



TECHNOLOGY AUDIT

# Privilege Guard 2.6

Avecto

## SUMMARY

### IMPACT

Privilege Guard allows businesses to lock down end-user desktops in a flexible way to reduce support costs and improve security. By applying a principle of “least privilege”, Privilege Guard eliminates the problems that prevent businesses from applying universal lockdown policies, while sparing end users the negative effects of lockdown.

### KEY FINDINGS

<b>Strengths:</b>	<ul style="list-style-type: none"><li>✓ Fine-grained policy-based allocation of administrator rights to both specific applications and end users, and the auditing of end-user actions.</li><li>✓ Ability to allow power users to install only authorized applications.</li></ul>
<b>Weaknesses:</b>	<ul style="list-style-type: none"><li>✗ Privilege Guard only works with Windows desktops and servers.</li></ul>
<b>Key Facts:</b>	<ul style="list-style-type: none"><li>i Privilege Guard’s client software does not alter the Windows client kernel.</li><li>i Privilege Guard can be managed as an extension to Microsoft Active Directory Group Policy among other methods.</li></ul>

### OVUM VIEW

Desktop lockdown is fast becoming a standard IT practice because of its effects on support costs and security. However, when IT departments attempt to implement lockdown using only native Windows controls they face problems concerning end-user productivity and the need to exempt many desktops from the policy. This is because Windows presents IT administrators with what is effectively an all-or-nothing choice between full lockdown (standard user rights) or zero lockdown (administrator rights). Recent changes to the way that administrator rights are allocated in Windows 7 have not significantly altered this.



Avecto is one of a very small number of suppliers that are addressing this problem with software that allows user privileges to be granted in a more flexible way. Avecto launched Privilege Guard in 2008 and has since racked up an impressive list of large implementations by businesses in a wide range of industries. As well as lowering the cost of desktop support, Privilege Guard increases desktop security and has very strong prospects of delivering rapid return on investment.

### Recommendations

- Businesses with 1,000 end users or more should consider including Privilege Guard as part of their standard desktop build.
- Planned desktop migrations from Windows XP to Windows 7 should be considered as an opportunity to implement Privilege Guard.

## FUNCTIONALITY

### SOLUTION OVERVIEW

Desktop operating systems are a major vulnerability with respect to IT security. For this reason many IT organizations lock down desktops by denying local administrator rights or privileges to end users. As well as preventing unauthorized changes to firewall and anti-virus settings, this prevents the installation of most unauthorized software that can compromise security and reduce desktop reliability. The latter is very significant.

Although the cost of desktop ownership is extremely difficult to gauge and varies considerably according to the sophistication of IT operations, lockdown certainly has major benefits. As a result, one recent and large survey found that about two-thirds of businesses have implemented a desktop lockdown policy. However, when using only native Windows controls, lockdown suffers the following problems:

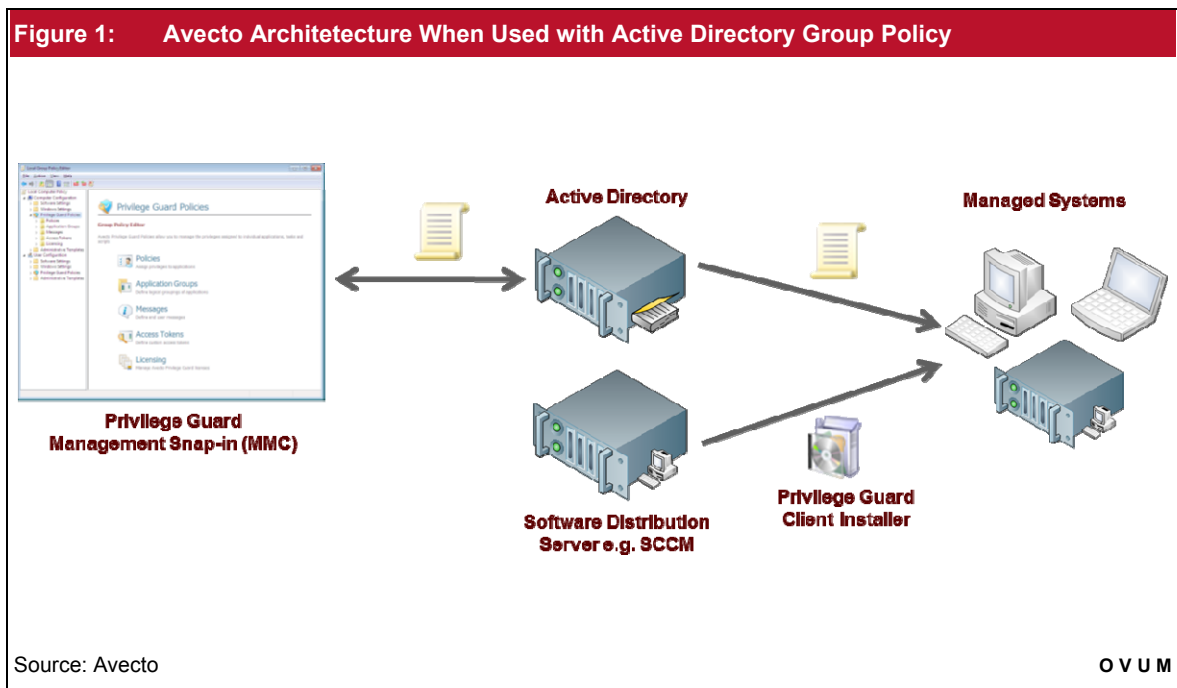
- **Lockdown reduces end-user productivity:** Although it might lower the total number of support calls, lockdown forces end users to call support desks to perform even simple tasks such as installing printer drivers or changing time and date settings. This makes lockdown unpopular with end users.
- **Awkward applications prevent universal lockdown:** Some applications cannot run on locked-down desktops because they need administrators' rights. These include widely used off-the-shelf packaged applications, Java and Active-X controls that need administrator rights to update, and in-house-developed applications. This forces businesses to create exceptions to their lockdown policies, potentially leading to compromised security. Large organizations that run hundreds of applications are likely to suffer from this problem.
- **Power users prevent universal lockdown:** Some groups of users such as developers need to be able to independently install applications.

Privilege Guard solves these problems by allowing administrative rights to be granted in a fine-grained, flexible, and audited way. The design principle is to allow minimum necessary privileges to be granted (least privilege), eliminating the stark choice between total lockdown and the granting of full administrative privileges.

Privilege Guard can grant administrator rights to specific applications that require them without raising the overall rights of end users or other applications. Where necessary, Privilege Guard can grant elevated rights to power users and allow them to install white-listed or authorized applications while auditing all the systems actions that these users complete.

Although Privilege Guard is mostly used for desktop control, it can also be applied to Windows servers, giving fine-grained and audited control of changes to a server's underlying configuration such as registry settings, system files, and services.

Most implementations will see Privilege Guard managed via extensions to Microsoft's Active Directory Group Policy, but the software also works with Novell's ZENworks' Group Policy, or can be exported and then deployed as an XML file.





## SOLUTION ANALYSIS

### Windows User Account Control

Microsoft recognizes the conflict between the benefits of locking down desktops and the limitations that it imposes on end users, as well as the impossibility of locking down desktops that run applications that require administrative rights. For this reason it added a feature called User Account Control to Windows Vista, and then refined UAC for Windows 7. Given the large number of organizations that are about to migrate desktops from Windows XP to Windows 7, UAC is worth examining.

UAC makes only minor differences to users who log on with standard user rights. It eliminates the need for administrators' rights to perform basic actions that do not threaten security, such as changing time and date settings, or using Windows Update to apply OS updates. It also reduces the number of badly-behaved applications that need administrators' rights to run, by virtualizing file systems and registries. For the many remaining applications that still require administrators' rights, UAC delivers one more benefit. Those applications no longer simply crash when they need elevated privileges. Instead, UAC tells users that they need to enter an administrators' password to allow that application to proceed.

That means that to support awkward applications, users must still be given an administrators' password. Although UAC makes logging on as an administrator safer than it was previously, it does not make it hugely safer. Customers will still face major risks if they give administrators' rights to end-users. Before UAC, logging on as an administrator automatically gave elevated rights to all applications. With UAC, whenever an application requires elevated rights, users who have logged on as administrators are prompted to give their consent by pressing "OK." This improves security and integrity for administrators, by applying a manual check, and a block against malware. However it does not change the fact that users who are given administrators' passwords have been given the keys to the kingdom, and can install whatever applications they want, and can change system settings.

### Fine-Grained Rationing of Privileges

Unlike UAC, Privilege Guard enables users to log on with a standard user account and does not require them to have access to an administrative account. It works seamlessly with UAC and will eliminate inappropriate UAC prompts. It allows very fine-grained or detailed adjustments of the rights granted to individual applications and end users.

When Privilege Guard is used to raise the rights of individual applications, it does not increase the rights of end users or other applications. All other applications continue to run in the context of the logged-in user. To be technically accurate, Privilege Guard elevates rights on individual processes.

When Privilege Guard is used to raise the rights of applications or white-listed applications, it can identify applications or installation packages based on combinations of trusted file paths, trusted publishers, or hashes for unsigned code.

Alternatively, Privilege Guard can grant end users the right to install any application regardless of white lists. In these cases the Windows “run as” and “run as administrator” menu items can be replaced with Privilege Guard’s “on-demand” elevation capability, which provides a controlled and audited mechanism to handle more flexible lockdown. Power users can also be granted rights to change Windows settings for firewalls and systems tools, although this is not common practice.

### **Warning Messages and Audits**

Granting elevated rights to power users opens the door to security risks and support problems resulting from application conflicts. For this reason Privilege Guard can be configured to issue messages designed to make users think about what they are doing. The messages, which remind users that their actions are audited, can request them to make “for the record” statements that they are aware of their actions. The messages, which are customizable and available in multiple languages, can give users the option to send requests for extended rights to administrators, such as to install a specific application.

All actions completed using elevated rights are audited, as is the granting of those rights. The audits can be cross-referenced to application licensing. Avecto says the level of auditing is flexible and comprehensive.

### **Compliance**

Avecto’s customers already include about 10% of local government organizations in the UK that use Privilege Guard to help achieve compliance with the UK’s Government GCSX Code of Connection (CoCo) security controls. CoCo controls include explicit requirements for users’ web browsers to run with standard user rights, as well as restrictions on the use of unauthorized software and changes to system configurations, and the auditing of end users.

In the US, Privilege Guard allows businesses to meet one of the requirements of the Federal Desktop Core Configuration, which says that contractors’ desktops must be configured with minimum user privileges. Privilege Guard carries the Windows Compatible logo, and Avecto has attained Microsoft Gold Partner accreditation.

### **No Modification to Windows Kernel**

Privilege Guard requires client software to be installed on desktops. Importantly, the client software does not modify the host Windows OS kernel but operates as a system level service in “user mode”. This significantly reduces the chances of software conflicts.

### **Working with Virtualized Desktops**

Avecto demonstrated Privilege Guard to Ovum on a desktop that was a VM running on VMware’s ESX/ESXi bare-metal hypervisor. Privilege Guard also works with Microsoft and Citrix hypervisors as well application virtualization products such as Microsoft Application Virtualization (App-V) and Symantec SVS.



## PRODUCT STRATEGY

Avecto was founded in 2007 and is headquartered in Manchester, UK. It launched Privilege Guard in September 2008 and has sold the product to over 100 organizations in a wide range of industries. Compliance and security concerns have driven sales to a number of large financial services suppliers, defense contractors, and pharmaceutical companies, and the customer base also includes organizations in the retail, publishing, and insurance industries. High-profile users of Privilege Guard include global civil engineering services supplier Balfour Beatty, nuclear services supplier Atomic Energy of Canada, global health insurance provider BUPA, and pharmaceuticals manufacturer Astra Zeneca. Large installations of Privilege Guard include 125,000 seats at one US engineering firm, and 25,000 seats at a major bank.

Avecto is working in a “white space” or business opportunity created by the absence of flexible privilege allocations in Windows. Microsoft’s efforts to address lockdown and security issues have revolved around the UAC feature it introduced in Vista. UAC has had two principal effects on lockdown.

First, it allows privileged users to run most applications with standard rights and to elevate privileged applications through consent dialogs as required. This improves security, but only for Vista and Windows 7, and it does not solve the problem of desktop lockdown because once users have administrative accounts they effectively have complete control over their desktops.

In Microsoft’s own words, the second major effect of UAC is “to remind developers to design their applications to work with standard user rights.” It remains to be seen how effective this strategy will be. In the meantime Avecto is addressing a market created by the sizable number of legacy applications that were written to require administrators’ rights, and which are not practical to amend. Ovum shares Avecto’s confidence that this market will exist for some years to come.

The major rivals to Privilege Guard are BeyondTrust’s PowerBroker and ViewFinity’s System Management solution. Avecto says the major advantages of Privilege Guard over its competitors are that it is the only solution that does not modify the Windows kernel, and that it provides more comprehensive auditing and flexibility in the allocation of rights.

Avecto focuses on sales to businesses with 1,000 or more end users. For smaller businesses it is also considering hosted or software-as-a-service implementations of Privilege Guard.

## IMPLEMENTATION

Avecto says the product can be configured in minutes and deployed to desktops and servers using Microsoft Active Directory Group Policy. Privilege Guard is implemented as a Group Policy extension and does not alter the Active Directory schema. The Privilege guard management console is a Microsoft “snap-in” to the Group Policy Editor. Policy settings are cached on servers and desktops so that devices remain protected even when offline. Group Policy background refresh ensures that policies are updated, even during users’ logged-on sessions.

Privilege Guard also works with Novell's ZENworks' Group Policy integration. Alternatively, policies can be exported and then deployed as an XML file.

Pilot projects covering 20 or so desktops typically take about five days to implement using one full-time IT administrator and the services of an Avecto consultant. Divisional implementations covering, for example, 1,000 desktops usually take 10 days and require stronger skills in Microsoft Group Policy Objects and a moderate understanding of application packaging and deployment. Larger implementations across, say, 10,000 desktops will take about 20 days.

The client occupies less than 5MB and uses about 2MB of desktop memory and typically less than 1% to 2% of CPU cycles, mostly during application start-up. Avecto says the majority of its customers include the Privilege Guard client as part of their standard desktop build. The client runs on Windows XP, Vista, Windows 7, and Windows 2003 and 2008.

Perpetual licenses for Privilege Guard cost £20 per seat. Systems integrators are offered non-perpetual rental contracts. Annual maintenance and support during either North American or European working hours costs £5 per seat. Avecto also offers premium 24x7 support at negotiable prices. Avecto says a typical entry-level implementation covering 500 desktops will cost about £15,000 including licensing, support, and services. Deals covering 2,000 desktops will cost about £50,000, and very large implementations will carry six-figure prices.

Sales to UK and North American business are made either directly from the company or through systems integrators. For Asia and the rest of Europe, Avecto began appointing distributors early in 2010. Avecto's primary integrators are HP and CSC. European distributors include Head in Central and Eastern Europe, Inuit in Sweden and Iceland, and TD Azlan | CDG in Benelux.

**Deployment Example:** Bradford City Council is a local government organization in the UK, which has implemented Privilege Guard across 8,000 desktops. All users of these machines now log on as standard users with no administrative rights, and consequently cannot install unauthorized software. Problem applications only are automatically granted elevated rights. Privilege Guard helped the council achieve compliance with the UK's Government Code of Connection (CoCo).

**Deployment Example:** Shop Direct is one of the UK's largest home-shopping organizations. The company deployed Privilege Guard during a migration of 2,000 head-office desktops from Windows XP to Windows 7. It plans to do the same when it migrates a further 10,000 desktops late in 2010 or early 2011. Many applications required elevated rights and these were accommodated by Privilege Guard.

**Deployment Example:** National Government Services is a subsidiary of US healthcare provider WellPoint, and provides healthcare administration services to the US federal government. It has deployed Privilege Guard across 2,300 desktops to maximize end-user productivity while meeting the requirements of US HIPPA regulations concerning the handling of personal health data.



Table 1: Contact Details	
<b>Avecto UK</b> 5300 Lakeside Cheadle Royal Business Park Cheadle SK8 3GP Cheshire UK Tel: +44 (0)845 519 0114 Fax: +44 (0)845 519 0115 Email: info@avecto.com www.avecto.com	<b>Avecto Americas</b> 790 Turnpike Street Suite 202 North Andover MA 01845 USA Tel: +1 (978) 557 0714 Fax: +1 (978) 557 0792

Source: Avecto OVUM

**Headquarters**

Shirethorn House,  
37/43 Prospect Street,  
Kingston upon Hull,  
HU2 8PX, UK  
Tel: +44 (0)1482 586149  
Fax: +44 (0)1482 323577

**Australian Sales Office**

Level 46, Citigroup Building,  
2 Park Street, Sydney,  
NSW, 2000,  
Australia  
Tel: + 61 (02) 8705 6960  
Fax: + 61 (02) 8705 6961

**End-user Sales Office (USA)**

245 Fifth Avenue,  
4th Floor, New York,  
NY 10016,  
USA  
Tel: +1 212 652 5302  
Fax: +1 212 202 4684

**Important Notice**

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Ovum cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Ovum will not be liable for any interpretations or decisions made by you.

For more information on Ovum's Subscription Services please contact one of the local offices above.

