Avecto Use Case

Adopting a Least Privilege Approach with Windows 8

Contents

Introduction

As organizations become aware of the heightened internal and external security risk caused by local administrator users, and the need to meet industry or governmental regulations becomes more commonplace, many businesses are using the migration away from Windows XP as a catalyst to achieve a state of least privilege. These migrations to Windows 7/8 are presenting IT managers across the globe with significant challenges.

Two of the largest issues facing IT teams are legacy applications that are not compatible with Windows 8, and User Account Control (UAC) prompts which are displayed whenever an action is taken that requires administrator access.

To overcome these challenges, privilege management technologies such as Avecto's Defendpoint can be implemented as part of the Windows 8 rollout, enabling a range of benefits that remove the burden on the IT team, while empowering the end user.

In this paper, we take a look at these challenges in more detail and learn how by effectively deploying Defendpoint as part of a Windows 8 rollout, it is possible to overcome issues with legacy applications and access rights.

“ Two of the largest issues facing IT teams are legacy applications that are not compatible with Windows 8, and User Account Control (UAC) prompts which are displayed whenever an action is taken that requires administrator access. ”

What's new in Windows 8?

While building on Windows 7 to bring improvements in security, reliability, manageability and performance, Windows 8's new Modern UI brings the most visible difference. Running in parallel with the desktop, it incorporates the Start screen, which replaces the desktop Start menu, and Windows Store apps, which run on the new Windows Runtime (WinRT). The Modern UI and apps are designed to allow Windows 8 to run on a variety of different devices and form factors, including traditional PCs and touch-enabled devices, such as tablets and smartphones.

Press attention and user concerns about the new interface compelled Microsoft to update Windows 8, improving integration between the Modern UI and desktop, and some changes were introduced to make the Modern UI more mouse-friendly. With the latest updates, working with store and desktop apps simultaneously on a traditional PC is a fairly seamless experience.

Despite the emphasis on the new touch-friendly interface and apps, access to the desktop can't be disabled in Windows 8. This results in the same security concerns that existed in Windows 7.

Security and performance

Windows Store apps are more secure and resource-efficient than their desktop counterparts, running in a sandbox that isolates them from each other and the operating system. Apps are suspended automatically when not in use, significantly reducing memory footprint and CPU utilization, which helps to maximize battery life on portable devices and increase virtualization density in datacenters. Apps are updated automatically by the Windows Store, making it easier for organizations to ensure software is always up-to-date.

Businesses can create their own apps and side-load them onto Windows, i.e. bypass the public Windows Store. Side-loaded apps can 'break free' from the WinRT sandbox and access the Windows API and desktop applications by calling libraries using Brokered Windows

"Windows Store apps are more secure and resource-efficient than their desktop counterparts, running in a sandbox that isolates them from each other and the operating system."

Runtime Components, or Network Loopback, where apps interact with Windows using locally installed web services. User Account Control (UAC) remains largely unchanged in Windows 8, and AppLocker, the built-in application whitelisting technology, has been updated to support store apps.

The desktop has not gone away

Despite WinRT being designed from the ground up to be secure, desktop applications are still fully supported in Windows 8, and along with that come the security concerns that were present in Windows 7. Furthermore, side-loaded apps can access the full Windows API under certain conditions, and that introduces an entry point for potential compromise that doesn't exist with standard Windows Store apps.

Least privilege security on Windows 8

In the Modern UI environment, there is no concept of an administrative user. The ability for users to install apps from the Windows Store can be controlled using Group Policy, and application whitelisting used to block users from running apps not approved by IT.

While this presents a considerably improved security outlook for Windows 8, with the exception of Surface RT, the desktop and its inherent security issues are still a major concern. As such, any privilege management issues that existed on Windows 7, are also present in Windows 8. In addition, there may be Windows features, such as the disk defrag utility or the ability to manage advanced features, that users will still need administrative privileges to access.

“ Any privilege management issues that existed on Windows 7 are also present in Windows 8. ”

Limitations of Microsoft's privilege management tools

Windows Vista introduced User Account Control (UAC), a collection of technologies designed to make it easier to run without administrative privileges and to persuade developers to adhere to Microsoft's coding best practices. UAC requires that users have access to administrative privileges, and is largely intended as a way to protect consumers from themselves, thus doesn't provide organizations enough control to meet compliance obligations or ensure basic security.

The Application Compatibility Toolkit (ACT) is a free tool from Microsoft for developing compatibility fixes to solve problems commonly faced when running legacy desktop applications on modern versions of Windows. ACT and UAC both address some issues that might be caused by a lack of user privileges (using file and registry virtualization is one example of this) but neither ACT nor UAC provide the control and flexibility of a full privilege management suite.

For example, a compatibility fix to allow standard users to run installers on demand that require administrative privileges cannot be provided by any of Microsoft's tools. Only a privilege management and application control solution, such as Defendpoint, can solve this problem.

Only a privilege management solution, such as Avecto Defendpoint, allows organizations to completely remove administrative rights from end users.

From the end user standpoint, a privilege management solution is required to transparently integrate privilege elevation into their workflow. UAC requires users to give consent or provide administrative credentials to complete an operation, and prompts cannot be customized, preventing organizations from improving the out-of-box security experience.

> "A privilege management solution such as Defendpoint addresses the limitations of Microsoft's built-in tools, and helps organizations meet compliance obligations."
>
> Andrew Avanessian, EVP Consultancy and Technology Services

Avecto Defendpoint

An endpoint security solution such as Defendpoint addresses the limitations of Microsoft's built-in tools, and helps organizations meet compliance obligations, while providing users with the flexibility needed to work with Windows 8 and desktop applications in a productive manner.

Completely remove administrative privileges

Unlike Windows UAC, Defendpoint allows organizations to completely remove administrative privileges from users, and instead use centrally defined policies to assign elevated privileges to processes, using a locally installed agent. The complete removal of administrative privileges is required to meet most regulatory codes, and eliminates the need to assign users with both standard user and administrative user accounts.

Supporting remote users

The additional challenge presented by notebook users makes removing administrative privileges especially difficult. In cases where an operation cannot be completed due to lack of privileges, Defendpoint allows IT to provide remote users with a one time ability to elevate privileges through challenge/response authentication options and allows management via Remote PowerShell.

On demand elevation

Policies can be created to allow users to elevate processes on demand, and messaging configured to require users to provide a justification for the action. All elevation attempts are audited by Defendpoint, and the Windows 'Run As' options can be removed from the shell context menu to improve the user experience.

End user messaging

UAC prompts represent all-or-nothing options for users to manage privilege issues in Windows. Removing admin privileges results in the most secure desktop, but when administrative privileges are removed, they result in a large increase in calls to the helpdesk so that everyday tasks can be completed. This user frustration often results in users being granted administrative privileges to provide a quick solution.

"Removing admin privileges results in the most secure desktop, but when administrative privileges are removed, they result in a large increase in calls to the helpdesk so that everyday tasks can be completed."

Andrew Avanessian, EVP Consultancy and Technology Services

It's common that these privileges are never revoked, a phenomena referred to as 'privilege creep' and left unchecked. This leaves the IT team exposed through lack of visibility and puts the business under increased security risk.

Defendpoint's end user messaging replaces standard UAC prompts, and allows messages to be branded using logos, with custom text and multilingual support to ensure messages are clear and straightforward – with options for the user to easily request access if the application falls outside of standard policies.

Application control

Defendpoint improves upon Windows AppLocker by providing support for all versions of Windows, from XP through to Windows 8, including support for Windows 8 store apps. It leverages a flexible policy engine so that rules can be quickly deployed either company-wide, or targeted to individual devices or small groups.

Auditing and reporting

Auditing privileges allows IT to analyze which applications require administrative privileges and the reasons why, to allow organizations to generate policies based on this information. The built-in reporting can be used to analyze collected data and the optional enterprise reporting solution uses SQL Server, providing dashboards and advanced reporting capabilities to give IT greater insight into privilege use. Admin users can be tracked and analyzed over time to demonstrate a reduction in privileged users for compliance, and ensure complete visibility of activity.

Summary

Without a flexible endpoint security solution in place, businesses that operate with Window 8 across their employee base will be presented with the same ongoing dilemma as Windows 7 and Vista users, finding it impossible to balance security with user productivity.

The danger represented by administrator rights means that their use within an organization is no longer a viable option. This means that a solution must be found to ensure users can operate effectively using a standard account – and the native tools provided by Microsoft do not offer this flexible capability.

Defendpoint therefore allows businesses of all sizes to achieve a positive user experience, which drives productivity – without compromising organizational security.

About Avecto

Avecto is a security software company that sees security as an enabler. We're all about finding technical solutions aligned with commercial benefits. We know, from experience, that technology has the power to facilitate transformational change.

Our proactive endpoint security software Defendpoint delivers on this promise by uniquely combining the technologies of Privilege Management, Application Control and Sandboxing. The benefits of the individual modules and our consultative methodology provides clients with a clearly mapped journey against measurable objectives to ensure project success.

And our focus on the end user means you can finally empower people to work freely without security compromise. So, with this positive approach, endpoint security can be the startpoint of freedom.

SC Magazine Awards 2013 Europe Winner

2013 Computing Security Awards Winner New Product of the Year

Deloitte. Technology Fast50 UK 2014

Microsoft Partner Gold Application Development

UK

Hobart House
Cheadle Royal Business Park
Cheadle, Cheshire, SK8 3SR

Phone +44 (0)845 519 0114
Fax +44 (0)845 519 0115

Americas

125 Cambridge Park Drive
Suite 301, Cambridge, MA 02140
USA

Phone 978-703-4169
Fax 978 910 0448

Avecto
@avecto
+Avecto

avecto.com
info@avecto.com