

Windows Desktop Enforcer

Enforce ABAC & Externalize Authorization



OVERVIEW

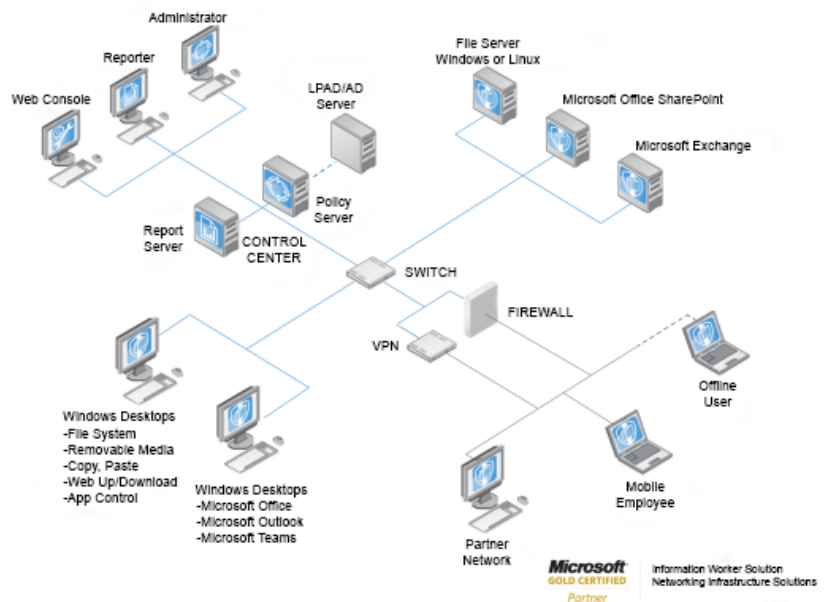
With increasing availability and access to information, inappropriate handling of sensitive information at an end user's desktop or laptop often results in data loss. End users can easily move data on their desktop to attached devices or through the network without knowing the risk of data loss. The challenge is further exacerbated in cases where data loss has already occurred but there is no detailed activity log to trace the path of loss with data moving from server to end point and from one user to another, complicating audit and incident investigations.

THE SOLUTION

The Windows Desktop Enforcer is policy enforcement software that runs on desktops and windows server and laptops to monitor and control user activities, covering:

- USB device
- CD/DVD burners
- File system (local and remote shared files)
- Clipboard (copy and paste)
- Application execution
- Web uploads and downloads (including web mail, posts through forms, blogs)
- File transfers (rcp)

It works in the background without needing any user attention and interacts only when a policy applies to help the user follow proper information handling procedures.



THE RESULTS

- **Prevent Data Loss Proactively**
Stop endpoint data loss in real-time, online or off-line, through USB devices, Web uploads, file copying, and sharing.
- **Ensure Electronic Data Storage Compliance**
Prevent storing data in locations that expose sensitive information to unintended audiences.
- **Simplify Data Security with Interactive Remediations**
Automate remediations to deliver real-time policy education, data classification, data cleansing and much more.
- **Illuminate Audit and Incident Investigation**
Use detailed endpoint activity logs to reconstruct sequences of events across systems and users to investigate incidents.

KEY FEATURES

Proactive Data Loss Prevention

Monitor and control activity at the endpoint in real-time, avoiding traces of data on the wire or on other systems, thereby reducing audit and incident investigations:

- **Alert:** alert user when policies apply
- **Warn:** prompt user and let user decide to proceed with an action
- **Block:** stop user from performing an action and inform user about policy

Broadest User Action Coverage

Whether user is accessing file, uploading to the Web, or running an application, the Enforcer logs and controls these activities constantly, online and off-line:

- **Data Access:** Open, create, edit, delete, rename
- **Data Use:** copy, embed, move, paste, print and file transfers
- **Application Execution:** prevent running applications based on application fingerprint, regardless of executable file name or location

Fine-Grained Data Control

Prevent data loss by selecting right data to protect with precise, fact-based data identification:

- **Location:** local, remote shares, or mapped drives and folders
- **Classification:** public, confidential, restricted, and etc.
- **Content:** search keywords and patterns
- **Attribute:** document tag to identify customer or use any customer property

Identity-based Policy Enforcement

Accurately enforce policy by pinpointing the user based on user name, email address, group membership, assigned roles, or any user attribute defined in enterprise directory, such as Active Directory.

DLP for Mobile and Remote User

Data protection policies may vary depending on the user's device and physical location. Location awareness and device detection provides tunable controls that dynamically restrict or allow access and use:

- **User Location:** in main or branch office, at a hotel or at home connecting through VPN or RDP (Remote Desktop Protocol) to a host in the internal network
- **Device Type:** host name, domain, platform, OS version, site location

Policy Assistants

Help end-user perform remediation tasks with interactive wizards, simplifying data security for end-users and improving compliance policy adoption:

- **Document Classification:** tag document with user selected class or automatically classify based on content.
- **Policy Communicator:** deliver policy education with immediate

Compliance Audit and Incident Investigation

Provide the most comprehensive activity monitoring on the end point with full details about not only who accessed what information, but also from where that data came, where are other copies, and who else modified or copied it. Investigators can reconstruct the path of data loss to hone in on how and what data is loss.

Automatic Policy Update

Periodic policy updates and user identity changes are automatically delivered to the enforcer without any end user interaction.

Offline Enforcement and Logging

User actions are monitored, controlled, and logged regardless of network connectivity. Store-&-forward logging collects activity details and uploads logs when network is available.

Tamper-Resistance of Enforcer Software

The Enforcer is password protected and prevents users with elevated privileges including administrators from terminating or removing the software. This ensures ongoing compliance with enterprise policies.

Secured Communication

Encrypted communication via SSL between the Windows Desktop Enforcer software and the Policy server protects the policy set download and log upload. The enforcer authenticates the policy set to ensure it comes from the trusted Policy Server.

Desktop Enforcement Suite

Combining the data access and use controls in the Enforcer for Windows Desktop with the communication controls in the Enforcer for Outlook and delivers a robust enforcement suite on the desktop, simplifying data protection for end users and preventing data loss at the end point device or through communication channels.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations –whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit <http://www.nextlabs.com>.