

Knight Frank Builds Stronger Web Security with FaceTime

CASE STUDY



ABOUT UNIFIED SECURITY GATEWAY™ (USG)

- Enforces corporate Web usage policies through block, allow or personalized “coaching” and customizable filtering categories
- Simple to install, integrating into existing network infrastructures with zero latency
- Secures real-time content across all communications channels, preventing inadvertent or malicious leakage of information
- Protects against inbound and outbound threats (SpIM, spyware, rootkits, worms, botnets and Trojans)
- Allows tamper-proof logging and archival of IM and UC conversations and file attachments
- Provides visibility, and application level control for more than 2,000 Internet and Web 2.0 applications, including social networks, IM, P2P, IP TV, and Virtual Worlds
- Time and bandwidth allocation quota setting across Web and real-time communications
- Detailed analysis reporting by employee browsing, application usage, time spent, data downloading and IM content transferred

When Singapore’s leading real estate company had a problem with spyware infections coming from its use of Web 2.0 applications, it was FaceTime Communications that provided the most comprehensive solution to today’s web security needs.

Knight Frank Singapore, one of the region’s leading real estate consultancies, can trace its roots back to 1940 when the company was just a two storey shophouse. As part of the global Knight Frank Network, the company provides a full complement of real estate services to both the commercial and residential property markets, handling some of the most prestigious landmark projects in Singapore.

From its offices in the central business district by Raffles Place, Knight Frank’s one hundred and thirty employees regularly use internet based communications to contact partners and customers. It’s an important business tool that allows the company to connect to external partners and customers in order to work more efficiently and productively.

Just a short while ago the Internet was primarily about transmitting and accessing fairly static information via HTTP, FTP and e-mail. But as Facebook’s popularity wanes in favor of newcomers like Twitter, it is clear that the Internet continues to change dramatically. Now dominated by Web 2.0 applications such as instant messaging, P2P, VoIP and social networking sites, organizations are finding that traditional security infrastructures are no match for subversive techniques these applications deploy to ensure users have the full experience.

Spyware Infections Posed Greatest Risk

Knight Frank Singapore was all too aware that its employees were using the network to contact friends and family using instant messaging and sharing files via P2P, even though their use was not authorized. This not only placed the company at risk from unknowingly downloading potentially illegal material, but presented a backdoor for malware to enter in too.

Despite using Websense for protection against internet threats, an increasing amount of spyware was finding its way onto the desktop through the use of Web 2.0 applications. As spyware infections started to become more frequent, Richard Teng, IT Manager of Knight Frank Singapore realized that their current security measures were no match for new internet threats.

“Each spyware infection would take about a half a day to fix, occasionally longer,” says Richard. “It was not economical use of our time and was extremely unproductive for the user. In addition, users accessing some internet applications took up large amounts of bandwidth, restricting the amount available for legitimate business use. The situation became untenable, so we started to look for a replacement secure web gateway.”

Knight Frank compared several internet gateway security products alongside FaceTime Communications’ Unified Security Gateway (USG), including Barracuda and Websense, but found that USG offered a more comprehensive package than its competitors, at a much lower cost.

Web 2.0 Policy Enforcement

FaceTime USG provides Knight Frank with total visibility of all Web 2.0 and real-time applications running on its network, as well as the ability to control access to them without curbing employee productivity and collaboration. This allows the company to enforce its internet usage policy, without relying on employees to police their own activity.

Richard Teng liked USG's easy navigation and found it a simple task to allow or block certain groups of employees or individuals access to specific applications or types of applications. In addition, time of day policies and usage quotas means that employees can still have limited access to authorized non-work related web applications and sites. This feature helps organizations to strike the right balance between productivity and an employee's expectation of web access today.

Another feature of USG's URL filtering is "coaching", which enables Knight Frank to warn employees that the website they are trying to visit is outside the company's internet usage policy. This is an excellent way to educate and remind users of acceptable use when introducing new measures and frequently encourages users to be more amenable to the changes that policy enforcement brings.

Since deploying FaceTime USG, spyware infections are a distant memory. USG delivers real-time protection against malware, rootkits and botnets, and prevents users from accidentally visiting malware infected websites. Zero-day worms that can traverse different IM networks are also blocked with challenge response and message throttling; ensuring that Knight Frank's network is fully protected against Web 2.0 threats.

As Richard Teng concludes, "Without the proper tools to control our users' access to internet based applications they were regularly putting the network at risk of infection and using up large amounts of bandwidth on non-work related matters. Since switching to FaceTime we have not had a single infection, we are confident that our users are only able to access the parts of the internet that are productive and saved a considerable amount of budget too."

About Knight Frank

Knight Frank LLP is a world renowned, UK headquartered global property consultancy that encompasses more than 165 offices in 36 countries across six continents. Along with US based real estate partner, Newmark Knight Frank, the company offers a unique global force in property transactional, management and advisory services with over 5,300 experienced professionals handling some £18.3 billion (US\$36.1 billion) worth of commercial, agricultural and residential real estate annually, advising clients ranging from individual owners and buyers to major developers, investors and corporate tenants. Strong local presence in established and emerging markets around the world, combined with powerful central research and intelligence-sharing, enable Knight Frank to identify opportunities for clients to maximise value in every aspect of their property dealings. Whatever the scale, whatever the location, Knight Frank's global network has the scope and the services to help you achieve your property goals.

About FaceTime Communications

FaceTime Communications enables the safe and productive use of instant messaging, Web usage and Unified Communications platforms. Ranked number one by IDC for five consecutive years, FaceTime's award-winning solutions are used by more than 1,500 customers for security, management and compliance of real-time communications. FaceTime supports or has strategic partnerships with all leading public and enterprise IM network and unified communications providers, including AOL, Google, Microsoft, Yahoo!, Skype, IBM and Jabber.



FaceTime Communications, Inc.
 (888) 349-FACE (3223) *toll free*
 (650) 598-2820 *fax*
 info@facetime.com

Worldwide Headquarters
 1301 Shoreway, Suite 275
 Belmont, CA 94002 USA
 (650) 631-6300 *phone*
 sales@facetime.com

EMEA Headquarters
 400 Thames Valley Park
 Reading, Berkshire, RG6 1PT UK
 +44 (0) 118 963 7469 *phone*
 emea@facetime.com

Asia Pacific
 00 91 80 4112 5250 *phone*
 apac@facetime.com