Surf-SeCure 1000 for Small Businesses

Nowadays organizational network environment states multiple risks and challenges for IT managers. It is estimated that employees spend over an hour a day on non work-related web activities including surfing to online games, shopping, and inappropriate content sites and gambling. More than 75% of all corporate desktops are infected with various forms of Spyware, and new threats are introduced to the Internet on a daily basis. Lack of proper auditing can also lead to unnecessary consumption of the organization's bandwidth, with employees installing and using Peer-to-Peer (P2P) and other file sharing applications, thus suffocating the organization's network traffic with non-work related (and sometimes dangerous) files. PineApp™ Surf-SeCure™ as Software provides a real-time filtering system for protecting businesses' networks from Internet-based threats, as well as providing organization's surfing policy enforcement. Customers who seek a cost-effective web protection solution, with flexible deployment options for in-house hardware platforms, will find Surf-SeCure as Software the most suitable solution for their needs.

Multiple operation modes
Surf-SeCure can be easily implemented in any existing network topology, as a web proxy server, transparent bridge or as the organization's network gateway.

Policy Enforcement
Surf-SeCure's innovative Three-tier policy enforcement system enables administrators to define rules for users, groups or the entire organization. This flexibility enables the System Administrators to enforce the organization's policy for Internet surfing and application control. Surf-SeCure enables user and group synchronization and authentication by smoothly interconnecting with any existing directory service using the LDAP protocol.

Category-Based URL Filtering
Surf-SeCure provides URL classification, sorted according to various content categories. This dynamically updated engine provides the ability of blocking certain content types (pornography, gambling, sports etc.) completely, according to a simple, checkbox-based policy rule creation.

Application Layer Blocking
Many applications are now sophisticated enough to bypass traditional policy enforcement tools. Surf SeCure is able to identify and block hundreds of applications such as P2P, instant messaging, radio streaming, VoIP and games. By blocking these applications, Surf-SeCure reduces bandwidth consumption and prevents malicious content from entering the network.

Features & Benefits

- Advanced Management
- Accelerated Web Surfing
- Phishing Prevention
- Major reduction in bandwidth consumption
- NTLM support
- Virus and Trojan Horse protection
- Real-time Technology Implementation
- A System and Network Resources-Friendly Solution
- Multiple Caching Methods
- Rapid ROI
- Seamless Integration
- Kerberos support
- Quota enforcement
- Upstream-proxy support

PineApp Ltd. 8 Hata'asia street, Nesher, Israel, 3660201, POB 285
T +972-4-8212321 **F** +972-4-8203676 **E** info@PineApp.com **W** www.PineApp.com

SPECS

Surf-SeCure 1710

Number of end points (recommended)	**25**
CPU cores	Intel Pentium Dual Core G2030
Memory	DDR 3 4G/1600 Hynix
Ethernet port	2x1Gbe
Disk capacity	Hitachi 500 Gb SATA 2 16MB
Power	Seasonic PSU 250W 1U A.PFC 80
Dimensions (WxDxH)	19.00" x 1.75" x 11.00" 482.6 mm x 44.4 mm x 279.4 mm
Form factor	iStarUSA 1U Case Mini ITX Rackmount
Weight	6 Kg
Advanced appliance management	CLI
Inspected protocols	SMTP, POP3
Mail delivery protocols	SMTP/S, POP3 Pull-mode and Local
Mail services protocols	ESMTP/S with LDAP Authentication support, POP3/S, IMAP4/S
Domains	Up to 5
Policy enforcement	Four-tier policy enforcement (Global, domain, group & user)
Licensing	Revolutionary unlimited user licensing program
Warranty	1 year limited warranty
Certifications	CE, CB, FCC, UL, RoHS

Surf-SeCure 1720

Recommended Number of end points 50

* Other specs same as Surf-SeCure 1710
* Optional RAID based platforms