

Software Distribution joins Advanced Security

NEW INNOVATIVE APPROACH ON APPLICATION MANAGEMENT

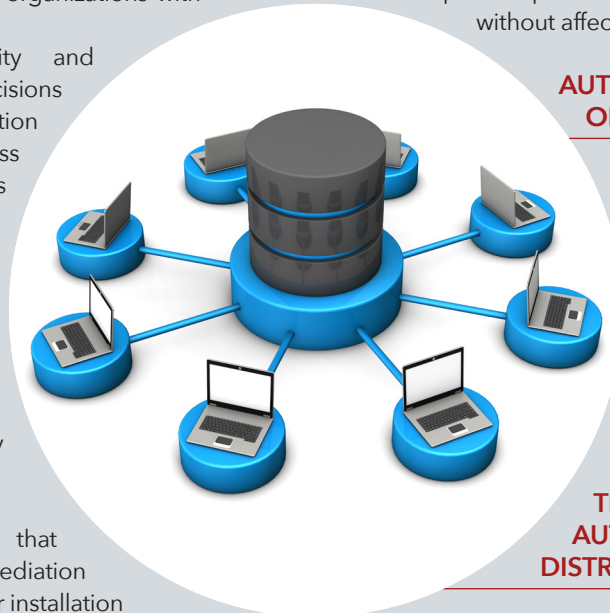
Application Management remains one of the unsolved problems, in an efficient way, for organizations with certain number of workstations.

The choice between security and productivity takes to strategic decisions that do not provide a suitable solution altogether. The safer the less productive a system is. Windows systems require administrator permissions to install software but lack the flexibility to not penalize productivity. Traditional solutions are based on the use of accounts with administrative rights that, in most cases, are different to the ones which finally make use of the applications.

This entails a tedious problem that requires a laborious process of remediation and configuration to be done after installation and considerably lengthens the integration of new applications, as well as the risk of compromising the administrator password.

Simarks Deployment Manager (SDM) provides a solution with a completely different and innovative approach. Based on a

patented technology of privilege management at process level, Simarks SDM allows to build an application corporate catalog where the end user is who installs the applications without granting him administrator permissions. This approach allows complete implementation of the principle of least privilege without affecting the productivity.



AUTHORIZATION SYSTEM BASED ON A WIDE RANGE OF FILTERS

The end user accesses the corporate application catalog where he can access only those applications the administrator has authorized to him. This authorization is based on a wide range of filters, both inclusion and exclusion, as a user, group, computer, brand, model, department, subnet, site, role, S.O. version, 32/64 bits, etc.

TRADITIONAL SYSTEM OF AUTOMATIC AND UNATTENDED DISTRIBUTION

Although focused on self-service, SDM provides a complete and improved system of traditional distribution, automatic and unattended, enabling the deployment of applications in stages, allowing the same application to be deployed automatically for users which meet certain filters while others are offered the possibility of installing on demand.

FUNCTIONALITIES

Flexibility and efficiency

Application deployment can be performed by the user and/or in an unattended way by the use of categories:

- Mandatory
- Uninstallation and/or forbidden
- On demand
- Periodic

It uses the original application package, supporting all versions of Windows from XP to Windows 10 (32 and 64 bits).

1

2

Planned Activation

Package Execution planned to be performed automatically:

- Application Updates
- Uninstalls
- Repairs
- Emergency Distributions.

3

Elevation of Privilege at execution

Applications that need special privileges at execution time can be configured to always run with the correct permissions without granting these permissions to the user. File spoofing is avoided by digital signature and internal file name checking.

4

Categorizing and labeling

In addition to setting applications into categories, SDM gives the administrator personalized labeling for the construction of the corporate catalog and the optimization of searches.

5

Inventory and Reporting

Hardware and software inventory on every computer in the domain. Detailed reports on application deployments.



BASED ON ACTIVE DIRECTORY WITHOUT ADDITIONAL ELEMENTS

SDM is based on Active Directory and does not require additional elements (servers, databases, etc.). It only requires shared resources to store binary files. There are three operating environments integrated with each other (test, pre-production and production) in the same instance of Active Directory. The production repository can be replicated, allowing the user to access always the nearest one.

PORTAL OF ADMINISTRATIVE TASKS

The main element of SDM is the process. Any software package is configured as a succession of commands to execute in order to install, uninstall, update, etc. This feature allows you to add an element whose command is the execution of an administrative task such as changing the network configuration, install a printer driver, adjust the clock, etc.

APPLICATION MANAGEMENT

- **On Demand Application Management:** effective solution that allows users to install, update, etc., any application from the catalog which is authorized without granting him administrator permissions.
- **Maximum flexibility:** self-service distribution based on a wide range of filters, both inclusion and exclusion (user, group, computer, model, brand, department, subnet, place, role, OS version, 32/64 bit architecture, etc.).
- **Multiple deployment methods:**
 - Installation/Update mandatory and automatic.
 - Installation/Update on demand (possibility for the user to install when they want).
 - Periodic execution of administrative tasks.
 - Automatic repairing and troubleshooting.
 - Automatic application uninstalling.
 - Automatic and unattended updating.
 - Emergency Distribution. Ability to run specific commands configured by the administrator in case of emergency.
- **Scripting Language:** specially designed for application management.

CENTRALIZED MANAGEMENT

- **Flexible and centralized management:** management tool based on MMC (Microsoft Management Console). Active Directory-based, uses all its power for the replication of objects and bandwidth to access the closest domain controller.
- **Repositories:** SDM stores the contents of the installation products (binary, CD content etc.) in shared resource folders that can be hosted on any server, including the cloud.

MONITORING, ANALYSIS AND REPORTING

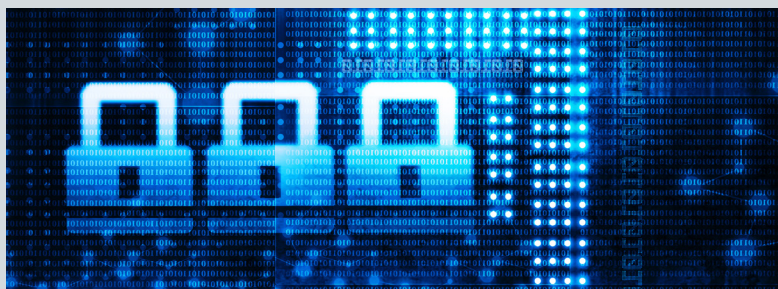
- **Logs:** Integration with any SIEM system.
- **Statistics:** report use of applications and processes for license control, unauthorized software, etc.
- **Reports:** possibility of a wide range of reports.

LOCAL ADMINISTRATOR'S PASSWORD MANAGEMENT

- **Daily change:** daily change of the password for the local administrator account on every computer in the domain.
- **Different password** on each computer.
- **Secure Management:** a tool for obtaining the current password in custody. No network connection required.

MAXIMUM EFFICIENCY AND COST REDUCTION

- **Cost reduction:** drastic reduction of Total Cost of Ownership (TCO) of the computers of the organization.
- **Efficiency:** significant reduction in Help Desk support.



BESTSAFE SUITE: INTEGRAL PRIVILEGE MANAGEMENT

SDM IS PART OF THE SIMARKS BEST PLATFORM SUITE, THAT UNIFIES PRIVILEGE MANAGEMENT WITH SOFTWARE DISTRIBUTION INCLUDING:

- PRIVILEGE MANAGEMENT FOR SERVERS AND WORKSTATIONS.
- TRADITIONAL PRIVILEGE MANAGEMENT AT USER AND COMPUTER LEVEL.
- ELEVATION/RESTRICTION OF PERMISSIONS AT PROCESS LEVEL.
- MAXIMUM PRODUCTIVITY BY THE CONFIGURATION OF RULES TO CONTROL THE SECURITY CONTEXT OF PROCESSES DEPENDING ON THE USER OR GROUP CURRENTLY LOGGED ON.
- CENTRALIZED MANAGEMENT. FLEXIBLE AND CENTRALIZED MANAGEMENT. RULES ARE STORED IN ACTIVE DIRECTORY TAKING ADVANTAGE OF THE OBJECT HIERARCHY AND ACCESSING THE CLOSEST DOMAIN CONTROLLER
- COMPLIANCE: COMPLY WITH BOTH INTERNAL AND EXTERNAL REGULATION BY APPLYING THE PRINCIPLE OF LEAST PRIVILEGE AND MONITORING APPLICATION ACTIVITY.

THE SET OF FEATURES OFFERED BY SIMARKS BESTSAFE SUITE ALLOWS COMPREHENSIVE SAFETY MANAGEMENT OF MICROSOFT WINDOWS-BASED COMPUTERS WITHOUT AFFECTING PRODUCTIVITY. THE MANAGEMENT PLATFORM IS VERY QUICK AND EASY AND DOES NOT REQUIRE ADDITIONAL ELEMENTS SUCH AS SERVERS, DATABASES, ETC.



simarks
cybersecurity

CONTACT

Tel: +34 810 526 675

info@simarks.com