Virtualizing the Browser Against Security Threats: The Dell KACE Secure Browser

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Dell KACE
July 2010
# Table of Contents

Executive Summary .............................................................................................................................................1

The Browser: Today's Target of Opportunity for Attackers ........................................................................1

A Better Approach: Browser Security through Application Virtualization ...............................................2

The Dell KACE Secure Browser: Taking Control of Browser Threats .........................................................3

Virtualization + Containment = Threat Resilience ....................................................................................3

Controlled Execution, Constrained Against Manipulation .........................................................................3

Centralized Management ............................................................................................................................4

EMA Perspective ...........................................................................................................................................4

About Dell KACE .........................................................................................................................................5
Executive Summary

The boundless flexibility of the browser has made it more than the preferred endpoint platform for today’s applications. Its ubiquitous availability, flexibility and extensibility have also made it an increasingly popular target of attack. The browser has become one of the most adaptable computing platforms ever conceived. This adaptability can be leveraged by the malicious, as well as by legitimate users—no small threat considering just how pervasive the browser has become, and the extent of sensitive content it handles.

Many of today’s browser attacks have been designed to evade a number of legacy defenses. This has made it not just important but critical for defenses that will protect the browser itself—and one of the most effective tools of defense is browser virtualization.

With the introduction of the Dell KACE Secure Browser as a freely available resource, Dell KACE introduces security specifically for the browser that features enterprise manageability. The Secure Browser is a virtualized browser that offers control over browser execution; optional white and black list control over browser processes; constraints on changes to the browser and its extensions, add-ons and other browser enhancements; and resilience against browser attacks. Attempted threats or illicit activity are contained within the virtual browser environment, and can be eliminated with a single click by either individual users or centralized remote administration. The Secure Browser can be reset on-demand to roll it back to its initially installed state. This control can be exercised by the individual user, or can be initiated remotely throughout the enterprise via the KACE K1000 Management Appliance.

With these capabilities, KACE introduces a new level of security specific to the browser and browser threats. As part of a defense-in-depth strategy, KACE leverages browser virtualization to provide an added layer of insulation and control against attacks that seek to exploit the seemingly limitless capability of the browser. By leveraging the capabilities of virtualization to secure the browser, KACE acknowledges a need that enterprises can no longer afford to ignore, with a new and potent weapon in the arsenal of defense against today’s browser-focused attacks.

The Browser: Today’s Target of Opportunity for Attackers

The impact of the Web has been nothing short of revolutionary. What began as an evolution in client-server computing has come to dominate—and in many ways, define—today’s application landscape. The seemingly limitless flexibility of the Web has made its universal client, the browser, into an equally universal platform for delivering application content of nearly any kind.

Part of this broad flexibility is enabled by browser extensions, add-ons and so-called “helper objects” that make browsers adaptable to an open-ended range of applications and content. Even greater flexibility has resulted from expanding the client-side execution capability of browsers themselves, through techniques such as those collectively known as AJAX (Asynchronous JavaScript and XML).
Increased opportunity often brings increased risk, however, and the dynamic expansion of the browser has been no exception. Attackers as well as legitimate users can take advantage of the browser's expansive capability. Browsers can be exploited to surreptitiously download threats, through exploitative techniques such as phishing, cross-site scripting (“XSS”), illicit applications, or even through visiting legitimate Web sites having vulnerabilities that have been compromised by attackers. The latter is an example of a systematic approach to exploit, where the attacker first compromises a vulnerable Web site or Web application, then exploits the vulnerability to get the site to host malware (malicious software) as well as the means to propagate “drive-by” downloads of malware using exploits often hidden in what appears to be legitimate Web site content.

This extreme capability, extensibility and flexibility of the browser have made it one of today’s most popular targets of attack. The malicious have turned their attention to the browser and browser enhancements, not only because they expand the attack surface, but because this rich capability is often under the direct control of the user. Users can often make changes to the browser at will, adding extensions, changing security policy, accessing malicious applications that run in the browser, or even simply visiting legitimate Web sites that may have been compromised to become purveyors of drive-by attacks, unknownst to the unsuspecting individual.

When these exposures are exploited to the detriment of the enterprise, the effective result is that the enterprise has placed its security in the hands of the user, and what the user can do with the browser’s virtually unlimited potential. These exploits may not only be transparent to ordinary users—they may also evade common security tools such as desktop antivirus and host intrusion prevention.

A Better Approach: Browser Security through Application Virtualization

What can enterprises do to get better control over the browser’s many security vulnerabilities? One approach is to get better control over the browser itself—and a compelling way to do this is through browser virtualization.

Browser virtualization is an example of application virtualization for the endpoint. Application virtualization may be served from the data center, or it may be a locally executing encapsulation of an application in an isolated virtual environment. This isolated environment can be defined and managed by the enterprise in order to balance browser flexibility with more direct control over a wide range of security risks through the unique capabilities of virtualization. As part of a defense-in-depth strategy, browser virtualization offers a number of distinct security advantages over alternatives.

One approach that combines the management advantages of a connected endpoint with local execution of virtual applications that allows endpoints to work in both online and disconnected mode is the Dell KACE Virtual Kontainer. Recognizing the high security potential of this technology for giving businesses better control over browser security risks, KACE has applied this technology to deliver the Secure Browser.
The Dell KACE Secure Browser: Taking Control of Browser Threats

The Dell KACE Secure Browser is a distinctive implementation of application virtualization in which a defined browser configuration runs in an isolated virtual environment under defined control. This virtual browser executes locally on the end-user system. Any changes that affect the virtualized browser are isolated from areas of the physical system normally accessed by browser activity—including many security threats.

The Secure Browser is more than a virtual browser, however. The Secure Browser augments the inherent security advantages of virtualization with finely grained control over browser actions that enable the Secure Browser to control and prevent a number of browser threats.

The Secure Browser is configured with two of the most popular browser-related applications pre-installed and ready to use: Adobe Acrobat Reader and Adobe Flash Player. Initially, the Secure Browser will feature Mozilla's Firefox, with support for Microsoft Internet Explorer expected to follow.

Dell KACE will make the Secure Browser available as a free tool available from www.dell.com/kace. Although freely distributed, the Secure Browser offers a number of advantages through centralized management via KACE K1000 Management Appliances.

This combination of virtualization, highly granular control over browser activity and centralized management gives the enterprise a powerful new weapon in the fight against browser threats.

Virtualization + Containment = Threat Resilience

The isolation of browser functionality within the Browser Kontainer does more than insulate the underlying system from malicious or high-risk activity. It also combines with the ability of virtualization to bring a new level of resilience against browser threats.

When a threat attempts to compromise the virtual browser, any changes are contained within the virtualized browser environment, and can be eliminated with a single click. By resetting the virtual browser, all changes since its initial installation are quickly undone. This can be initiated either directly by the user, or remotely by an administrator when needed.

This provides a level of protection against threats not available in a physical browser, where compromise may be permanent, difficult to clean up, or may leave concerns about lingering traces which could necessitate a complete system re-installation.

Controlled Execution, Constrained Against Manipulation

The Secure Browser augments these security values with a wide range of control over browser activity, including:

- Alerting of users to the start of processes that might otherwise be unknown to the user. This increases user awareness of potentially malicious processes that would otherwise proceed silently, introducing threats beyond the user's awareness.
• When alerting should be escalated to control, the Secure Browser provides for optional white or black list restrictions on process execution, enhancing the flexibility of control over both known and unknown threats.

• Optional white or black lists can also be applied to Web site access to defend against known malicious sites or cross-site scripting threats. This extends control beyond the browser to include browser-accessible resources. For example, if a legitimate Web site were compromised by a cross-site scripting attack and made to run a script on a remote server, the malicious code would not be allowed to execute as its host site would not appear on the managed white list.

• When managed centrally through the KACE K1000 Management Appliance, these controls can be extended throughout the enterprise while assuring consistency in application.

These features offer direct control over some of the most common browser threats, by placing constraints on where and how the browser can be used.

Centralized Management
Management of the Secure Browser can be accomplished from the KACE K1000 Management Appliance. This enables management functionality to be easily deployed in any environment, with an easy-to-use Web-based console that simplifies access to control.

In addition to centralizing the distribution and control of the Secure Browser, centralized management also gives administrators insight into the details of browser execution, such as running processes, number of blocked attempts to execute a process, and more.

Centralized management also enables the enterprise to respond more effectively to browser security incidents. Should IT operations or security teams be alerted to a potential browser threat, execution of the Secure Browser can be remotely controlled when needed. Should an attack attempt to compromise the virtual browser, that browser instance can be eliminated with a quick reset initiated by a central administrator to reestablish a known good state.

EMA Perspective
The extreme flexibility of the browser has made it the preferred end-user platform for today’s business applications. Unfortunately, these qualities have also attracted an entire breed of threats directed specifically against the browser and its many enhancements and supporting applications.

The severity of these threats cannot be underestimated. Those that succeed in exploiting the browser may gain access to even deeper levels of functionality on the personal endpoint. Many of these are multi-functional attacks that pose a number of threats, not just to multiple system vulnerabilities, but to a number of security risks as well. From the ability to exploit sensitive information directly in the browser itself, to those that leverage the browser as a vector for wider attack propagation, today’s more sophisticated adversaries also see the wide range of capability offered by the universal Web client.

No one can afford to disregard this avenue of attack any longer. Much more direct measures are required to protect both individuals and businesses from browser security risks, given the impact of today’s threats.
No one can afford to disregard this avenue of attack any longer. Much more direct measures are required to protect both individuals and businesses from browser security risks, given the impact of today’s threats. Consider that the browser is not just confined to one underlying system or platform. The browser is truly ubiquitous, and can be found on a wide variety of mobile devices, as well as on traditional personal systems and in freely accessible kiosks. It is used to deliver some of the most highly sensitive content in any business, as well as to access some of the most uncontrolled (some might say “out of control”) functionality available on public networks.

Old models of endpoint security simply are not sufficient in the face of today’s browser threats. Today’s attacks are often multi-functional, able to challenge a wide range of defenses. This means that defense in depth remains a viable strategy—but one in which virtualization can play a central role. As a new and potent element of defense in depth, the Dell KACE Secure Browser leverages application virtualization to introduce a new weapon in the battle against today’s browser threats.

The Secure Browser offers more than threat isolation. In combination with its management via the Dell KACE K1000 Management Appliance, the Secure Browser offers enterprises a new level of control over browser security, through containment, controlled usage, controlled execution, and resilience against browser threats through the advantages of virtualization.

By making the Secure Browser freely available—one of the first such offerings, if not the first, of a secure virtualized browser package—Dell KACE is providing more than a highly worthwhile and much needed public service. It is also offering the Secure Browser to the enterprise in a manageable—and managed—way, giving enterprises a potent new weapon in the battle against threats that recognize the unbounded potential of the universal Web client.

**About Dell KACE**

Dell KACE™ is a leading provider of systems management appliances. The award-winning Dell KACE family of appliances delivers easy-to-use, comprehensive systems management capabilities. Dell KACE customers typically install in one day and enjoy a low total cost of ownership.

Dell KACE is headquartered in Mountain View, California. To learn more about Dell KACE and its product offerings, please visit [www.dell.com/kace](http://www.dell.com/kace) or call 1-877-MGMT-DONE.
About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that specializes in going “beyond the surface” to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2010 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com