

HP CM8050/CM8060 Color MFP security

White paper



Introduction

HP CM8050/8060 Color MFPs with Edgeline will be the first HP MFP devices to include a controller running Microsoft Windows technology. This document will address common concerns about Microsoft® Windows® architecture embedded in MFP devices and its applicability to Edgeline technology.

No accessibility to the Windows® XP Embedded environment

Edgeline architecture does not allow the user or an attacker to have access to many features that are part of the core operating system. For example, we do not allow users to log in and run programs as they can with a desktop PC. We are able to carefully control exactly what applications and services within Windows XP Embedded are allowed to run. By doing this, we can prevent users from accessing features that have security vulnerabilities.

Edgeline does not require frequent Microsoft security patches

Because Windows desktop operating systems require frequent patches, there is a concern this will apply to Edgeline. The Windows XP Embedded operating system is a modular subset of the full Windows XP operating system. We are able to remove applications and infrastructure that are not needed, reducing exposure to features with vulnerabilities, which lessens our dependence on patches. By doing this, we estimate that only one or two patches per year should require HP to immediately release a firmware upgrade. Additionally, each time an Edgeline firmware upgrade is released to customers; we include all Microsoft security hot fixes available at that time.

Edgeline architecture is resistant to Windows viruses

In the following ways, Edgeline architecture makes it very safe from infection by viruses:

- Incoming e-mail is disabled by default. Even when enabled, e-mail is only processed by the Chai VM interpreter, so Windows viruses cannot execute.
- Web page processing is not supported. Viruses spread by web pages, such as ActiveX control viruses, cannot run because Edgeline does not allow web browsing of arbitrary web pages on the network.
- There are no known document viruses that would affect Edgeline. Such viruses are activated when the document is opened by Word or Excel, something that cannot happen on the MFP because it receives only the print-ready version of the document.
- The host USB connection to Windows XP Embedded is restricted to allow only simple file system and I/O connections. Autorun is disabled, preventing viruses and malware from executing from a USB device. Edgeline is resistant to attack by worms by default and can be configured to be even more resistant.
- Jetdirect and the LynxOS firmware provide a firewall between the network and the XP Embedded operating system on Edgeline.
- The firewall prevents worms from detecting that Edgeline has Windows XP embedded installed. Worms that scan the network should ignore Edgeline when they don't detect this Windows "signature."
- Almost all Windows protocols are blocked by the firewall and cannot be accessed by a worm attempting to spread via the network. The few protocols that are allowed through the firewall are analyzed for vulnerabilities and hardened to resist attack.
- The customer can configure Jetdirect to block all network traffic, except from a secure spooler or other known good host PCs. This prevents worms from being able to make any connection to the MFP.

To learn more, visit www.hp.com

© Copyright 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft, Windows and Windows XP are U.S. registered trademarks of Microsoft Corporation.

4AA1-2795ENW, May 2007

