Avecto Use Case

Least Privilege in the Data Center

Introduction

Removing excess administrator privileges is considered to be one of the most essential risk mitigation strategies for organizations and IT departments globally; immediately improving the security posture of any organization and enabling regulatory compliance.

This approach of 'least privilege', where sysadmins access servers with a standard account, with no more permission than is necessary to complete their day-to-day tasks, results in the reduction or complete removal of administrator accounts from the network.

However, while this approach significantly reduces the attack surface and potential for security breaches, it has traditionally created challenges in the data center. Without a carefully considered approach to admin rights removal, sysadmins find themselves overly locked down and prevented from performing their day-to-day roles.

The solution lies in privilege management and application whitelisting technologies, which enable the effective removal of powerful administrative rights, without restricting the behavior of the sysadmin, so that security and productivity are both improved.

> "More than 50% of IT security professionals say their sysadmins pose a moderate to high risk to their network."

Survey at McAfee FOCUS 2013

Defendpoint for servers

Avecto's proactive endpoint security software, Defendpoint, allows sysadmins to perform their daily job functions in the data center, but under the security and protection of a standard user account. The technology provides the seamless elevation of tasks, applications and scripts – rather than elevating the permissions of the user. This ensures that the number of administrator accounts in the business can be dramatically reduced or removed altogether.

In addition, comprehensive reporting functionality ensures that all privileged operations can be identified, with reason justifications provided for auditing purposes. This intelligence can be used to build and develop rules that fit the specific needs of the sysadmin role, and of the business.

Removing admin rights from the network significantly reduces the attack surface and potential for security breaches. However, this approach has traditionally created challenges in the data center, causing sysadmins to be overly restricted and prevented from performing their day-to-day roles.

A more accepted approach to security is one of 'least privilege', where sysadmins access the server with a standard account, with no more permission than is necessary to complete their day-to-day tasks. This concept results in the reduction or complete removal of administrator accounts from the network.

> "Privileged Accounts are an [attackers] critical path to success 100% of the time in every attack regardless of the threat."

Cyber Sheath 2014.
The role of privileged accounts in high profile breaches.

Features and benefits

By utilizing a single policy across all servers, organizations are able to create rules for all sysadmins logging in to a server (or group of servers), within the environment. Once logged in with standard user rights, the server policy may provide elevation, application blacklisting or application whitelisting based on specific requirements.

A powerful filtering engine ensures that specific policy 'workstyles' can be assigned to different environments. Workstyles can be assigned to individual users, or groups, and can be time-bound so they are only effective during scheduled maintenance windows. Advanced filtering using WMI allows focused delivery of privileged tasks only to servers with a particular role(s). Workstyles can also offer levels of flexibility based on job description or seniority, where junior sysadmins and external consultants are given tighter, more regulated restrictions than more senior roles.

With a wide range of filtering options available, individual or teams of sysadmins can be managed based on role, job function or even specific tasks, rather than as a one-size-fits-all.

Exception handling options are also established, ensuring that any sysadmin trying to access restricted tools has the option of requesting access when prompted. This can be achieved by implementing challenge and response functionality, whereby the user needs to request a secure 8-digit code from the IT helpdesk to gain the access they need; all within the context of a standard user account.

The entire process can be automated with ticketing systems, and email / web alerts as well as customized with corporate branding and text, ensuring a rich and intuitive user experience, without heavy resource requirement. Importantly, the user experience is vastly improved through greater flexibility and customized messaging. This multi-level authentication can also aid with compliance, as dictated by mandates such as the 'never alone' principle as stated in MAS and PCI DSS 3.0.

Example Workstyles

A junior sysadmin needs access to perform some low level maintenance tasks such as check/clear event logs, defragment and cleanup disks, etc. Privileged access to these specific tasks is granted during out-of-hours only.

A security engineer needs access to manage the servers firewall configuration. Privileged access to the Windows firewall control panel, as well the ability to restart *only* the Windows Firewall service is granted.

An external consultant needs access to manage the configuration of a VOIP server. Privileged access is granted to only the VOIP management tools and the VOIP service.

A senior sysadmin needs to diagnose a server outage, and requires access to the server to diagnose the issue. A flexible 'on demand' policy is assigned, allowing the sysadmin privileged and audited access to core windows debugging tools. Access to Windows services is gated with Challenge/Response, requiring authorization from a support desk.

A maintenance engineer needs to install a patch/hotfix on a server. Privileges are assigned to run the specific patch MSP only.

Appendix: Typical server use cases

There are many scenarios where Defendpoint can be deployed to provide benefits in the data center – including;

Application elevation

Defendpoint removes the reliance on local administrator accounts for the execution of applications that require elevated privileges. Instead, an organization can provide a focused policy to ensure applications will execute under the context of a standard user account. This process allows an application to elevate securely, while conforming to Microsoft best practices.

On-demand privilege elevation

Through integration into the Windows shell menu, Defendpoint can be configured to replace the "Run as Administrator" option, providing specific users with the ability to elevate their privileges using an appropriate approval method. This ensures users can gain the access they need for one-off requests, without ever exposing the Administrator account or password. Audits and reports on activity provide reports to monitor use.

User Account Control (UAC) replacement

User Account Control is designed to provide a confirmation prompt before an application can make changes to the OS. These prompts are often confusing for end users and can lead to increased demand on helpdesk teams to service their requests. Defendpoint allows an organization to harness the UAC trigger and replace standard messages with customized messages that can be configured to block, elevate or audit activity. With complete flexibility of content and branding, the messages provide enhanced communication to improve the end user experience.

Application control

Application control (specifically whitelisting) is recognized as one of the most effective ways of securing a server build, preventing unknown applications from executing. With support for all common forms of script, Defendpoint can secure scripted tasks with strong SHA-1 verification and certificate verification, ensuring that authorized scripts have not been modified or tampered with.

When combined with a privilege management solution that provides the flexibility of an on-demand elevation of privileges, application control can provide all the benefits of a full whitelisting solution, without the administrative overheads.

Application blacklisting

For restricted or unauthorized tasks, a policy can be designed to explicitly block applications or scripts from execution. By using advanced matching criteria, applications can be blocked using any combination of rules, or classifications – such as trusted ownership, or by tracking the origin of where an application was downloaded from. Avecto always advocates application control where applicable to whitelist trusted applications and by default, prevent the unknown.

License control

When used in conjunction with an application control policy, it is possible to eliminate the installation and execution of unlicensed applications, providing a cost effective method of controlling or even reducing license budgets, and ensuring you remain compliant with license mandates.

Mitigation of "temp admin" processes

When using the on-demand elevation feature within Defendpoint, any existing temporary admin process can be mitigated. A customized confirmation prompt is displayed based on the user's level of access within the organization. The prompt is extremely flexible and can be configured to include a challenge and response code, over-the-shoulder authentication or self-authentication. In addition, the messages can ask for a reason for the elevation, either through an open text field or pre-populated drop down list.

Prevent rogue admin use

Ensure that users are able to perform effectively with standard user accounts by providing access to the applications, tasks or scripts that have been explicitly provided by the Defendpoint policy. Any application required outside the predefined list can be executed through an on-demand privilege elevation (appropriate to the user's role), backed by full auditing functionality for full visibility.

With in-built security, Avecto's patented anti-tamper feature prevents any changes to local privilege groups (including the administrator account/group) to prevent any user elevating their privileges. Users are also prevented from changing or altering the Defendpoint technology, ensuring the deployment is protected.

Service control

One of the most common administrative tasks performed on servers is the stopping and starting of Windows services. The Windows Service type allows individual service operations to be whitelisted, so that standard users are able to start, stop and configure services without the need to elevate tools such as the Service Control Manager. No modifications are made to any service DACL, keeping the security and integrity of the server build intact.

COM Elevation

Embedded within the operating system, over 120 User Account Control (UAC) functions require COM elevation. Using Defendpoint, administrators can replace all unwanted UAC prompts with any degree of granularity. Without this feature, tasks such as managing network and advanced network settings, or changing firewall settings would require an administrator account.

Remote PowerShell management

When enabled, Remote PowerShell authorizes targeted sysadmins to connect remotely to a computer via WinRM with standard user credentials, which would normally require local administrator rights. Once connected, the sysadmin is then able to execute PowerShell scripts or cmdlets that Defendpoint can elevate, block or audit using a flexible rules engine. This removes the requirement for users to create a terminal connection on a remote machine which exposes more functionality than may be required to complete the task. Remote PowerShell activity is fully audited, with comprehensive reports.

URL filtering

Defendpoint includes patented a URL tracking feature, which tags and tracks all downloaded applications with the origin URL. These tracked downloads can then be enforced in policy to ensure that only applications from approved, or reputable sources are allowed to execute – with all untrustworthy downloads being blocked and audited.

Challenge and response

This feature provides the user with a single use 'challenge' code that requires a matching 'response' approval code. Once the user has the response code from the helpdesk, they are granted access to the application in an audited and controlled manner, even in areas without network connectivity. Applications can be approved by the helpdesk for a single use, for the remainder of the sysadmins session, or can be approved on a permanent basis.

Multiple authentication methods can be combined to create a dual authentication process, adding additional security layers to meet compliance requirements.

Delegated Run As

This feature provides a targeted, policy controlled alternative to Windows Run As, whereby applications and tasks may be executed in the context of a secondary account. The applications where Delegated Run As can be used, by whom, and also the accounts or group of accounts that can be used, are all predetermined by Defendpoint policies.

Advanced policy filtering

Defendpoint policies can be filtered to accommodate for advanced use cases associated specifically with servers. Filters can be based on Security Group membership, machine or host name, time of day/ week, and can be set with a date/time to expire – which can be used in combination with identity management solutions where provisioned credentials are given a minimal shelf life.

Defendpoint supports Microsoft Remote Desktop Services and Citrix XenApp remote connections, allowing policies to be targeted at remote sessions based on the hostname or IP Address of the remote user. Privileges can then be assigned only to approved remote clients, or through specific routed IP ranges.

A powerful WMI filtering engine allows policies to be targeted at specific server infrastructures using just any combination of the thousands of properties available through WMI. For example, policies granting privileged access to IIS administration tools can be targeted at servers with the IIS role.

Discovery of applications

Defendpoint can be placed into a discovery or learning mode to gather information to inform the design of policies. Using its reporting tools, you can identify all applications being executed across the estate. Importantly, you can identify applications requiring administrative rights to execute. This information can then be analyzed to build a focused set of Privilege Guard policies.

Workflow automation

Leveraging the scripting functionality of Defendpoint, an application that is capable of triggering a script can provide instant feedback into existing workflow or management systems. When required, changes to the policies can then be automated through the PowerShell API.

PowerShell API

Avecto's PowerShell API provides full policy automation. Administrators can now create and modify Defendpoint policies directly through external workflow management solutions. Through the PowerShell API, you can create and modify any Defendpoint configuration within Domain Group Policy, Local Group Policy, or any local configuration.

Enterprise auditing and reporting

Avecto's enterprise reporting dashboard leverages the power of SQL and SSRS to provide a breakdown of all user and application privileges. This data can be used to gain a holistic view of all application privileges across the enterprise, including trends in application demand, applications executed outside the core policy and details of user activity.

Patch Management/Control

Utilizing the on-demand privilege elevation feature, you can allow patches and updates to be applied without having to add them to a fixed policy, and importantly, without providing an administrator account. Avecto's PowerShell API can be used to create/modify policy on a targeted set of machines, to authorize the update under specific conditions.

About Avecto

Avecto is a pioneering security software company with a vision to transform business cultures, freeing all users to be creative, productive and profitable. Established in 2008 by UK entrepreneurs Paul Kenyon and Mark Austin, Avecto is headquartered in Manchester (UK) with a network of global partners and offices in Boston (US), and Melbourne (Australia).

Avecto's consultative approach delivers technical solutions to commercial challenges; empowering global enterprises to strike just the right balance between security defense in depth and user flexibility.

About Defendpoint

Avecto's proactive endpoint security software, Defendpoint, uniquely combines the technologies of privilege management, application control and sandboxing to protect the operating system, software environment and user data from unknown cyber threats.

Defendpoint empowers employees to be free, without security compromise. Complementing existing patching and antimalware strategies, it offers strength and depth across both desktops and servers as a holistic solution to endpoint security.

> "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

Avecto + You...

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

Australia

Level 8
350 Collins Street, Melbourne,
Victoria 3000, Australia

Phone +613 8605 4822
Fax +613 8601 1180

Avecto
@avecto
Avecto

avecto.com
info@avecto.com