THYCOTIC PREVENTS CYBERATTACKS

BY SECURING PASSWORDS, PROTECTING ENDPOINTS, AND CONTROLLING ACCESS

YOUR SECURITY CHALLENGES

Privileged account passwords and credentials for domain admin accounts, root accounts, and superuser accounts are the preferred targets for hackers. Exploiting vulnerabilities among endpoints and users, attackers seek to compromise credentials and escalate privilege 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 Endpoint and Privileged Access solutions that enable you to address the **privileged credential risk continuum** across your enterprise.

THE 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 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.

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.

Endpoint Application Vulnerabilities

Endpoints are the target of choice when it comes to compromising a network. Controlling what applications can run on the network greatly mitigates the risks of threats, such as Ransomware, from crippling your infrastructure.

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

thycotic

DC | LONDON | SYDNEY

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

OUR SOLUTION

As the global leader of next-generation IT security solutions, Thycotic prevents cyber attacks by securing passwords, protecting endpoints, and controlling access.

Thycotic provides an end-to-end security 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 security solution set to protect your most valuable information assets from cyber attacks and insider threats. Thycotic Secret Server, Privilege Manager, Local Security, and Security Analysis solutions protect privileged accounts and enable 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 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 7,500 organizations worldwide, including Fortune 500 enterprises, Thycotic is simply your best value for securing your sensitive infrastructure.

AWARDS & RECOGNITIONS

INC. 5000 Fastest Growing Companies in America: 2013, 2014, and 2015

Best of VMWorld - Security and Compliance 2014, 2016: Finalist

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 Business Category

Info Security Products Guide Global Excellence Awards 2015: Bronze, Database Security, Identity Management

5-Star Stevie Award 2015: Best Privileged Account Management Solution

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

> **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

SECURING PASSWORDS

Secret Server
Available in on-premises, cloud, and free editions. 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.

Privileged Behavior Analytics
Privileged Behavior Analytics can help IT and Security administrators quickly detect breaches before they happen, analyze distribution of privileged accounts and access across your organization, and add a layer of security to your Secret Server deployment.

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.

PROTECTING ENDPOINTS & CONTROLLING ACCESS

Privilege Manager
Provides advanced security to manage application rights with a combination of privilege management, application whitelisting, and real-time application reputation and threat intelligence for both Windows and Mac endpoints.

Group Management Server
Empowers non-IT personnel to securely manage their department's Active Directory groups without assigning them a privileged account.

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

Unix Protection
Unix Protection, enables Secret Server administrators with two more powerful functions: Unix command whitelisting and SSH Key Management. Command whitelisting ensures that admins are limited to a subset of SSH commands when launching a session through Secret Server. SSH Key Management can protect and rotate SSH private/public keypairs, while updating public keys on corresponding endpoints when necessary.

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.

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

See for yourself why Thycotic 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.

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

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.

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

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 a 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.”
- Alert your team to abnormal use of credentials.
- Facilitate adherence to compliance standards across your entire spectrum of users.

Monitor & Control
- Collect, record, monitor, and manage privileged account activity.
- Flexible whitelisting/ blacklisting.
- Control endpoint application privilege escalation by revoking or limiting privileges among IT admin and business users.
- Limit privileges for business and 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.

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