

Centralized Security Control for IM and P2P Networks

About FaceTime Greynet Enterprise Manager

Greynet Enterprise Manager (GEM) provides total visibility and control over IM and P2P communications channels with integral targeted spyware infection remediation. Working in conjunction with FaceTime's RTGuardian, the most advanced gateway security solution for greynets, GEM delivers clientless, non-intrusive targeted remediation and inoculation to efficiently clean and prevent spyware infections at the desktop.

KEY FEATURES

- Aggregates reports from multiple RTGuardian appliances
- Provides a unified view of IM and P2P traffic and endpoint spyware infections across the distributed enterprise
- Resolves usernames and machines with Active Directory integration
- Patent-pending endpoint inoculation prevents spyware from downloading or executing on the client
- Identifies and blocks known-bad or suspect ActiveX controls to prevent drive-by downloads
- Gateway detection of spyware automatically triggers targeted remediation of infected clients
- Manages spyware prevention over all greynet channels (IM, P2P, HTTP)
- Detects and removes known spyware from clients without the need for local agents

The Importance of Real-Time Communications

Real-time communications applications like IM and P2P, particularly in industries such as financial services that rely on instant information, represent the fastest growing communications revolution in the history of business. Enterprise IM (EIM) products, public IM (PIM) services, industry-focused IM communities, Voice over IP (VoIP) networks like Skype, and online conferencing services such as WebEx all provide the ability for employees to communicate with one another as well as with customers, partners, and others outside the corporate network in real time.

All of these applications, along with their less well-intentioned spyware cousins, are part of a category 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 information security infrastructure.

While businesses are adopting these tools with increased confidence, securely managing this growth is a challenge for IT professionals. While greynet applications are delivering significant business benefits, they are also increasingly becoming vectors for the distribution of spyware and other malware, bringing with it the potential for loss of productivity, confidential information leakage and falling out of compliance with regulatory and corporate policies.

GEM Manages the Greynet Threat

GEM harnesses the power of RTGuardian installations across the network to deliver total visibility, manageability, and control of real-time communications channels across the network. These greynet channels operate largely outside the radar of traditional information security solutions, challenging IT departments to find a way to effectively manage, monitor, and protect their use without adversely impacting the productivity gains they bring. GEM comprises of two components:

- The GEM Management Console provides an aggregated view of all the reports generated by the multiple RTGuardians distributed across the enterprise, delivering total visibility and control of greynet traffic at the client level. Additionally, the Management Console enables the centralized device management of RTGuardian to provide health, status and firmware version reports.
- GEM Endpoint Remediation uses information from the aggregated RTGuardian gateway reports to trigger targeted remediation of infected endpoints. This patent-pending clientless technology cleans and inoculates the endpoint to prevent future infections from known spyware.

GEM integrates with RTGuardian and other components of FaceTime Enterprise Edition to deliver a true defense-in-depth solution for real-time communication security within a single management and reporting framework.

Benefits of GEM

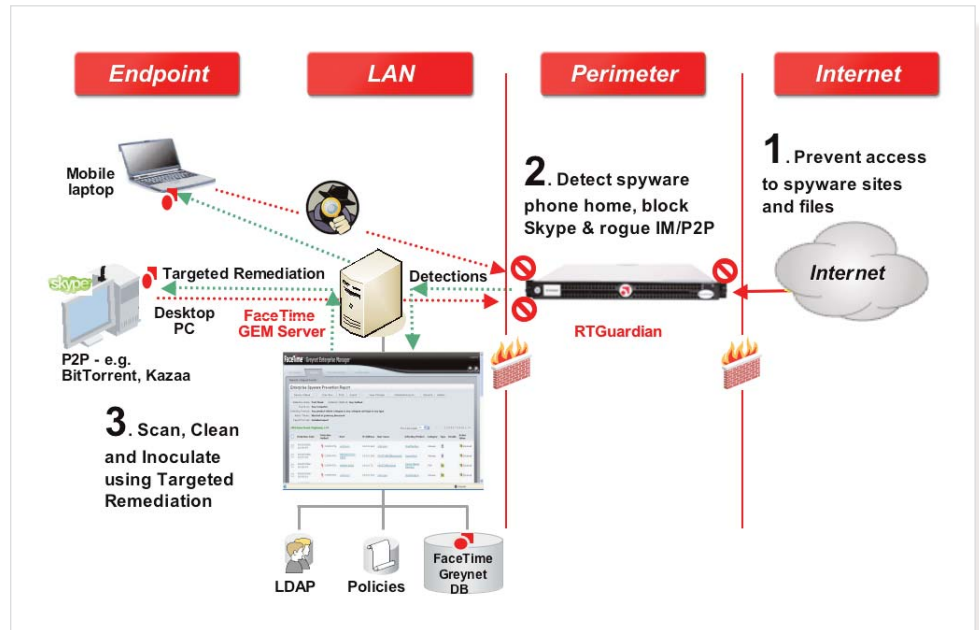
With GEM, FaceTime delivers an integrated management console that provides total visibility, control, and remediation of threats entering the organization through greynet channels. Centralized reporting and targeted endpoint remediation lower the risk of exposure to the threats, preventing loss of productivity and confidential information leakage. Infected endpoints are thoroughly analyzed and detailed information provided (threat level, host name, user name, and more), enabling GEM to direct only the required remediation at only the infected desktops without the need for client software, lowering the cost of deployment and management.

Both GEM and RTGuardian are also integral parts of FaceTime Enterprise Edition, the comprehensive framework for managing security and compliance for real-time communications, organizations can protect their investment and adapt to new protocols and applications by leveraging their existing infrastructure.

GEM and RTGuardian

When configured to work with RTGuardian, GEM provides these additional benefits:

- Retrieves detailed information about spyware detected at the gateway from RTGuardian
- Applies appropriate anti-spyware policies to scan, clean, and inoculate infected endpoints
- Provides statistical information reports



GEM Deployment Scenario

GREYNET ENTERPRISE MANAGER FEATURES

GEM Management Console

- Provides detailed reports on spyware infections and actions taken down to the machine and user level, not just IP addresses.
- Discovers IM and P2P installations and cross-referenced with policies governing their usage to determine enforcement levels.
- Data collected from RTGuardian installations
 - Real-time IM, P2P, HTTP, other TCP, and UDP traffic monitoring, including spyware
 - IM network activities, unauthorized port usage, attempted policy breaches and other non-typical behavior
 - Gateway enforcement actions such as blocking network access, file transfer, protocol type and client connection
 - Prevention, usage, policy and events reports with a dashboard summary

GEM Endpoint Remediation

Deployment

- No client software deployment is required; endpoint scanning is enabled through the launch on-demand of a remote scanning agent.

Anti-Spyware Policies

- Anti-spyware policies used to determine the preventative activities to be performed on a specified group of computers.
- Policies can be global or custom, and can be used to enable, disable, or schedule scanning, cleaning, and inoculation.

Targeted Remediation

- Gateway-triggered endpoint remediation is a two-stage process—remove existing infections and inoculate the clients against future infections.

Scanning and Cleaning

- Acting on gateway detection of spyware phone-home behavior, endpoints are scanned and cleaned for known spyware infections.

Inoculation

- Endpoints are protected from any future infections by inoculating with known spyware signatures
- Administrators can specify either or both of two mechanisms for inoculating the endpoints
 - Set kill flags on Active X to prevent drive-by infections through Internet Explorer
 - Enforce Software Restriction Policies (SRP) to prevent any resident spyware applications from executing

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

RTGuardian Requirements

- RTGuardian v3.1

Client Requirements

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