McAfee

Securing Mac OS X

Why we've come to the end of "security through obscurity" for the Mac

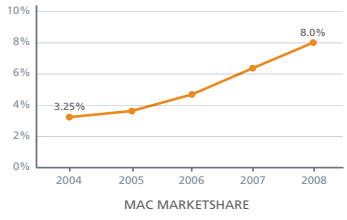
Apple Mac computers are gaining in popularity in business environments, encouraged by a strong marketing campaign from Apple and the growing ability of users to transfer data easily between Windows and Macs. Chances are good some of your own employees are asking to use a Mac rather than a Windows-based PC. Before you say yes, it would be prudent to consider the security implications. Are Macs as inherently secure as many people believe them to be? Does bringing Apple into the workplace create new vulnerabilities? If so, how significant is the risk?

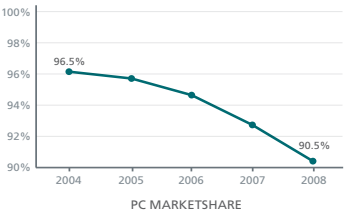
Marketing vs. Reality

Myths and misconceptions abound when it comes to Mac computers. One of the more interesting is the idea that Macs are somehow impervious to the kinds of security attacks (viruses, Trojans, spyware, etc.) that Windows-based PCs are. Perhaps not surprisingly, Apple itself has encouraged this view through its "Mac vs. PC" ad campaign, suggesting over and over in these ads that viruses (and malware) are a PC issue and not a concern for Macs. If only that were the case.

The reality is that Macs are just as vulnerable. If anything, the belief of Mac users that they're impervious exacerbates the vulnerability. For example, the near-total lack of anti-virus/security software installations on Macs increases the likelihood that a successful attack on the community of Mac users will be severe.

Moreover, because well-written malware does not reveal itself to the user, an infected machine with no security software monitoring it can operate at will, with no awareness on the part of the user. Thus, the use of unsecured Macs in the enterprise perforates your security perimeter, creating small gaps that are just large enough to allow hackers in and provide them with an opening into the rest of your network.





Source: Global Market Share Stats

No Longer Flying Under the Radar

This view of Macs as being impervious seems to derive from the fact that, until recently at least, there were so few of them around. They were considered too small a target for hackers and others interested in stealing data. Larger targets generate a bigger "bang for the buck" for cybercriminals, who like legitimate businesses want to maximize their investment. That's helps explain why criminals didn't pay much attention to Macs when they made up a tiny fraction of market share and were used primarily by college students, designers, and musicians. But that's changing.

Macs are gaining market share—roughly doubling in the last three years—while the market share for Windows-based PCs is dropping. In fact, over the past three years, the number of Macs in use has increased by 120 million units. And it's not just the home market that's growing. Today, Macs are the preferred platform of more and more business users, from marketers to engineers to executives. Macs in the workplace often contain the same sensitive data—or have access to that data—as PCs. As a result, hackers and cybercriminals are coming to see Macs as a target with a much greater potential payoff than in the past. It's not coincidental that from 2007 to 2009 the number of Mac-based exploits grew at the same rate as the change in market share for Macs.

An example confirms this changing reality. When users on the Internet sought the notoriously leaked Erin Andrews Peephole Video in July 2009, criminals were quick to seed the internet with bogus links that led users to a fake version on a malicious web server. The server checked the user's browser-agent

and downloaded a Trojan customized to their platform, Win32 or Mac OS X. The fact that the coder went to the trouble to include OS X clients in their attack and did so on a tight schedule suggests that Mac users are now clearly on their radar.

A Window into the Rest of Your Business

The increasing mobility of your workforce and the use of Macs by a growing population of business users, including executives, means that more than just marketing materials are at risk. It's sensitive data, after all, that cybercriminals are after. In the case of high-profile employees, the data on their hard drives (whether Mac or PC) may be significant. But the truly valuable data most likely lives elsewhere, and the unsecured laptop becomes a portal to that data.

For example, a cyberciminal may plant a type of malware on an unsecured Mac that the Mac is immune to. However, because the Mac is on the company network and has access to and is accessible by other computers on the network, the cybercriminal can use the Mac to remotely gain access to data stored on servers for which there is no other opening.

In addition, Macs are susceptible to some types of cross-platform attacks that affect UNIX-style systems in general such as Perl or Bourne-Shell scripts, as well as platform-agnostic technologies such as Java and JavaScript. Vulnerabilities in common cross-platform tools such as Shockwave/Flash players can also expose Macs. Some threats are based not on the underlying code of the platform itself, but on the applications that run on the platform; for example, Microsoft Office macro files with viruses can damage Macs that don't have the security PCs do. Lastly, user behavior is "platform agnostic": users who do not follow safe practices can jeopardize the company's security, regardless of the type of computer they use.

Conclusion: Is Less Than 100% Compliance Acceptable?

If your organization needs to demonstrate the security of your systems, chances are good your auditors won't be happy with 92 percent compliance. Those Macs that now own eight percent or more of the market share need to be secure too. If you're using Macs in your business and they're not secure, can you be sure your business is?

The conclusion is clear: As the market share for Macs grows and Macs play a continually more important role in the enterprise network, companies must make sure they're protected. Fortunately, with McAfee® Endpoint Protection for Mac meeting this requirement is just as easy and economical as it is for the Windows-based PCs in your organization.

McAfee Endpoint Protection for Mac secures Apple Macintosh endpoints with complete, advanced protection, including anti-virus, anti-spyware, firewall, and application protection. McAfee Endpoint Protection for Mac stops malware and other security threats before they can damage or infect Macintosh desktops and laptops and spread throughout your company's network. McAfee Endpoint Protection for Mac also addresses compliance requirements by ensuring that Macs meet the same level of protection as Microsoft Windows–based PCs.

In addition, McAfee is unique in offering a single-console approach to managing endpoint security for both Macs and PCs. McAfee ePolicy Orchestrator® (ePO™) enables you to:

- Respond faster to security incidents, regardless of where they originate
- Update security settings on all endpoints—PCs and Macs—at the same time
- Lower operational management costs by making it easier to manage all endpoints with fewer resources

For more information, visit www.mcafee.com

McAfee®

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

7160brf_tops_apple-os-state-sec_0909_ETMG