



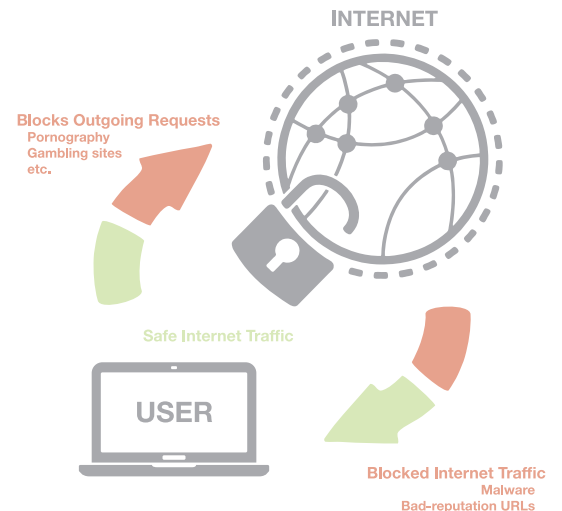
# Web Protection

## Stop malware before it starts with SecureSurf™

Malicious Web content can expose your company to higher costs, lower productivity and legal issues. SecureSurf can protect your network from Web-based malware and viruses, and shield your employees from offensive content. SecureSurf requires no onsite hardware or software and it won't require constant attention from your IT staff.

## Hassle-Free Web Protection

With SecureSurf, sites known to have malicious content are blocked automatically. SecureSurf allows you to set your own policies to determine what other types of sites are prohibited and permitted risk-free for 30 days.



## Features & Benefits

- A decision by the DNS engine or a check by the proxy server. Unlike other Web filtering services that inhibit Web surfing performance by forcing all traffic through a proxy server, SecureSurf's DNS lookup engine will immediately determine whether or not a site violates a company's policy. Customers can set policies regarding sites that might be classified as containing questionable content. These sites can be further evaluated through a hosted proxy server.
- Comprehensive policy settings and reporting. Administrators can set specific parameters regarding their employees' surfing habits, including listing Web sites known to be safe and that should be whitelisted. SecureSurf can also provide information on Web surfing trends, including which Web sites are visited the most.
- Real-time security based on data from a number of sources. SecureSurf's DNS engine captures information about bad URLs from a number of sources, enabling the service to protect companies from emerging insidious sites. Among the security sources employed are the most effective anti-spam and virus protection services available.