PRIVILEGE MANAGER

LEAST PRIVILEGE THAT'S EASY FOR IT SUPPORT AND SEAMLESS FOR USERS

85% of data breaches start on user computers

Block Social Engineering Attacks, Malware and Ransomware at the Gate

SIMPLE LEAST PRIVILEGE IMPLEMENTATION

Remove All Admin Credentials from Endpoints at Once.

Local admin accounts are privileged accounts. If a local admin clicks on a malicious link and downloads malware, their workstation could become "patient zero" in a catastrophic attack. When hackers gain privileges on one machine they can progress through your network and even cover their tracks by changing event logs.

Privilege Manager automatically removes admin rights from domain and non-domain managed endpoints, including hidden or hard-coded credentials. As a result, virtually all critical vulnerabilities are mitigated.

By focusing your endpoint protection plan first on removing privileged credentials you'll tighten your attack surface and avoid spending time and resources on reactive detection and remediation.

PRODUCTIVITY THROUGH APPLICATION CONTROL

Easy for IT/Desktop Support. Seamless for Users.

Most least privilege policies fail because removing admin rights negatively impacts users and creates more work for IT support teams.

Privilege Manager uses policy-based controls to elevate applications users need, without requiring admin credentials or requesting IT support.

It automatically adds trusted applications to a whitelist, relies on the latest intelligence from threat databases such as VirusTotal to create blacklists, and adds unknown applications to greylists. Sandboxing elevates applications in a limited way so they don't have access to system controls or OS configurations.

Because Privilege Manager elevates applications and not the user, it never leaves a window open for hackers.

> Application control is a very effective method to block malware-based attacks, including new and targeted attacks, malicious insider attacks and dangerous user behavior.
>
> **- Gartner**

e: sales@thycotic.com
t: @thycotic
www.thycotic.com

A SINGLE TOOL MAKES LEAST PRIVILEGE EASY TO DEPLOY & MANAGE

- Discover privileges
- Inventory applications
- Customize groups
- Remove credentials
- Create policies
- Whitelisting
- Blacklisting
- Greylisting
- Sandboxing
- Elevate applications
- Customize workflow
- Share reports
- Show compliance

MEET COMPLIANCE REQUIREMENTS

HIPAA, PCI DSS, FDDC, Government Connect, FISMA, and SOX recommend or require that organizations apply Least Privilege to endpoints for proper data protection.

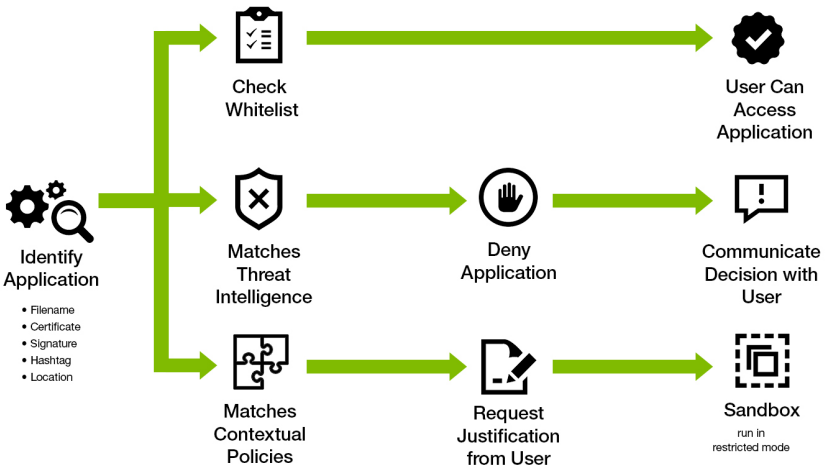
Build compliance reports for execs and auditors that demonstrate:

- How many endpoints are in compliance with Least Privilege.
- How many applications are governed by a policy for application control.
- Which/how many malicious applications been blocked from executing.
- Which endpoints or users are attempting to run unsafe applications or processes.

SUPPORTED PLATFORMS

- 32-bit and 64-bit versions
- Windows XP, Vista, 7, 8, 8.1 and 10

Automated Application Control



SET POLICIES BASED ON SECURITY AND BUSINESS REQUIREMENTS

IT Security teams have granular, contextual control:

- On who may run processes that require administrative credentials.
- If processes can run on certain endpoints but not others.
- If processes are allowed in certain regions or during certain times of day.
- Whether to allow child processes to run.

Business productivity

- Business users can still run conferencing applications such as GoToMeeting and WebEx.
- Remote workers can continue to install printer drivers.
- Power users or developers can continue to run applications that connect to SQL Studio and DevOps tools and run scripts that connect to code libraries, and cloud controls.

ABOUT THYCOTIC

Thycotic is focused on the most vulnerable attack vector – privilege. With Thycotic you can adopt a multi-layered approach that covers your privilege security needs from endpoints to credentials, ensuring protection at every step of an attacker's chain.

Privilege Manager is installed with hundreds of customers, including large, global enterprises and organizations that demand adherence to the strictest security and compliance requirements.