



WHITE PAPER

Securing and Controlling Today's Internet at the Web Gateway

FaceTime Communications, Inc.

Table of Contents

The New Internet in Today's Business Environment	3
Increasing Communications Channels = Increasing Security Risk	4
Understanding Evasive Techniques	5
Securing the Web Gateway	6
Key Requirements to Consider	6
FaceTime's Unified Security Gateway	7
URL Filtering	7
Not Just Gateway Malware control	7
Granular Control of Web Based Applications	7
Managing and Reporting	7
Logging, Archiving and Providing the Ability to Retrieve	7
The Application Control Engine	8
Leveraging the New Internet: Safely and Securely	8
Summary	9
About FaceTime Communications	9
More Information	9

This white paper is for informational purposes only. FaceTime makes no warranties, express or implied, in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of FaceTime Communications, Inc. © 2001 - 2008 FaceTime Communications, Inc. All rights reserved. FaceTime and the FaceTime logo are registered trademarks of FaceTime Communications Inc. FaceTime IMAuditor, RTGuardian, Greynet Enterprise Manager, GEM, RTG and Enterprise Edition are trademarks of FaceTime Communications Inc. All other trademarks are the property of their respective owners.

WP0122-1108 Web Sec

The New Internet in Today's Business Environment

The Internet has changed. It's no longer just about Web and email traffic.

Instead, it's dominated by Web 2.0 applications such as IM, P2P, social networking, voice, and video. Today, these applications are pervasive in the enterprise, brought in by a new generation of employees.

Recognizing the benefits of these technologies organizations are deploying enterprise-grade unified communications platforms – such as Microsoft Office Communications Server, IBM Sametime and Cisco – that offer the full suite of real-time communications capability including IM, web conferencing, and Voice over IP.

The combination of evasive consumer applications and enterprise-class UC platforms is leading to an increasingly heterogeneous and complex environment – an environment that multiplies the security, management and compliance challenges faced by IT today – issues such as inbound malware, information leakage and compliance concerns, and the need for a common policy and reporting framework to simplify administration top the list.

This complex landscape is alive with participation and collaboration. FaceTime's 2008 survey, *The Collaborative Internet: Usage Trends, Employee Attitudes and IT Impact*, reports that:

- 97 percent of employees use Internet based applications (IM, P2P collaboration or file sharing, etc), up from 87% in 2007
- 79% of employees use social networking sites (LinkedIn, Facebook, You Tube) at work for business reasons.
- More than half of employees access social networking sites on a daily basis, and 26% access them several times a day
- Nearly three-fourths of employees (74%) use their work PC for personal reasons.

The real-time communications revolution has rapidly embedded itself into all aspects of today's business. Sales transactions are being concluded over Skype, shares have been traded over Yahoo for many years now, marketing campaigns are rolled out through social media, and it's common practice for candidates' online activities to be reviewed as part of the hiring process.

Anecdotal evidence suggests that access to, and in some cases, proactive use of social networks is a plus-factor for new hires in many sectors of the job market, attesting to the real value younger employees place on this type of collaborative activity for business.

Increasing Communications Channels = Increasing Security Risk

All this openness and collaboration between social and business networks creates many more opportunities not just for malware to enter the corporate network – but also for intellectual property to leak out.

Left unsecured and unmanaged, the widespread use of Web 2.0 applications can:

- Compromise network security from malware spread through uncontrolled real-time communications channels
- Create holes for information leakage, resulting in the loss of confidential information, intellectual property and privacy issues
- Increase help desk calls and support costs due to malware infections

This year, for the first time FaceTime's Collaborative Internet study tracked incidents involving intellectual property and regulatory compliance in addition to those involving malware. Four in ten IT managers report incidents involving non-compliance (37%), while another 27 percent have seen unintentional release of confidential corporate information.

These applications allow users a great deal of freedom to implement active content like JavaScript and ActiveX, for example in social networking profiles, activities which can then render those profiles vulnerable to hackers looking for new ways to distribute malware, phish for logins, and distribute viral attacks over IM and chat. When those IM and chat channels intersect with corporate networks, the malware floodgates can open and the result is malware infections spreading across the corporate network, utilizing an IT-sanctioned tool in real time.

All publicly available, real-time communications networks are designed to allow ease of communication and ubiquitous access. These applications are evasive by nature, exhibiting behaviors that render them invisible to traditional corporate network security tools.

Total Visibility of Web and Real-Time Communications Traffic

FaceTime RTDiscover™ is a FREE network visibility tool that provides comprehensive reporting of real-time communications traffic such as web browsing, instant messaging and P2P on the corporate network.

- Visibility of IM, P2P and web usage on your network at user, group and organizational levels
- Identification of compliance gaps by learning what unauthorized IM and P2P may be circumventing policies
- Assessment of malware threats including spyware, adware, keyloggers, rootkits and more
- Identification of PC endpoints that are currently infected with malware
- Employee use of Web 2.0 and social networking sites

[Request free RTDiscover Tool](#)

Real Time Applications Database

The Greynets Guide is an online resource center focused on the real-time Internet and the communication and collaboration applications that power it. This site is maintained by FaceTime Security Labs and dedicated to the collection, analysis, associate threats and management of real-time applications. With research facilities on three continents, FaceTime Security Labs understands the tools and information organizations need to discover, control and secure real-time communications for the benefit of the enterprise.

Understanding Evasive Techniques

The goal of real-time communications is to enable ubiquitous access to create a positive user experience. To achieve this goal, real-time communications applications use a range of techniques that render their activities impossible to monitor or control using traditional security measures.

Port hopping randomly uses open ports in a non-deterministic way to provide connectivity, bypassing existing access control policies that look for applications on typically used ports. For example, Yahoo! Instant Messenger runs over Port 23 or Port 80 when the native port is blocked.

Port, or protocol tunneling uses common protocols such as HTTP and FTP to masquerade IM and P2P traffic. All mainstream instant messaging protocols are able to tunnel via HTTP. In addition, Web conferencing chat conversations use port tunneling.

Onion routing enables pseudonymous (or anonymous) communication because messages travel from source to destination via a sequence of proxies (onion routers) which re-route encrypted messages via an unpredictable path. At each stage of the route, only enough information is revealed to send the message to the next stage. Skype and Tor use onion routing, for example.

Encryption can prevent content visibility and control. Skype, GoogleTalk and AIM Pro all encrypt their payload contents to insure message privacy often using proprietary encryption technologies.

Random session behavior alters anticipated session content information such as payload, packet size and rate. Skype, for example, employs random session behavior.

Highly evasive, randomized behavior typified by these applications requires a very specific response to enable organizations to take advantage of the strengths of real-time communications while protecting corporate assets against their vulnerabilities. There is, however, one common factor: these applications enter the corporate network via the Internet gateway, so it is at this point that the detection and policy control must happen. This issue can be compounded when employees remove their laptops from the confines of the secure enterprise network. When they return, the gateway must be able to detect that there has been an infection, or whether a new unsanctioned application has been downloaded and is operating over the enterprise network.

Securing the Web Gateway

Gartner Defines a Secure Web Gateway

According to Gartner, Inc., a secure Web gateway “filters unwanted software/malware from user-initiated Web/Internet traffic and enforces corporate and regulatory policy compliance. To achieve this goal, secure Web gateways must, at a minimum, include URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications, such as instant messaging (IM) and Skype.”

Source: Gartner, Inc., Magic Quadrant for Secure Web Gateway, Sept. 2008



Historically, the available methods of securing the Web gateway have been restricted to URL and content filtering. While this aspect of security is clearly a requirement, when considering the evasive techniques of these real-time collaborative applications, URL filtering is obviously inadequate. While these applications may use HTTP, they don't actually need the HTTP channel to communicate. Therefore any URL filter which focuses purely on HTTP channels and port 80 will miss the randomized, port-hopping, multi-protocol activities of real-time communications applications – and whatever malware might be hitching a ride with them.

Key Requirements to Consider

In its Magic Quadrant for Secure Web Gateway, Sept. 2008, Gartner Inc. outlines the key criteria used in its evaluation of vendor offerings.

- URL Filtering – Databases of known web sites categorized into groups to enforce acceptable usage and productivity and to reduce security risks. Secure Web gateway URL filters should offer page-level categorization, categorization of new sites, dynamic risk analysis of uncategorized sites and pages, and the categorization of search results.
- Malware Filtering – Secure Web gateways should be able to filter malware from all types of inbound and outbound Web traffic. Both signature-based and non-signature-based malware filtering should be provided, as well as a wide range of inspected protocols, ports and traffic types. The identification and remediation of infected PCs would be a nice-to-have capability.
- Application Control – Granular, policy-based control of Web-based applications, such as IM, multiplayer games, Web storage, wikis, P2P, public voice over IP (VoIP), blogs, data-sharing portals, Web conferencing, chat and streaming media is a core requirement for Web 2.0 security. The ability to selectively block or manage features of applications based on numerous policy parameters further increases the value of this functionality.
- Manageability and Scalability – Products should offer consolidated monitoring and reporting, as well as role-based administration.
- Extensive Reporting – Products should support the creation of custom reports and the ability to drill down through summary reports to examine individual protocol usage data. Organizations need to be able to aggregate reports across multiple geographic locations and automatically distribute reports to appropriate executives according to predetermined criteria.

FaceTime's Unified Security Gateway

“FaceTime gives us the perimeter protection and manageability we need to prevent spyware from getting onto our network, taking care of the problem before it can turn into a labor-intensive clean-up operation for the helpdesk.”

Ed Riley, assistant director, networking, telecommunications and systems
Eastern Kentucky University

“FaceTime is an outstanding choice for organizations looking for fine-grained Web communication application controls.”

Source: Gartner, Sept 2008, Secure Web Gateway Magic Quadrant Report

FaceTime's Unified Security Gateway (USG) integrates FaceTime's best-in-class Web filtering, malware protection and application management technologies into a single purpose-built, hardened appliance. From a family of products that stretches back to 1998, the USG has grown to provide organizations with the ability to enable the productive use of Web 2.0 real-time communications technologies, while at the same enforcing safe usage practices, alone or in the context of a unified communications deployment.

USG addresses four key areas of security, control and compliance for real-time communications through a single gateway device, which map to the requirements outlined by Gartner for Secure Web Gateways.

URL Filtering

USG supports the top URL filtering databases and manages user access to those URLs through granular access control policies that integrate with Active Directory and LDAP. As an out-of-band appliance, USG is optimally positioned to handle Web filtering with zero latency – a critical attribute when dealing with real-time applications.

Not Just Gateway Malware control

USG scans all channels – inbound and outbound – for malware traffic, not just the expected port 80/HTML channel, ensuring that port-hopping malware can be accurately tracked and controlled. Benchmarked by third parties at more than 98 percent efficacy, USG provides unique targeted, clientless remediation for only those endpoints showing signs of active infection. All malware detection and remediation is backed by FaceTime Security Labs, the leading lab for real-time communications threat research.

Granular Control of Web Based Applications

USG, with support for more than 1,300 real-time applications as well as tens of thousands of additional applications built on Facebook's social networking platform, can scan and shut down rogue applications immediately. Controls available for public instant messaging include content checking, antivirus checking, ethical boundary setting – even file transfer control over Skype.

Managing and Reporting

FaceTime provides the only true enterprise-scale solution to the challenge of managing the secure and productive use of real-time communications. USG works in heterogeneous environments, integrates with all major directory services, including Active Directory, IBM Lotus Domino, SunOne, iPlanet, and LDAP, and supports multiple authentication mechanisms, such as NTLM, Kerberos, DC Agent, Redirect Authentication, and the ISA plugin. Centralized management and reporting is supported out of the box through the use of a common shared external database to store configuration and reporting information.

Logging, Archiving and Providing the Ability to Retrieve

USG supports the selective or global archiving of messages and file transfers, preserving context and making use of existing email/WORM storage for ease of comprehensive topic matter retrieval – particularly important for e-Discovery compliance. Anti-tampering checksums ensure the integrity of all stored data, and a full range of auditing reports is available.

The Application Control Engine

At the core of the USG is FaceTime's patented technology for classifying and identifying network traffic flows, the Applications Control Engine, or ACE.

ACE provides unparalleled accuracy and application coverage through active monitoring and dynamic correlation of network, content, traffic and other session characteristics. ACE creates a profile of both the specific application in use along with the unique feature being executed (e.g. a file attachment sent via instant messaging) allowing granular policy and control over real-time applications.

Purpose built for today's applications, the engine includes built-in support for daily auto-updates of new applications provided by FaceTime Security Labs. These updates occur through the ongoing collection, analysis and categorization of application information from hundreds of thousands of end-points deployed throughout the world both in enterprise networks and on consumer PCs. This data is analyzed and confirmed by FaceTime Security Labs' researchers to insure that its application database is current.

Leveraging the New Internet. Safely and Securely.

FaceTime USG delivers total protection for real-time communications channels, ensuring that your organization is able to:

- Get visibility into and control over the use of sanctioned and unsanctioned real-time applications
- Enforce security and usage policies across real-time communication and web channels
- Apply granular controls for web usage – for example, allow access to Facebook pages but not to use the Facebook chat real-time communications function
- 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 Web 2.0 world
- Optimize administrative efforts through a unified control center for all data channels

Taken together, these capabilities enable businesses to leverage the benefits of the new Internet, without impacting security or productivity, by delivering an enterprise-grade solution that provides management, security and compliance across the broadest set of consumer and enterprise collaborative applications.

“With unerring accuracy and quick, unobtrusive performance, FaceTime Communications’ Unified Security Gateway appliance easily thwarted virtually all Internet-based malware in our tests, and it gave us complete control, at a fine level, over which social networking and other non-business applications we wanted to allow on our network ...The Unified Security Gateway did a particularly good job of recognizing IM and P2P protocols and applications, thwarting all spyware regardless of their channels of propagation.”

Source: Network Testing Labs



Summary

Web 2.0 is operating inside the enterprise today, and organizations need to address its security and control requirements sooner rather than later. FaceTime approached this challenge from a best practice viewpoint, developing the Unified Security Gateway (USG) as a single point of enforcement and enablement to allow IT to both control and facilitate the productive use of real-time communication, including social networks. Traditional e-mail and web content filtering controls are unable to fully address the security and management vulnerabilities introduced by Web 2.0 alone; FaceTime has the expertise to provide for its safe and productive use by leveraging existing investments for the new layers of protection required.

About FaceTime Communications

FaceTime Communications 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 including 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.

More Information

For more information about FaceTime Communications and FaceTime solutions please visit:

<http://www.facetime.com>
FaceTime Communications
1301 Shoreway Rd
Belmont, CA 94002
Phone: (650) 631-6300
Email: info@facetime.com