



Non-Browser Applications: Off the Web, Into Trouble

By The Forsite Group

Introduction

Browserless Internet use was already on the rise in 2004, when Nielsen//NetRatings noted that 76 percent of all home and workplace computer users were accessing online resources and content via media players, instant messaging tools, and file sharing.

The Internet Acceptable Use Policies are clear and up to date. The filter is fine-tuned to block access to unauthorized Web sites as they become known. Employees are educated in how to avoid the worst of what the Web has to offer, and, just to keep them honest, the latest monitoring and reporting capabilities are fully up and running.

Time to sit back and relax?

Of course not. As IT security pros know, there's no resting easy when it comes to managing the inherent risks of the Internet. Just when they might think they have all their bases covered, the soaring use of so-called non-browser applications reminds them there's always something to worry about.

Browserless Internet use was already on the rise in 2004, when Nielsen//NetRatings noted that 76 percent of all home and workplace computer users were accessing online resources and content via media players, instant messaging tools, and file sharing. These days, that number is probably closer to 100 percent—while other non-browser applications like online gaming and remote PC access have become an almost everyday part of users' online activity.

The problems these applications pose will be familiar to any organization that's tried to impose control over workforce Web use. They can severely impact employee productivity. They put sensitive corporate data and network systems at risk. They take a bite out of performance by consuming too much bandwidth. And they raise a range of legal and regulatory compliance concerns.

The steps organizations can take in addressing these issues should also be familiar. Even if you think your employees are sufficiently educated in how to use the Internet safely, heightening their awareness of the particular problems posed by non-browser applications is a smart (and necessary) move. Tailor your organization's Internet usage policy to reflect the added emphasis on non-browser applications—and make sure that mechanisms for enforcement are in place.

Of course, it also helps to supplement those steps with Internet filtering technology that targets the problem. In addition to blocking unauthorized sites, IM, and proxy anonymizers, a Web filtering solution should also boast application-control filtering features that provide the ability to categorize and block streaming media applications, remote access control applications, and online games. That way, companies are much better equipped to deal with the potential dangers of the Internet—whether their employees are using a Web browser or not.

Thinking Outside the Browser

Want a sense of where the online action is? Just look around the workplace.

Want a sense of where the online action is? Just look around the workplace. The graphic designer heavy into house music is streaming cuts from that underground station in Houston. The junior sales rep with a weakness for online gaming is engaged in the final assault on his unseen opponents. The account executive that wants to tweak the dinner party menu on her home computer is using a remote access application to do so. And just about everyone is using IM—to trade jokes, make weekend plans, and maybe even do some work.

It's all going on outside the "confines" of the Web browser—and thus in many cases not monitored, controlled, or secured in any way. Consider it a logical consequence of the progress developers have made in harnessing the power of the Internet as an application platform—and of the appeal and popularity these applications enjoy among users of all kinds.

- A study in October 2007 by Nielsen Media Research found that one in four Internet users had streamed full-length television episodes online in the last three months, including 39 percent of people ages 18 to 34 and 23 percent of those 35 to 54.
- In its survey of 9,000 trend-setting consumers from 17 countries, The Future Laboratory found that 17 percent take part in massively multiplayer online role playing games (MMORPGs). Gary McGraw, author of the book *Exploiting Online Games*, says that there are as many as 12 million people worldwide who are now regularly playing MMORPGs; the game *World of Warcraft* by itself has 8 million subscribers. At any one time, he notes, about half a million people are playing these games together.
- P2P remains popular, with some broadband equipment makers pegging the amount of file-sharing via applications like BitTorrent at 35 percent to 45 percent of all data downloaded in the U.S.; others put it as high as 50 percent to 90 percent.

Clearly, with usage patterns like this, non-browser applications are now thought of as an essential part of the online experience. And, in fact, there sometimes is a legitimate business reason for using them in the workplace, whether for collaborating with other employees in real time or streaming a sales seminar. But it's those other uses that organizations should be concerned about.

A High-Risk Environment

Here's why: Non-browser applications expose organizations to the same vulnerabilities and liabilities that can arise from online activities in a Web browser. These include reduced productivity; security breaches and data leakage; unnecessary consumption of bandwidth; and non-compliance with regulations like HIPAA, Sarbanes-Oxley, and PCI DSS (Payment Card Industry Data Security Standard).

Consider the use of browserless applications in the context of the current environment, as illustrated in the following statistics:

- According to a 2007 survey conducted by Salary.com, employees spend roughly 20 percent of their day on Internet activities not related to their jobs; in a 2006 Harris Interactive survey, 60 percent of respondents admitted to using the Internet for non-work activities while at the workplace.

- The Computer Security Institute (CSI) found that the average annual loss due to security breach doubled for U.S. companies from 2006 to 2007, from \$168,000 to \$350,424. Nearly one-fifth of companies that suffered one or more security incidents said there were victims of targeted malware attacks.
- Malware is ubiquitous—and more dangerous than ever. When researchers at Google ran an analysis of 4.5 million URLs in 2007, they found that 10 percent of those sites (450,000) delivered drive-by downloads of malicious scripts; the researchers suspected 700,000 more sites of harboring malware. Meanwhile, cybercriminals are no longer interested in simply making mischief or gaining notoriety; rather, they're looking to make off with information they can turn around and sell in a thriving underground market. Thus there's a compelling financial incentive to develop malware that's more sophisticated and harder to detect.
- Researchers at the 14th Annual HIPAA Summit in 2007 reported that as of March of that year, nearly 26,000 complaints of HIPAA violations had been lodged, with nearly 400 cases referred to the U.S. Department of Justice for possible criminal prosecution.
- Fines for PCI DSS noncompliance can reach \$25,000 per month—a manageable amount for some larger companies, but less so for smaller ones. It's worth keeping in mind, however, the experience of the TJX Companies: A January 2007 breach of cardholder data may ultimately cost the organization more than \$500 million, according to outside experts—not including associated damage to its brand and reputation.

Given this environment, it's clear that organizations need to take a close look at the risks posed by non-browser applications.

Off Browser, In Trouble

When a much-anticipated MMORPG was scheduled for release in 2004, a major gaming newsletter facetiously noted that workplace productivity would drop by 80 percent.

From streaming and gaming to remote PC access, IM, and P2P, browserless applications pose a range of specific risks—some high, others lower, but all of potential concern to organizations seeking greater control of their employees' online activity.

Streaming Media

When workers are streaming songs, video clips, movies, or other content, they're not doing work. In the Harris Interactive survey cited above, 25 of respondents said they use streaming media at least once a week during the workday. Industry experts have long noted the spike in streaming that occurs in the two hours following lunch in organizations of all sizes and in all sectors. High-profile events like the Olympics or political campaigns also invite abuse of streaming; in fact, outplacement firm Challenger, Gray & Christmas in Chicago estimated that U.S. companies suffered as much as \$1.7 billion in lost productivity as employees streamed or otherwise followed the NCAA Men's Basketball Tournament in March 2008.

Streaming doesn't just sap productivity; it also drains network bandwidth, putting the performance of mission-critical applications in peril. Organizations should also be concerned about the content of the clips employees are streaming: The viewing of inappropriate material could spawn workplace lawsuits, while streaming copyright-protected material might put companies in violation of the law.

Online Gaming

When a much-anticipated MMORPG was scheduled for release in 2004, a major gaming newsletter facetiously noted that workplace productivity would drop by 80 percent. While hard statistics are difficult to come by, there's no question that online gaming can interfere with employee productivity.

Much of that has to do with the very nature of MMORPGs: They never officially end; they require regular, time-consuming participation to keep up with opponents; and they often give rise to a virtual, online social life as players interact with one another. In fact, Online Gamers Anonymous considers the MMORPG the most addictive form of gaming there is.

But gaming also introduces security risks. Observers have long noted that players may seek advantage over opponents by surreptitiously snooping into their systems. If it's an employee's workplace machine or connection that's compromised in such a ploy, then the organization and its data are obviously at risk as well.

But gaming expert Gary McGraw notes there's a security threat coming from the another direction too: the game's manufacturer, which installs monitoring software deep in the kernel to keep track of what's happening on the PC. This software reports back not just on game information, but on other kinds of user behavior unrelated to the game itself—essentially functioning as spyware.

Of course, the ever-increasing complexity and "reality" of MMORPGs poses another problem: excessive consumption of corporate bandwidth.

Remote PC Access

Remote access applications like GoToMyPC, pcAnywhere, and Virtual Network Computing (VNC) have been a boon to harried users who need to track down information on machines at other locations. But they also introduce headaches for IT.

For one thing, they raise the likelihood of security breaches: Typically, those remote aren't as well defended as corporate systems, which means users could be bringing infected data back inside the perimeter, or giving entry to unwanted intruders. For another, they allow sensitive corporate data to slip outside the organization—putting organizations at risk of regulatory noncompliance and increasing exposure to legal liability.

Further, they can serve as distractions when employees should be doing real work. And they also make use of corporate bandwidth that should really be reserved for legitimate purposes.

IM and P2P

The potential risks of these applications are well documented. Both are vectors for worms, Trojans, and other malicious content. Both raise the possibility of data leakage—and thus exposure to legal liability and regulatory noncompliance.

Unfettered use of these applications can also consume valuable bandwidth, as users upload files via IM or download songs, videos, and movies via P2P. Of course, organizations also have to worry about what kind of material is being transferred—and whether it's potentially offensive to other workers or legally protected by its creators.

Gaining Control

By now, organizations know that education and enforcement are the twin pillars to an effective Internet Acceptable Use Policy. In addition to elucidating the dangers of non-browser applications to their employees, companies should make it clear that violating the rules will result in consequences, from warnings to a reduction in Internet privileges—or worse, depending on the behavior. Of course, organizations also need to stay abreast of the dangers and trends in order to update the Internet AUP as needed.

But because an effective Internet AUP isn't sufficient on its own, organizations also need to deploy the appropriate filtering technology. When it comes to addressing the issues associated with browserless applications—as well as with employee Web use in general—a filtering solution should feature the following:

- Pattern-detection capabilities that help in blocking access to IM/P2P, streaming media, gaming, and remote access applications running outside the Web browser
- Filtering of URLs and/or IP addresses, file types (like MP3, MPEG, .zip), HTTP, HTTPS, FTP, newsgroups, and TCP ports
- Defense against threats like spyware, malicious code, phishing sites, and botnets
- Real-time probing that allows administrators to monitor employee Internet activity as it occurs
- Lock-down of a user's workstation when administrator-defined thresholds for accessing inappropriate Web sites or non-browser applications are exceeded
- Blocking of anonymous Web-based proxies using unique proxy-pattern detection
- Forced activation of safe-search mode for all searches, including images, in search engines like Google, Yahoo, and AOL

Having such technology in place helps organizations address the specific risks posed by browserless applications. And when these capabilities work in tandem with a range of other filtering functions, they are able to take a comprehensive approach to monitoring and controlling their employees' Internet activity—giving them a way to preserve productivity, reduce security risks, limit consumption of bandwidth, and reduce their exposure to legal liability and regulatory non-compliance.

Conclusion

The increased use of non-browser applications presents familiar problems for organizations seeking to gain control of their employees' Internet activity. Applications like streaming media, online gaming, remote PC access, and IM and P2P run outside the Web browser and thus may not be covered by traditional Web filtering technology. Thus they pose potential risks to productivity, security, and efficient consumption of bandwidth, while increasing exposure to legal liability.

Fortunately, through a combination of employee education, pro-active enforcement of Internet Acceptable Use Policies, and deployment of Internet filtering technology that makes use of pattern detection to block access to non-browser applications, organizations can become better equipped to address all of the challenges associated with workplace Internet use.