## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>3</td>
</tr>
<tr>
<td>The Principle of Least Privilege</td>
<td>4</td>
</tr>
<tr>
<td>Definition of Least Privilege</td>
<td>4</td>
</tr>
<tr>
<td>Benefits of Least Privilege</td>
<td>4</td>
</tr>
<tr>
<td>Business Challenges</td>
<td>6</td>
</tr>
<tr>
<td>Endpoint and Server Security</td>
<td>6</td>
</tr>
<tr>
<td>Compliance and Best Security Practice</td>
<td>7</td>
</tr>
<tr>
<td>Migration</td>
<td>8</td>
</tr>
<tr>
<td>A Policy Based Solution — Privilege Guard</td>
<td>10</td>
</tr>
<tr>
<td>A Privilege Management Solution for Business</td>
<td>10</td>
</tr>
<tr>
<td>Application Policies</td>
<td>10</td>
</tr>
<tr>
<td>Custom End User Messaging</td>
<td>11</td>
</tr>
<tr>
<td>Application Whitelisting</td>
<td>11</td>
</tr>
<tr>
<td>Advanced Features</td>
<td>12</td>
</tr>
<tr>
<td>Conclusion</td>
<td>13</td>
</tr>
<tr>
<td>About Avecto</td>
<td>14</td>
</tr>
<tr>
<td>References</td>
<td>15</td>
</tr>
</tbody>
</table>
Summary

This paper introduces the concept of least privilege security and discusses the business challenges involved in endpoint security. It includes information on the security issues organizations face when meeting compliance mandates, how moving to Windows 7 or Windows 8 can improve security and the problems faced when migrating from Windows XP. Finally, there is a brief overview of Privilege Guard, a solution that enables privileges to be assigned to individual applications, providing a practical implementation of least privilege security in corporate environments.
The Principle of Least Privilege

Definition of Least Privilege

The principle of least privilege was first put forward as a design principle by Jerry Saltzer and Mike Schroeder over 30 years ago. According to Saltzer and Schroeder, “Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur.”

Benefits of Least Privilege

Logging on with administrator rights puts systems at much greater risk of contracting malware. Malicious software is more likely to infect a system and cause damage when its payload runs with administrator rights as it does not need to exploit a security flaw to gain privileged access. An administrator has full control over a system, so malware can use these privileges to install drivers, intercept logon passwords, create user accounts, install root kits, replace system files and disable security software.

Malicious software is not the only reason to adopt least privilege. A user with excessive privileges can either deliberately or accidently cause system configuration problems, resulting in downtime and an extra burden on the helpdesk. Users with administrator rights are also free to install software which leads to unlicensed applications on corporate systems and system stability problems.

Most corporate environments strive to deploy a standard image, providing users with a consistent experience and a ‘known’ configuration that the helpdesk can support, reducing the overall total cost of ownership. However, this effort is futile if users run with administrator rights as they have the necessary privileges to alter the desktop configuration or, in the case of system administrators, make changes to servers. If an organization is to succeed in an initiative to deploy locked down desktops and provide a reliable server infrastructure, then it must remove users and system administrators from the local Administrators and Power Users groups.
Although least privilege is not limited to removing administrator rights from users, this is a crucial first step; and one that has the biggest security benefit for the majority of organizations. Statistics provided by Gartner show that 90% of critical security vulnerabilities in Windows 7 can be mitigated by removing administrative privileges.
Business Challenges

With the threat landscape constantly evolving and employees expecting access to line-of-business applications from an ever-expanding array of devices, security should be a primary concern.

Endpoint and Server Security

Many IT departments focus on antivirus and intranet firewalls as the primary form of defence, but recent studies have shown that antivirus should not be the principal endpoint defence mechanism as it is increasingly ineffective at protecting against attacks if not used as part of a defence-in-depth strategy. Microsoft’s addition of privilege management features in Windows highlights the importance of least privilege as a means to improve endpoint security. Prior to Windows 8, Microsoft’s own free antivirus solution, which debuted after User Account Control (UAC) and Software Restriction Policies, was available only as an optional download.

User Account Control is an umbrella term for several technologies that make it easier to run Windows without administrative privileges. UAC was launched as part of Vista and Windows Server 2008, and fine-tuned for Windows 7 to make it more user friendly and remains a key security technology in Windows 8 and Server 2012. Application whitelisting, also a least privilege security technology, prevents users from running unapproved applications. It first appeared in Windows XP as Software Restriction Policies (SRP). SRP later evolved into AppLocker in Windows 7 and Server 2008 R2, a more sophisticated and easier to implement application whitelisting solution.

The least privilege strategy and focus on security has proved effective for Microsoft. Data from Microsoft’s quarterly security intelligent reports, which use live data collected from Windows devices, shows that Windows has become less prone to successful penetration with every new version of the operating system. This is good news for business and home users, but it should be remembered that while UAC has played a significant role in this trend, it is not an enterprise-class technology and is best suited to home users and small businesses without any IT support.

Although UAC is a welcome addition to Windows, it puts security decisions in the hands of end users making it impossible to maintain a secure environment. This provides a challenge for businesses: UAC is unlikely to be enough for organizations to meet internal governance requirements or regulatory compliance mandates.
Likewise, though AppLocker is a considerable improvement on Windows XP’s Software Restriction Policies, it doesn’t provide organizations with the flexibility to respond quickly to changes in the operating environment. For example, when notebook users are disconnected from the corporate network and need to install an application that isn’t approved by IT and therefore blocked by policy. This kind of challenge is one reason why least privilege is not readily adopted.

The ubiquitous nature of antivirus as a security solution is largely because it is a well understood technology and is easily managed. The slow adoption of least privilege in the enterprise is due to the management challenges and application compatibility issues it poses and additionally the continued popularity of Windows XP, which doesn’t lend itself to least privilege use. However, least privilege is essential for compliance and security, so businesses need to find a way to manage standard user accounts and enforce a list of approved applications while maintaining the flexibility to quickly approve new apps and allow users to perform everyday tasks as needed.

Least privilege also applies equally to server computing. Server administrators should only be granted the necessary privileges to carry out a task at the required time. Maintaining the operational consistency and configuration integrity of a server can only be achieved if access to the device is carefully controlled and monitored. Businesses often suffer service outages due to unapproved configuration changes, which could have been avoided by implementing least privilege and a suitable change control process.

Compliance and Security Best Practice

Least privilege security is a requirement for all industry and government compliance mandates, including PCI DSS, MAS Technology Risk Management, HIPAA, SOX, Federal USGBC and more. Whether referred to explicitly or implicitly, compliance requirements cannot be met unless least privilege is implemented. Even if your organization isn’t subject to compliance, it is good practice to employ least privilege as the basis of your security best practices.

In the last couple of years, governments have undertaken research that shows least privilege security to be one of the most effective defences against cyber-attacks. For the first time, governments are issuing new compliance mandates based on this research, which collected real-world data to determine what kind of attacks were most common and how they could be prevented. Least privilege security and application whitelisting are in the top four defence recommendations provided in the Australian Department of Defence’s intelligence agency Top 35
Mitigation Strategies report, along with patching the most commonly exploited applications and the operating system. The mitigation strategies in this report can also be mapped to the SANS Institute CSIS 20 Critical Security Controls.

Whatever the wording of a given mandate, compliance cannot be met if users are running with administrative privileges. Problems related to administrative privileges include configuration management, installation of unlicensed software, installation of devices or software that IT is unable to support, or that cause conflicts with line-of-business applications.

Migration

With general support ending for Windows XP in 2014, there is a pressing need for organizations to start planning a migration to Windows 7 or Windows 8. Not only will this be necessary to ensure that the operating system stays patched and secure, but Windows 7 and 8 also bring many advantages in terms of usability, performance and security.

One of the biggest challenges when moving to Windows 8 and a least privilege desktop is legacy application compatibility. Microsoft guidelines and certification for Windows 8 require that applications should run without the need for users to have administrative privileges. While those guidelines have been in place for many years, many applications – especially those developed in-house – often require that users have administrative privileges for the application’s features to work correctly.

While the best solution is to upgrade to software that is certified for use on Windows 8, or get your in-house development team to make the necessary changes to the application code, this is not always possible. It may be that development has been stopped for a particular application or the upgraded version still doesn’t comply with Microsoft’s certification requirements. Windows 8 UI apps, previously known as Metro apps, use a different security model than traditional desktop applications and may need to be controlled at a more granular level than can be provided by the OS out-of-the-box.

The Application Compatibility Toolkit (ACT), which can solve many compatibility and privilege problems commonly associated with legacy applications, is a free tool available from Microsoft’s website. Though ACT is a useful tool, application compatibility shims need to be developed, tested and deployed, making the migration processes riskier, time consuming and doesn’t give your organization the necessary tools to respond quickly to changing needs.
Even if servers generally have a known work load and are not usually subject to the constant change that users require on endpoints, when migrating to Windows Server 2012 testing line-of-business applications is crucial to ensure compatibility. Similarly, it is important to consider a privilege management solution to assign system administrators elevated privileges only as and when needed.
A Policy Based Solution — Privilege Guard

Although Windows XP has the ‘Run As’ capability, and Vista and later versions of Windows have User Account Control (UAC), both of these features still require users to have access to an administrator account to perform administrative tasks. This limitation tends to make these built-in features more appropriate for home users or real system administrators as it enables them to log on as a standard user and only use the administrator account when they need to perform administrative tasks.

A Privilege Management Solution for Business

The corporate environment requires a solution that can elevate individual applications based on policies defined by the IT department and not determined by users or the operating system; a solution that allows users to log on with standard accounts and one that does not require users to have access to an administrator account. Avecto Privilege Guard was designed with these goals in mind.

Application Policies

Privilege Guard application policies are extremely flexible, with support beyond executable images. Application policies may be defined for the following types of file:

- Executable images (.exe)
- Control panel applets (.cpl)
- Management consoles (.msc)
- Windows installer packages (.msi, .msu, .msp)
- Windows scripting host scripts (.vbs, .js)
- PowerShell scripts (.ps1)
- Batch files (.bat, .cmd)
- Registry settings (.reg)
- Windows Explorer (COM)
- ActiveX controls (installation)

Privilege Guard also contains templates that make it easy for administrators to configure policies that allow users to run Windows functions with elevated privileges. Applications may be matched on any combination of 18 properties,
such as file path, command line, hash (SHA-1) and trusted publisher. Custom access tokens can be defined if an application doesn’t require full administrator rights, making it possible to give an application only the privileges it actually requires to run correctly.

To help create policies, Privilege Guard can be configured to passively monitor the behavior of applications and identify those applications that require elevated privileges to run. In addition to identifying the applications, Privilege Guard can also capture detailed activity, highlighting operations that would fail under a standard user account. An important aspect of all security products is auditing and Privilege Guard audits all or selective application elevations, giving details of how the application was invoked and the policy that was applied. Comprehensive reporting is also available in the Enterprise Reporting Pack.

Shell integration provides the ability for more advanced users to launch elevated applications “on demand” via a shell context menu option. This menu option can be restricted, i.e. limited to a set of applications, as opposed to being available for all applications.

Custom End User Messaging

Optional end user messaging may be configured to warn users before running privileged applications, which includes the ability to force a user to re-authenticate and provide a reason for running the application. Smart card authentication is also supported. Hyper-links can be embedded and unlike UAC elevation prompts, Privilege Guard messages can be branded and customized to give users confidence that they are responding to genuine requests for approval, and not malware.

Application Whitelisting

Application whitelisting in Privilege Guard provides a more flexible solution than AppLocker or Software Restriction Policies and integrates with other Privilege Guard features, such as end user messaging, auditing and challenge/response authentication. Privilege Guard application whitelisting works in all versions of Windows, starting from Windows XP.
Advanced Features

Challenge/response authentication provides users with a one-time password (response code) that may be used to elevate or install an application that is blocked by policy. This feature is especially useful for notebook users, where it is usually impossible to create policies that predict every possible elevated action a user might need to undertake in the field.

Policies can also be created that automatically elevate applications downloaded from specific websites, which is useful if you want to trust applications from particular vendors. The latest version of Privilege Guard adds support for policies that control the installation and execution of Windows 8 UI apps.

The implementation of the Privilege Guard solution provides security, operational and compliance benefits on both desktops and servers. Integration with McAfee ePolicy Orchestrator (EPO) gives organizations the opportunity to deploy Privilege Guard using EPO and collect information from Privilege Guard for better risk and compliance management.
Conclusion

This paper has introduced the principle of least privilege and the benefits of implementing this approach in a corporate environment. Although developments in the Windows operating system have made it possible for users and system administrators to run with minimal rights, the need to log on with administrator credentials to run some applications introduces its own set of security challenges.

Avecto Privilege Guard was designed to meet the requirements of implementing least privilege in corporate environments on both desktops and servers. By enabling users to run with minimal rights and elevating individual applications without giving users access to an administrator account, Privilege Guard provides a practical solution to the issues that prevent most organizations from adopting least privilege.
About Avecto

Avecto is a pioneer in least privilege management, helping organizations to deploy secure and compliant desktops and servers. With its innovative Privilege Guard technology, organizations can now empower all Windows based desktop and server users with the privileges they require to perform their roles, without compromising the integrity and security of their systems.

Customers of all sizes rely on Avecto to reduce operating expenses and strengthen security across their Windows based environments. Our mission is to enable our customers to lower operating costs and improve system security by implementing least privilege. Avecto is building a worldwide channel of partners and system integrators and is headquartered in Manchester, UK. For more information, visit www.avecto.com.

For more information, visit www.avecto.com

Copyright ©2008-2013 Avecto Ltd. All rights reserved.
References
