



The FactPoint Group: Safely Unlocking the Promise of Enterprise 2.0

CONTENTS

Introduction	2
First Take: Web 2.0 Look Dangerous	2
Where Enterprise 2.0 Emerged	2
Departmental Adoption Boosts Enterprise 2.0	2
Micro-blogging Finds Fans	3
Social CRM Emerging in 2010	3
Behind the Growth of Enterprise 2.0	3
IT Challenges with Enterprise 2.0	4
How SonicWALL Addresses Enterprise 2.0 Challenges	4

Tim Clark, Partner
The FactPoint Group
349 First St., Suite A
Los Altos, CA 94022
(650) 233 1748
tclark@factpoint.com

Introduction

Web 2.0 technologies have swept into the workplace, initially to the chagrin of IT administrators and security specialists. However, growing adoption of social networks, blogs, online video and collaboration tools have shifted attitudes into a tentative acceptance of what is now dubbed Enterprise 2.0.

For example, 45% of the Inc. 500, a list of fast-growing U.S. companies, were blogging in 2009, although adoption by more staid Fortune 500 firm was lower¹. In addition, 80% of the Inc. 500 used social networking, and at least 87% said use of Enterprise 2.0 tools had been successful.

First Take: Web 2.0 Looked Dangerous

As Web 2.0 tools and other Web applications began to emerge at work, IT administrators saw them as dangerous, distracting or undesirable, particularly in regards to content downloads

Some saw Web 2.0 as a dangerous productivity killer, luring workers to waste time on popular Web 2.0 sites. Online polling firm YouGov found in 2008 that 42% of office workers aged 18-29 use blogs and social networking sites to discuss work-related issues², raising fears that proprietary data could leak out to social sites.

Where Enterprise 2.0 Emerged

Against those anxieties, however, organizations began to recognize benefits. The Communications department at American Red Cross and Seattle's United Gospel Mission quickly recognized value in this new channel, initially by monitoring what others were saying about them in social media, a defensive activity now called "online reputation management."

Next came CEO Blogs, external and internal, quickly followed by corporate blogging rules on what could and could not be shared. American Express vice chairman Ed Gilligan started an internal blog to communicate with more than 21,000 global employees in its B2B division. On average, each post generated 100 responses, which Gilligan handled personally.

One example that shows the power of social media occurred when the "Mentos eruption" became viral and apprehension turned to a PR opportunity. A YouTube video captured the effect of dropping mint Mentos candies into a two-liter bottle of Diet Coke, causing the Diet Coke to spew foam into the air, producing a coke geyser—and billions of impressions online and on television. U.S. sales of Mentos jumped 20%.

Departmental Adoption Boosts Enterprise 2.0

Corporate departments, such as customer care, looked for ways to incorporate Web 2.0 tools into their missions. Marketers tapped Web 2.0 as a market research tool. For tax season 2010, H&R Block trained 1,000 professionals not only to answer tax questions on its Web site, but also to monitor forums and communities in order to respond to issues as they arose.

¹ "Social Media in the 2009 Inc. 500: New Tools & New Trends," Nora Ganim Barnes, Ph.D., Eric Mattson CEO, Financial Insite Inc., University of Massachusetts, Dartmouth, November 2009.

<http://www.umassd.edu/cmrr/studiesresearch/socialmedia2009.cfm>.

² YouGov, 2008.

Wikis and shared online workspaces became popular tools for collaboration inside and, soon thereafter, outside the enterprise. In Castro Valley, Calif., healthcare provider Sutter Health launched a social media project to win support for a new, seismically safe hospital to replace an old community hospital. Sutter Medical Center used blogs, social networking (Facebook, MySpace, YouTube, and LinkedIn), Twitter, and other free online tools to promote the upgrade. The campaign boosted community support from 80% to above 90%, addressed misinformation about the project, and helped with hospital fund-raising.

Mimicking the success of business-oriented social network LinkedIn, legal publisher Lexis-Nexis Martindale-Hubbell launched a social network strictly for attorneys. Launching in March 2009 with 3,000 beta members, in less than five months Martindale-Hubbell Connected had grown to 15,000 members in 115 countries.

Micro-blogging Finds Fans

The “micro-blogging” application Twitter, which gives users 140 character-or-less “tweets” to impress, has also seen growing popularity as a marketing tool. Think tank Aspen Institute sought to broaden awareness of its Aspen Ideas Festival and stimulate discussion beyond the festival’s meetings. A session to train over 500 people to use Twitter created such intense interest (three times as many as expected and more than half of attendees) that Twitter thought the flood of new users coming from Aspen was a denial-of-service attack.

Similarly, for The Macallan Single Malt Scotch Whisky, tweets were a way to build online buzz among bloggers. The brand invited bloggers about food, spirits and lifestyle to a scotch tasting with paired food courses at a high-end New York City restaurant. The event generated more than 800 tweets plus blog posts that reached 150,031 impressions.

Social CRM Emerging in 2010

The term “social CRM” began to emerge in 2010, and Phoenix International Raceway, which draws 250,000 NASCAR fans to races in April and November, is a pioneer. To stay in touch with fans the rest of the year, it launched a Facebook and Twitter campaign for ongoing dialogue with fans. This has resulted in more demographic data on fans, strong indications of their likes and dislikes, responses to detailed questions, and additional sales.

Faced with fewer donations in the recession, nonprofit War Child Canada chose to use social networking in its “Help Child Soldiers” campaign to raise awareness of the estimated 300,000 child soldiers in the world. It recruited Canadian social media and blogging figures to proselytize its cause and drive donations. The campaign included YouTube video, Twitter and a revamped Facebook page. The result has been over 12,000 new members, an 80% increase in volunteers and a 30% increase on donations.

Behind the Growth of Enterprise 2.0

The 2008-09 economic downturn spurred social media, says analyst Jeremiah Owyang of Altimeter Group. “With overall reduced marketing budgets, companies must innovate and find new channels that are more efficient than the ‘carpet-bombing’ techniques of traditional marketing,” he writes³.

³ Jeremy Owyang, Altimeter Group, blog post Jan. 9, 2010, <http://www.web-strategist.com/blog/2010/01/09/matrix-breakdown-of-advocacy-marketing/>

Despite a perception that Enterprise 2.0 is driven bottoms-up, the 2.0 Adoption Council—an association of large companies that have adopted these technologies—found that management was involved in 73% of its members' projects. Top business drivers included connecting colleagues across teams and geographies (92%); enabling access to subject experts (88%); increasing productivity (81%); capturing and retaining institutional knowledge (78%); and fostering innovation (78%). Gartner predicts that by 2014, social networking services will replace email as the primary vehicle for interpersonal communications for 20% of business users.⁴

IT Challenges with Enterprise 2.0

Despite social media going mainstream, IT departments have cause to be skittish. Web applications threaten to undermine control and policy enforcement across network boundaries. Evolving threats are finding new routes into the corporate network.

The most glaring issue is bandwidth-hungry Internet video. In 2009, Forrester Research reported that 50% of surveyed companies said social networking traffic consumed at least 30% of their bandwidth. To avoid overloading internal networks, administrators seek to prioritize usage so that mission-critical SAP applications do not compete for bandwidth with light-hearted YouTube videos.

In addition, Web 2.0 applications serve as new potential sources of malware, as demonstrated by periodic phishing attacks on Twitter and Facebook users. The Georgia Tech [Information Security Center](#) predicted that malware disguised as benign social networking links would be the top security threat of 2009.⁵ These applications also open new territory for “social engineering” exploits, in which cyber criminals trick users into giving up valuable corporate data.

For example, a series of threats have targeted YouTube users. In mid-2009, cyber criminals used the “comments” and “annotation” features to send users to Web sites, frequently porn sites that subjected them to malware.⁶ In early 2010, hackers showed their versatility by using legitimate YouTube links to distribute spam.⁷ With so many employees using YouTube from work (not to mention other social sites such as Facebook or LinkedIn), these threats to individuals quickly become corporate security headaches too.

Businesses also have reported cases of data leakage, where employees—whether unwittingly or maliciously—have sent proprietary data outside the enterprise.

How SonicWALL® Addresses Enterprise 2.0 Challenges

Traditional firewalls are inadequate to protect environments from Web 2.0 threats. In SonicWALL devices, an Application Firewall with deep packet inspection can determine the nature of network traffic.

The San Francisco Boys & Girls Club, with 275 computers, turned to SonicWALL to block inappropriate YouTube and MySpace content for children and to limit bandwidth for Internet video traffic. Likewise, Birmingham Southern College turned to SonicWALL for network security for 1,000 college-owned PCs, blocking access to troublesome URLs from student labs.

⁴ Gartner Inc., press release, “Gartner Reveals Five Social Software Predictions for 2010 and Beyond,” Feb. 2, 2010. <http://www.gartner.com/it/page.jsp?id=1293114>

⁵ “Emerging Cyber Threats Report for 2009,” Oct. 15, 2008, George Tech Information Security Center, <http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf>

⁶ Panda Labs blog, June 3, 2009 <http://pandalabs.pandasecurity.com/cyber-criminals-target-air-france-youtube-e3-microsoft-project-natal-and-more%E2%80%A6/>

⁷ Panda Labs blog, Feb. 1, 2010, <http://pandalabs.pandasecurity.com/category/YouTube/>.

SonicWALL's Application Firewall can, for example, detect YouTube video traffic and limit bandwidth for that application through a security policy. It can also detect peer-to-peer (P2P) applications⁸, such as BitTorrent, which trades files between users and can introduce mischievous files. Administrators can assign higher bandwidth priority to business-critical applications (e.g., CRM, ERP, accounting, etc.) or groups (C-level executives). The SonicWALL Application Firewall lets administrators fully manage all applications on the network.

Web applications increase opportunities for social engineering threats, such as tricking employees into downloading malicious code. SonicWALL offers a layered approach to social engineering, starting at the Application Firewall, where traffic from known or suspected hackers is blocked. A second layer applies to email messages, the most prevalent social engineering target, by scrutinizing message content for known or suspected social engineering tricks. Underlying SonicWALL's defense is its GRID Network, which collects and vets threat-related information from millions of sources, then shares that information in near real-time.

To stem data leakage, SonicWALL enables IT to create rules that prevent employees from sending email messages tagged "company confidential" outside the company, even through Yahoo! or Gmail accounts. Likewise, IT can identify and block dangerous or noncompliant email attachments.

SonicWALL Unified Threat Management (UTM) firewalls consolidate multiple security and network management functions into a single appliance. That makes security and network bandwidth management easier, more cost-effective and more efficient. Consolidated management and reporting also increase security and improve compliance.

With SonicWALL, organizations can unlock the promise of Web 2.0 while avoiding all the common pitfalls.

⁸ Equifax, 2007, reported that 25% of employees did peer-to-peer file sharing at work.