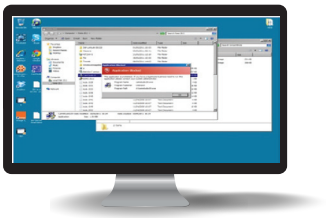
CYBERARK®

On-Demand Privileges Manager™ for Windows

Dramatically reduce costs by implementing 'least privilege' policies on desktops and servers.



Transparently elevates to administrative privileges without users needing to insert privileged credentials. Should the user not have the privileges to install or run an application, a notification will appear.

Why CyberArk?

CyberArk is the trusted expert in stopping cyber attacks before they stop business.

The Challenge

Windows desktops and servers are commonplace throughout the organization yet the business environment in which they serve is heterogeneous. Business users' needs vary, some need to run applications which require installing an active x whereas others simply need to define a printer on their machine. Many activities, such as these, require administrative rights yet granting the entire organization such powerful and unlimited rights lead to significant implications to the organization:

- **Security Challenges.** When desktops or servers run with privileged rights, the system's security is compromised directly and indirectly. With more privileges, there is more likelihood of the system being abused and as a result damaged. Moreover, most malware will take advantage of admin rights, indirectly damaging the system and putting the organization at risk to internal and external threats.
- **Productivity Challenges.** With unlimited rights, the chance of an end-user damaging the desktop is greater which inadvertently creates overhead on the IT team with calls for repair. In Windows Server environments, administrators can make unauthorized or unwanted changes which can also lead to damage and impact productivity.
- **Compliance Challenges.** When desktop or server users are configured by default with administrative rights, not only does this negate a number of compliance directives but without a 'least privilege'; solution, activity cannot be tracked and accounted for which is necessary to pass compliance regulations and internal audits. On the other hand, an organization can decide to revoke all admin rights on desktops however this too has a productivity price. Users will rely heavily on IT for performing tasks mandatory for their jobs. This creates greater overhead on IT and bottlenecks which slow the business down. The result is high expenditure on desktop helpdesk calls and IT personnel. Without a solution that allows for central policy management of 'least privilege', the organization needs to incur a tradeoff between security and productivity, which in both cases means higher total cost of ownership to the organization.

The Solution

On-Demand Privileges Manager™ (OPM) for Windows dramatically reduces the usage of privileged rights within the organization and enables organizations to enforce a 'least privilege' policy for administrative rights on desktops and servers. It is known that as many as 90% of Windows vulnerabilities are mitigated when running with 'least privilege'. By enabling users to run in standard user mode and elevating the rights of individual applications in a controlled and pre-defined manner, organizations can enjoy cost efficiencies and improved security.

With OPM for Windows, you can:

Do Business Better. Empower users to perform the administrative tasks necessary for their job, reducing the dependency on IT while improving end user satisfaction.

Approach Compliance with Confidence. Improve the day-to-day operations as standard users no longer have unlimited local admin rights, as required by FDCC, Government Connect, PCI DSS, HIPAA, SOX and others.

Eliminate Threats. Most malware fails to run on standard user permissions reducing internal and external threats.

OPM for Windows offers you unique value:

- Reduce total cost of ownership and IT overhead with less helpdesk tickets as a result of inappropriate level of privileges
- Enterprise policy enforcement and complete visibility over privileged activities for a better security posture
- Reduce the risk of infecting desktops with malware which can result in desktop corruption and high costs to the organization

Benefits

OPM for Windows gives you tighter control over which users or groups are granted admin rights for specific applications, scripts or tasks. By centrally defining policies for enterprise-wide deployment, you can empower users to perform the tasks they need to do on a daily basis while reducing IT overhead and costs. OPM for Windows offers a robust set of capabilities such as:

- **Centralized Management through Windows Group Policy.** Tightly integrated with Windows Group Policy for setup and configuration, leveraging Active Directory infrastructure for instant deployment across the enterprise with no additional backend infrastructure required.
- **Simple Policy Configuration.** Identify the applications which can run with elevated rights and define its identification options e.g. filename, file hash, trusted publisher, command line etc. Then classify the application to the users who require elevated privileges.
- **Flexible Policy Definitions.** Users can be limited to the applications, commands or tasks they can run on their local desktop in a transparent manner where they will not even be required to enter a username or password. Additional options may also be set such as end user messaging, prompts for reason submission or additional authentication requirements, auditing and privilege monitoring.
- **Transparent User Experience.** Seamless integration with Windows' User Account Control (UAC) eliminates or replaces inappropriate UAC prompts for applications equiring elevation, giving a superior end user experience.
- **Ongoing Desktop and Server Protection.** Once OPM is deployed, policies are cached on the client machine ensuring policies continue to be enforced when there is no network connection. Support for background refresh ensures that policies are updated even if the user remains logged on.
- **On-demand Elevation.** For more skilled users who require more flexibility like IT professionals and developers, OPM integrates with the Windows shell whereby the user logs on with a standard user account and can elevate applications from a shell context menu. To avoid end user confusion, the standard Windows "Run as" menu option can also be hidden.
- **Detailed Audit Trail.** All user activities running privileged operations are written to the event log.
- **Enterprise Readiness.** Scales across the organization when needing to manage hundreds of thousands of desktops and even integrates with legacy applications to enforce 'least privilege' in these environments. All user activities running privileged operations are written to the event log.

The Power of On-Demand Privileges Manager™

Superusers using 'root' in Unix/Linux environments can also be controlled using CyberArk's On-Demand Privileges Manager (OPM) for Unix/Linux. With granular access control, you can control the commands superusers are entitled to run, enabling on-demand elevation to 'root' for specific tasks and text record all input/output for full traceability. OPM provides a unified view and correlation of superuser and privileged accounts giving 360 visibility and control across the enterprise.

Specifications

Supported Platforms:

- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

Both 32-bit and 64-bit versions are available for all platforms

Comprehensive Application Support:

- Executables
- Control panel applets
- Management console snap-ins
- Windows installer packages
- Windows Scripting Hosts scripts
- Batch files
- Registry settings
- PowerShell scripts
- ActiveX controls

Flexible and Secure Application Rules:

- File path matching
- Command line matching
- File hashing (SHA-1)
- Trusted publisher
- Trusted ownership
- Product and file information
- Leverage Active Directory infrastructure with no additional backend infrastructure required