

PCI-DSS Compliance in the Real-Time Enterprise

About FaceTime Unified Security Gateway

FaceTime Unified Security Gateway (USG) is an enterprise-class appliance that enables organizations to comply with PCI-DSS sections 1.3.7, 1.4.1 and 5.1.1.

It allows organizations to manage the secure and compliant use of the real-time Internet. USG gives IT control over Web 2.0, Social networking, IM, P2P applications and enterprise unified communication platforms, all through a single dedicated appliance.

KEY PCI COMPLIANCE FEATURES

- Prevents unauthorized web, instant messaging, and P2P traffic not blocked by firewalls
- Provides gateway malware prevention and targeted remediation of infected endpoints
- Enforces policies, manages use, and prevent information leakage over permitted IM channels using industry leading URL databases
- Enables unified policy management and enforcement across all real-time Internet traffic
- Prevents inadvertent or malicious data leakage over all channels with real-time content filtering
- Protects against inbound and outbound threats (SpIM, spyware, rootkits, worms, botnets)
- Ensures non-repudiation of archived messages with tamper-proof logging and archival of online conversations

The Reality of Real-time Communications

PCI compliance requires that organizations block all non-approved channels of communication – do you know what unapproved communications channels are operating on your network?

Today's workforce expects instant messaging and other real-time communications tools - Web conferencing, Voice over IP, and social networking - to be "always on", just as their predecessors viewed email. The edge of the corporate network is rapidly moving beyond the physical network perimeter to include the broader community of customers and trading partners, and end users are driving the process.

More than half of today's Internet traffic is Web 2.0, instant messaging, P2P, and other protocols not monitored by firewalls, proxies, and intrusion prevention systems. These "greynet" applications are freely downloaded and installed by users in the workplace, regardless of whether enterprise instant messaging and other IT-sanctioned unified communication tools are available. Greynet applications are characterized by their evasive behavior, which renders them invisible to IT and introduces a new security risk into the enterprise.

Because they can't be seen, they can't be managed, and they can't be secured, resulting in a significant risk of violating PCI compliance.

Meeting PCI-DSS requirements

The Payment Card Industry – Digital Security Standards (PCI – DSS) is a collaborative effort between multiple credit card organizations to achieve a common set of security standards for use by entities that process, store or transport payment card data. Members include Visa, MasterCard, American Express, Diner's Club, Discover Card, and JCB.

Many of the requirements will be familiar to anyone dealing with SOX, HIPAA, G-L-B, and other data protection/information privacy legislation, with the subtle but important difference that cardholder data is extremely portable, fluid, and exhibits multiple points of vulnerability through the PCI system's interaction with other networks which may have any number of insecurities – not least of which is the use of real-time communications.

How FaceTime can help

FaceTime Unified Security Gateway (USG) enables enterprises to enforce acceptable-use policies for real-time communications and improve visibility into, and decision-making about, security issues related to real-time Internet use. By providing a single point for enablement, access management, security, and control for web and real-time channels, USG delivers a security solution that addresses future as well as current threats while maximizing existing investments in security infrastructure. With flexible deployment options, USG fits seamlessly into existing network topologies to offer the highest level of security with zero latency and a low total cost of ownership.

FaceTime recognizes that real-time communications deliver real business benefits, and that organizations need a way to control, monitor and secure these communications that's efficient, compliant, and makes maximum use of existing investments in security technology, and does not impact the organization's ability to do business.

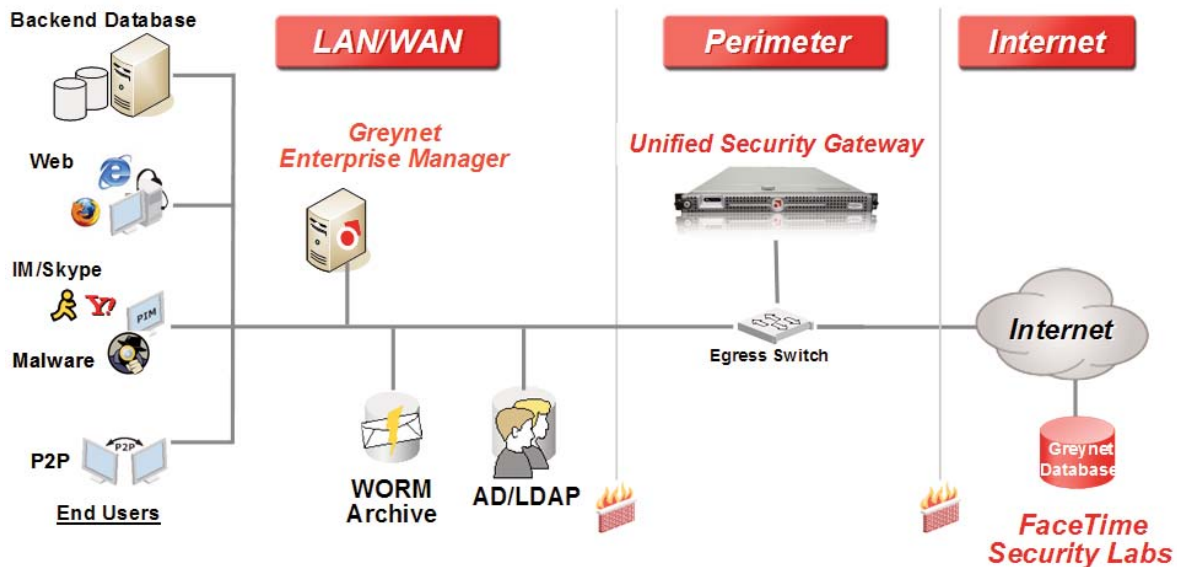
With mature, proven technologies, FaceTime's Unified Security Gateway, when used in conjunction with Greynet Enterprise Manager (GEM), delivers against these requirements for PCI-DSS compliance:

PCI – DSS Requirement	FaceTime Solution	Benefit
1.3.7: Denying all other inbound and outbound traffic not specifically allowed	Deploy USG at the gateway to filter web traffic, prevent unauthorized IM/P2P use, and block malware at the gateway	<ul style="list-style-type: none"> • Prevents unauthorized traffic not detected by firewalls or IPS from entering the or leaving the network
1.4.1 Implement a DMZ to filter and screen all traffic and prohibit direct routes for inbound and outbound Internet traffic	Deploy USG at the gateway to <ul style="list-style-type: none"> • locally route public IM traffic • filter credit card data in IM traffic • block malware over IM channels 	<ul style="list-style-type: none"> • Prevent credit card information leakage over IM • Achieve compliance for real-time communication channels
5.1.1: Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware	Deploy USG with GEM for gateway detection and prevention	<ul style="list-style-type: none"> • Complements desktop firewalls • Remediate infected endpoints without deploying an agent on the client

Unified Security Gateway

USG delivers on that knowledge with

- Hardened, proactive security that's built on years of research and partnerships to put enterprises ahead of the game
- Flexibility and security in a single appliance, enabling organizations to evolve their real-time Internet security protection as their needs grow and change
- The ability to leverage existing investments in anti-virus and apply those traditional tools to the real-time communications environment



UNIFIED SECURITY GATEWAY FEATURES

FaceTime's Unified Security Gateway delivers next-generation greynet protection through unified visibility, management and policy control across all unified communications channels. USG empowers enterprises to:

- Get visibility into and control over the use of sanctioned and unsanctioned real-time communications in the enterprise.
- Enforce security and usage policies across real-time communication and web channels.
- Reduce the business risks from exposure to malware (worms, viruses, SpIM, spyware) and from data leakage.
- Ensure compliance with corporate and regulatory requirements through tamper-proof logging, archival and easy retrieval of electronic conversations.
- Leverage existing security investments by providing an infrastructure that addresses the real-time communications universe.
- Optimize effectiveness with an integrated solution that provides a unified control center for all data channels.

FaceTime's Greynet Enterprise Manager adds:

- Aggregated reports from multiple appliances provide visibility into real-time communications usage as well as endpoint spyware infections
- User and host level visibility through Active Directory integration
- Identification of endpoints with phone-home spyware infections
- Application of appropriate anti-spyware policies to scan, clean, and inoculate infected endpoints without the need for local agents
- Patent-pending endpoint inoculation to prevent spyware from downloading or executing on the client

About FaceTime Communications

FaceTime enables the safe and productive use of the real-time Internet, including both public and enterprise instant messaging and unified communications platforms. Ranked number one by IDC in market share among instant messaging management vendors for the fourth consecutive year, FaceTime's award-winning solutions are used by more than 900 customers, among them nine of the ten largest U.S. banks. FaceTime supports or has strategic partnerships with all leading public and enterprise IM network providers, including AOL, Google, Microsoft, Yahoo!, Skype, IBM, Reuters, and Jabber.

For more information about FaceTime Communications, visit <http://www.facetime.com>



FaceTime Communications, Inc. 1301 Shoreway, Suite 275, Belmont, CA 94002
(888) 349-FACE (3223) toll free (650) 631-6300 phone (650) 598-2820 fax
General Information: info@facetime.com Sales: sales@facetime.com