Managing privileges

Comparing PIM and PM approaches for the removal of admin rights

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.

Organizations striving to meet the demands of internal auditors and industry regulators can interpret the requirement for least privilege in a number of ways. Frequently, this means the extensive benefits offered by a privilege management solution are not fully realized.

This article explores the available solutions for managing privileges and compares the advantages of each.

Privileged Identity Management (PIM)*

The traditional approach has been to adopt a PIM solution, which is designed to grant access to privileged user accounts via a password vault. This type of solution allows the sysadmin to request access to a specific server. The vault then grants access to the user using a temporary admin account, and attempts to record the sysadmin's activities. Once the session is finished, the admin account is revoked and the session recording is logged.

While this approach can be used to limit and monitor access to critical resources, it offers only a basic level of control and limited security benefits. The control is all or nothing, with users either checking out an admin account with full privileges or having none at all. While this technique was once sufficient to meet the requirements of basic security mandates, issuing even temporary privileges poses just the same security risks as a full admin account. Regulators are now calling for increasingly granular control, which means that the security bar has been raised.

*Some vendors refer to this as Privileged Access Management (PAM) or Privileged User Management (PUM).

Privilege Management (PM)

To overcome the limitations of PIM, privilege management solutions take a more robust approach to managing user privileges by allowing sysadmins to operate under the security of a standard user account. Admin rights are assigned only to the individual tasks, applications or scripts that require them. This granular level of control ensures the number of admin accounts within an organization can be dramatically reduced or eliminated.

In addition, using comprehensive reporting, privileged operations can be identified. This allows organizations to request user justification for audit purposes or implement challenge / response mechanisms for additional security and control on critical systems. This approach not only improves security and regulatory compliance, but allows for a much better user experience.

> "85% of critical Microsoft vulnerabilities in 2015 being mitigated by removal of admin rights."
>
> Avecto Vulnerabilities Report 2015

Comparing PIM and PM approaches

	Privileged Identity Management	Privilege Management
Account type	Full admin account	Standard user account
Granular control of privileges?	No	Yes
Reduces admin accounts?	No	Yes
Mitigates Microsoft vulnerabilities?	No	Yes
Additional security controls	Reactive session recording and audits	Proactive challenge / response and audits

Auditing the administrators

There is often a desire to audit admin users. This usually stems from a lack of granular privilege management controls, leading to users operating in a dangerously over-privileged environment. Although recording the activity of sysadmins may appear to be a useful activity, in reality it is an extremely resource-intensive task. Who is going to audit all the data? What use is it after a compromise has occurred? With a PIM solution, you are effectively handing over the keys to the vault and hoping that a few rarely watched CCTV cameras have you covered.

Whilst PIM solutions can play a part in meeting compliance and regulations, the security benefits of managing the actual privileges, rather than the identity, are clear. PIM alone can only offer less access to privileged accounts, and not least privilege. Removing admin accounts altogether and operating from a position of true least privilege is one of the most essential and effective risk mitigation strategies you can adopt.

Without access to a full admin account, malware and threats cannot easily compromise the system, and accidental or malicious actions by the user can be mitigated. Most importantly, this is a proactive strategy, compared to a reactive strategy where activities are recorded after the fact.

> “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 the privileged accounts in high profile breaches.

Conclusion

When seeking to achieve compliance or improve security though the removal of administrator privileges, the best approach is to remove the admin account completely rather than simply reassigning them on a temporary basis. Whilst PIM solutions go some way to address some of the challenges associated with free access to admin accounts, this approach does little to handle the dangers presented by using unrestricted administrator accounts.

Privilege management solutions offer capabilities above and beyond those of PIM, allowing standard accounts to be provisioned instead of full admin accounts. Specific privileges are then assigned based on the user’s job function in a policy-controlled and fully audited manner, ensuring no misuse or abuse can occur. This helps organizations fully meet compliance mandates such as MAS which require the full removal of administrator accounts.

Avecto’s endpoint security software, Defendpoint, empowers organizations across the globe to achieve true least privilege. Defendpoint provides administrators with a secure environment, without impacting their ability to administer some of the largest data centers in the world.

defendpoint

Defendpoint by Avecto is a security software solution that makes prevention possible. For the first time, it uniquely integrates three proactive technologies to stop malware at the endpoint. It’s this innovative approach that protects the operating system, software environment and your data from internal and external threats.