GUIDE *(Cybersecurity)*

Privileged Access Management: Why Sudo Is No Longer Enough

The new privileged access management solutions available on the market today provide highly efficient and effective alternatives to sudo. Using these modern approaches, you will be able to reduce the risk of insider fraud, streamline regulatory compliance, and greatly reduce the effort required to administer your server estates.

Sudo is a free open-source access control tool that requires costly and labor-intensive custom configuration to meet privilege access management and compliance requirements.

Sudo may be a reasonable solution for controlling privileged accounts for organizations with small server infrastructures, but it lacks the administration efficiencies, architectural vision, and security-related compliance requirements that are needed to effectively protect critical assets for organizations running hundreds and thousands of diverse Unix and Linux servers. **There are five primary challenges with using sudo to control privileged accounts:**

First, sudo lacks efficient, centralized administration. System administrators can spend considerable time building and distributing sudoers files across the server estates. Sudo lacks the ability to easily put servers into local categories, classify users by various roles, and define the associated access rules, methods readily available through the latest privileged access management solutions on the market. The point is that it does not integrate well with Identity Management systems.

Second, sudo introduces a security risk because it is controlled by local files. The burden is on the security admins to distribute these files appropriately. To do the distribution well, each server typically needs to have a unique file, but in most cases, shortcuts are taken by administrators, which results in giving administrative users too much privilege. As well, the sudo configuration file is stored in a way that local administrators could easily make modifications… a big security risk.

Third, sudo may create a compliance issue. The distributed sudo conf files are not liked by auditors because they utilize "static trust". The sudo configuration files need to be secured. Organizations using sudo may have problems passing audits because of this.

"Sudo is a free open-source access control tool that requires costly and labor-intensive custom configuration to meet privilege access management and compliance requirements."

Fourth, organizations using sudo must be able to distribute the file. Regardless of the methodology the distribution method must be maintained, resulting in hidden costs.

Fifth, sudo does not inherently provide the ability to link multi-factor authentication as part of the privileged user authorization process. Elevating the authentication requirements in order to elevate privilege provides greater flexibility in the methods used to authenticate any given user, based on the access request parameters.

There are other options to sudo for controlling privileged account access. A good example is Powertech Identity & Access Manager (BoKS), which transparently grants privileged access permissions, without sharing privileged account passwords. With Identity & Access Manager, policies can be created that adapt to the circumstanced based on the factors such as: who is asking, from where, to where, using what protocol, when, what they want to do.

Following is a comparison between Sudo and Identity & Access Managers' privileged access management capabilities:

OpenWare/Sudo	Powertech Identity & Access Manager (BoKS)
Access is allowed if the local sudoers file permits it, unless configured to only use LDAP. This could create a security risk.	There is no access to privileged accounts unless a fine-grained access rule is defined and then granted in real-time by Identity & Access Manager
Sudoers config files must be manually copied to each local machine (or the files must be transfer periodically) for any change. Can be viewed as "static trust" by auditors, which is undesirable. Using sudo, an admin can create a method for each host to get the file it needs with "least privilege", but it isn't automatic, and it isn't easy.	Access policies reside in a central database and updates are almost instantaneous. Enables organizations to pass audits since the local trust relationships do not reside in operating system files that could then be exploited and create a security risk.
The default with sudo is to put user activity logs on the local server. You could configure sudo to send logs to remote server, but that requires configuration effort and it is more complex.	Audit log are automatically stored on the master security server in a directory only readable by root. Most importantly, audit logs are stored in a way that local administrators cannot modify them.
Statically defined permissions.	If and when an access policy is changed by security officers, it is then available to all Identity & Access Manager protected servers immediately. As well, authorization/access permissions adapt based on time of day, day of week, who is making request, etc.
Cumbersome to implement, manage, and maintain.	The Identity & Access Manager system is managed centrally and changes are immediately implemented throughout the domain. System admin doesn't spend hours building and distributing sudoers files. Simple method of creating and managing access routes. Regular updates to new functionality under maintenance programs.
Control of sudoers file may not be limited by privilege. This is a problem where a server is running critical applications, and sudo controls which privileged commands can be run against privileged data. If the control is the sudoers file, then the control issues are: • Who has the right to update the file? • Logging of file update • Link to change management processes • Versioning of file • Exclusion by authority and role to RW file • Access to RW the file on the server by some other priv. route (i.e. su)	Identity & Access Manager centrally controls the authorization to utilize privileged accounts, without sharing the privileged account password, based on fine-grained access rules. In addition, administration of these authorizations is separately controlled with granular sub-administration.

While sudo provides an adequate method for privileged access management in small server estates, it is a cumbersome utility with the potential to create increased exposure to insider fraud for organizations trying to control access across large, diverse server infrastructures. In addition to requiring highly paid system administrators to spend a great deal of time building, and distributing sudoers files, sudo also forces you to rely on the individual expertise of your system administrator to plan and implement sudo in such a way that provides "least privileges". The new privileged access management solutions available on the market today provide highly efficient and effective alternatives to sudo. Using these modern approaches, you will be able to reduce the risk of insider fraud, streamline regulatory compliance, and greatly reduce the effort required to administer your server estates.

About Identity & Access Manager

Identity & Access Manager transforms your multi-vendor Linux and UNIX server environment into one centrally managed security domain. It simplifies your organization's ability to enforce security policies, and control access to critical systems and information. With full control over accounts, access and privilege, IT and security teams can proactively prevent internal and external critical system attacks before they start.

Identity & Access Manager protects your most critical systems and data so that you can focus on what is more important—accelerating the growth of your business. Visit www.helpsystems.com/products/privileged-access-management to learn more or request a demo.

helpsystems

www.helpsystems.com

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.