

Introduction

Facebook is rapidly extending its influence from the personal world to the corporate world as employees use these applications to get their jobs done. At the same time, many organizations are looking at the nearly 400 million Facebook users as an opportunity to conduct research, execute targeted marketing, gather product feedback and increase awareness. The end result is that Facebook can help organizations improve their bottom line. However, formally enabling the use of Facebook introduces several challenges to organizations. Many organizations are unaware of the how heavily Facebook is being used, or for what purpose. In most cases, policies governing specific usage are non-existent or unenforceable. Finally, users tend to be too trusting, operating in a “click now, think later” mentality which introduces significant security risks.

The Challenge: Enable Usage While Protecting the Business

Like any application that is brought into the enterprise by end-users, blindly allowing Facebook may result in propagation of threats, loss of data and damage to the corporate reputation. Blindly blocking is also an inappropriate response because it may play an important role in the business, and may force users to find alternative means of accessing Facebook (proxies, circumvention tools, etc). Organizations should follow a systematic process to develop, enable and enforce appropriate Facebook usage policies while protecting network resources.

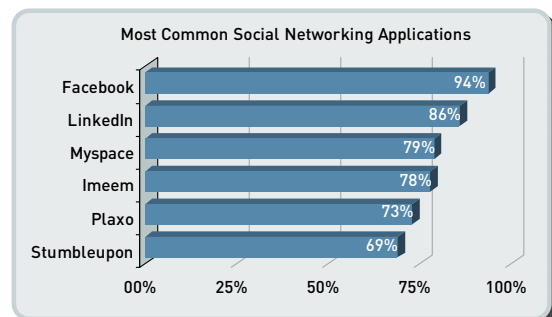
1. **Find out who’s using Facebook.** There are many cases where there may already be a “corporate” Facebook presence established by marketing or sales, so it is critical that IT determine which social networking applications are in use, who is using them and the associated business objectives. By meeting with the business groups and discussing the common company goals, IT can use this step to move away from the image of “always saying no” and towards the role of business enabler.
2. **Develop a corporate Facebook policy.** Once visibility into Facebook usage patterns are determined, organizations should engage in discussions regarding what should and should not be said or posted about the company, the competition and the appropriate language. Educating users on the security risks associated with Facebook is another important element to encouraging usage for business purposes. With a “click first, think later” mentality, Facebook users tend to place too much trust in their friend network, potentially 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 safely and securely enable use of Facebook within enterprise environments.

Documenting and enforcing a social networking usage policy can help organizations improve 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 business groups.

The Solution: Apply Policy Control Over Usage, Block Threats

The [Palo Alto Networks Applopedia](#), provides a list of all social networking applications supported by our next-generation firewalls. According to the [Application Usage and Risk Report \(Fall Edition, 2009\)](#), Facebook was the most popular social networking application, appearing on 94% of the 200+ networks analyzed.

Figure 1: Most common social networking applications detected across more than 200 organizations.



Solution Note: Enabling the Secure Use of Facebook

Reaping the Benefits of Social Networking Applications in a Secure Manner

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

- **Identify Who is Using Facebook:** The first step in safely enabling the use of Facebook (or other social networking applications) is to identify which applications are being used and which employees are using them. Facebook, along with other social networking applications, have added companion applications like email and chat and have opened their platform to developers with Facebook Apps.
- In addition to the base Facebook application, Palo Alto Networks can identify and control Facebook Apps, Facebook Mail, Facebook Chat, Facebook Posting (read-only) and Facebook Social Plugins.

The addition of companion applications helps grow the user-base and strengthen loyalty, but it also makes enabling the secure use of these applications significantly more challenging for organizations. Visibility into Facebook, its companion applications and other social networking applications can help IT better understand the usage patterns in order to make a more informed policy decision.

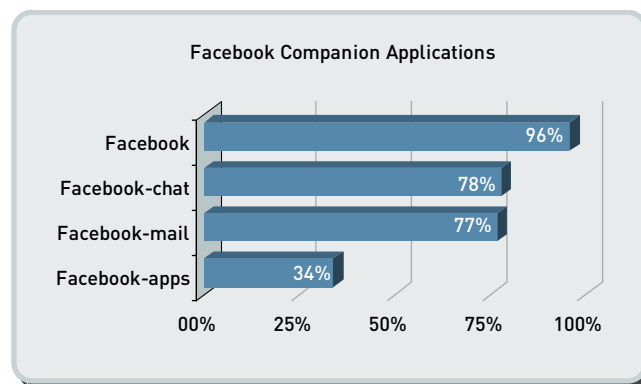


Figure 2: Most common Facebook applications detected across more than 200 different organizations.

- **Define and Enforce Appropriate Usage Policies:** Once the Facebook applications and associated users have been identified (via directory services integration), administrators can apply appropriate usage policies that support the goals and objectives. Enforcing policy control that spans both personal and professional use of Facebook requires a delicate balancing act. Policies must be flexible enough to enable the business and allow some personal use (where appropriate), yet be effective enough to protect the enterprise from security or business risks. For example, a Facebook “read-only” policy can be enabled to strike a balance between block or allow. Using the identity of the specific applications combined with the user information from directory services (Active Directory, LDAP, eDirectory) enables administrators to apply policies that go far beyond the traditional allow or deny. Policy options include:
 - 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

Solution Note: Enabling the Secure Use of Facebook

Reaping the Benefits of Social Networking Applications in a Secure Manner



- **Protect the Network From Attacks Propagated Across Facebook:** With nearly 400 million users exchanging images, links and documents at a breakneck pace and a “click now, think later” mentality, the Facebook population represents a very target-rich environment for cyber criminals. Studies done by [Kaspersky labs](#) show that social networking sites are 10 times more effective at delivering malware than previous methods of email delivery.

The reasons are obvious—social networking users trust each other implicitly and it is easy to entice a user to “click here” by including a reference to a personal photo or video. Koobface is one example of the threats that are being propagated via social networking sites. Koobface can take several different forms. Initially, users were prompted to click on a URL, which downloaded to the PC which looks for personal data. Another variant was released was an “old school” phishing attack that looked like a message from a bank requesting that user credentials be updated. And most recently, Koobface manifested itself by downloading some malware that can disable desktop applications.

With a Palo Alto Networks next-generation firewall, a detailed Facebook application control policy can be augmented with an equally detailed threat prevention policy can be enabled using Palo Alto Networks integrated threat prevention engine. The threat prevention engine detects and blocks a wide range of threats (spyware, Trojans, viruses, application vulnerabilities) including Koobface.

- **Monitor and Control Unauthorized File and Data Transfers:** As part of the balancing act between personal and professional use, organizations must also evaluate how best to implement policies that are designed to limit unauthorized transfer of files and data. Taking advantage of the Palo Alto Networks data filtering capabilities, administrators can apply policies to detect the flow of confidential data patterns (credit card numbers, social security numbers and custom patterns) with varied response options depending on the policy. In addition to the data filtering capabilities, file blocking by type can also be enabled. More than 50 different file types are identified and can be controlled with response options that include outright blocking, block and send the user a warning message or log and send an alert to the administrator.

Summary

Facebook is rapidly gaining acceptance in the enterprise as a tool to improve communication, productivity, and the bottom line. Unfortunately, the speed of adoption is so rapid that many organizations are responding in one of two ways. One response is to block all social networking applications, which results in lost productivity and business opportunities. The other response is to allow all social networking, which can expose the business to unnecessary business and security risks. The best approach is to place the emphasis on control of social networking applications. IT departments must work with the business groups to determine the key business requirements and how they can enable the secure use of Facebook or other social networking applications without hindering workflow. With a Palo Alto Networks next-generation firewall, the IT department can achieve the best of both worlds through unprecedented control that enables usage while protecting users and the company from a wide range of business and security risks.