WHITE PAPER • SEPTEMBER 2017

ca technologies

Reducing the Risk of Data Breaches on Your Most Critical Servers: How CA Can Help

Table of Contents

Executive Summary

Challenge

Businesses today must reduce the risk of security breaches to protect the valuable data within their organizations. At the same time, IT auditors are increasingly enforcing ever more stringent requirements on the business. The bottom line is that privileged accounts and privileged access are being targeted by hackers as a new attack surface and focused on by auditors who are insisting on greater controls around privileged accounts.

Opportunity

The right privileged access management solution provides comprehensive protection for your mission-critical servers with powerful, fine-grained controls over operating system-level access and privileged user actions. Capable of enforcing access controls on powerful native Superuser accounts—like the UNIX® and Linux® root and Microsoft® Windows® administrator—this system-level, host-based privileged access management solution controls, monitors and audits privileged user activity, improving security and simplifying audit and compliance.

Benefits

CA Technologies provides easy-to-deploy and comprehensive privileged access management solutions with integrated credential management, strong authentication, zero-trust access control, proactive command filtering, session monitoring and recording, and fine-grained controls over high-value servers. CA Privileged Access Management provides capabilities and controls that actively prevent attackers from carrying out key components of their attacks, while reducing risks and improving operational efficiency. Benefits include reduced risk, increased accountability, improved auditing and compliance, and reduced complexity.

Introduction

Businesses today must reduce the risk of security breaches to protect the valuable data within their organizations. At the same time, IT auditors are increasingly enforcing ever more stringent requirements on the business. The bottom line is that privileged accounts and privileged access are being targeted by hackers as a new attack surface and focused on by auditors who are insisting on greater controls around privileged accounts.

The sad fact is that stealing and exploiting privileged accounts is a critical success factor for hackers in 100 percent of all advanced attacks, regardless of origin. These accounts include privileged users, accounts and credentials—employees, third-party contractors and countless applications and scripts containing privileged credentials (often hard-coded and visible to any number of individuals) that exist in your IT infrastructure.

Moreover, operating systems such as UNIX, Linux and Windows are built on the concept of a "superuser" that can bypass most or all of the security controls on your systems. These high-privilege accounts are used by administrators for legitimate purposes but can also be misused by malicious insiders or external attackers.

Protecting those users and their credentials is a critical element in helping to prevent attacks, and privileged access management has become a new and necessary component of a defense-in-depth strategy—as essential as firewalls and anti-virus for protecting your business. The right privileged access management solution provides comprehensive protection for your mission-critical servers with powerful, fine-grained controls over operating system–level access and privileged user actions. Capable of enforcing access controls on powerful native superuser accounts—like the UNIX and Linux root and Windows administrator—this system-level, host-based privileged access management solution controls, monitors and audits privileged user activity, improving security and simplifying audit and compliance.

This white paper examines the challenges in securing mission-critical servers and some of the approaches available today, and introduces CA Privileged Access Manager Server Control, which provides the most mature, proven and powerful solution for protecting your mission-critical servers. CA Privileged Access Manager Server Control is based on a proven mainframe security model to allow you to apply proactive access controls and superior auditing that are uniquely effective, even against superusers.

Today's Challenges in Securing Mission-Critical Servers

Malicious insiders and external hackers are determined to take over and exploit the privileged user accounts on your mission-critical servers. Just a single breach can cause extensive reputational and financial damage to any organization. IT departments are under tremendous pressure to stop targeted attacks and mitigate insider threats while also complying with industry security requirements and standards in order to achieve and sustain compliance. IT is also tasked with managing and securing an increasingly complex hybrid infrastructure while trying to achieve operational efficiency through automation and scalability. The scope of responsibilities seems enormous.

Typically, risk is reduced to an acceptable level based on the mission-criticality of what is stored on the server. Some servers are simply more valuable than others because of the information they contain, such as credit card information, social security numbers, personally identifiable information, healthcare records, email addresses or intellectual property such as plans, financial results and insider information. While privileged access management reduces risk, you must take extra steps to protect your most critical servers. Let's look at some of these approaches.

Key Approaches: Protecting Critical Systems Requires More Than Basic "Hardening"

It's clear that one of the most pressing challenges for IT is to ensure the security of the servers that host the organization's sensitive electronic assets, such as customer data, financial records and intellectual property. These assets are the very lifeblood of many organizations, and a breach could result in unrecoverable damage.

The typical "server hardening" can:

- Install all patches before connecting to a network
- Remove unnecessary services
- Delete unused software and sample files
- Install anti-virus/anti-spyware/anti-phishing software
- Encrypt sensitive drives
- Use strong passwords
- Only share the superuser password with a small number of key administrators

While most of these steps are good advice and follow generally accepted security principles, the last relies upon the fundamentally flawed assumption that it is impossible to effectively control administrative system accounts. This leaves a gaping hole in a server's security that can be exploited by not only a malicious insider but by external attackers as well. No matter the source, the most damaging attacks involve the use of privileged identities. By their nature, these accounts have the permissions to affect significant change to a system, application or database. Actions using these accounts have the potential to be exceptionally destructive and must be monitored closely.

Native Operating System Security

At the heart of the security challenge of native operating systems controls is the fact that they are fundamentally founded on the concept of a superuser—a level of privilege that essentially bypasses, and thereby negates, every security control on the server. This is most commonly seen in cases such as the Linux/UNIX "root" account, as well as the Windows "administrator" account.

The design of the operating system itself assumes the unrestricted nature of these accounts. For this reason, the superuser accounts are coveted and targeted by attackers. Once the attacker has control of the account, he has virtually unrestricted access to anything on the server, as well as anonymity, since the account is not associated with a named individual. For this reason, most commercial server-based solutions attempt to control and limit a user's ability and need to use the superuser account. ***The gaping deficiency in such approaches is that they are unable to defend the server against a user who is already exploiting superuser privileges***. Even the security controls themselves can be defeated by skilled and motivated attackers. Moreover, the security controls are usually administered and maintained by the systems administrators, who in fact represent one of the groups that the solution should be trying to control. It's a case of the fox guarding the hen house.

For the reasons cited above, protecting an organization's most sensitive electronic assets, such as customer databases, hospital patient records or proprietary information, is difficult because native operating system capabilities do not provide adequate protection against inadvertent or intentional attack, nor do they provide reliable auditing of the entire server environment. This problem is intensified when the hosting systems for external customers contain confidential data and critical applications, or when critical systems or information are exposed to contractors or hosted by service providers.

Operating system access controls are also at risk of being analyzed and avoided because they are **known controls**. When a malicious attacker gains access to a privileged account—either an outsider with unauthorized access or an insider—a common first step is to do research on the security settings. This includes viewing operating system permissions and looking for vulnerabilities in the controls that can be exploited. Malicious users will also look to modify operating system logs in order to hide their tracks. Even on systems where access controls are rigorously enforced, well-trained attackers will simply avoid taking actions that would generate alerts and lead to detection. Only a fully externalized security system i***n which even superusers are regulated*** can bring **unexpected** and **unknowable** elements to a security system and provide the access controls and user activity logs needed to truly secure a system.

Operating systems are also inherently incapable of ensuring the integrity of their own controls. All systems have privileged accounts that can change or bypass that system's security controls. A user with the proper access can disable the controls necessary to perform an unauthorized action and can modify system log files to erase records of that activity.

Another problem with relying on operating system security controls is their **lack of uniformity**.

There can be significant variance of capabilities and availability of security controls across platforms (UNIX file/directory controls are significantly different than Windows). This can lead to tangible security issues:

- Security policies are created to accommodate systems limitations, not to meet business needs.
- Errors and omissions are caused by added complexity of security management.

Shell Wrappers

A common method for controlling privileged users' use of operating system controls is to use a shell wrapper that can be configured to allow or deny access to certain commands by specified individuals. A shell wrapper runs in user mode on the operating system, where commands are executed by the kernel (a lower-level component of an operating system).

Shell wrappers have many weaknesses:

- They cannot protect against the superuser account itself. Users with access to the root account, as well as other users who are technically savvy, can always bypass a shell wrapper using the following techniques:
  - The root user kills the current shell process, and the kernel creates a new shell without wrapper restrictions.
  - A user uploads a script to the target system and executes the file. All commands will bypass the shell wrapper to be executed by the operating system kernel. This script could modify, delete or send sensitive data outside of the system and be entirely invisible to, and not controlled by, the shell wrapper.
- Shell wrappers can only protect against commands entered into a shell. Other applications on a system (like Oracle) may have security holes that could be exploited to run malicious commands. These will not be detected, controlled or logged by a shell wrapper.
- Key loggers can also be ineffective if they are part of a shell wrapper because they only capture which keys are pressed, not which commands are run. A malicious user (administrator or otherwise) could upload a script that performs multiple actions. A key logger can only record that a script was run—not what it actually did. This leads to a lack of accountability—defeating the very purpose of a key logger.
- Vendors advocating shell wrappers often recommend never using or sharing the root password. This is often not operationally feasible. Applications frequently require the root password in order to install or function.

Sudo

Sudo (superuser do) is a freeware program that allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands used. Sudo is used in most UNIX/Linux environments where operations personnel do not need access to a root shell but are still required to execute certain commands as root, such as starting/stopping processes, updating specific configuration files and rebooting the server. Sudo provides an important capability (privileged task delegation), but it is an inadequate control by itself.

Sudo has many weaknesses:

- It depends on the use of one or more sudoers files, the administration of which can be time-consuming, resource-intensive and error-prone. Moreover, the sudoers file(s), and the administration of these files, can introduce security risks due to being managed by privileged identities, which may themselves be compromised.
- Sudo does not provide enterprise-class logging capabilities. Sudo relies on the UNIX syslog, which is vulnerable to tampering by the root user. It does not provide accountability for each sudo action. Not every command executed via sudo will be logged to track the original user. This fails to facilitate compliance with requirements from PCI and SOX.
- Sudo will not audit and track actions based on the original user ID invoking "vi," even when the user breaks out into a shell. When a user uses sudo to invoke "vi" as root, there is an option to break out of "vi" and run shell commands with root privileges. With CA Privileged Identity Suite sudo, any such shell commands that are executed are traced back to the original user who invokes sudo.
- Sudo has critical functionality restrictions. Sudo cannot assign/restrict a user-specific file/folder or command access.
- Sudo fails if a user escalates privileges. A regular user that exploits an OS vulnerability to gain 'root' access bypasses all sudo restrictions.
- The use of native operating system controls also often leads to inconsistent enforcement of security policies across servers and platforms. A single set of strong access controls that is enforceable across disparate platforms is needed to neutralize platform differences.

Proxy Controls

Another method for implementing access controls is the proxy. In this method, all commands go through a centralized "choke point," which can filter (deny) all commands specified by a rule set. This method can prevent a privileged user from "killing" the shell by recognizing and blocking the commands necessary to do so.

Proxy has many weaknesses:

- It can be circumvented using applications. A user can create an executable file using a text editor (such as vi) and fill it with restricted commands. A proxy will not be able to understand what actions the user is performing inside the application. A proxy cannot detect commands that have been "autocompleted" or pieced together.
- Proxy can be circumvented using external downloads. Similar to shell wrappers, a user can also bypass the proxy entirely by downloading a file that contains restricted commands on the target system using multiple methods—from FTP or SSH to a physical USB drive. It is not always possible to deny access to these file transfer utilities, as they are often needed for common administration and system tasks.
- A single command that is not secured may be used as a backdoor to bypass the proxy controls.
- Proxy can be ineffective against software vulnerabilities. Proxy-based controls are completely ineffective against attacks that compromise vulnerable software, such as zero-day exploits.

Access Controls/Host Security

As we have already mentioned, the use of shared Superuser accounts typically results in privileged users having unnecessary access to critical systems and data. This violates the security principles of "least privilege" and "separation of duties." Operating systems do not have the ability to restrict actions and access for multiple people using a shared account. Fine-grained access controls go beyond OS security to ***examine a user's original identity to determine whether an action should be allowed or denied***. This enables true least privilege access.

The capabilities described below are required to help ensure that administrators have only the privileges they need to do their job and none beyond that.

How CA Can Help

CA Technologies provides easy-to-deploy, comprehensive privileged access management solutions with integrated credential management, strong authentication, zero-trust access control, proactive command filtering, session monitoring and recording, and fine-grained controls over high-value servers. The solution has two deployment options, providing the appropriate level of defense for different security needs and enabling in-depth defense of privileged accounts to minimize security and compliance risks.

- **CA Privileged Access Manager** delivers the comprehensive functionality needed to prevent breaches, demonstrate compliance and boost operational efficiency—providing protection across the broadest and deepest range of infrastructure, including the data center, software-defined virtual data centers and networks as well as public/private clouds.
- **CA Privileged Access Manager Server Control** improves security and simplifies audit and compliance by controlling, monitoring and auditing privileged user activity on key servers, with powerful fine-grained controls over operating system-level access and privileged user actions.
- **CA Threat Analytics for PAM** provides a powerful set of user behavior analytics and machine learning algorithms that help you detect and combat breach attempts before they impact your business.

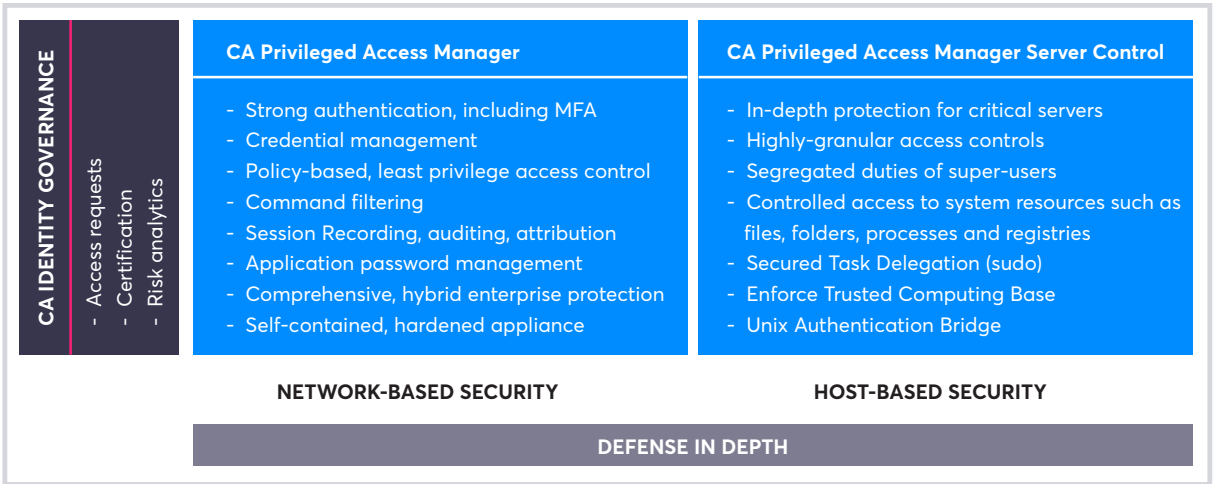


FIGURE A.
The key elements of a defense-in-depth security approach from CA.

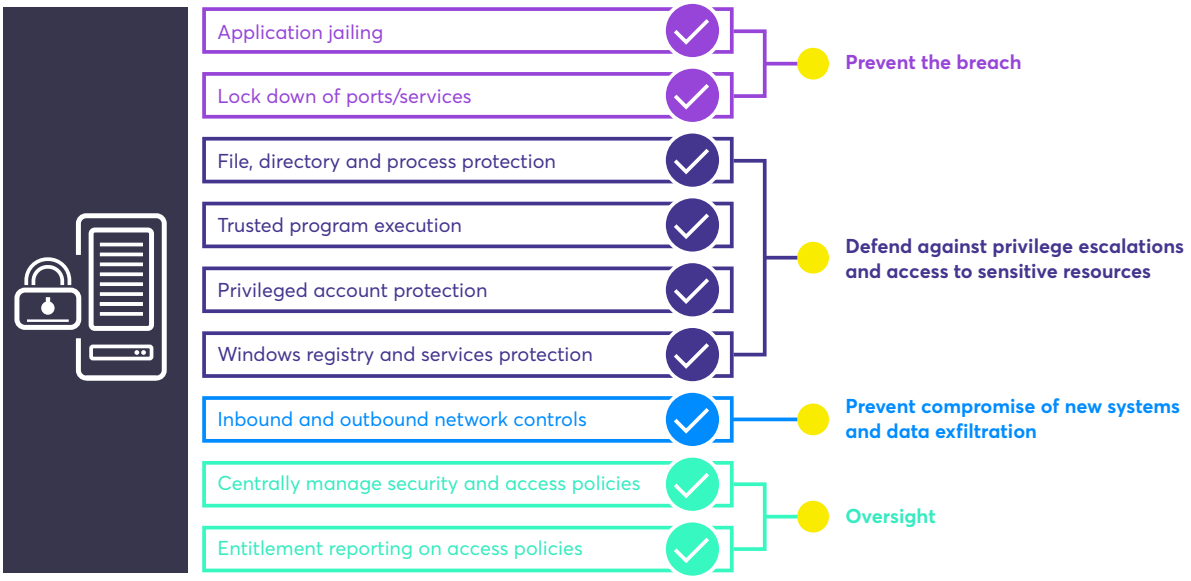
A Deeper Look at CA Privileged Access Manager Server Control

For organizations with additional security requirements for high-value servers hosting business-critical assets, CA Privileged Access Manager Server Control provides localized, fine-grained access control and protection over operating system-level access and application-level access. Agent-based, kernel-level protection is available for individual files, folders and specific commands based on policy and/or fine-grained controls on specific hosts.

CA Privileged Access Manager Server Control uniquely and elegantly handles the security gaps inherent in the faulty Superuser-based security models of mission-critical servers. CA Privileged Access Manager Server Control delivers:

- Use of the original user ID tracking for segregation of duties (SoD) and accountability, even when the superuser account is being used. This fundamentally changes the superuser-based security model. For example, User A using the Linux root account will have different privileges than User B using the Linux root account. Additionally, tamper-proof audit logs will identify the actual identity of the user behind all superuser operations.
- Fine-grained access control to file, directory and system process resources
- User ID and login enforcement protections
- Kernel module load/unload on UNIX/Linux
- Windows registry protection
- Incoming and outgoing TCP/IP protection
- Task delegation (secured Sudo replacement) for UNIX/Linux and Windows
- Hide root password capability
- File and program integrity monitoring
- Self-protecting against bypass or termination

FIGURE B.
A deeper look at CA Privileged Access Manager Server Control.



Solution Benefits

CA Privileged Access Manager provides capabilities and controls that actively prevent attackers from carrying out key components of their attacks, while reducing risks and improving operational efficiency. More specifically, CA Privileged Access Manager enables organizations to:

- **Reduce risk.** Prevent unauthorized access and limit access to pre-approved resources once entry is granted to the network. Protect passwords and other credentials from unauthorized use and compromise. Limit the actions users can perform on systems. Prevent the execution of unauthorized commands and lateral movement within the network.
- **Increase accountability.** Observe full attribution of user activity, even when using shared accounts. Using comprehensive logging, session recording and user warnings, capture activity and provide a deterrent to unauthorized behavior.
- **Improve auditing and facilitate compliance.** Simplify compliance by providing support for emerging authentication and access control requirements, and limit the scope of compliance requirements through logical segmentation of the network.
- **Reduce complexity and boost operator productivity.** Privileged single sign-on not only limits risk, but also boosts productivity of individual administrators by making it easier and faster to access the systems and resources they need to manage. Centralized policy definition and enforcement simplify the creation and enforcement of security controls. This solution can protect the broad hybrid IT infrastructure, covering the traditional physical data center (servers, networking devices, databases, switches and related resources) and growing virtual and cloud platforms. This helps protect the underlying management infrastructure and resources deployed in software-defined data centers and networks, IaaS environments and SaaS offerings.

Customers find that CA solutions are easy to adopt and avoid hidden hardware costs. The ease of administration/ease of use helps deliver time to value as well as the ability to scale, so you can not only future-proof your hybrid IT infrastructure but also reduce risk and achieve as well as maintain compliance. We recommend that customers who currently have CA Privileged Access Manager in place and wish to protect their most mission-critical servers upgrade to CA Privileged Access Manager Server Control. If you are just beginning to improve your organization's security posture with a defense-in-depth program, consider CA Privileged Access Manager to mitigate the risk of insider threat and abuse of privileged accounts.

Conclusions

To guard against costly data breaches, smart companies are protecting and automating access to privileged accounts on their most critical servers. Employing a zero-trust model with a defense-in-depth approach to security that includes privileged access management offers your organization the best chance of protection against ever-evolving threats. CA Privileged Access Manager provides capabilities and controls that actively prevent attackers from carrying out key components of their attacks, while reducing risks and improving operational efficiency.

Next Steps

Read the **CA Technologies Privileged Access Management Buyers Guide** to learn more about safeguarding access and what companies can do to prevent data breaches.

To learn more about Privileged Access Management from CA, visit:
ca.com/pam

Connect with CA Technologies

CA Technologies (NASDAQ: CA) provides IT management solutions that help customers manage and secure complex IT environments to support agile business services. Organizations leverage CA Technologies software and SaaS solutions to accelerate innovation, transform infrastructure and secure data and identities, from the data center to the cloud. CA Technologies is committed to ensuring our customers achieve their desired outcomes and expected business value through the use of our technology. To learn more about our customer success programs, visit ca.com/customer-success. For more information about CA Technologies go to ca.com.

CS200-305094_0917