P protocol classification and deep analysis, monitoring and filtering suitable for security suites, standalone Parental control applications or home gateway appliances.

PureSight PC - Client-based Standalone Parental Control application for Internet Content filtering and IM filtering for home users

COMPANY OVERVIEW

PureSight develops a proprietary next-generation AI based child protection and content classification technology for safe Internet environment.

PureSight's award-winning Child protection solutions are based on a proprietary [Active Content Recognition \(ACR™\)](#) technology and IM&P2p application classifier. PureSight dynamically analyzes and classifies various Internet protocols contents types, in real-time to ensure compliance with safe Internet usage policies while maintaining complete coverage of the constantly changing Internet environment.

PureSight's technology addresses the extended issues of online protected surfing environment for children and Internet content access by providing it technological solutions for security vendors such as consumer security suites and parental control applications, added value services for Internet Service Providers, mobile operators, all **VIA OEM partners** that provide integrated solutions for such markets.

PureSight's products are offered globally. With over 120 ISPs in more than 35 countries an estimated fifteen (15) million children around the world are protected by the PureSight products directly or via PureSight's OEM partners The Company is headquartered in Israel with an additional office in the UK.

Founded in 1998 by Mr. Royi Cohen, (VP R&D), PureSight developed and implemented child protection technologies for the last ten years. PureSight is a privately held company. It is fully self sufficient in terms of all financial parameters. PureSight customer base is spread across wired and mobile Internet markets, with many OEM partners such as CA, F-Secure, Authentium and PC Security Shield in the wired market and Comverse, Adaptive Mobile and Ericsson in the mobile market. Over 120 ISPs, Telco's and Mobile Operators utilize PureSight

products with an estimated subscriber base of 15 million end-users. PureSight is headed for the last 5 years by Mr. Ouri Azoulay (CEO).

BUSINESS MODEL OVERVIEW

PureSight products are available to end users as standalone products or integrated as part of security suites, with prices ranging from \$30 - \$70 per year for the end user. It is also available as a service via ISPs ranging from all costs covers by the ISP to \$5/month/user.

When PureSight licenses its technologies and products to OEM partners, it is usually applying a revenue share based model, in which royalties are paid by the partner to PureSight based on an agreed percentage share. This relatively risk free business model makes it very attractive to start-up companies and new companies entering the child protection market.

PureSight also acknowledges the special needs and budget limitations of non-profit and educational organization and develops special programs with its OEM partners to support these markets.

MORE INFORMATION

For more information on PureSight, please visit <http://www.puresight.com>

For more Information on PureSight's ACR please visit: <http://www.puresight.com/technology/>

CONTACT INFORMATION

Ouri Azoulay, CEO, ouri.a@puresight.com, Tel.: +972-9-7631-934, Fax: +972-9-7637-923, PureSight Technologies Ltd., Atir Yeda St. 15, Kefar Saba, 44201, Israel

REFERENCES

1. Ketchum Global Research Network: Parents' Internet Monitoring Study, February 2005
2. *ibid.*

"I certify that I have read and agree to the terms of the Internet Safety Technical Task Force Intellectual Property Policy." The IP Policy can be found at <http://cyber.law.harvard.edu/research/isttf/ippolicy>.