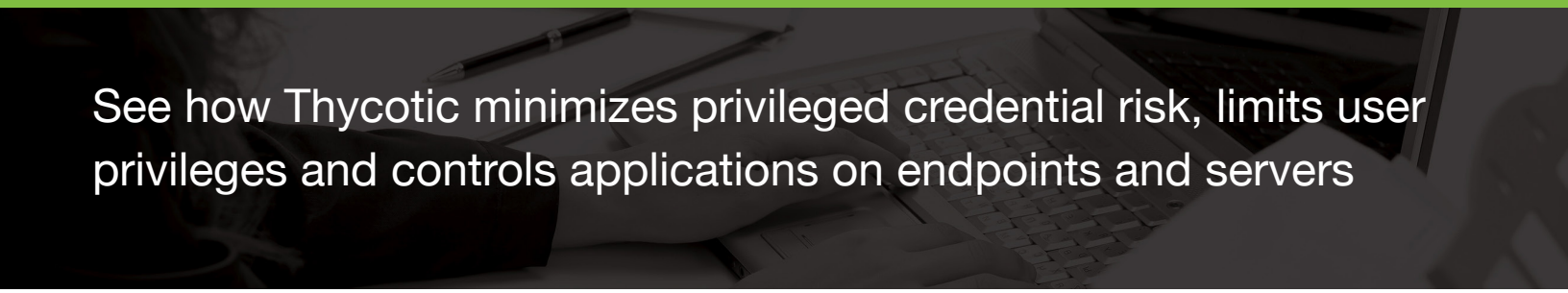
SIMPLY INDISPENSABLE PRIVILEGED ACCOUNT MANAGEMENT



See how Thycotic minimizes privileged credential risk, limits user privileges and controls applications on endpoints and servers

YOUR PAM CHALLENGES

Privileged account passwords and credentials for domain admin accounts, root accounts, and superuser accounts are the preferred targets for hackers these days. Exploiting vulnerabilities among all users, attackers seek to compromise credentials and escalate privileges to get at the "keys to the kingdom." This allows them to gain access as a trusted user to your most sensitive and critical information and often go undetected for months.

To protect your organization, you need Privileged Account Management (PAM) solutions that enable you to address the **Privileged Credential Risk Continuum** across your enterprise. These risks include:

Privileged Credential Exposure
Struggling to manage increasing workloads with fewer staff resources, IT administrators frequently rely on default account names and passwords that have never been changed. Even worse, manual spreadsheets that are used to track privileged accounts and passwords are error prone, unreliable and unsafe. The result is a proliferation of unknown and unmanaged privileged credentials.

Privileged Credential Sharing
Far too many IT departments still share the same privileged superuser/root accounts, service accounts and password credentials even though security policies require employees to rotate passwords and implement multi-factor authentication. These informal practices continue to persist despite security policies designed to prevent them.

Privileged Credential Creep
Applying privileged credential controls in daily practice can often become too much hassle or too big an obstacle to keeping applications running. This morphs over time into "Privilege Creep" that allows low-level admins or even business users to accumulate dangerously high levels of privilege—putting your entire enterprise at risk.

Thus, privileged accounts and IT Admin rights are all too often unknown, unmanaged, uncontrolled and unprotected, leaving your organization exposed to disastrous consequences.

Our Solution

As the global leader of next-generation IT security solutions, Thycotic protects organizations against cyber-attacks that use privileged accounts and privilege escalation to strike at the core of the enterprise.

Thycotic provides an end-to-end Privileged Account Management solution that:

- Combines industry-leading Privileged Account Security and Password protection with proven end-point security and application control for Windows and UNIX.
- Dramatically lowers risk by stopping the progress of malware-based attacks at the endpoint and servers, limiting an attacker's ability to move beyond their initial point of entry, as well as preventing installation of Remote Access Tools (RATs).
- Ensures secure Privileged Account credential protection while preventing privilege escalation by removing and/or limiting privileges for business users and IT admins without impacting productivity.

Thycotic Secret Server delivers a comprehensive Privileged Account Management solution set to protect your most valuable information assets from cyberattacks and insider threats. Thycotic Secret Server, Application Control, Local Security and Security Analytics solutions protect privileged accounts and enables organizations to enforce least privilege policies for business and administrative users, as well as control applications to reduce the attack surface without halting productivity.

The solution helps organizations revoke everyday local administrator privileges from business users while seamlessly elevating privileges when required by trusted applications.

Complementing these privilege controls, the solution also delivers application controls, which are designed to manage and control which applications are permitted to run on endpoints and servers and prevent malicious applications from penetrating the environment.

Unlike any other security offering, Thycotic PAM products are the fastest to deploy, easiest to use, scalable enterprise-class solutions offered at a competitive price. Already securing privileged account access for more than 3,500 organizations worldwide, including Fortune 500 enterprises, Thycotic is simply your best value for PAM protection.

Products:

Thycotic Secret Server
Thycotic Password Reset Server
Thycotic Group Management Server
Thycotic Application Control Solution
Thycotic Local Security Solution
Thycotic Security Analysis Solution

Acquisitions: Arellia acquired 2016

Microsoft Windows end-point security and application control solutions that stop the progress of malware-based attacks at the endpoint, limiting an attacker's ability to move beyond their initial point of entry.

Customers:

More than 3,500 organizations worldwide, including Fortune 500 enterprises.

Used by more than 180,000 IT admins and security pros.

Over 1 million endpoints protected

Awards/Recognition:

INC. 5000 Fastest Growing Companies in America: 2013, 2014, and 2015, jumping 1,000+ rankings each year

Best of VMWorld - Security and Compliance 2014: Finalist / runner up

SC Magazine Awards 2015:
Finalist, Best Customer Service

SC Magazine Awards Europe 2015:
Finalist, Best Customer Service, Best Identity Management Solution

Washington Business Journal Best Places to Work 2015: #17 Medium Sized Biz Category

Info Security Products Guide Global Excellence Awards 2015: Bronze, database security, identity management

5-Star Award 2016:
Best Privileged Account Management Solution

> **“ Our IT admins were able to get up to speed within minutes and our control over privileged accounts improved immediately. Because Secret Server helps us manage sensitive credentials across privileged accounts, we no longer face the inefficiencies and security risks that can plague an organization as big as ours.”**
>
> **Michael Boeglin,**
> **Director of Global Infrastructure – International Rescue Committee**

Our Innovative Products

PRIVILEGED ACCOUNT MANAGEMENT

Secret Server

Creates a fundamental security layer – managed from a single console – to protect against cyber-attacks that use these privileged accounts to strike at the core of the enterprise. Available in on premise, cloud and free editions.

LEAST PRIVILEGE AND APPLICATION CONTROL

Application Control Solution for Windows

Provides advanced security to manage application rights with a combination of privilege management, application whitelisting, and real-time application reputation and threat intelligence.

Privilege Manager for UNIX

Enables Secret Server administrators to build a Unix command whitelist so that when users run any SSH launcher, they are limited to a subset of commands. Helps increase security with granular control of root credentials to limit privileges, while meeting compliance regulations and policies for Unix Superuser Privilege Management (SUPM).

ENDPOINT CONFIGURATION SECURITY

Local Security Solution for Windows

Delivers comprehensive endpoint security by managing Windows local group membership for business and admin users, and enforcing policies to remove administrator rights from unauthorized accounts.

Security Analysis Solution for Windows

Identifies security configuration issues using Security Content Automation Protocol (SCAP) profiles, and remediates misconfigurations automatically.

END USER AND ADMIN PRODUCTIVITY

End-User Password Reset Server

Provides simple, self-service password management to free up IT help desk staff from time-consuming and inefficient processes, and enforces stronger end-user password controls.

Group Management Server

Empowers non-IT personnel to securely manage their department’s Active Directory Groups without assigning them a privileged account.

See for yourself why Thycotic Secret Server deserves to be on your short list with these key benefits:

Simply Secure— Assures multiple layers of built-in security with easy access management for IT admins, robust segregation of role-based duties, and military-grade AES 256 bit encryption.

Protected Productivity— Enables seamless elevation of approved applications for users while minimizing the risk of running unauthorized applications.

Endpoint Enforcement — Automatically enforces policies to ensure membership rights for business and IT Admin users are controlled according to least privilege best practices.

Highly Scalable — Supports large-scale distributed environments, all major OS, DB, apps, hypervisors, network devices, and security appliances, for on premise and cloud.

Always Available— Delivers high availability disaster recovery options, as well as hot backups, database mirroring and our unique unlimited admin mode for "break-the-glass" scenarios.

Readily Customizable— Easy to customize without any need to spend time or money to hire expensive consultants.

Faster & Easier— Software installs in minutes, is easy to use and flexible so you can get tasks done with minimal effort.

Auditable Too— Out-of-the-box and custom reports satisfy security regulations with minimal effort.

WHAT WE DO	HOW YOU BENEFIT
DISCOVER • Automatically identify and securely store privileged accounts. • Discover local users with admin rights, and applications that require admin rights. • Identify security misconfigurations.	• Easily detect all privileged accounts and store the passwords in our secure vault. • Accomplish in minutes what would take countless IT hours.
MANAGE & AUDIT • Audit, analyze, and manage privileged user and account activity. • Standards based auditing and reporting.	• Automatically rotate passwords to manage the keys to the kingdom. • Alerts your team to abnormal use of credentials. • Facilitates adherence to compliance standards across your entire spectrum of users.
MONITOR & CONTROL • Collect, record, monitor, and manage privileged account activity. • Flexible whitelisting/blacklisting. • Control Windows application privilege escalation by revoking or limiting privileges among IT admin and business users.	• Limit privileges for business & IT users and stop malware at the endpoint • Know how your privileged accounts are being used and deter abuse. • Provide full view to your SOC with SIEM integration of privileged account use • Enable seamless elevation of privileges when required by trusted applications.
SECURE & PROTECT • Prevent and detect unauthorized use of privileged accounts while removing or limiting privilege escalation • Lock down endpoints by limiting the risk of running unauthorized users	• Protect privileged accounts and business/admin users from hackers and malicious insiders • Secure authorized admin accounts to lower risk without impacting productivity • Stop the progress of malware –based attacks at the endpoint, limiting attackers ability to move beyond the initial point of entry

thycotic

1101 17th Street NW Suite 1102
Washington DC 20036
DC | LONDON | SYDNEY

p: +1 202-802-9399
t: @thycotic
www.thycotic.com