



Products

[Overview](#)
[Web Security](#)
[Data Security](#)
[Messaging Security](#)
[Technology & Services](#)
[Product Resources](#)

Web Security

[Overview](#)
[Express](#)
[Hosted Web Security](#)
[Web Security](#)
[Web Filter](#)
[Web Security Gateway](#)

Add-On Modules

Extend The Value Of Your Solution

Websense Content Gateway is a central gateway for controlling Web content. Websense Content Gateway integrates with Websense Web Filter and Websense Web Security to further increase the level of security for the Web. The Websense Content Gateway provides visibility into SSL encrypted Web traffic, to ensure that malicious content cannot enter your network. It also enables real-time categorization of dynamic Web 2.0 content, as well as identifying previously unvisited sites that might only exist for a very short period of time such as those used for phishing attacks and proxy avoidance Web sites.

- Prevent encrypted SSL Web traffic from circumventing defined Web security policy
- Categorize Web 2.0 sites in real-time, based on actual content, rather than the Web site category
- Identify and block previously unvisited malicious sites, such as phishing or proxy avoidance sites, which typically only exist for hours

Websense Client Policy Manager provides a comprehensive endpoint security solution for desktops, laptops, and servers and actively protects organizations against known and unknown endpoint security threats. Websense Client Policy Manager prevents the installation and execution of unauthorized applications and enforces application use policies with its wide-ranging database of categorized applications, which is updated daily. It provides an easy-to-implement, low risk, highly effective alternative to behavior-based host intrusion prevention systems (HIPS). The complete coverage of both "whitelist" (good) and "blacklist" (bad) applications allows for granular, dynamic, and highly flexible application policies. This provides a critical layer of application awareness that complements desktop antivirus and personal firewalls while stopping fast-moving and blended security threats.

- Addresses weaknesses in existing antivirus, anti-spyware, personal firewall, and patch management processes to render attacks harmless
- Provides application awareness and usage policy enforcement on the endpoint for blocking malicious software while ensuring compliance and productivity
- Prevents malicious applications from changing registry settings and tracks suspicious registry activities
- Protects remote and mobile users operating outside of the network or without standard security updates or patches
- Includes protection from the threats and compliance risks around Web access and URL content for remote and mobile users
- Works with network access control (NAC) solutions to enforce policy on devices trying to enter the network, denying access to non-compliant endpoints
- Via integrations, enables network-level protection from inbound threats and creates dynamic and application-aware firewalls
- Provides multiple levels of control to prevent the launch or mitigate the propagation of security attacks

Websense Remote Filtering extends the Websense industry-leading Web filtering and Web security technology to protect corporate laptop users outside as well as inside of your organization's network. Remote Filtering protects remote users and frequent travelers from external security threats and prevents access to inappropriate and malicious sites. A critical component of any organization's endpoint protection strategy, Remote Filtering ensures secure employee internet use anytime and anywhere.

- Protect remote laptop users from phishing sites, spyware, malicious mobile code (MMC), and inappropriate content
- Minimize remote laptop user downtime and frustration resulting from computer issues stemming from spyware, MMC or other threats while on the road
- Cut overhead and capital equipment expenses by implementing a Web filtering and Web security solution for mobile laptop users
- Apply the same policies and level of protection to laptop users, whether they are outside or inside of the organization's network
- Get the same level of reporting for remote laptop users as for corporate users, providing a more complete picture of your organization's Internet usage