

Viewfinity Privilege Management Product Overview

Many enterprises are implementing least privileges to add a solid layer of defense for desktop environments, further protecting against malware and Advanced Persistent Threats. Viewfinity provides enterprises with the solutions needed to manage and execute an end-to-end automated and non-disruptive move to a least privileges environment.

Viewfinity Privilege Management suite provides tighter, yet flexible control over the types of applications and desktop functions your distributed workforce are allowed to run through lockdown, application control and privilege management.

- Application Blocking/whitelisting
- Privilege elevation
- Automated policy creation and management
- Audit trail reporting, policy validation and privileged account activity auditing
- Compliance Reports
- Mobile Workforce Support

Viewfinity's End-to-End Non-Disruptive Transition to Least Privileges

Viewfinity's End-to-End Non-Disruptive Move to Least Privileges process encompasses the following automated steps:

1. Discovers user accounts and groups that are members of the local "Administrators" built-in user group on computers in your Windows domain.
2. Silently discovers applications requiring administrative rights prior to revoking privileges.
3. Provides "Readiness Statistics" based on end user activity that is collected over a period of time to ensure all events requiring administrator rights are captured.
4. Once the collection and analysis has completed, policies to elevate privileges are automatically created and prepared in advance so that when administrative rights are removed, the policies are in place to ensure a non-disruptive move to least privileges.
5. Supports future needs, exceptions and maintenance. Viewfinity:
 - Collects user requests with corresponding business justification
 - Provides a policy authorization workflow management & approval process
6. Ongoing auditing and reporting for compliance validation.



Viewfinity Major Capabilities and Select Differentiators

Implementation Methods: Viewfinity Privilege Management can be implemented as an extension to Group Policy, through our SaaS/Cloud platform or via on-premise servers as part of a private cloud. Viewfinity delivers value quickly and scales with your business needs.

Zero Touch Policy Automation: Automatic detection of a user's need for elevated permissions, with the ability to create the appropriate policy and authorize the privilege elevation on the fly.

Viewfinity Local Admin Discovery: Identify user accounts and groups that are members of the local "Administrators" built-in user group on computers in your Windows domain. Having detailed information related to which users and groups have administrator rights on corporate desktops allows you to reassess who should have these rights. Once the analysis has been run, IT Administrators can take action, if needed, by removing the users or suspicious groups from the Administrators group.

Pre-Discovery of Applications Requiring Elevated Permissions: Silently gather information and monitor which applications, processes, and administrative actions will require administrative permission before users are removed from the local admin group. Our Application Admin Rights Analysis is based on end user activity and is collected over a period of time to ensure all events are captured. Once the collection and analysis is completed, policies to elevate privileges can be automatically created and prepared in advance so that when administrative rights are removed, the policies are in place to ensure a non-disruptive move to least privileges.

Support for Mobile Workers: Viewfinity does not require PCs to be part of the Active Directory domain or to be directly connected to the corporate network in order to activate policies that manage administrator privileges. All policies continue to be enforced even while working offline.

Intelligent Reporting through Policy Auditing: To ensure compliance, Viewfinity has built-in audit reporting that provides automated confirmation of the delivery and enforcement of policies. Viewfinity provides detailed reporting on all administrator privilege policies, screen recorded video of user activity and administrator's actions and activity.

Integration of policy reports with SCCM: This component is deployed on SCCM servers and reports on privilege management policy usage status and information regarding privilege access request from end users. The SCCM agent collects Viewfinity policy events such as policy usage, insufficient privileges to install applications or ActiveX, requests from users to perform Administrative tasks such as disk defragmentation or the ability to change power options, etc. The status of Viewfinity policies and privilege access requests are tracked through the SCCM Console.

