APPLICATION CONTROL
SOLUTION

Don't be the next victim of cyber crime

APPLICATION CONTROL SOLUTION

- Application Reputation and Intelligence
- Application Sand-boxing
- Application Firewall
- Security Operations Center Integrations for Real-Time threat alerts
- Enhanced Mitigation Toolkit Support
- Mobile Approval App

Improve application security by enforcing if and how applications execute:

- Application Rights Analysis
- Privilege Management
- Flexible Whitelisting
- Control Child Processes
- Compatibility Adjustment
- UAC Override

Privilege Management, Whitelisting and Intelligence

Application Control Solution helps organizations secure Windows systems and reduce the risk of Cyber Threats by controlling if and how applications execute.

DYNAMIC, INTELLIGENT WHITELISTING WITH APPLICATION REPUTATION

Application Control Solution controls what and how applications are permitted to run in an environment.

- Create dynamic whitelists using reference systems, managed software, trusted sources, and file owners.
- This results in fewer applications to manage. Apply a broad set of intermediate "Intelligent" actions to software that is not in the whitelist, but may be legitimate. greylist actions limit an application's ability to impact the system while allowing end user productivity.
- Classify known applications as allowed or disallowed and thereby allow or prevent their execution. Classification can be based upon discovery date, administrator security rating, location and digital code signing, etc.
- Application control policies can be applied to an application based upon the Internet zone or even the specific URL from which the application is downloaded. Thycotic stores URL's for historical forensics and policy creation.

ENHANCE END-USER EXPERIENCE

Enable Least Privilege

Organizations today want to lockdown desktops for better security, stability, and lower management costs. Legacy applications, software installers, and many system utilities require administrative rights to function. Organizations face a dilemma to either give end users administrator accounts or face limited functionality.

Application Control Solution enables seamless elevation of approved applications for standard users while removing unnecessary rights from untrusted applications. By only elevating specific applications the desktop can be locked down while supporting important business applications.

Thycotic empowers the administrator to seamlessly route the user's execution request to the service desk.

thycotic

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

Established service desk workflows are employed to route and review the request. Once the request is approved in the service desk, the user is notified and the application can immediately run on the endpoint. Additionally, policies can be deployed so that the organization can overwrite the behavior for any time a UAC dialogue would normally appear.

PROTECTION AGAINST ZERO-DAY VULNERABILITY EXPLOITS

Stop the Unknown Threat

According to Microsoft, over 60% of vulnerabilities in Microsoft Security bulletins were mitigated by running with reduced user rights. The impact was even greater for Mozilla and Adobe. Malicious software often exploits software vulnerabilities and takes advantage of the rights of the logged in user to infiltrate the computer.

Infiltrations could include installing a bot, adware, keyboard logger, data harvester, or any other payload that can be used for future malicious activity. It could also disable security software or change the operating system to facilitate malicious activity such as creating open shared folders or changing permissions. Newly introduced exploits commonly invoke other processes as part of their ability to compromise the system; with Thycotic these methods will be blocked.

With Application Control Solution, the administrator is able to better leverage core Windows security models to isolate untrusted applications from accessing system resources without requiring the complete denial of the application from user productivity.

> Privilege management and application control tools help achieve total cost of ownership (TCO) reasonably close to that of a locked and well-managed user, while giving users some ability to control their systems."
>
> **Gartner**
> "The Cost of Removing Administrative Rights for the Wrong Users" (April 2011)

APPLICATION ADMINISTRATOR RIGHTS AND COMPATABILITY ANALYSIS

Solve Application Limitations

One of the first challenges of any privilege management project is determining what applications need administrator rights. Application Control Solution discovers applications that need administrator privileges and whether they will have compatibility issues with Windows 7.

The resulting analysis can be used to easily create policies to add privileges to the application so that the application can run by a standard user. The same analysis can be used to apply compatibility adjustments and enable legacy applications for Windows 7.