

## Prevent Spyware and Secure IM and P2P Use in the Enterprise

**About RTGuardian**

Real-Time Guardian (RTGuardian) is the most advanced perimeter security solution for blocking the spread of spyware and adware in the enterprise and securing unauthorized IM and P2P usage. RTGuardian integrates with FaceTime's Greynet Enterprise Manager (GEM) and IMAuditor to create FaceTime Enterprise Edition, the leading solution for securing and managing all greynet applications.

**KEY FEATURES**

- Prevent spyware from spreading across the network
- Stop unauthorized IM and P2P connections
- Ensure safe and secure IM usage by blocking high-risk features
- Create a standardized profile of IM use within the enterprise
- Block unauthorized VoIP applications such as Skype
- Ensure non-stop protection with the latest protocol updates
- Mitigate business and security risk by controlling greynet applications
- Gain insight into bandwidth abuse, source and destination IP addresses, and port abuse
- Add GEM to provide:
  - o Centralized management and reporting across distributed RTGuardian appliances
  - o Targeted remediation of spyware-infected endpoints

Real-Time Guardian provides comprehensive visibility and control for real-time communications in the enterprise – public and enterprise IM, P2P, VoIP, professional communities, IRC and other chat systems – as well as spyware. Used in conjunction with Greynet Enterprise Manager (GEM), RTGuardian delivers end-to-end spyware management, leveraging detection at the gateway to deliver targeted remediation to the infected endpoint.

**Real-time Communications in the Enterprise**

Instant messaging (IM), Web conferencing and other real-time communication and collaboration tools have become requirements for strategic and competitive advantage in today's real-time enterprises. The productivity benefits reaped from the use of these tools have dramatically expanded the use of IM, peer to peer (P2P) file sharing and Voice over IP (VoIP) for many organizations.

IM and Web conferencing programs, as well as their less-well-intentioned cousins, P2P and spyware, are part of a category of applications that FaceTime terms 'greynets.' Greynets are network-enabled applications that are installed on an end user's system without the permission or knowledge of the IT department (or frequently the user) and are largely invisible to the existing security infrastructure.

Instant messaging in particular has quickly moved from personal communications niche to a valuable business tool – so much so that email is sometimes regarded as being as slow and outdated as postal mail. According to IDC, more than 28 million business users today use IM to send nearly 1 billion messages each day at work, making it the fastest-growing communication system ever.

Because greynet applications tend to operate below the security radar, their widespread and uncontrolled use brings with it new risks for malware infection, loss of intellectual property, falling out of compliance with government regulations and more. While some greynets, such as IM and Web conferencing, have significant business value, others can pose serious security risks. However all need to be controlled and managed according to policy set by the enterprise.

**About RTGuardian**

Purpose-built for the security of real-time communications, RTGuardian is designed to fit seamlessly within the enterprise network without the need to change other network elements such as firewalls or anti-virus. Designed for deployment in the internal LAN as well as the corporate DMZ, RTGuardian acts as a security gateway to protect against the spread of spyware, as well as the ability to block unauthorized connections and file transfers, and delivers comprehensive IM and P2P usage statistics.

RTGuardian's unique anti-spyware design encompasses four key components:

**Prevents Infections:** Prevents users from visiting known spyware and adware infection sites and blocks the download of known spyware file types.

**Secures IM and P2P Use:** Secures the use of all major public and enterprise IM and P2P networks, some of the largest distribution vectors for spyware and adware today.

**Blocks Phone Home Behavior:** Interrupts spyware's "phone-home" behavior and stops the delivery of hijacked data and online advertising server requests before they reach their destination.

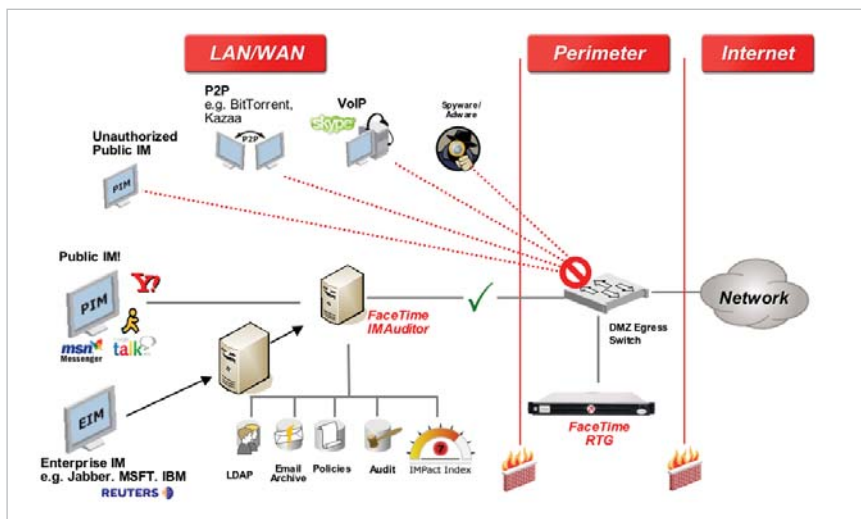
**Targeted Remediation:** In conjunction with Greynet Enterprise Manager (GEM), enables targeted remediation and inoculation of spyware-infected endpoints without the need for client software deployment.

## DEFENSE IN DEPTH

RTGuardian integrates with IMAuditor and Greynet Enterprise Manager (GEM) to form FaceTime Enterprise Edition for defense-in-depth protection against spyware and other real-time communication security threats.

IM Auditor's integrated trust relationship with RTGuardian allows FaceTime to deliver the industry's only TrueCompliance™ solution.

RTGuardian (RTG) Deployment



## RTGUARDIAN FEATURES

### Security

- Reliably distinguish between authorized and rogue IM connections
- Block users from visiting known spyware infection sites
- Prevent the download of known spyware file types
- Block the delivery of hijacked data and online advertising server requests before they reach their destination by interrupting spyware's "phone home" behavior
- In conjunction with GEM, provide proactive targeted remediation and inoculation of endpoints with no client software deployment
- Prevent IP address exposure by blocking direct IM client-to-client connections
- Prevent loss of productivity by blocking IM games
- Block unsafe public IM application functionality such as file and image transfers
- Control the port-crawling behavior of IM and P2P applications
- Block P2P applications such as KaZaA, Morpheus, FastTrack, Gnutella, Grokster, Limewire, Bearshare, Xolox, eDonkey
- Block VoIP applications such as SKYPE
- Integrate with GEM and IMAuditor to form FaceTime Enterprise Edition for defense-in-depth protection against spyware and other real-time communication security threats

### Management

- Create and enforce a standardized profile for public and enterprise IM use
- Map the extent of IM and P2P use in the enterprise
- Gain critical insight into bandwidth and port abuse as well as source and destination IP addresses
- Schedule searchable, customizable reporting with policy event notification
- Export reports using FTP or email
- Add GEM to aggregate output from multiple RTGuardian appliances across distributed network environments

### Ease of Deployment and Operations

- Plug-and-play deployment with no need to change existing 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
- Automated protocol updates

### Certified by Security Industry Partners

- Cisco Technology Developer Program Certified: Certified interoperability with the Cisco network infrastructure



- Symantec SESA Certified: Adheres to the Symantec SESA framework for centralized IM and P2P monitoring

### 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
- Power: 280W
- Operating System: Hardened 2.6 Linux kernel
- 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:
  - o Safety: FCC (U.S. only) Class A
  - o DOC (Canada) Class A
  - o CE Mark (European Union) EN 55022
  - o Class A, EN55024, EN61000-3-2, EN61000-3-3 EN60950
  - o VCCI Class A
  - o UL 60950
  - o CAN/CSA-C22.2 No. 60950
  - o IEC 60950