Internet Safety Technical Task Force
Technology Submission

DeepNines Technologies / Hamid Karimi
http://www.deepnines.com

JULY 21, 2008

ABSTRACT
DeepNines presents the iTrust platform as a new framework for children's educational trusted computing. iTrust is a bundled suite of products and services that work together in an integrated fashion to provide comprehensive online protection to children and thus empower and enable a more powerful learning environment. iTrust has transformed the shape of Internet access for millions of students and educators and for the first time has created the possibility of access to secure information –anywhere, anytime.

KEYWORDS
Content control, children safety, security, protection, compliance

FUNCTIONAL GOALS
The functional goals of the DeepNines' technology are as follows:

- ✓ 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
- ✓ Prevent minors from accessing particular sites without parental consent
- ✓ Prevent the use of special tools such as proxy sites and enforce Acceptable Use Policies (AUP)

PROBLEM INTRODUCTION
Ubiquitous access to information and productivity tools are placing enormous pressure on parents, educators and IT administrators. For children in particular and K-12 educational institutions specifically, this has become a daunting challenge. Children by nature are often curious and at times mischievous and these combinations create a dangerous mix that makes them intentional or inadvertent targets of abuse and predatory practices. Under the rapidly growing financial strains, parents and schools are forced to choose from a myriad of technology choices while understanding little of complexities that plagues their good intentions. Often a lot of precious resources are spent on disparate or inadequate piecemeal approaches. The time for a system overhaul and paradigm transforming approaches has arrived.

PROPOSED SOLUTION
At the heart of iTrust resides SEP or Security Edge Platform which offers a 360 degree of network traffic and related protocols by using an all-protocol-inclusive Deep Packet Inspection (DPI) engine combined with profiling, forensics, reporting and scanning tools to examine every packet that traverses the network regardless of its origination or destination target. In essence SEP may be viewed as the next generation Unified Threat Management (UTM) for which DeepNines is the only patent holder. SEP combined with URL filtering constitute the iTrust bundle; more importantly unlike other solutions, iTrust is capable of identifying, blocking and reporting proxies that are the most recent and dangerous tool to bypass existing Internet access policies.

VISIBILITY: DeepNines provides a real-time view of who is on the network, who they are communicating with, how much bandwidth they are consuming and what port(s) they are using. This in-depth view of the network quickly and easily shows which end users are behaving inappropriately and how they are doing it.
CONTROL: Through DeepNines Deep Packet Inspection (DPI) engine, every type of traffic on every port is scanned for unwanted proxy connections. Every attempt to connect to a proxy server is immediately blocked, forcing students to adhere to the security policies of the school. The DPI engine has proprietary signatures associated with blocking peer-to-peer file sharing, instant messaging systems, pornography, malware, spyware and phishing. In addition, customized signatures can be created to block or control other applications.
SECURITY: The SEP integrates multiple security technologies into a single device to prevent attacks. The SEP includes firewall, behavior based intrusion prevention, signature-based intrusion prevention, anti-virus, anti-spyware, anti-phishing and traffic management. The SEP's patent-pending Zero Footprint Technology allows it to sit invisibly inline, with no IP or MAC address. The ability to maintain true transparency prevents both students and outsiders from locating the system and attempting to take it down.

TECHNICAL ATTRIBUTES
The solution is appliance based that runs on RH 2.6 based Linux or MAC OSX operating systems. The appliance runs on standard X86 CPU and operates as a bump in the wire offering full invisibility. GUI is based on JAVA and the

design blocks are written in C and C++ languages. The appliance can reside anywhere in the network but typical deployments are at the edge either behind the router or in front of it with WAN or LAN interfaces. There is a sophisticated traffic management capability built into SEP. that allows it to control connections or application usage based on any given policy, be it time of the day, machine IDs or user identities based on X500 certificates. Backend connections to AD/eDirectory, OpenDirectory and LDAP are transparent. These systems operate from fractional T1 to Gigabit speeds. In real-time, the state machine keeps track of 256 top protocols; it is possible to track other less often used protocols through the use of special signatures or expressions.

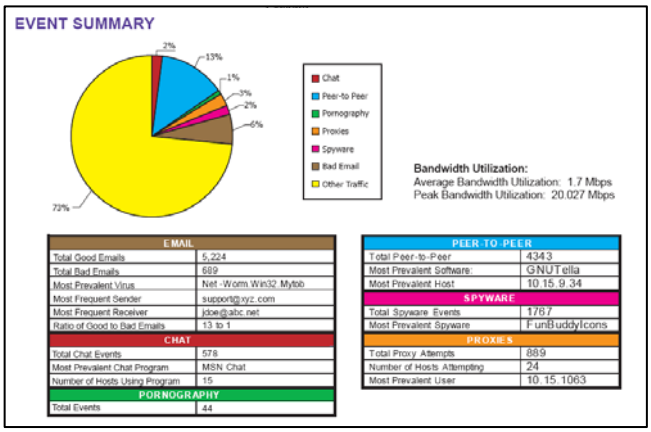
BENEFITS

-Eliminates unwanted proxies that allow students to bypass security rules and policies
-Improves network performance by reducing the amount of unwanted traffic that is consuming network bandwidth
-Prolongs infrastructure lifecycle by more effective utilization of Internet connection, routers and switches
-Leverages existing security investments by ensuring that their rules and policies are enforced
-Tighter security on legitimate traffic by preventing viruses, worms, blended threats and other malicious traffic
-Ability to define different access policies for different groups of users (example: can allow the administration to use instant messaging but not the students.)
-Provides granular control to ensure that good, mission critical traffic gets to the network quickly and attack-free.

STRENGTHS & WEAKNESSES

DeepNines initially developed its solution for the large enterprise and ISP markets and almost by accident discovered its unique value proposition for the K-12 and children's protection space. Whereas the company offers an abundance of technologies that may, on the surface, seem irrelevant to the Internet safety space, it continues to develop new tools to better serve the newly-found focused market. One area of new development focus is remote monitoring of laptops and home sites and extending the full protection to all mobile spaces.

Typical installation of DeepNines solution takes about 10 minutes. The users that company deals with are far less technical than the typical IT staff at enterprises and thus require more hand-holding and automation. Because the technology is IP-centric and is independent of infrastructural deployments, all sites find it irresistible to test or deploy permanently. DeepNines experiences a high ratio of trial to purchase through Internet Content Audit program (ICA) which is an obligation-free deployment. The primary goal of customers is to comply with CIPA regulation. Internationally, there are other standards and regulations at play that make DeepNines an attractive provider. DeepNines has so far protected more than 6 million users worldwide and within US, it has deployed its solutions at more than 300 educational institutions.



A screenshot of ICA report

EXPERTISE

DeepNines has been in the business for 9 years and has built partnerships with likes of SUN, Novell, and Apple. The company executives have more than 100 years of combined high-tech experience.

COMPANY OVERVIEW

DeepNines is a venture-funded company that has achieved a sustainable financial model with over 200% year to year CAGR growth. The CEO, Sue Dark, comes out of MIT and NASA and other executives have proven background in the security and high tech industry. DeepNines is based in Dallas, TX and has its R&D offices in San Jose, CA. The largest deployment is at PeachNet, the biggest educational ISP and comprises of more than 115 installations providing around the clock support to hundreds of campuses, libraries, dormitories and other sites. Main partners include SUN, Novell and Apple. Other relevant information can be found at www.deepnines.com

BUSINESS MODEL OVERVIEW

DeepNines sells both direct or through channel partners. Most prices range from $5000 to $50,000 for end users. However, special discounted pricing is available for institutions that cannot afford these prices and educational organizations are also beneficiaries of additional discounts.

MORE INFORMATION

Most datasheets and case studies, as well as educational videos are available at www.deepnines.com

CONTACT INFORMATION

The author's contact information follows:

Email: hkarimi@deepnines.com, Tel: 408-538-1318

CERTIFICATION

I certify that I have read and agree to the terms of the Internet Safety Technical Task Force Intellectual Property Policy.