

Introduction

Since the mid 1990's, web conferencing applications have grown in both popularity and functionality. Even in times of prosperity, this class of applications presents tangible benefits by enabling productive meetings to occur without requiring the time and expense burden associated with business travel. To a certain extent, web conferencing applications exemplify an application whose success is solely dependent upon the Internet. Certainly group meetings could occur by sending the presentation and then making hosting a conference call, but the logistical and ease of use challenges would no doubt limit the success of this style of meeting. Using data from the [Application Usage and Risk Report \(5th Edition, Spring 2010\)](#), 65% of the nearly 350 participating organizations are using at least one web conferencing application. Figure 1 shows the five most commonly used web conferencing applications.

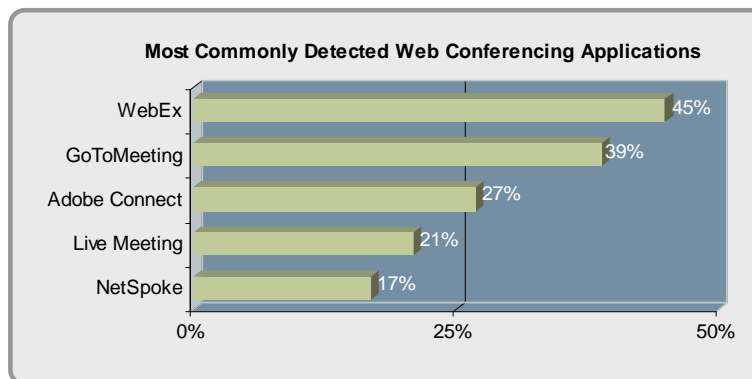


Figure 1: Five most commonly detected Web Conferencing applications.

The reduction of business travel, the ability to perform ad-hoc presentations and collaborate with a worldwide audience are just a few of the tangible business benefits that web conferencing applications can bring. Most would agree that the primary use of web conferencing applications is for business and to that end, the potential risks that they pose are slightly different than those that are introduced by other Internet-borne applications like webmail, social networking and instant messaging.

Web Conferencing Business and Security Risks

The most significant business and security risks that web conferencing applications represent are compliance and vulnerability exploit related. Both of these risks need to be taken into consideration for both an inbound (people presenting to you) and outbound (you are presenting to others) perspective.

- **Compliance:** There are two compliance risks that web conferencing applications pose to organizations. The first is the fact that web conferencing traffic is an unmonitored and unrecorded communications channel. In many, highly regulated industries such as financial services and healthcare, unmonitored communications are not allowed. The second compliance risk that is applicable to all industries is the risks that uncontrolled access to a trusted system pose. Several of the web conferencing applications in figure 1 enable outside users to have access to an employees desktop via companion desktop control functions. Two examples are Webex and Adobe Connect, both of which have added functions that enable remote desktop control. The added remote access function in web conferencing applications can represent a violation of both regulatory and internal policies that dictate which outside sources can access an employee's desktop.
- **Vulnerability exploits:** The incidence of vulnerabilities across web conferencing applications is somewhat small when compared to other applications, due primarily to the fact that they are server applications, however, the risks should not be minimized.

According to the CVE database, nearly all of the web conferencing applications in the top five shown in figure 1 have had known vulnerabilities. For example, WebEx has had 12 reported vulnerabilities, many of which are considered to be high severity [[CVE List](#)] while Adobe Connect has had 9, most of which are Flash related [[CVE List](#)]. The exploits that these vulnerabilities introduce run the gamut of denial of service, remote code execution and browser hijacking.

In order to strike the appropriate balance between enabling the business benefits that web conferencing applications represent and their associated risks, organizations must take a systematic approach to policy control.

The Challenge: Enabling Web Conferencing Policy Control

Whereas other web-based applications are used for both professional and personal purposes, web conferencing applications are used primarily for business (typically, WebEx is not used to share vacation photos). It is very clear that web conferencing applications enable businesses to be more efficient in their sales, marketing and training efforts, all with a target to improving the bottom line.

Organizations need to follow a systematic process to develop, enable and enforce appropriate web conferencing policies, inclusive of companion functions. The primary business use of web conferencing applications makes both the “block or limit web conferencing” and the “head in the sand, allow all” approach is equally inappropriate.

1. **Find out which web conferencing applications are being used and who the users are.** The focus on this investigative phase should be to determine which web conferencing applications are being used and more importantly, which of them have companion functions and what exactly do these functions do. The other piece of information to determine is who is using these applications. These three data points will allow IT to better determine the potential risks and then have a meaningful discussion with the business groups and agree upon the common company goals. Equally important, is that this step can help IT move past the image of “always saying no” and towards the role of business enabler.
2. **Develop a web conferencing application usage policy.** Once visibility into web conferencing usage patterns are determined, the policy development should incorporate those employees who may be in highly sensitive or regulated positions. The policy should incorporate the usage patterns and knowledge of what the companion functions are. Security policies should be documented and conveyed to the users.
3. **Use technology to monitor and enforce policy.** Included in the policy documentation should be an explanation of how IT will apply and enforce the security policies to enable the secure use of web conferencing applications across the organization.

Documenting and enforcing a policy around web conferencing applications can help organizations maintain compliance with government regulations while simultaneously protecting the network from potential vulnerabilities. An added benefit is that it can help bridge the chasm that commonly exists between the IT department and the business groups.

The Solution: Maintain Compliance and Stop Vulnerability Exploits

Palo Alto Networks next-generation firewalls allow organizations to take a very systematic approach to enabling the use of web conferencing applications by determining usage patterns, matching them with business objectives and then establishing (and enforcing) policies that enable the achievement of those business objectives in a secure manner.

- **Identify web conferencing usage patterns.** As stated earlier, it is highly likely that IM is already in use due to its ubiquitous nature. Palo Alto Networks identifies 24 different web conferencing applications (see list [here](#)), with new variants added on a regular basis via a weekly content update. The goal of this phase is to determine which web conferencing variants are in use, by whom, how heavily and for what purpose.

Additional data points will include which of these applications have additional functions outside of the conferencing capabilities. Once the variants in use are found, the behavioral characteristics (file transfer, evasiveness, malware vector, known vulnerabilities) can be used to further determine the level of risk associated with the application.

- **Define and enforce appropriate usage policies.** After determining the usage patterns and business requirements, administrators can apply appropriate usage policies that support the organization's goals and objectives. The ability to delineate which web conferencing applications in use and by whom, means that appropriate enablement policies can be deployed. The identity of the application tied to the user information from enterprise directory services (Active Directory, LDAP, eDirectory) enables administrators to apply policies that go beyond the traditional allow or deny:
 - Allow or deny
 - Allow based on schedule
 - Allow and apply traffic shaping (QoS)
 - Allow certain application functions
 - Allow but scan
 - Decrypt and inspect
 - Allow for certain users or groups
 - Any combination of the above

Using a policy editor that carries a familiar look and feel, experienced firewall administrators can quickly create a web conferencing policy that:

- Allows all employees to use WebEx for web conferencing.
- Scan WebEx traffic for known vulnerabilities.
- Block WebEx Desktop Control function for all employees to maintain compliance.
- Using User-ID, block the use of all other web conferencing applications for those users who are in sensitive or highly regulated positions.
- Apply QoS to ensure that web conferencing applications are neither bandwidth starved, nor do they consume more than they should when compared to more business critical applications.

The use of web conferencing brings clear business benefits to the company so it is important to enable the use while managing the business and security risks.

Summary

At one time, the response to the use of unapproved applications took one of two forms. 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. In the case of web conferencing, the recommended approach to make every attempt to exert the appropriate levels of control. 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.