

Why Choose Thycotic

Stay Ahead Of Attackers. Prepare For Audits. Protect What Matters Most.

Thycotic empowers more than 10,000 organizations around the globe, from small businesses to the Fortune 500, to manage privileged access. We make enterprise-grade privilege management accessible for everyone by eliminating the need for complex security tools and prioritizing productivity, flexibility and control. You'll achieve more with Thycotic than with any other privilege security tool.

10,000+

CUSTOMERS
WORLDWIDE

95%

CUSTOMER
SATISFACTION RATE

97%

CUSTOMER
RETENTION RATE

Your Time And Energy Are Too Valuable To Waste

Thycotic gives you the agility to stay one step ahead. No more manual provisioning or cumbersome password management. No more combing through audit logs to create reports. You'll be able to answer questions from executives and auditors before they are asked.

Thycotic Helps You Get People On Your Side

Our solutions are readily adopted by security teams, IT Ops, Sys Admins, helpdesk/support teams, developers, and everyone who relies on privileged access to do their job.

Why Privileged Access Management Should Be Your #1 Cyber Security Priority

Privileged account credentials for domain admins, service, application, and root accounts are valuable targets. When attackers gain these credentials they can exploit your most sensitive information and critical systems. Privileged access gives them power to alter data, change configurations or even shut down your operations. Masquerading as privileged users, they can cover their tracks and go undetected for months or longer.

GARTNER INSIGHTS

PAM should be a security team's #1 priority

FORRESTER

PAM can reduce the risk of a breach by 80%

GARTNER BEST PRACTICES FOR PAM

PAM lowers the risk of advanced threats by 50%

Become a Self-Sufficient Security Champion with Thycotic

SECRET SERVER

Privileged Access Security and Password Protection.
The only enterprise-grade PAM solution available both on premise and in the cloud.

Establish Vault – Set granular permissions, users, and structure to map to your organization.

Discover Privileges – Identify all service, application, administrator, and root accounts to curb privilege sprawl.

Manage Secrets – Provision, deprovision, ensure password complexity, and rotate credentials.

Delegate Access – Implement role-based access control, workflow for access requests, and approvals for third parties.

Control Sessions – Implement session launching, proxies, monitoring, and recording capabilities.

Secure DevOps – Remove hardcoded passwords and secure privileged accounts within your software development lifecycle.

Protect Unix – Implement Unix command whitelisting and SSH Key Management.

PRIVILEGE MANAGER

Least Privilege Enforcement and Application Control.
The only all-in-one least privilege and application control solution that scales to thousands of endpoints.

Deploy Agents – Agents continuously discover endpoints, applications, and processes tied to privileges on domain and non-domain accounts.

Implement Least Privilege Policy – Remove excess privileges, permanently control which accounts are members of local groups, including administrators, and control credentials of accounts in these groups.

Define Policies – Create granular application control policies for whitelisting, blacklisting, and greylisting applications based on advanced threat intelligence.

Elevate Applications – Approve applications that require admin privileges to execute with policy-driven controls that consider endpoint, location, user, and process requested.

Improve Productivity – Allow people to use applications and controls to do their jobs without requiring admin rights.

PRIVILEGED BEHAVIOR ANALYTICS

Proactively Detect Breaches and Prevent Data Theft.
Actionable data, automated alerts and integrated controls that discover and contain a privileged account breach.

Establish Baselines – Understand typical behavior patterns for privileged accounts so you can detect red flags.

Monitor and Identify – Monitor privileged accounts, view and prioritize activity in custom dashboards.

Identify and Alert – Identify and confirm suspicious activity and alert incident response teams.

Take Action – Rotate credentials, force MFA, or require approvals to contain the impact of an attack before it causes more damage.

SECRET SERVER SDK FOR DEVOPS

Extend Privileged Account Protection to DevOps teams. Secret Server SDK provides added PAM security while meeting demands for workflow efficiency in application development, improving security without impacting productivity.

Protect Code – Enables DevOps to remove hardcoded passwords from code.

Secure Credentials – Provides unique accounts and credentials to containers and services.

Avoid Repositories – Helps avoid using insecure repositories where secrets can be hijacked and exploited.

Scale on Demand – Readily scales to meet dynamic, rapidly changing needs with maximum resiliency.

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.