

### Introduction

Twitter is a popular micro-blogging tool that enables users to communicate to an audience of “followers” using a combination of characters, images and URLs (tiny URLs) – all of which must fit into a 140 character limit. Like email, IM from years ago, and more recently, Social Networking, end-users are rapidly making Twitter an integral part of the corporate application infrastructure. The benefits of using Twitter is it enables users to interact bi-directionally with a wide audience. Marketing can “tweet” about the latest press release or success story; engineers can solicit answers to a perplexing question; and corporate bloggers can tweet about the latest blog post.

There are, however, several challenges that the rapid adoption of Twitter has introduced. Many organizations are unaware of who is using Twitter and for what purpose—and as is the case with social networking applications, policies governing specific usage are non-existent. Finally, users tend to be too trusting, blindly downloading images or accessing shortened, and effectively obfuscated, URLs which can introduce malware to the network.

### The Challenge: Love it or Hate it, Twitter Must be Safely Enabled

Love it or hate it, Twitter use is increasing within the enterprise. According to the [Application Usage and Risk Report \(Fall Edition, 2009\)](#), Twitter was found in 89% of the participating organizations, more than doubling from 35% in the *Application Usage and Risk Report (Spring Edition, 2009)*. More interestingly, the sessions consumed per organization by Twitter users increased 252%, indicating more frequent periods of use, while bandwidth consumed jumped 775% to 184 MB per organization. Even if image transfer is taken into account, this increased usage is significant, given that Twitter communications are limited to a mere 140 characters. As Twitter use explodes, IT is tasked with keeping the network secure while enabling the use of Twitter. Blindly blocking is an inappropriate response because it may be detrimental to organizational productivity and may force users to find alternative means using Twitter (proxies, circumvention tools, etc). Blindly allowing it is also an inappropriate response because it may result in propagation of threats, as well as potential data leakage. Enterprises should follow a systematic process to develop, enable and enforce policies that allow the use of Twitter in a secure manner.

1. **Find out who’s using Twitter.** There are many cases where there may already be a “corporate” Twitter account has been established by marketing or sales, so it is critical that IT determine if these accounts exist, who is using them and what are the associated business objectives – if for no other reason than to be prepared from a public exposure perspective. By meeting with the business groups and discussing the common company goals, IT can use this step to move past the image of “always saying no” toward the role of business enabler.
2. **Develop a corporate Twitter policy.** Once visibility into Twitter usage patterns are determined, enterprises should engage in discussions around what should and should not be said or posted about the company, the competition and the appropriate language. In some cases, determining who can and cannot post may be an appropriate step to take. Educating users on the security risks associated with Twitter is another important facet to encouraging usage for business purposes. With a “click first, think later” mentality, Twitter users tend to place too much trust in what is being posted, introducing malware while placing personal and corporate data at risk.
3. **Use Technology to Monitor and Enforce Policy.** The outcome of each of these discussions should be documented with an explanation of how IT will apply security policies to enable the secure use of Twitter within enterprise environments.

Documenting and enforcing a policy around Twitter can help enterprises improve communications, productivity, and their bottom line while boosting employee morale. An added benefit is that it can help bridge the chasm that commonly exists between the IT department and the business groups.

# Solution Note: Controlling Twitter Use

Enabling Productive Use of Twitter in a Controlled and Secure Manner



## The Solution: Apply Policy Control Over Usage, Block Threats

Palo Alto Networks next-generation firewalls allow enterprises to take a very systematic approach to enabling the secure use of Twitter by determining usage patterns, establishing and enforcing corporate policies that enable the business objectives in a secure manner.

- **Identify Who is Using Twitter:** The first step in safely enabling the use of Twitter is to identify which employees are reading Twitter (reading Tweets) and which are posting to Twitter (Tweeting). Palo Alto Networks identifies Twitter at the service level, which means that even if a desktop client such as TweetDeck, Twhirl or Twitterfeed is in use, the Twitter traffic is identified.
- **Define and Enforce Appropriate Usage Policies:** After determining who is reading Tweets and who is Tweeting, (via integration with Active Directory, LDAP, eDirectory), administrators can apply appropriate usage policies that support the organization's goals and objectives. The ability to delineate between Twitter use overall and Tweeting (Twitter posting), means that user-based policies for reading vs. posting can be deployed as a means of enabling the business, allowing some personal use (where appropriate), while protecting the enterprise from security or business risks. The policy control options go beyond the traditional allow or deny:
  - Allow or deny
  - Allow based on schedule
  - Allow and apply traffic shaping
  - Allow certain application functions
  - Allow but scan
  - Decrypt and inspect
  - Allow for certain users or groups
  - Any combination of the above
- **Protect the Network From Attacks Propagated Across Twitter:** The increased use in social networking applications such as Twitter combined with their relentless barrage of messages have created a very fertile environment for cyber criminals. Studies done by [Kaspersky labs](#) show that social media sites are 10 times more effective at delivering malware than previous methods of email delivery. The reasons are obvious—users trust each other implicitly and it is easy to entice a user to “click here” by including a reference to an article, or an image via a URL. In the case of Twitter, URLs are shortened to maximize the 140 character limit and as such, it is now even easier to propagate malware because the URL is shortened and indecipherable. Once the Twitter usage policy has been created, an equally detailed threat prevention policy can be enabled to detect and block a wide range of threats including spyware, Trojans, viruses, and application vulnerabilities.
- **Monitor Twitter Traffic for Unauthorized Posting:** As part of the balancing act between personal and professional use, enterprises must also evaluate how best to implement policies that are designed to limit unauthorized posting of confidential information. Taking advantage of the Palo Alto Networks data filtering capabilities, administrators can apply policies to detect the posting of confidential data patterns such as project code names, executive names, or emails with varied response options dependent on the policy.

## Summary

The explosive use of Twitter has many enterprises responding in one of two ways; blindly blocking, which may result in lost productivity and business opportunities or blindly allowing, which can expose the business to unnecessary business and security risks. The recommended approach to managing Twitter use is for IT departments to work with the business groups to determine key business requirements and how they can enable the secure use of Twitter without hindering workflow. With a Palo Alto Networks next-generation firewall, the IT department can achieve the best of both worlds by enabling usage while protecting users and the company from a wide range of business and security risks.