PRIVILEGE MANAGER FOR WINDOWS

PROTECTING ENDPOINTS AND CONTROLLING ACCESS

PRIVILEGE MANAGER FOR WINDOWS

Provides a number of application control implementations

- Whitelisting
- Blacklisting
- Graylisting
- Least Privilege Policy
- Application Privilege Elevation
- Sandboxing / Isolation
- Contextual Application Policies
- Endpoint Grouping
- Monitoring and Logging
- Discovery and Reporting

The flexibility you need to satisfy any number of security requirements:

Privilege Manager for Windows operates on Three simple steps:

Identify an Application

Evaluate a Policy in Context

Apply an Action

Simple, Contextual, Endpoint Protection through Application Control

Privilege Manager for Windows helps organizations secure systems and reduce the risk of Cyberattacks by controlling if and how applications execute.

DYNAMIC, INTELLIGENT WHITELISTING WITH APPLICATION REPUTATION

Privilege Manager for Windows controls what and how applications are permitted to run in an environment.

- Create dynamic whitelists using reference systems, managed software, trusted sources, and file owners.
- Apply a broad set of intermediate “Intelligent” actions to software that is not in the whitelist, but may be legitimate. Graylist actions limit an application’s ability to impact the system while allowing end user productivity.
- Classify known applications as allowed or disallowed and thereby allow or prevent their execution. Classification can be based upon discovery date, administrator security rating, location and digital code signing, etc.
- Application control policies can be applied to an application based upon the Internet zone or even the specific URL from which the application is downloaded. Thycotic stores URL’s for historical forensics and policy creation.

ENABLING LEAST PRIVILEGE POLICY

Nearly every attack on an endpoint can be prevented by removing administrative privileges on that machine. Without administrative rights, most people will not be able to download, install, and run any software that could potentially compromise their computer.

However, this would require an IT Administrator to enter their administrative credentials everytime something needed to be updated - and that can be disruptive.

Privilege Manager for Windows enables seamless elevation of approved applications for standard users while removing unnecessary rights from untrusted applications. By only elevating specific applications the desktop can be locked down while supporting important business applications.

Privilege Manager for Windows Overview

Extend your endpoint protection, combine Privilege Manager for Windows with Secret Server

Privilege Manager for Windows allows your end-users to continue doing their job without requiring administrative rights by elevating the application with the rights needed to run. Secret Server, with it's automated discovery, can find local administrative accounts on endpoints and take control of them - effectively removing them from use.

Secret Server is a Privilege Account Management solution for protecting your most valuable assets - privileged accounts.

By combining both solutions, you can implement a defense in depth approach that stops the two methods that attackers use to gain access to your core network services: compromised endpoints and administrative credentials.

SUPPORTED PLATFORMS

32-bit and 64-bit versions

- Windows XP, Vista, 7, 8, 8.1, 10
- Server 2003, 2008, 2012

> Privilege management and application control tools help achieve total cost of ownership (TCO) reasonably close to that of a locked and well-managed user, while giving users some ability to control their systems."
>
> **Gartner**
> "The Cost of Removing Administrative Rights for the Wrong Users" (April 2011)

PROTECTION AGAINST ZERO-DAY VULNERABILITY EXPLOITS

Stop the Unknown Threat

According to Microsoft, over 60% of vulnerabilities in Microsoft Security bulletins were mitigated by running with reduced user rights. The impact was even greater for Mozilla and Adobe. Malicious software often exploits software vulnerabilities and takes advantage of the rights of the logged in user to infiltrate the computer.

Infiltrations could include installing a bot, adware, keyboard logger, data harvester, or any other payload that can be used for future malicious activity. It could also disable security software or change the operating system to facilitate malicious activity such as creating open shared folders or changing permissions. Newly introduced exploits commonly invoke other processes as part of their ability to compromise the system; with Thycotic these methods will be blocked.

With Privilege Manager for Windows, the administrator is able to better leverage core Windows security models to isolate untrusted applications from accessing system resources without requiring the complete denial of the application from user productivity.

APPLICATION ADMINISTRATOR RIGHTS AND COMPATABILITY ANALYSIS

Solve Application Limitations

One of the first challenges of any privilege management project is determining what applications need administrator rights. Privilege Manager for Windows discovers applications that need administrator privileges and whether they will have compatibility issues with the latest Windows Operating System.

The resulting analysis can be used to easily create policies to add privileges to the application so that the application can run by a standard user. The same analysis can be used to apply compatibility adjustments and enable legacy applications for Windows 7.