

# LOCAL SECURITY SOLUTION

## Protect, Detect and Audit privileged accounts

### LOCAL SECURITY SOLUTION

- Utilize Group Policy Objects
- Integration with Service Desk
- Policy Filters by Internet Zone
- Internet-facing Agent Connection
- UAC Override

### Secure Privileged Users and Configuration

Thycotic Local Security Solution is used to secure privileged users, groups, applications, and operating system components. Thycotic Local Security Solution supports functions to better utilize Group Policy Objects – GPOs - within an organization.

**According to Microsoft, over 60% of the vulnerabilities addressed in Microsoft Security bulletins could have been mitigated by eliminating administrator rights for end users.**



### ENFORCE GROUP MEMBERSHIP AND MEET COMPLIANCE STANDARDS

#### Eliminate unnecessary administrator accounts

Discovery of administrative accounts and policy-based enforcement of users and groups are important so that unauthorized users are not granted excessive privileges. IT management increasingly wants to lock down desktops, because users with administrative privileges may easily create and modify local system configuration and compromise security. Local Security Solution will discover local accounts and their rights, while group provisioning policies help preserve the integrity of your local group accounts with automated group membership enforcement. This helps ensure that unauthorized users are not maliciously or mistakenly added to administrative group accounts. Combine that with analysis of Domain Groups and you have a complete picture of where privileged accounts need security.

### LEVERAGE GROUP POLICY OBJECTS

#### Empower Policies with GPO Definitions

Group Policy definitions can be imported into the Thycotic Server, and then the settings can be configured, deployed and applied on managed systems. For remote computers, the Thycotic agent receives updates and executes the GPO's on a schedule from any location. Using Local Security Solution, organizations can apply GPOs to even non-domain attached computers. Policies can be targeted to any groups, collections or isolated systems known to Thycotic or an integrated configuration manager. Local Security Solution also provides feedback to the server that a GPO was applied and working across the organization.

## INTEGRATIONS

Extend your existing infrastructure to deploy and manage Thycotic solutions.

Thycotic integrates with:

- LANDesk Management Suite
- LANDesk ServiceDesk
- Microsoft SCCM
- Symantec Management Platform; ITMS
- ServiceNow

## SUPPORTED PLATFORMS

32-bit and 64-bit versions

- Windows XP, Vista, 7, 8, 8.1, 10
- Server 2003, 2008, 2012

## RANDOMIZE AND CYCLE PASSWORDS WITH DISCLOSURE LOGGING

### Protect, Detect and audit privileged accounts

Avoid problems with a single password that works on all instances of local administrative accounts in your environment. Local Security Solution significantly tightens security in your environment by automating the cycling of administrative passwords and ensuring that every instance of a managed user has a complex and unique password. Once passwords are randomized, disclosure of managed user passwords is logged for future auditing.

## HARDEN CRITICAL APPLICATIONS

### Prevent application and service tampering

When end users run with administrator rights Windows components can be maliciously or inadvertently changed resulting in compromises to security. Users will often disable critical services or applications that they deem a nuisance. Using Local Security Solution, services and their associated files and registry keys can be secured so that even an administrative user cannot disable or delete them.

OPERATION	MANUAL	LOCAL SECURITY	SAVINGS
Changing local administrator account passwords	5 minutes per system 3.5 days [1000 systems]	5 minutes for policy setup No recurring costs	<b>99% reduction in cost</b>
Auditing administrator account usage	10 minutes to review logon events, 7 days [1000 systems]	Report identifies accessed accounts, 2 minute review per account accessed	<b>95% reduction in cost</b> assuming 250 accounts accessed
Identifying users with administrator rights	5 minutes per system 3.5 days [1000 systems]	Built-in report based on automated security audit	<b>100% reduction in cost</b>
Apply change in Global Policy Definitions	10 minutes per system 7 days [1000 systems]	10 minutes for policy setup No recurring costs, applied to non-domain systems with report	<b>90% reduction in cost</b> with increased function

