Avecto Use Case

Adopting a Least Privilege Approach with Windows 7

Contents

Introduction

Organizations across the globe are becoming increasingly aware of the heightened internal and external security risk caused by local administrator users.

The Edward Snowden data breach has served as an example of the damage that can be caused by employees with excessive privileges.

With support for Windows XP having ended in April 2014, many businesses are using the migration to Windows 7 as a catalyst to achieve a state of least privilege to improve their security defenses, which is presenting IT Managers across the globe with significant challenges.

Two of the largest issues facing IT teams when migrating to Windows 7 are application remediation and User Account Control (UAC) prompts which are displayed whenever an action is taken that requires administrator access.

To overcome these challenges, endpoint security technologies such as Avecto Defendpoint can be implemented as part of the Windows 7 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 share a real life example of how Avecto's software was effectively deployed by a large engineering organization during its Windows 7 rollout.

> "When users run with standard user rights instead of administrative rights, the security configuration of the system, including antivirus and firewall, is protected. This provides users with a secure area that can protect their account and the rest of the system."
>
> TechNet.microsoft.com

Planning for application remediation

Prior to the deployment of a new Windows 7 image, all applications in the organization's eco system must be first identified and then tested to determine if the application needs retirement, upgrade, recoding, shimming or virtualizing before the rollout takes place. The plan for checking and updating all of the applications as required must be then included in the wider project plan.

This process is extremely resource intensive, but additional complications arise from the sheer number of applications installed across all desktops. Recent research conducted by Forrester has identified that on average, circa 1,500 applications will be supported by a global enterprise. However, this figure does not account for additional applications that may have been installed by users over time, which will need to be identified as part of the project migration.

Defendpoint allows the application to write directly to the paths it needs, rather than requiring any change to the application itself. This saves the time and resource of application testing and updating before the Windows 7 rollout.

The application can be added to a trusted area for users to download, or the hash of the application can be added as a trusted execution. Importantly, even Windows Store apps or applications that do not need admin rights to install, such as Dropbox, can also be controlled and access restricted if required, even when running on a standard account.

> "In practical terms, the benefit is illustrated in the significant drop of application and printer install requests we receive and this has freed resource to focus on the next big project."

Mark Stephensen,
Desktop Infrastructure Lead,
University of Dundee

Overcoming UAC prompts

Prior to the deployment of a new Windows 7 image, all applications in the organization's eco system must be first identified and then tested to determine if the application needs retirement, upgrade, recoding, shimming or virtualizing before the rollout takes place. The plan for checking and updating all of the applications as required must be then included in the wider project plan.

Analysts such as Gartner and IDC agree that the benefits of operating without administrator rights are impossible to ignore. The process of removing admin accounts from employees and adopting standard user accounts is itself straightforward - when User Account Control (UAC) is enabled in Windows 7/8, all user accounts will run with standard user rights. However, once users are deployed with a standard user account, users will be subjected to UAC prompts asking them for credentials of an administrator account every time an action affects the OS in some way. A large number of OS features for customization and basic system maintenance are locked away behind the safety of UAC, with the standard user receiving a UAC message when they try to perform these actions.

Popular tasks requiring admin rights in Windows 7/8:

- Changing power setting
- Updating time
- Network settings
- Connecting a printer
- Setting data backups

These out-of-the-box prompts cannot be customized in any way and the 'all or nothing' approach often results in confusion and loss of productivity for the user, with an influx of helpdesk calls for the IT team.

The danger here, as well as the resource impact, is that users are gradually granted administrative rights to solve their immediate requirement, rather than solving the underlying problem. Over time, the organization finds itself with unmonitored and uncontrolled admin accounts, which creates a significant security risk. Malware seeks out

> "Avecto's software was clearly designed to make user rights management as simple as possible. The fact that it eliminates a lot of overhead, saves time and is affordably priced, makes the ROI easy to demonstrate."

Jon Bain, Technical Lead, Client Support Group, Crutchfield

admin accounts where it can attack the operating system, extend to the data centre and inflict the most damage.

The solution is to adopt an approach of least privilege whereby the applications, tasks and scripts themselves are assigned administrative rights as needed, rather than elevating the permissions of the user. This allows organizations to increase security without user lockdown.

In practice: Customer scenario

During a recent Windows 7 migration project at a European engineering organization, the IT department discovered over 15,000 unique applications that were installed across the Windows XP estate. The team knew that although these applications were installed, owing to the size of the estate and geographical restrictions, they had no visibility of how many were in use and relied upon for day-to-day operations.

The large proportion of these applications could only be installed because many of the users had been given local administrative accounts to aid with the migration to Windows XP in the first place. Most other users eventually became administrators when the support desk couldn't resolve issues such as with legacy applications, or when a user was disconnected from the internal network beyond standard IT support's reach. As is often the case, it was considered easier to give the user an administrative account to overcome their immediate problems than fix the underlying cause.

> "The number of privileged accounts in any organization is typically 3–4 times the number of employees."

CyberArk 2013 Privileged Account Security & Compliance Survey

Using Defendpoint to gain visibility of the challenge

Using Defendpoint the organization made use of the Admin Rights Audit feature to identify the detail of the applications being executed and the privileges required for execution, giving a complete picture. Once complete, the organization had an accurate picture of which applications needed to be included in their Standard Operating Environment (SOE) and which ones could be safely excluded.

By utilizing Defendpoint's seamless elevation, those applications that previously needed admin rights to function on XP now worked perfectly under a standard user account on Windows 7, without the risk of administrative access.

Designing granular policies

Through analysis of user roles and requirements, the organization was able to work with an Avecto technical consultant to design policies to improve the user experience, while hardening the underlying OS from exploitation and misconfiguration.

Using advanced matching criteria, designed to reduce administration over time, any application, task or script would be blocked from running unless explicitly trusted. When combined with one of multiple "break-glass" options, the IT team was able to ensure that no user was ever without the ability to elevate an application if required, but importantly, they gained full visibility of the actions through Avecto's enterprise reporting.

This meant that any applications not included in the SOE could still be securely executed by users, which was a critical factor to project success. Through regular review of the reporting dashboard, the team was able to identify trends in application demand to provide proactive application management and deployment. This information was then fed back into the policy design as all application definitions were carried through from the endpoint.

> "Privileged accounts have become a favored target for attackers as they open the doors to a company's core assets once the perimeter of an organization has been breached."

IDC Technology Spotlight,
October 2013

Overcoming UAC challenges

Secondary to application remediation, User Account Control prompts in Windows 7 are often sighted as being responsible for inflated helpdesk calls post deployment.

Utilizing Avecto's software, the organization was able to replace all UAC prompts with a message that was much more recognizable and informative to the end users. Unlike the built-in Windows UAC functionality, which is either on or off, the solution can be configured to replace any or all of the prompts using granular targeting.

With this approach, the organization could now truly provide the granularity required within the Windows 7 environment. Best of all, these prompts were customized with the company logo and written in the company's own tone of voice, containing full details of how the user can self-service their own requirements and providing reason codes for audit trails. These prompts were then assigned to different user types, giving a personalized experience for all employees.

Summary

By working with Avecto and adopting a least privilege approach, the organization was able to successfully deploy Windows 7 across its large estate of desktops, increasing security without impacting on user productivity.

Avecto was able to aid them the entire way. By firstly conducting an initial audit to identify demand for applications and usage across the company, Avecto was then able to provide seamless elevation of applications, tasks and scripts on the new Windows 7 operating system. In addition, customized messages and branding improved the end user experience, while ongoing reporting will ensure that rules and policies are updated over time. This was achieved from one console, and all while driving down helpdesk calls.

> “Any business that is upgrading to Windows 7 should use Avecto’s software. Not only did it save us a lot of time and effort, it gave our employees the capability to do their jobs without having to grant everyone full admin rights.”

Rick Bywalski, IT Support Technician, Holland & Knight LLP

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