



What employees do on your network isn't your business.

Our Point Exactly

Introducing the Vericept™ monitoring solutions for business.

Welcome to the age of technology – where low productivity, sexual harassment and even corporate espionage are now just a click away. The Internet has changed the way business gets done. And, unfortunately, the way business doesn't get done as well.

Today, companies of every size are facing the challenge of internet abuse in the workplace. Corporate liability, productivity and even overall business success could be at stake.

Like any other corporate process, Internet usage needs parameters, guidelines and monitoring. Especially when you consider that roughly a third of all corporate network activity is personal. And the judicial system has made it clear that the network is a company's responsibility to control. The question is, just how exposed are you?

At Vericept, we think it's time to define your e-boundaries.

The Vericept solution puts your organization back in control of the Internet. At the heart of the Vericept solution is an advanced, plug-and-play appliance that sits passively on your network analyzing all traffic for activity that the company has specifically defined as inappropriate.

But the Vericept solution is more than a piece of hardware. Each device includes information on how to design and implement an Acceptable Use Policy (AUP) tailored to your specific organization. Plus the device itself can be easily customized to control Internet use in the way that best works for you. With a wide variety of categories and easily adjusted sensitivity levels, you can quickly tailor the device to the culture of your organization.

Vericept Solutions ...

- Allow e-boundaries to be defined by the customer
- Fill holes that blockers leave open
- Monitor all network activity – web, email, chat, IM, web-based email, telnet and FTP
- Protect the organization from harassment, discrimination and security liabilities
- Provide low Total Cost of Ownership
- Give visibility to who the "hackers" are in your company.



Vericept monitoring devices are Linux-based appliances that plug directly into a corporate network. Just give the device an IP address and you're in business. Then, using sophisticated linguistic and mathematical analysis, the device passively monitors all IP traffic – Internet, intranet, e-mail, chat, ftp, telnet, instant messaging and even print jobs – for content that falls outside of a company's pre-defined Appropriate Use Policy.



When someone goes out of bounds, the Vericept V1100 appliance logs the abuse and reports it. The appliance has a browser-based interface that easily allows management to view high-level log summaries of the inappropriate activity and quickly drill down to view the actual content of specific activity.

Any inappropriate activity, such as hacker communication, day-trading, pornography, job hunting, even e-mails that contain pre-determined, unacceptable or corporate-sensitive wording is captured, and it's totally customizable by the user. Categories of abuse and sensitivity levels for each can be tailored exactly to your corporate needs and culture. In the end, you gain total control over what occurs on your network.

Vericept Solutions currently available:

Vericept Pro – enables users to manage their AUP.

- V1100 Appliance
- VCORE software

Vericept Enterprise –allows network managers to share administration of the company's AUP by distributing management rights.

- V1100 Appliance
- VE CORE software (includes User Management)

Key Features

- True plug-and-play network appliance that's easy to install and maintain
- Quick, non technical installation – just give the device an IP address
- Browser-based interface allows viewing high-level log summaries or drilling down to view content of logged infractions
- Powerful user management tool allows several users to view and manage activity (included with Vericept Enterprise)
- Secure-system password protection assures information remains confidential
- Completely customizable to match your corporation's policies and needs
- Frees up valuable network bandwidth
- Passively monitors without affecting network performance
- 30-day money back guarantee

Vericept V1100 Specs

Dimensions (mm)
45 (h) x 438 (w) x 500 (d)

Voltage (auto-detection)
100-240Vac

Electrical Frequency
50-60 Hz

Operating Temperature
+5 C +28 C

Net Weight
8.2kg

Network Connection
RJ 45

Network Protocols
TCP/IP

Monitoring Capabilities
Web visits, e-mail, chat, instant messaging, ftp, network print jobs, other TCP/IP traffic

Interface Languages
Simplified Chinese, Traditional Chinese, English, French, German, Japanese, Spanish

Vericept Corporation
(formerly eSniff, Inc.)
750 West Hampden Ave, Suite 550
Englewood, CO, 80110
303.798.1568
800.262.0274
303-268-0520 (fax)
info@vericept.com