ContentKeeper Technologies:

Solutions for Education

The ContentKeeper suite of products enables organisations within the Education sector to more effectively Monitor, Manage, Control and Secure Internet resources. It addresses the specific problems faced by most schools, universities, and other educational institutions, including protecting students from inappropriate content, cyber-bullying, harassment and grooming, and legal liability. ContentKeeper Technologies has a commanding market share of the education sector within Australia, and is rapidly expanding its overseas ventures, in a bid to provide the Education sector with technologically superior and cost effective tools and services to address Internet Management and IT Security issues.

"ContentKeeper is proud to be deployed as the market leader of enterprise level Unified Threat Management products with Education sector specific solutions."

ContentKeeper Technologies Pty Ltd

Date: January 2007

Solutions for the Education Sector

Overview

The ContentKeeper Suite of products enables Schools, Universities and other educational organisations to more effectively, Monitor, Manage, Control and Secure Internet resources. It provides technologically superior and cost effective tools and services to address industry-specific Internet Management and IT security issues.

ContentKeeper Technologies

The leader in the provision of technologically superior and cost effective Internet Management and IT Security tools

Company overview

ContentKeeper Technologies is an Australian-based, world-recognised IT Security company that provides and tools and services to allow organisations to Monitor, Manage, Control and Secure Internet usage and access to Internet resources. Its rapidly expanding suite of products allows management to take back control of the ways in which corporate resources are utilised, enabling a more business oriented, safe and cost effective usage of the Internet.

Product overview

ContentKeeper Web

ContentKeeper Web is a management tool that enables organisations to manage employee access to the Internet in a wide variety of ways, and puts the power back into the hands of management to Monitor, Manage and Control access to corporate Internet resources. In doing this, it can greatly reduce any organisation's exposure to issues such as legal expenses, legal claims and damage to company reputation resulting from inappropriate use of the Internet. It uses a patented Closed Loop Collaborative Filtering™ technology, which is ContentKeeper's closed circuit system designed to globally collect, analyse, categorise, edit and distribute site URLs worldwide.

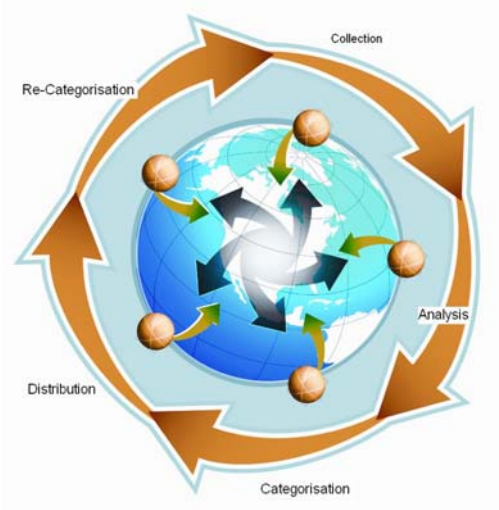

Figure 1 - ContentKeeper's Closed Loop Collaborative Filtering

Advanced Reporting Module (ARM)

ContentKeeper ARM provides comprehensive reporting on Internet and email usage for large and small enterprises, with support for ContentKeeper Web, ContentKeeper Mail, as well as popular firewall and proxy applications, in a simple-to-use interface.

ARM has been designed to efficiently load and analyse Gigabytes of data to a single workstation, providing an enterprise-scale monitoring solution and offering a completely automated reporting function for small and large organisations.

ContentKeeper Anti Virus (CK-AV)

ContentKeeper Anti Virus is a fully automatic, high-performance Anti Virus solution that protects networks from virus threats from the web (HTTP and FTP over HTTP), and email (SMTP), using the world-renowned F-Secure virus definitions.

ContentKeeper Guardian

ContentKeeper Guardian is a unique and effective Internet security solution that acts as a safety net for student PC users at school. ContentKeeper Guardian is currently one of the only solutions in the market offering such a comprehensive way to capture all abuse on PC networks. ContentKeeper Guardian underpins e-safety and behaviour management strategy, demonstrating commitment to the highest duty of care standards.

The problem

Internet management and IT Security issues in the Education sector

Technology is rapidly becoming an important part of everyday life, within the home, schools and businesses. Schools in particular are rapidly embracing new technologies and practices as they bring with them new opportunities and experiences for both teaching staff and pupils.

Information and Communications Technology (ICT) plays a vital role in enhancing the process of learning providing a wealth of information for students and teachers. As technology continues to play an important part in the teaching process the need for regulation to ensure against misuse has been recognized. Most educational institutions have in place an ICT policy that outlines how the schools core values and goals will be underpinned by ICT. The implementation of the ICT policies will prove difficult without adequate education and Internet security tools. ContentKeeper Technologies is dedicated to child safety online and aim to provide a solution to provide children safe access to the wealth of experiences that technology has to offer.

Continuous exposure to Inappropriate and Harmful Content

There are numerous online dangers for children growing up in the information age, children are exposed to inappropriate and harmful content on a daily basis. Content such as pornography, gambling, religious hatred, racism, drugs and other offensive material is far too easily accessed, for which children are often unable to understand and deal with.

Whilst online safety is important it should not detract from the benefits the use of Internet resources can provide. The appropriate level of access must be provided for students and teachers alike. ContentKeeper Technologies enables schools to filter inappropriate content while allowing relevant information to reach students. By providing customized Acceptable Usage Policies the ContentKeeper Web filter enables staff to access a different range of products to students, to ensure a safe environment that facilitates learning.

Cyber Bullying, Harassment and "Grooming"

Incidences of Internet bullying have increasingly come to public attention over the past few years. Online harassment has a serious detrimental effect on the victim, as does bullying within the schoolyard. However, online harassment has the potential to inflict more emotional damage that simple schoolyard bullying as it is potentially more widely distributed, adding to the embarrassment for victims and potentially encouraging more participants in bullying.

Cyber bullying can occur through the use of Instant Messaging (IM), chat rooms, blogs, message boards and web pages. The first national study of cyber bullying was conducted in 2005 by Clemson University researchers in the U.S.A, who found that 25% of girls and 11 % of boys of United States "middle school" age had reportedly been harassed using Internet-related tools in some way within the previous three months, although the actual figures are expected to be far greater[i]. Wiredsafety.org, an organisation dedicated to securing the safety of children online, have estimated around 85% of children aged between 12 and 13 have been somehow victimised by cyber bullies[ii].

Cyber Bullying is described as a combination of the effects of the increased availability of new Internet technology, and too little supervision for the students using it. ContentKeeper Technologies aims to provide schools with a range of products that enables schools to enforce a 'zero tolerance policy' on Internet bullying and harassment that will surpass state and federal requirements.

Chat rooms, blogging and IM also expose children to dangers far worse than bullying. Online grooming, is defined by the Australia Government as, "a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes."[iii] Contact is usually initiated with the intention of establishing a sexual relationship with the child, and worldwide incidences of online grooming are rising.

Legal Liability and Commercial Considerations

On an international scale government bodies have begun to develop and enforce legislation and guidelines to protect online child safety whilst they are at school. School supervisors owe a duty of care to each child to take the appropriate action to protect children online. For example, according to the recently introduced Children's Internet Protection Act in the United States, a school head can be held personally liable if instances of online bullying occur[iv].

In addition to this, there are legal and commercial considerations regarding IPR, copyright theft and the use of unlicensed software. Under certain legislation, school administrative departments can potentially be held liable for student misuse of technology. For example, in 2003 3 recording firms, Festival, Sony, and EMI, brought legal action against three Australian universities for widespread breaches of copyright concerning music files being illegally copied and downloaded.[v]

Insufficient technological and financial resources available

A lack of adequate resources, financial and technical, is a common problem for educational institutions, particularly in the public education system. Many schools suffer a lack of designated and dedicated IT resources and mixed old and new equipment and software. Without adequate finance it is difficult to provide children with all of the benefits technology has to offer.

The implementation of Internet management solutions works to conserve the use of expensive network bandwidth by preventing misuse of resources and the download of large files, often saving money. In addition, by preventing the incidence of malicious attacks on educational networks, IT staff costs of maintaining the technology is reduced.

The solution

A technologically advanced, cost-effective Internet Content Filter

An Internet content filter that provides transparent, accurate and effective filtering of websites is essential to protecting students and staff at educational institutions. The minimum features of such a product should include the following:

Independence from the proxy server and existing firewall and gateway technologies

This is required as it combats the problem of network latency, which can be produced by products that sit inside the proxy server. Additionally, a product which can be utilised in many different network topographies also enables educational institutions to work with their existing infrastructure, reducing the need for costly additional equipment and/or software in order to integrate new solutions.

Dynamic, up-to-date categorisation and filtering

In order to effectively control access to sites with the utmost of accuracy, an Internet content filter should provide dynamic filtering and should continually, automatically, search for new sites in order to address the fact that many millions of new URLs are created each day. Some traditional web filtering software solutions are ineffective because they do not identify new illicit content quickly or dynamically enough. Immediate detection and categorisation of sites based on artificial intelligence technology increases the effectiveness of a filtering solution, thus increasing the protection of students and staff of educational institutions.

This also assists in identifying and combating browsing-based malicious attacks, by (1) restricting access to malicious sites which can cause damage to educational networks and (2) detecting features of new sites that indicate malicious activity. Further, the ability to categorise new sites is essential for compliance with the Acceptable Internet Usage Policies of Educational institutions.

Flexible and adaptable policies

An Internet content filter should provide management and administrators with the power to define the boundaries of their own Internet Usage Policies. The capacity to create custom categories and to decide what actions should be taken to deal with various types of sites, or with individuals or groups

within an organisation, is essential. Various different types of educational institutions will have different filtering requirements, in accordance with their different Acceptable Internet Usage Policies. For example, students may have a different level of access to certain types of content than staff, and vice versa.

An in-depth, forensic reporting tool

The ability to rely on historical data to identify trends or to support an action is essential in both protecting Internet resources, and identifying problems and security threats related to Internet usage. The reporting tool should include:

Ability to generate comprehensive reports in a variety of formats

This should be included as part of an easy-to-use Report Wizard which help managers and administrators to quickly create comprehensive reports.

Enterprise-level

Given the sheer size of many corporate clients, any reporting tool used should be capable of analysing the often massive amounts of data generated by large-scale organisations, as well as the smaller amounts of data generated by smaller firms.

Automated tasking

The ability to schedule large data imports and report generation to occur automatically will both reduce on management overheads, and reduce the amount of time required to generate reports and gain information from Internet activity logs.

A highly accurate, fully automatic Anti Virus solution

An Anti Virus solution that offers virus protection for both web traffic (HTTP, FTP over HTTP) and email traffic (SMTP) is essential to help protect educational networks from malicious attacks, and also helps to identify Internet activity that contributes to these attacks. It should include:

Central installation and management

This significantly reduces on management overheads and provides educational institutions with the ability to identify threats form a centralised location making management of network threats much easier and less time-consuming.

Automatic updates of threat signatures

This is essential to ensure the highest level of virus protection at all times, and also to reduce the impact on the user experience of the solution.

Automatic reports of virus incidents

This is needed to identify trends and also to alert managers to malicious attacks on educational networks to enable immediate action to be taken.

ContentKeeper in the Educational Sector

The specific issues faced by Schools and other Educational Institutions in relation to Internet management and Network Security, as well as general issues faced by all organisations who need to Monitor, Manage, Control and Secure access to their Internet resources, can be addressed by a number of products ContentKeeper Technologies has to offer.

ContentKeeper Web

ContentKeeper Web is a technologically advanced, cost-effective Internet content filter. Using patented Closed Loop Collaborative Filtering™ Technology, designed to collect, analyse, categorise and distribute site URL's worldwide, coupled with AI techniques M.A.R.I.O™ real time blocking and classification technology, ContentKeeper technologies is able to ensure blocking of inappropriate content with complete accuracy. Using ContentKeeper web enables schools to filter out inappropriate content without affecting their educational experience.

ContentKeeper Web and Internet security products provide administration with the power to define the boundaries of their own Internet Usage Policies, in line with their broader ICT policies. The capacity to create custom categories for different users or user groups enable staff to access a different range of sites to students.

ContentKeeper provides automatic control list updates and automatic upgrades. ContentKeeper Web has a simple interface and requires minimal maintenance by the administrator, enabling a more efficient use of school financial resources.

ContentKeeper Anti Virus

The cost of disinfecting computer viruses, spyware and malicious content that have infected school computers drains already scarce school funding. ContentKeeper Anti Virus offers protection for both web traffic (HTTP and FTP over HTTP) and email traffic (SMTP).

To ensure the highest protection ContentKeeper Anti-virus provides automatic updates of threat signatures as well as automatic reports of virus incidents. The technology has been designed to require minimal interaction with IT supervisors enabling them to devote their time to improving facilities for students.

ContentKeeper Guardian

ContentKeeper Guardian is a unique and effective Internet security solution that acts as a safety net for student PC users at school on and off the network. ContentKeeper Guardian is currently one of the only solutions in the market offering such a comprehensive way to capture all abuse on PC networks.

ContentKeeper Guardian provides supervisors and administrators with an effective tool for Monitoring student use of the Internet, as well as acting as a deterrent for the initial occurrence of offences. Guardian exposes the hidden misuse that is taking place daily on school PCs and enables users responsible to be confronted with the irrefutable evidence of their activities, an effective deterrent for Cyber bullying.

Given the seriousness of potential abuse in any school environment and the legal liabilities that could result, Guardian minimises risk and acts as insurance that no school can choose to be without.

ContentKeeper Guardian word and phrase libraries are fully customizable, the administrator has the ability to add additional words and phrases and adapt the severity coding of a violation according to pastoral concerns. Reports on misuse are generated for supervisors to Monitor and Control student usage.

ContentKeeper: the solution for the Education Sector

ContentKeeper provides efficient, cost-effective solutions for Educational Institutions wishing to protect staff and students from inappropriate content, monitor student use of the Internet, combat cyber bullying and other Internet-related crime, and protect themselves from legal liability due to copyright infringement and other inappropriate uses of the Internet.

References

[i] Mental Health Association (MHA). Internet Adds New Dimension to Bullying. *Mental Health Review*. Issue 4, 2006.
http://www.mharochester.org/MHA/docs/MentalHealthReview.pdf

[ii] Wiredsafety. Cyberbullying and Harassment. 2006.
http://www.wiredsafety.org/cyberstalking_harassment/cyberbullying.html

[iii] Australian Government. What Is Online Grooming? NetAlert Limited Initiative. 2006.
http://www.netalert.net.au/01578-What-is-Online-Grooming.asp

[iv] Internet Free Expression Alliance. Children's Internet Protection Act. 2001.
http://www.ifea.net/cipa.html

[v] Lamont, Leonie. Recording firms ask to scan university computers. *Sydney Morning Herald.* February 19th, 2003.
http://www.smh.com.au/articles/2003/02/18/1045330603596.html