COMPANY
OVERVIEW

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%

SECRET SERVER

Privileged Access Security and Password Protection.

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.

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

PRIVILEGE MANAGER

Endpoint Privilege Elevation and Application Control.

Deploy Agents – Discover endpoints, applications, and processes on domain and non-domain accounts.

Implement Least Privilege Policy – Remove excess privileges, control group membership and credentials.

Define Policies – Create granular application control policies for whitelisting, blacklisting, and greylisting.

Elevate Applications – Approve applications that require admin privileges to execute with policy-driven controls.

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

CONNECTION MANAGER

Unified Management of Multiple Remote Sessions.

Remote Access – Launch and configure sessions across multiple environments.

Session Management – Credentials are automatically injected into sessions as needed.

Centralized Control – Access a single interface to manage and interact with sessions.

Session Recording – Create an end to end record of privileged user activity.

Tracking and Auditing – Provide an audit trail to demonstrate compliance

ACCOUNT LIFECYCLE MANAGER

Control Over Service Account Sprawl.

Establish Workflow – Get started easily with a few simple steps and customizations using workflow templates.

Delegate Ownership – Create users, groups and roles aligned to your needs with role-based permissions.

Provision Service Accounts – Define workflow(s) for automated account provisioning and set required approvals for each type of request.

Enforce Governance – Create accountability and ownership over your service accounts.

Decommission Service Accounts – Send automated notifications when accounts should be renewed, re-approved or even deleted.

PRIVILEGED BEHAVIOR ANALYTICS

Proactively Detect Breaches and Prevent Data Theft.

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.

DEVOPS SECRETS VAULT

Cloud Password Protection at DevOps Speed and Scale.

Establish a Secure Vault – Store privileged credentials in an encrypted, centralized vault.

Centralize Secrets – Eliminate the risk of disparate vault instances.

Enforce Access – Provide auditable management and enforcement of secret access.

Connect All DevOps Tools – Allow flexibility with a platform-agnostic solution.

Automatically Scale – Manage secrets at the speed and scale of DevOps pipelines.

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.