

Gateway-based Security and Control for Web and Real-Time Internet

About RTGuardian

Real-Time Guardian (RTGuardian) is the most advanced perimeter security solution for managing web browsing, securing unauthorized IM and P2P usage and blocking the spread of malware in the enterprise. RTGuardian integrates with FaceTime IMAuditor to form the industry's leading IM Security and Compliance Solution. With FaceTime Greynet Enterprise Manager, RTGuardian provides the ability to identify and remediate infected endpoints.

KEY FEATURES

- Detect, manage and secure all internet activity with zero network latency
- Set web global, group, user level policies through Active Directory integration
- Integrated industry leading Secure Computing's SmartFilter database with more than 7 million URLs according to 73 predefined categories
- Integrated real-time reporting and monitoring and compatibility with leading third-party reporting applications
- Block unauthorized IM and P2P connections
- Ensure safe and secure IM usage by blocking high-risk features
- Create a standardized profile of IM use and VoIP applications such as Skype within the enterprise
- Automatic updates and countermeasures to latest malware threats from FaceTime Security Labs
- Additional GEM module provides:
 - 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 web traffic and real-time communications in the enterprise – public and enterprise IM, P2P, VoIP, professional communities, IRC and other chat systems. It also detects and blocks the spread of malware at the gateway before it impacts the business. Used in conjunction with Greynet Enterprise Manager (GEM), RTGuardian delivers end-to-end malware management, leveraging detection at the gateway to deliver targeted remediation to the infected endpoint.

Real-time Communications in the Enterprise

Internet communications has evolved from point-to-point channels such as email to multi-directional, 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 introduce it to the workplace regardless of policy, because they know what a positive impact these tools can have on effectiveness and efficiency.

FaceTime terms these real-time communications applications 'greynets' – defined as network-enabled applications that are highly evasive and port-agnostic. They are installed on an end user's system without the permission or knowledge of the IT department and are largely invisible to the existing security infrastructure.

Many of these applications use evasive methods and often use the web as their transport medium. Since existing security infrastructure allows HTTP traffic without deep inspection, it has become an effective medium for these applications to bypass the security infrastructure to ensure ubiquitous access to the users.

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 web and 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 manage and control web access, protect against the spread of malware, as well as the ability to block unauthorized use of IM and P2P applications, and delivers comprehensive real-time reports and usage statistics.

RTGuardian's flexible architecture delivers following key benefits:

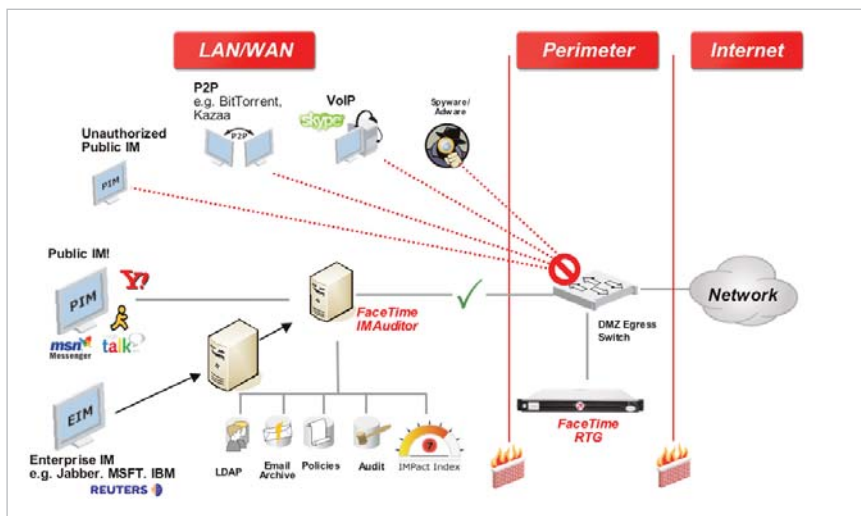
- Reduce operational expenses by consolidating disparate Internet security solutions into a single unified solution that is easier to deploy and maintain
- Improve decision-making about security issues and Internet usage through integrated real-time reporting and monitoring and compatibility with leading third-party reporting applications
- Monitor and control access to inappropriate Web sites that can waste company resources, create legal liability, and consume bandwidth required for business critical applications.
- Stop malware infections at the gateway before they can impact the business.



DEFENSE IN DEPTH

Deployed at the gateway, RTGuardian provides visibility, control for web and real-time communications applications and blocks malware before it impacts the enterprise. RTGuardian integrates with IMAuditor to form award-winning IM Security Solution - FaceTime Enterprise Edition. Combined with Greynet Enterprise Manager (GEM), it enables enterprise to gain visibility and total control for real-time Internet.

RTGuardian (RTG) Deployment



RTGUARDIAN 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
- Filter URLs according to 73 predefined and 10 customizable categories
- 7+ million URLs covered (HTTP and HTTPS) – updated daily
- Monitor and control access to public IM portals
- Prevent IP address exposure by blocking direct client-to-client connections
- Conserve productivity by barring IM games
- 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 version support
- 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 third-party applications
- Schedule searchable, customizable reporting with policy event notification
- Integrated real-time reporting and monitoring for web, IM and P2P usage
- Reporting compatible with SmartReporter and other third party applications
- 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 enables standard certificate generation for the console

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