BRADLEY STRATEGY GROUP

-Technology in Plain English-

Keep your PCs safe while surfing the Web

Using Qualys BrowserCheck to make sure your PCs and browsers are up to date

Abstract: Regardless of platform, the Web has become a hub of information and productivity. The browser has evolved to become one of the most-used applications, which has drawn the attention of cyber criminals—making it a potential Achilles heel for security.

What is the most used application on your PC? Stop and consider that for a moment. Depending on your role, and how you use your PC, your mileage may vary, but in an increasingly online, social, cloud-based world, the answer for most people will be the Web browser. From a business perspective, web apps and websites have become the primary gateway for getting things done.

This fact is not lost on cyber criminals. Attackers typically prefer to target the low-hanging fruit, and instigate attacks with the best odds of success. Exploiting vulnerabilities in Web browsers and browser plug-ins offers a very large pool of potential targets, and makes browsers a weak link in the chain for both businesses and consumers.

Under Siege

Qualys gathered information from over one million typical endpoints to survey the state of browser security and vulnerability management. Over half of the systems—more than 500,000 PCs—contained at least one critical vulnerability that could allow an attacker to log keystrokes, monitor financial transactions, or intercept sensitive information like usernames, passwords, bank account, or credit card numbers.

Are half of the companies and individuals in the world simply not keeping their operating systems and Web browsers patched and up to date? That may be the case for a smaller percentage of the vulnerable systems, but the real challenge is keeping up with the pace of frequent updates to more obscure software.

Overlooking the Weakest Link

Whether you're using Internet Explorer, Firefox, Chrome, or Safari, the major Web browsers all have systems in place to automate keeping them up to date. Some businesses prefer to manage the process rather than letting the browser update itself to avoid any potential conflicts or disruptions, but even in those situations they do a fair job at patching and updating the browser itself.

The problem is that there are other elements associated with the browser that may be forgotten or overlooked. As the browsers themselves have adopted more proactive patching and updating practices, the battle lines have shifted, and attackers have focused their efforts on new targets.

Vulnerable add-ons, extensions, and plug-ins may get lost in the shuffle and provide an Achilles heel attackers can use to compromise PCs. High profile browser plug-ins, such as Java or Adobe Flash are frequently the weak link in browser security, but more obscure add-ons are even less likely to be properly maintained and updated.

Qualys found that 82 percent of the systems it monitored have Java installed, and that more than a third of those systems have a vulnerable, outdated version of Java.

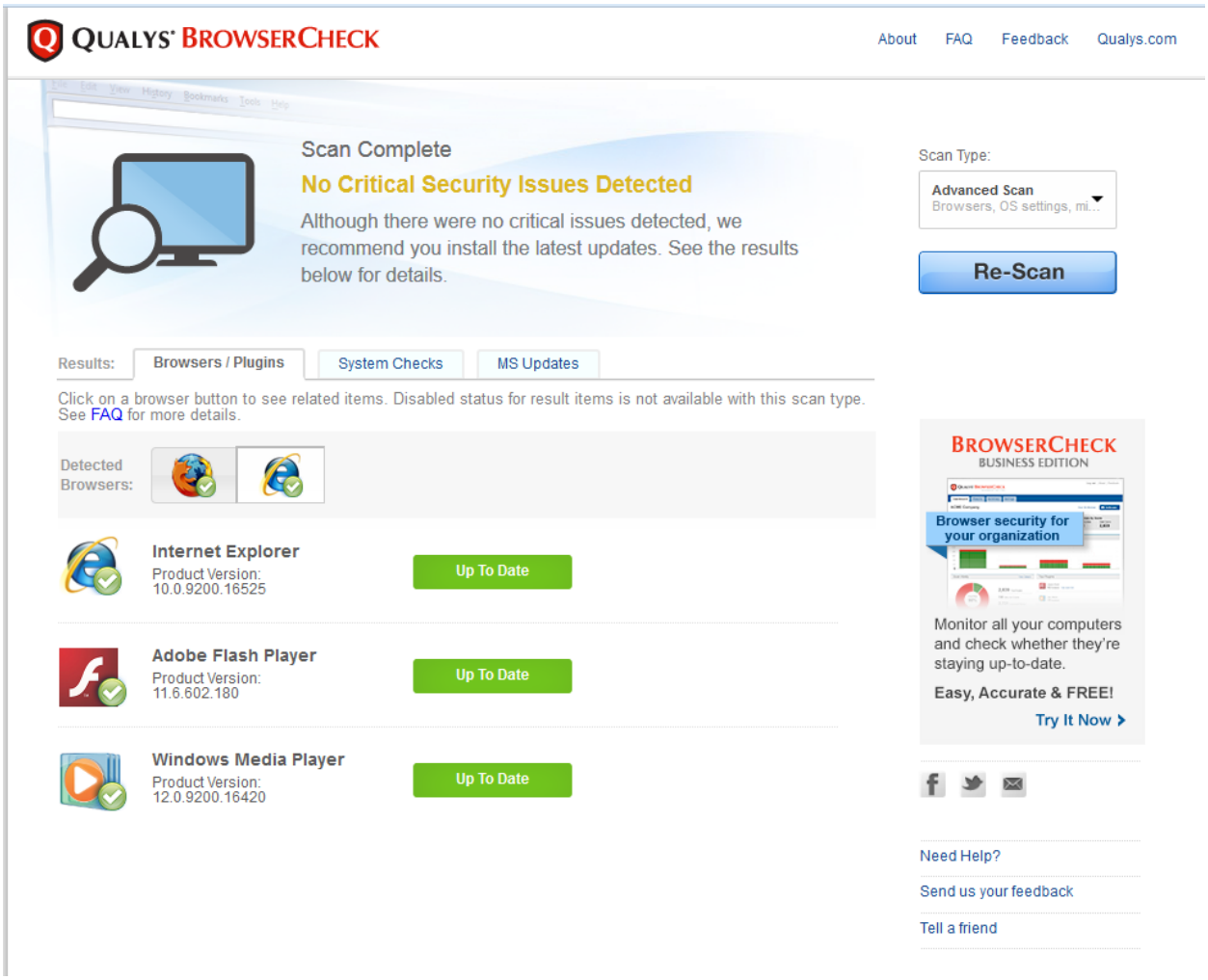
Adobe Flash was found on 67 percent of the tested PCs, and nearly a quarter of those were vulnerable.

Oracle and Adobe have been kept very busy in recent months, scrambling to deal with zero-day vulnerabilities being exploited in the wild. It seems as quickly as patches and updates are released, attackers start targeting a new unknown flaw and the cycle starts all over again.

Clearly, businesses and consumers need help to keep up with the frantic pace, and make sure these plugins and add-ons are patched.

BrowserCheck

The first and most important step is simple enough—make sure all patches and updates are applied when they become available. Unfortunately, that can be a full-time job in and of itself. That's where Qualys BrowserCheck comes in.



Qualys developed a free, cloud-based service to help organizations and individuals simplify the tedious process of figuring out whether their browsers, application plugins and OS patches are out-of-date and what to do to fix them when they are. BrowserCheck was initially designed specifically to scan Web browsers and their associated add-ons for vulnerabilities—hence the name. Since your browser is only as secure as the system it's running on, Qualys has since expanded the focus of BrowserCheck to scan for the latest security updates, and verify important operating system settings on Windows PCs.

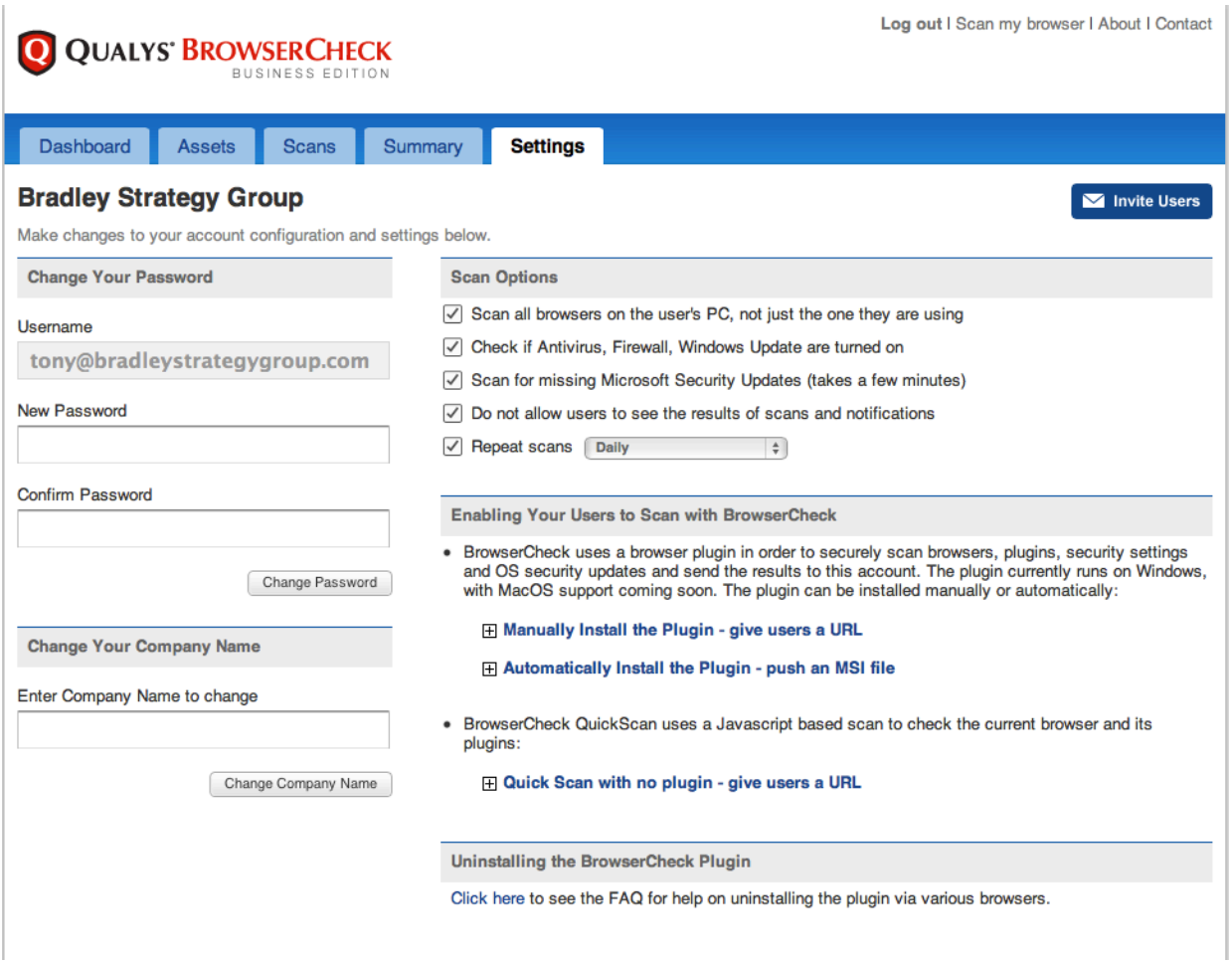
Setting up BrowserCheck only takes a few seconds, and conducting a scan doesn't take much longer than that. BrowserCheck will scan your browsers and plugins, and provide results identifying any issues. In most cases, BrowserCheck provides one-click access to download the latest update, or configure the necessary settings to address the problem and secure your PC.

BrowserCheck Business Edition

The playing field has shifted. According to data in Symantec's Internet Security Threat Report 2013[1], drive-by Web attacks increased by one third, in 2012, and 50 percent of all targeted attacks in 2012 were aimed at businesses with fewer than 2500 employees.

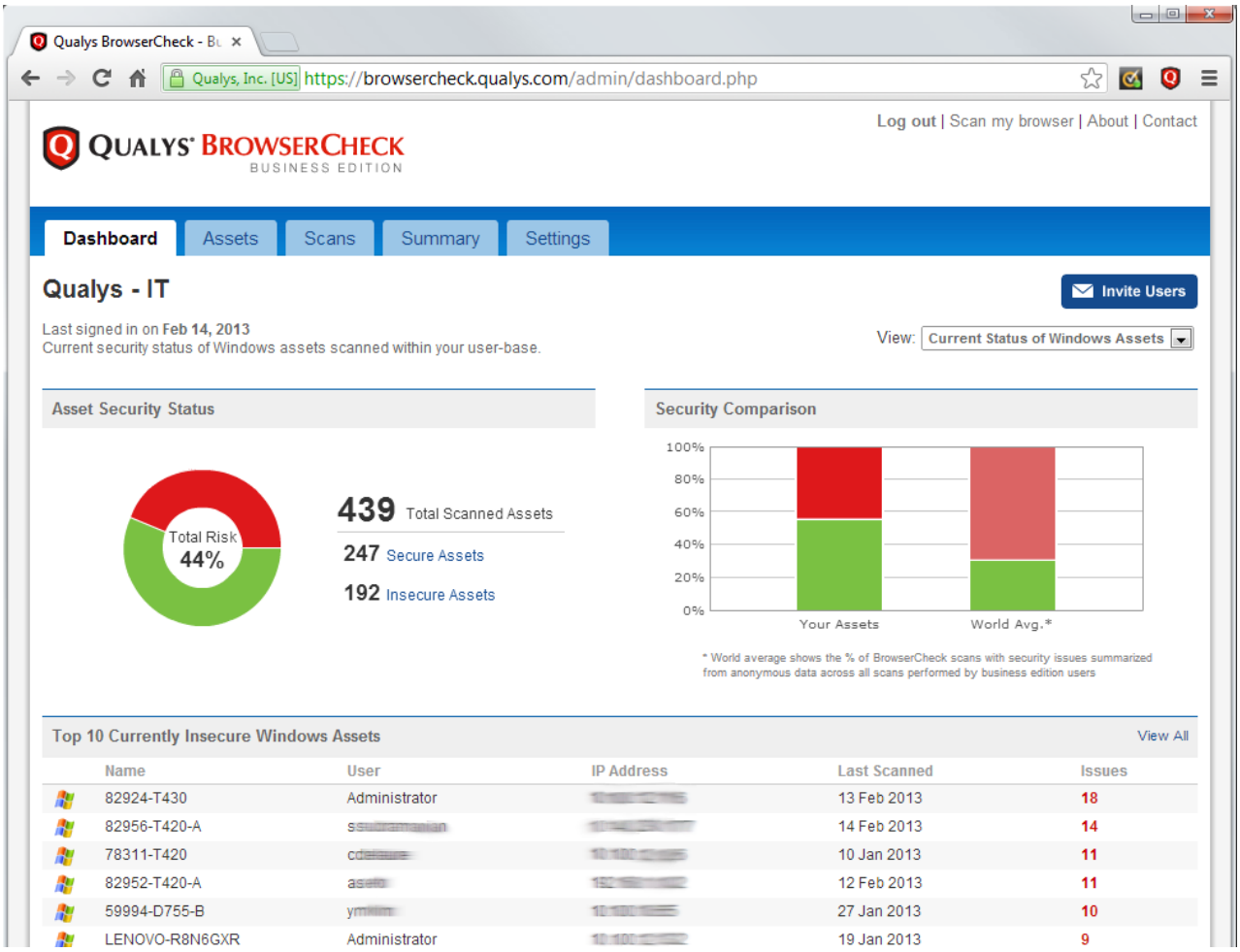
BrowserCheck is a great tool for individuals, but IT administrators need a tool that can be centrally managed and monitored. BrowserCheck Business Edition keeps multiple PCs and browsers up to date through the same free, cloud-based tool that can be managed by the IT admin through a Web-based dashboard.

With the BrowserCheck Business Edition console, IT administrators can view at-a-glance status, and drill down into specific machines to view recent scan results. The console provides the tools and steps necessary to determine how frequently automated scans should be performed, and deploy BrowserCheck to users PC. Organizations can verify that OS updates are installed, track which browsers and plug-ins are installed on each PC, and ensure vulnerabilities are addressed.



With BrowserCheck, businesses can quickly see if their computers are keeping current, or are falling behind, which potentially would give online thieves an

opportunity to steal information or break into corporate networks. Automating these tasks can make businesses more efficient, boost security and show compliance auditors that industry best practices are being followed.



BrowserCheck Business Edition also frees up the IT staff from tedious drudgery. The time and skills of IT personnel can be put to much more important use, and provide more value for the company.

Paul Simmonds, co-founder of The Open Group's Jericho Forum, points out that most small and medium businesses don't even have an IT department, never mind a security team. They just have a person designated to manage IT. Simmonds praises BrowserCheck Business Edition as a very simple way for these organizations to manage security, whether it's for five PCs, or a hundred.

Simmonds explains, "One of the beautiful things is that a lot of network tools out there only operate within their LAN. This is a cloud solution, which means anyone, anywhere can be a part of the systems you manage," adding, "It constantly keeps you up to date and tells you the state of the machines, and it will check issues across all installed browsers regardless of which browser you actually use the tool from."

The Bottom Line

The vast majority of attacks against businesses of all sizes rely on exploiting known vulnerabilities, and attackers are focusing their efforts on low-hanging fruit like browser extensions and add-ons that offer an easy back door into vulnerable systems.

As hackers are increasingly exploit vulnerabilities in browsers and their plug-ins, QualysGuard BrowserCheck is an easy, free way to reduce your risk of attack. For businesses, QualysGuard BrowserCheck Business Edition provides a solution that automates browser security for employee computers, strengthening their security against attack.

About Qualys

Qualys Inc. (NASDAQ: QLYS), is a pioneer and leading provider of cloud security and compliance solutions with over 6,000 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The QualysGuard Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations, including Accuvant, BT, Dell SecureWorks, Fujitsu, NTT, Symantec, Verizon, and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA).

For more information, please visit www.qualys.com/browsercheck.

---

[1] Symantec Internet Security Threat Report (ISTR) 2013: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf