Controlling and Managing Privileged Access

A Primer on Privileged Access Management

ONE IDENTITY by Quest

Abstract

Effective management of privileged accounts (sometimes called superuser accounts) and privileged access is becoming more and more critical. This is because security and compliance are driving forces behind most IT initiatives and privileged rights are the key – or downfall - to achieve both security and compliance. And in today's complex, heterogeneous environments, native privileged access management (PAM) tools and manual practices are inadequate.

This white paper explores the risks associated with privileged access, and explains how solutions from One Identity mitigate those risks with granular access control and accountability.

This paper is intended for CISOs, CIOs, IT directors and managers, security and compliance officers, and administrators, especially those who have not established firm control over all of their organization's privileged user access.

The challenges of privileged accounts

Privileged accounts are necessary but risky

Privileged accounts (known as 'root' in the UNIX and 'administrator' in the Windows world) are necessary from an administrative perspective.

Administrators need easy access to elevated and mission-critical IT assets that control the operation and function of the broader enterprise. Often, the only way to get that access is to use privileged accounts.

While operating systems have become significantly more powerful in recent years, privileged access has not evolved as quickly. So a single, all-powerful level of access still exists in some enterprises. For instance, many UNIX administrative tasks can't be carried out without root access, and many of those tasks are quite routine. While a small business may have only a single trusted person with privileged access, most midsize to large businesses have multiple privileged administrators that all need access to the same privileged credentials.

The problem is that operating systems do not natively offer a way to discriminate more granular privileged access: it's an all-or-nothing proposition. Therefore, a surprisingly large number of people can often wield incredible power within the native OS — much of which is unnecessary for each individual to fulfill his or her role. Since privileged accounts can be used to bypass standard controls and authorization levels, a person with a privileged account often has unlimited access and, if they become disgruntled, they can inflict significant damage to networks, servers, applications and data.

The problem is not only that too many administrators have elevated access but also that **administrators can work outside the network's identity management system** and hide their actions.

Today, this is further complicated by the explosion in remote access by privileged users, including third-party contractors. Sensitive data and other critical resources are being accessed by too many users – internal and external users - with very little accountability. When damage is done, many organizations are virtually blind to who specifically accessed what resource, which makes incident discovery and analysis extremely challenging, if not impossible. This antiquated admin philosophy of shared credentials opens up a level of risk – as well as serious audit and expensive compliance issues - that have no place in a modern IT environment.

Then there is compliance. Many organizations need to meet SOX, PCI DSS, HIPAAA, GDPR (and more) specifications, as well as local regulations. These regulations require organizations to control all access to sensitive information. Regulations and failed audits are becoming serious concerns for CIOs and CISOs, as auditors are paying closer attention to privileged accounts. Organizations must pass these audits as the direct and indirect costs of non-compliance is much higher than the investment in supportive processes and technologies.

The solution lies in a combination of policies, checks and balances, automated oversight and analysis that can enable more granular privileged access management.

Solving your privileged access management challenges

Establishing checks and balances

In the United States' system of government, constitutional checks and balances assign separate powers to the judicial branch, legislative branch and executive branch. Think of the executive branch (Office of the President) as the privileged account holder; the president wields the ultimate access rights and decision-making authority — but that power is mitigated by the oversight of the other two branches. In an enterprise environment, a similar system of checks and balances can be established to limit the power, authority and access rights of privileged users.

In most cases, granting the 'keys to the kingdom' to a single person is not really necessary — the operating system's privileged account system does not have to be used as is. A more granular delegation of authority, policy-based control, automated workflows and activity monitoring can add a layer of security to an inherently insecure designation, while still enabling administrators to get their jobs done efficiently and effectively.

A surprisingly large number of **people have unlimited privileged access within native OS management tools** — and much of this access is unnecessary for their role.

An optimal approach to privileged access management should include the following checks and balances:

- Credential vaulting
- Secure remote access
- Command control and granular delegation
- Keystroke logging and session audit
- Entitlements and behavior analysis

Through a policy-driven implementation of these areas, an organization can protect its data, prevent security breaches and ensure compliance with an ever-widening array of rules. This is the realm of privileged access management: a combination of processes, policies and technologies that ensure that privileged users and superusers who have access to administrative credentials are doing the right things, that access is delegated on an as needed basis and that an audit trail is kept in place at all times. In short, privileged access management adds accountability back into what is otherwise a free-wheeling and overly broad system of administrative access.

Managing privileged access: Who guards the guards?

The fundamental challenge of access management is that the IT department is usually delegated the role of managing access, authentication and authorization — but often no one imposes that control over the IT department. Those who have privileged access may have a common ethos for sharing information (including passwords), self-policing their actions and keeping that enhanced level of access to themselves.
But who guards the guards?

It's all too common for enterprises to lack any coherent strategy for privileged access. Most large organizations have multiple (internal or third-party) administrators, including Windows, UNIX and other administrators, each with his or her own tasks to complete. IT administrators have a culture of trust between themselves, and it's not unusual for multiple administrators to share a single superuser password. This is a friendly way to do business, but a risky one – and it's unnecessary.

IT people don't always appreciate what management sees as essential: the need to impose strict controls over themselves. As a result, something exceedingly powerful — the unlimited access that can be gained from privileged accounts — receives little oversight and is too often protected by just a cobbled-together, ad hoc, informal and frequently ignored set of administrative protocols. As a result, in any enterprise with more than a handful of IT staff, a number of people will have privileged access, which allows them to do just about anything they wish.

The basic challenges companies face with regard to privileged access include:

- No accountability, since there is (amazingly) no oversight or management system to control privileged access
- Too many people with access to superuser or root accounts, including admins with limited responsibilities but unlimited access
- Lack of control over the privileged access password, which is frequently shared
- Lack of detection and analytics capabilities related to privilege misuse

Safeguarding sensitive information and ensuring compliance

Protecting sensitive data and applications is a growing concern for CISOs and senior IT management. Faced with rapid growth in data volume, remote working (particularly by admins and other privileged users) organizations of all sizes need to ensure secure remote access. This naturally makes it difficult to protect data and comply with regulatory mandates.

Controlling and security admin-level access

Technologies, such as cloud computing and remote admin access - along with globalization and constantly changing economic conditions, have transformed how organizations conduct business. For example, organizations increasingly use third-party vendors and consultants to acquire specialized solutions and scale to business needs without adding full-time IT staff.

While this new business model brings many benefits, it also creates challenges, the greatest of which is secure remote access. Contractors require access to the corporate network, and in many cases, this must include a level of privileged access. Granting privileged access to people inside the company brings enough problems; but providing privileged access to consultants, who are working remotely and running computers that may not be firewalled or protected from malware, is a disaster in waiting.

The only good solution is to enable remote vendors with a controlled and continuously monitored privileged access. They get access, but only to the resources they need and only for a prescribed amount of time. This prevents them from snooping around your network, keeps them on task and limits your risk.

Privileged access management is a combination of processes, policies and technologies that ensure that **privileged users and superusers who share administrative credentials are doing the right things**, that access is delegated on an as-needed basis and that an audit trail is kept in place at all times.

Understanding the risks: When things go wrong

The risks of privileged accounts are not just theoretical. Disgruntled and terminated superusers have been known to steal or sabotage data on their way out the door, and industrial espionage occurs on a regular basis. Identity theft and theft of corporate secrets takes place more frequently than many people are aware, and it's often an insider who is the culprit.

Such was the case at Nuance a speech-recognition software firm when 45,000 patient records hosted on one of its medical transcription platforms were leaked. The leak came at the hands of a former employee who hacked into the company's servers to access the patient information.

Another instance of insider threat is when a former employee of SunTrust Bank attempted to pilfer the names, addresses, phone numbers and account balances of 1.5 million bank clients. The malicious insider was attempting to provide the data to a criminal outside the organization but got caught before it could be sent. The disaster was averted, but the situation could just as easily have gone the other way.

Privileged Access

An alternative to giving administrators unlimited access with no oversight

Clearly, administrators need to have access to do their jobs, but the 'all or nothing' approach native to the OS is inadequate and outdated. Most admins who have privileged access do indeed need privileged access to one or more areas of the network, but it is unlikely that they require privileged access to everything. What is needed is a way to allow easy, unfettered access to resources when it is needed and to restrict access to what is not needed. Such a system would:

- Delegate specific privileges to administrators based on role
- Include a policy engine that delegates access based on need
- Provide a complete audit record with full details of access and specific actions taken
- Detect anomalies and bad behavior using machine-learning algorithms

Traditional approaches to privileged access management are almost always inadequate

Motivating a group of IT people to adhere to a new management policy is a little like trying to herd cats. Upper management often has a hard time trying to impose its point of view over the IT department. Sometimes it just can't be done. IT people are an independent-minded lot. Managing IT from outside the department is difficult because management doesn't really understand everything that IT people do. When the operations manager, or any manager from outside IT, steps in and announces, 'We need to restrict your access,' that outside person had better be armed with a very compelling argument and a firm resolve.

Basic conflicts occur when **management views privileged or unlimited access as a problem**, while admins see it as standard operating procedure.

As a result, organizations tend to adopt one of three solutions:

- **Issue a memo**, which everybody understands will be uniformly ignored, but management has been placated.
- **Implement a manual solution** (often called a 'firecall ID') that involves writing the privileged access password on paper, sealing it in an envelope and storing it in a secure, physical location (such as a safe) controlled by an outside trusted employee or manager. That outside individual is tasked with changing the password each time it has been used.
- **Create individual solutions and policies** that lack unification, solving only one problem at a time.

The first approach above is clearly inadequate. The second solution attempts to address the issue, but because it is primarily human-controlled, it is still subject to error, loss and intentional misuse. In addition, this approach breaks down when there are dozens or hundreds of accounts at hand.

The third solution may be adequate in smaller company environments. The open-source solution sudo, for example, solves a lot of problems and may be all that is needed if there are only a handful of UNIX and Linux servers involved. But for larger installations, sudo offers no centralized management function to control multiple servers from a single management console, nor does it provide an audit trail. (For more on sudo, see the section 'The sudo project' below.)

Three basic policies are essential to success

Preventing disasters like the Nuance and SunTrust incidents described above is not rocket science, but most companies simply don't do it. An enforced policy of swiftly revoking the access of terminated individuals should be a standard policy of every company — and it's not that hard to implement. These organizations simply got bogged down in bureaucracy and unnecessary procedures, delaying pulling the plug on the administrator's access until it was too late.

These episodes could have been easily averted had the organization created and enforced three simple policies:

- **Limit the rights of administrators.** Native UNIX takes an 'all access' approach to administrator permissions, violating the basic premise that every security manager knows: 'Trust no one.' Granting administrators everything they need to do their jobs, but nothing beyond that, brings a new level of order and common sense.
- **Shut down access quickly when necessary.** Traditionally, this used to mean physically escort terminated employees and contractors off the premises, but today with so many admins and contractors working remotely, you have to have the capability to shut off access to privileged resources immediately. A single employee or contractor with a grudge can cause a lot of damage. Sound HR policy must include the immediate termination of all computer access.
- **Track and analyze administrator activity.** Many organizations have a system to track what employees are doing, but that tracking often doesn't extend to the superusers. Existing technology can record keystrokes and observe actions in real time, create an audit trail and alert upper management that something is amiss before the damage is done. And many solutions can also save the session for forensics analysis and playback later.
- **Secure your endpoints.** Traditionally, endpoint security is addressed in silos, which results in inconsistent security policies across the enterprise and vulnerabilities. A comprehensive PAM program implements least privilege and centralized policy for Unix/Linux, Windows desktops, macOS systems and AD/AAD networks.

Of course, a comprehensive answer to the problems of privileged access goes beyond a single solution; it involves a combination of enforceable policy and the right mix of broad enterprise solutions and specific technology solutions designed to satisfy compliance requirements and close the potential security holes created by the existence of multiple privileged access accounts.

The unlimited access that can be gained from privileged accounts usually receives little oversight and is too often protected by just a cobbled together, ad hoc, informal and frequently ignored set of administrative protocols.

Admins are busy, so convenience factors matter

Admins are overworked, which is why they tend to take shortcuts like writing privileged access passwords on paper and sharing them with one another. The idea of imposing a whole new protocol for privileged access will never get buy-in if it also imposes too many requirements that take extra time.

For instance, the largely manual and labor-intensive 'firecall ID' scenario can break down very quickly, and basic sudo doesn't work beyond just a few servers. It's too much extra work for a group of people whose task list is endless and don't have capacity to take on more work.

Instead, management of privileged accounts must be automated, role- based, easy to use, and centralized across all systems with policies uniformly applied.

Granular access: adopting the least-privilege model

Instead of the universal access granted by privileged accounts, organizations need to be able to provide access on an as-needed basis, based on each individual's specific role. This is the principle of least privilege: provide access to only what is needed, when it is needed. This is not available in the operating system, but must be implemented with added privileged account technology and supported by policy.

Implications for regulatory compliance

Compliance issues have impacted even the smallest businesses hard. Regulatory compliance requires businesses across all industries to implement a secure environment that safeguards personal information and proves compliance with auditable records.

Regardless of the particular piece of legislation with which a business needs to comply, privileged access is at the forefront of the compliance paradigm. Most compliance issues can be addressed, however, through separation of duties within the privileged access domain, along with access control and audit capabilities.

The sudo project

Native sudo

The open-source sudo project has gone a long way towards resolving privileged account challenges that many enterprises face. Sudo solves the immediate problem of admins accessing more than what they really need: it delegates authority and restricts access based on each person's role.

The free sudo project may be adequate in some circumstances. But for a larger enterprise with serious security requirements, it might not go far enough. The biggest limitation of sudo is that it is not possible to natively create a single policy and apply and manage it universally across all servers and networks.

Another limitation of sudo is that there is no audit trail and no visibility. Moreover, there is no centralized policy control, so management of the sudo environment is cumbersome and not standardized between servers. Sudo is widely used and a very common solution, but not a complete one for enterprise environments.

With One Identity solutions

A set of products that work together to solve your privileged access management challenges

One Identity's approach to privileged account and access management is a set of independent products, that work together to solve the vexing problems associated with privileged accounts.

Ease of use

One Identity solutions deliver the advantages of a common standards-based approach, without the heavy requirements and administrative burden required by an all-encompassing, 'big box' approach. With solutions from One Identity, companies use only what they need, keeping costs down and eliminating unnecessary layers of administration.

A credential vault enables centralized and policy-based release of privileged account credentials

One key function of One Identity's advanced approach to account management is a credential vault. One Identity Safeguard for Privileged Passwords allows for centralized and policy-based release of privileged account credentials, without limitations from platforms, servers or devices — it works across the board on everything. Safeguard for Privileged Passwords replaces the laborious, manual process of the 'firecall ID' with an appliance, making the process of password management automated, centralized and policy driven. Possession of the password can be set for a specific time or for a specific task, after which it is automatically revoked and changed.

Safeguard for Privileged Passwords is also designed to deal with the passwords that are typically hard-coded into applications. There may be dozens or hundreds of administrators who have, over time, learned those hard-coded passwords — an obvious security risk. One Identity eliminates the need for hard-coded passwords; instead applications and databases are configured to make runtime calls to Safeguard for Privileged Passwords. With this approach, nobody knows the application passwords, and the passwords can be changed rather than being locked into scripts, which is the real security and compliance concern.

Session management includes full keystroke logging and more

The ability to watch what people are doing is important to any system of checks and balances. One Identity Safeguard for Privileged Sessions supports full keystroke logging with search capability. In addition to recording keystrokes and specific commands, Safeguard for Privileged Sessions enables managers to watch over things as

they happen on the screen and play back recorded sessions like a movie after the fact.

One Identity Safeguard for Privileged Sessions provides an extra layer of accountability and visibility, including the ability to remotely kill a session or revoke access if needed. In addition, the chore of proving compliance or discovering the cause of trouble is bolstered by forensics-ready recording, full-text search and playback of privileged access sessions.

Analytics detects behavior anomalies with machine learning

With Safeguard for Privileged Analytics, organizations can know who their high-risk privileged users are, monitor questionable behaviors and uncover previously unknown threats from inside and outside of the organization. By using machine learning technology, Safeguard for Privileged Analytics detects anomalies and ranks them based on risk, so companies can prioritize and take appropriate action.

Attackers who steal user credentials **behave differently than real users**.

One Identity Safeguard for Privileged Analytics is able to detect the level of deviation from normal user activity. If the deviation is high, it sends an alert to the security team for further investigation. Suspicious activities can be confirmed by the user to detect identify theft, which dramatically speeds up forensic investigation and decreases false positives.

Extend control to Unix/ Linux environments

Beginning with version 1.8 (February 2011), sudo architecture allows anybody to write plug-ins and add functionality to sudo. One Identity is committed to improving the sudo platform, first by employing Todd Miller, the maintainer of sudo, to help keep the project alive and move it forward, and by offering a series of commercial enhancements. One Identity's commercial solution, Safeguard for Sudo picks up where sudo leaves off, providing more granular control over policy, enhanced monitoring and the ability to manage delegation across multiple servers.

In the past, one of sudo's limitations was that it had to be managed individually on every server on which sudo was installed, and there was no integration between servers. This led to a lot of redundancy and the need to rewrite identical policies for each server. Now, with Safeguard for Sudo, users can create policies from a single policy engine and push them out to everywhere they are needed.

One Identity also offers a keystroke-logging module for sudo, which adds an extra layer of visibility, accountability and auditability.

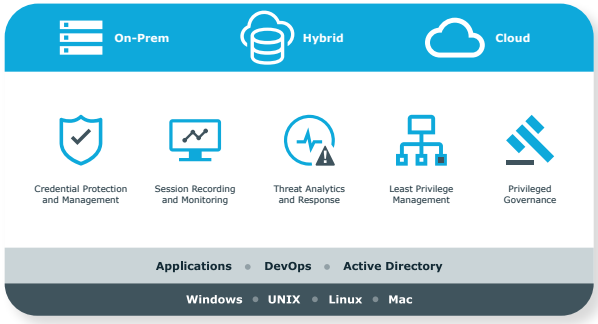

Figure 1. *One Identity security solutions include comprehensive offerings that address the privileged access management needs of even the most diverse and demanding enterprises.*

AD bridging unifies policy across systems

With Safeguard Authentication Services, organizations can extend Active Directory policies to Unix, Linux and macOS systems. The solution creates an AD bridge that enables users to log on to non-Windows systems using their AD credentials. It also extends Windows Group Policy to non-Windows systems, enabling unified policy management across operating systems.

ONE IDENTITY by Quest

Remote privileged access maximizes productivity

Safeguard Remote Access securely connects remote privileged users to critical resources without VPN. Using only a browser, privileged users can log in to any resource from anywhere in the world. There's no client software to install and all connection logistics are handled in the cloud and controlled by Safeguard.

Privileged account governance provides a complete view

One Identity provides a single platform for managing and governing all identity types. Identity governance and administration (IGA) and PAM technologies come together to ensure all users of privileged accounts gain and maintain the appropriate level of access. Users can request, provision and attest to privileged and regular user access. Organizations get a 360-degree view of all identities, and their associated user accounts, entitlements and activity. This perspective on identities complements a least privileged or zero trust initiative.

Appliance-based, host-based and agent-based options

A variety of delivery options are available to match every type of deployment need. Appliance-based solutions are extremely secure, easy to implement and easy to manage; just plug in the appliance and it is hacker proof. Host-based solutions are super secure, controllable and granular but slightly more expensive. Agent-based options deliver highly targeted, highly granular delegation for UNIX, Linux and Active Directory.

Conclusion

The problems that arise from uncontrolled access to privileged accounts can result in multi-million dollar losses. Fortunately, powerful, cost-effective solutions are readily available to protect your business.

One Identity's suite of privileged access management solutions give you the comprehensive accountability, granular access control, monitoring and analytics that are missing from native operating systems, delivering a framework of least privilege so that administrators have access to what they need, but only what they need at the time they need it.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (AD Mgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 500 million identities for more than 11,000 organizations worldwide. For more information, visit www.oneidentity.com.

ONE IDENTITY by Quest