

Total Control for Web and Real-Time Internet Communications

About FaceTime Internet Security Edition

FaceTime Internet Security Edition enables the safe and productive use of the Internet including web browsing, IM, P2P, Skype and other real-time communications applications. Purpose-built and integrated to provide total visibility and control, FaceTime Internet Security Edition allows organizations to implement powerful policies that detect, secure, manage and enable real-time collaborative applications while preventing malware threats, minimizing information leakage, and control employee Internet use.

KEY FEATURES

- Enable, secure, and manage all Internet communications channels using a single solution
- Centralized enforcement of Web filtering, malware, and compliance policies using FaceTime WebFilter or Secure Computing SmartFilter URL databases
- Detect and prevent spyware “phone home” activity from previously-infected clients
- Perform targeted remediation of infected endpoints without deploying client software
- Inoculate existing spyware applications and prevent re-infection
- Protect with the broadest anti-spyware coverage available over any channel – IM, P2P and Web
- Ensure protection from latest malware threats with automatic updates from FaceTime Security Labs
- Get visibility into usage, policies enforced and risks with flexible reporting options
- Lower cost of ownership with ease of deployment and integration with existing infrastructure

FaceTime Internet Security Edition is the next generation Internet security solution, providing total control over web usage and real-time communications. For the first time, enterprises can enable, secure and manage all Internet channels – web browsing, IM, P2P, Skype, and chat - with unified policy management through a single access point. FaceTime Internet Security Edition combines state-of-the-art IM & P2P security with an industry leading URL filtering database and award winning gateway anti-spyware solution.

Real-time Communications in the Enterprise

Internet communications have evolved from point-to-point channels such as email to real-time, presence-oriented communications like IM, P2P file-sharing, Skype, and web conferencing. For the new generation of workers, access to real-time communications is an assumption; if it's not available, they will download it to their computer regardless of policy, because they know what a positive impact these applications can have on effectiveness and efficiency.

FaceTime terms these real-time communications applications ‘greynets’ – often installed by end users without the permission or knowledge of the IT department and use highly evasive techniques to circumvent the existing security infrastructure.

The Evolution of URL Filtering

Because greynet applications operate below the security radar, they provide an ideal vector for malware infections, client-side code vulnerabilities, intellectual property loss, and identity theft. While some greynets, particularly enterprise instant messaging, web conferencing and Skype, deliver clear business benefits, others such as P2P networks and public IM portals can pose serious risks. Current security infrastructure designed for well-behaved applications fall short in detecting and securing greynet channels that use proprietary protocols and HTTP as their channels.

To maximize the value and minimize the risk of web and greynet applications, enterprises must gain visibility and control over their use.

FaceTime Internet Security Edition

FaceTime Internet Security Edition enables the safe and productive use of the Internet including web browsing, IM, P2P, Skype and other real-time communications applications. Purpose-built and integrated to provide total visibility and control, FaceTime Internet Security Edition allows organizations to implement powerful policies that detect, secure and manage real-time collaborative applications to prevent inbound malware threats, minimize information leakage, and control employee Internet use.

Through its defense-in-depth architecture, FaceTime Internet Security Edition provides comprehensive protection against worms, rootkits, spyware and other inbound threats that seek to use Internet-based communications channels, and targets infected endpoints with patent-pending clientless targeted remediation to clean and inoculate them. It is backed by FaceTime Security Labs, the industry's premier threat research team dedicated to malware and other threats coming over greynet channels. Choice from two industry leading web filtering databases - FaceTime WebFilter and Smart Filter from Secure Computing provides rich visibility and monitoring of web usage.

FaceTime Internet Security Edition comprises two components:

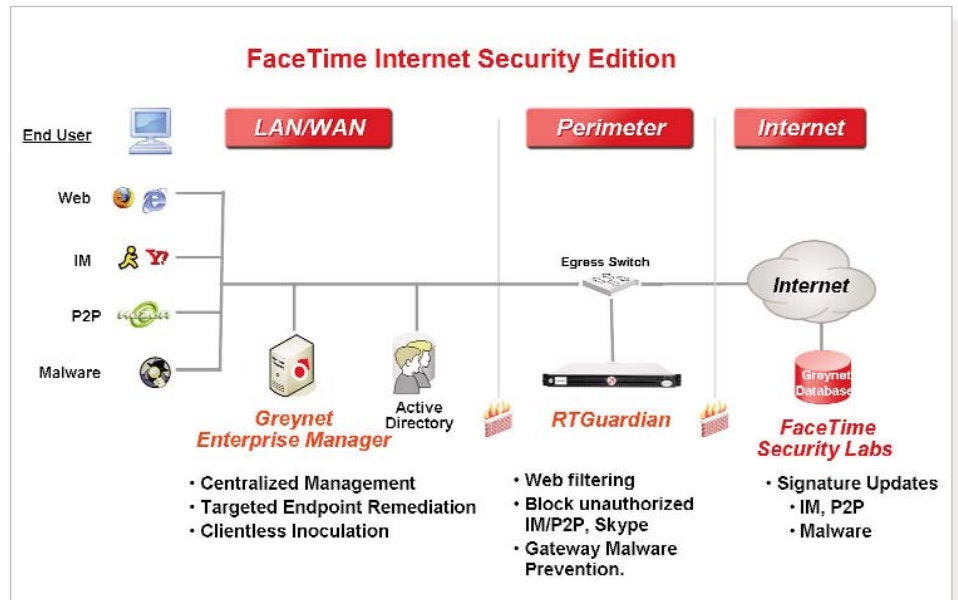
- RTGuardian — Purpose-built security solution for managing web browsing, preventing unauthorized IM and P2P usage and blocking malware in the enterprise before they impact the business.
- Greynet Enterprise Manager (GEM) — A centralized management, reporting and control server in the LAN that enables organizations to manage security policies and aggregate reporting for IM, P2P and spyware traffic across distributed enterprise environments.



KEY BENEFITS

- Reduce operational expenses by consolidating all Internet communications security controls into a single unified solution.
- Provide visibility into and control of real-time traffic channels
- Monitor and control access to Web sites to prevent inappropriate use of company resources
- Block malware at the Internet gateway, before it can impact the business
- Trigger targeted clientless remediation of infected endpoints
- Improve decision making about security issues and Internet usage with real-time reporting
- Reduce administrative overhead with centralized monitoring and enforcement of all Internet usage
- Optimize value of enterprise IM deployments by blocking the use of rogue communication tools

FaceTime Internet Security Edition brings together the benefits of Real-Time Guardian and Greynet Enterprise Manager to deliver the first fully-integrated solution to secure, manage and control web browsing and greynet applications.



FACETIME INTERNET SECURITY EDITION FEATURES

Security

- Support for more than 40 IM clients and 64 P2P applications, as well as a growing list of tunneling and anonymizer applications
- Reliably distinguish between authorized and rogue greynet connections
- Integrated URL databases: FaceTime WebFilter with over 21 million sites in 54 pre-defined categories and Secure Computing's SmartFilter with more than 7 million URLs classified in 73 pre-defined categories
- Monitor and control access to public IM portals
- Prevent IP address exposure by blocking direct client-to-client connections
- Block file and image transfers over public IM networks
- Prevent users from visiting known spyware infection sites
- Targeted remediation and inoculation of endpoints with no client software deployment
- Detect and report on evasive application behavior

Management and Control

- Gain critical insight into bandwidth and port abuse, source and destination IP addresses
- Create and enforce a standardized profile for public and enterprise IM use
- Map the extent of greynet use in the enterprise
- Apply granular controls to Skype usage, down to which versions are allowed.

- Set URL policy by users/groups of users through AD integration
- Customize URL filtering by IP or range of IP addresses
- Native real-time reporting and integration with SmartReporter and other third party applications.
- Schedule searchable, customizable reporting with policy event notification
- Integrated real-time reporting and monitoring for web, IM and P2P usage
- Use GEM to aggregate output from multiple RTGuardian appliances across distributed network environments

Ease of Deployment and Operations

- Plug-and-play deployment with pass by mode avoids changes to existing directories and network infrastructure
- Purpose-built and hardened configuration
- Multiple configuration options--RTG100, RTG500, RTG1000--for different throughput environments
- Easy-to-use interface allows for rapid set up and ongoing administration and management
- Configurable graphical dashboard provides visibility into greynet traffic, web usage, and policy enforcement
- Automated protocol and URL updates
- Full SSL console for secure administration and management

RTGuardian Specifications

- Dimensions: Mini 1U chassis 16.7"/42.42 cm W x 1.68"/4.2 cm H x 21.5"/54.6 cm D w/o bezel, 22.8"/57.9cm w/bezel
- Max weight: 27 lb./12.27 kg
- Processor: Intel 2.8GHz, 1MB Cache Pentium 4 with 800MHz FSB
- Memory: 2GB DDR,400MHZ,4x512
- Disk: 80GB SATA 7200 rpm
- Ethernet: 10/100/1000 (2)
- Certifications:
 - Safety: FCC (U.S. only) Class A
 - DOC (Canada) Class A
 - CE Mark (European Union)EN 55022
 - Class A, EN55024, EN61000-3-2, EN61000-3-3 EN60950
 - VCCI Class A
 - UL 60950
 - CAN/CSA-C22.2 No. 60950
 - IEC 60950

GEM Server Requirements

- Microsoft Windows 2003 Server with 2GB hard disk space and 1GB RAM
- Microsoft SQL Server 2005 Express Edition, Microsoft SQL Server Enterprise Edition
- IE 6 or later or Firefox 1.07 or later for administration

Client Requirements

- Windows XP, 2000, 2000 Server, 2003 Server or NT