Three Important Reasons for Privileged Access Management (and One Surprising Benefit)

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Centrify

June 2013

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Three Important Reasons for Privileged Access Management (and One Surprising Benefit)

Table of Contents

Three Important Reasons for Privileged Access Management (and One Surprising Benefit)

Executive Summary

High-privilege access is one of the most sensitive aspects of IT. Administrative accounts have the ability to make sweeping and fundamental changes to IT systems on which the business may depend. When used in ways not intended, the impact of this capability can cause a wide spectrum of damage, from security threats and compliance violations, to incidents that tarnish the reputation of the business itself.

For these reasons and more, privileged access visibility and control has been recommended – and often required:

- By a variety of regulatory mandates
- To assure responsible governance
- To improve security

Privilege management delivers these values – and more. In this report, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts examines the ways in which privilege visibility and control not only helps organizations achieve these objectives, but also delivers a benefit that many may not realize: improved IT reliability that can help reduce operational costs. The characteristics of an effective solution are examined, along with evidence from EMA research that supports the values of a more consistent approach to operational IT control.

High-Privilege Access: Advantages and Risks

When it comes to accessing and manipulating IT systems having high business value, privileged users such as administrators typically have the widest latitude of all. Often the most technically skilled users in an IT organization, they are typically responsible for deploying and managing functionality on which the business depends, from vital day-to-day functions to strategic capabilities that enable the business to maintain its competitive edge. They may also have considerable responsibility for line-of-business activities, such as ownership of business applications.

But there are risks to this power. The complexity of IT means that even minor changes can often have unintended consequences for availability, performance or resource integrity – even when made by highly competent staff. Malicious parties – inside the organization and beyond – can capitalize on administrative-level access to do more serious damage to the business than ordinary, less privileged user accounts. It is not uncommon for an attacker to exploit such privileges unbeknownst to capable, trustworthy personnel, given the increasing sophistication and stealth of modern attacks.

Privileged users such as administrators typically have the widest latitude of all, but there are risks to this power.

Privileged Access Management: Not Just a Good Idea…

For these reasons, organizations increasingly look to stronger controls on privileged IT access:

For Compliance

A number of regulatory measures either recommend or require controls specific to managing the risks of high-privilege IT access. Mandates such as the Sarbanes-Oxley Act ("SOX"), for example, require businesses to implement processes and controls to assure responsible governance. Considering the high importance of IT to managing and documenting business activity and performance, protecting business systems from the abuse of administrative privilege is one of the more tangible ways of assuring such control.

The Payment Card Industry Data Security Standard (PCI DSS) requires similar measures to protect cardholder data, particularly in separations of duties (Requirement 6) and in the monitoring and enforcement of control on high-privilege access (Requirement 7). In the utilities sector, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards mandate not only authentication, access control, access delegation and separations of duties, but effectively require as well the complete and continuous monitoring, archiving and auditing of access.

In government, guidance such as the U.S. National Institutes of Standards and Technology (NIST) Special Publication 800-53 is widely referenced and similarly addresses controls on sensitive IT access, separations of duties, and special care for administrative access. Government measures also affect industries such as healthcare. In the U.S., the Security Rule adopted to implement provisions of the Health Insurance Portability and Accountability Act (HIPAA) speaks to access control as a specific aspect of safeguarding electronic protected health information.

Why do these mandates speak so consistently to the need for privileged access monitoring and control?

To Assure Confidence in Business Practices

High-privilege accounts often control the most fundamental aspects of IT, from the deployment and configuration of foundations on bare metal to the nuances of applications and the end user experience. Without constraints, this capability can result in real damage – and not just to business-critical IT systems.

Regulations as diverse as the Sarbanes-Oxley Act and the PCI DSS, for example, emphasize separations of duties in assuring responsible control of business processes. Privilege management and monitoring in IT helps to assure that business systems cannot be manipulated to defraud a business or its customers or to misuse, steal or compromise assets through control over the systems that handle them.

High-privilege accounts often control the most fundamental aspects of IT. Without constraints, this capability can result in real damage – and not just to business-critical IT systems.

Separation of duties in administrative IT control helps to assure, for example, that business performance records cannot be compromised to hide irresponsible or illegal activity, or that systems that monitor and assure responsible business practices cannot be blinded or subverted. Because those having administrative IT privileges can create and modify such separations in the systems that handle business-critical transactions and data, the monitoring and control of administrative privilege thus helps assure that the definitions and enforcement of these separations remain intact and inviolate.

For Security

These values suggest the benefits to security that privilege management and visibility afford. Administrative privilege is rarely delegated to anyone not considered a trusted insider. But even highly skilled personnel on whom the business depends can become a threat when administrative privilege is abused. Examples include cases such as those of Roger Duronio, the UBS systems administrator convicted of planting a "logic bomb" that damaged a number of the financial giant's systems, or of Terry Childs, who kept control of San Francisco's FiberWAN network out of the city's hands by refusing to divulge administrative credentials.

A more widespread threat may be posed by external attackers who target administrative privilege as a tactical objective, since it can afford direct control over business systems that handle high-value assets or sensitive functionality. Taken together, the threat posed both from within and without points to the need for more effective security for administrative IT access. In Verizon's 2013 Data Breach Investigations Report (DBIR), 92% of breaches were perpetrated by outsiders. But when the entire body of more than 47,000 incidents (of which breaches are a subset) provided by this year's many contributors were considered, 69% of all security incidents in the 2013 Verizon report were attributable to internal actors.

For all these reasons – compliance, business assurance, and security – organizations have been motivated to deploy more granular visibility and control over administrative IT access, regardless of the nature of the system – Unix, Linux or Microsoft Windows hosts – for operating systems and application environments alike, in on-premises data centers as well as "in the cloud."

…but a Real Benefit to the Business

But there is one important reason businesses should consider privileged access management that many may not fully realize.

Improving IT Reliability, Reducing IT Costs

While 69% of all incidents in the 2013 Verizon DBIR dataset were attributable to internal actors, the report's authors comment on the role played in those incidents by insiders acting carelessly rather than maliciously. This suggests how the misuse of administrative privilege – intentional or not – contributes to increasing IT maintenance and support costs. Organizations should recognize the many other ways that poor control over administrative access increases the cost of IT operations, and how privileged access management can help reduce these costs:

Organizations should recognize the many other ways that poor control over administrative access increases the cost of IT operations, and how privileged access management can help reduce these costs.

- **Authorized personnel…but unauthorized change:** Many organizations adopt configuration and change control processes to minimize disruptions due to IT change. But a number of factors often contribute to administrative activity outside accepted change controls. Emergencies and urgent needs, personnel who are simply unaware of change constraints, simple mistakes or – perhaps more alarming – those exercising administrative access privileges which the business may not have known they had, are just a few such examples. Some of these, such as emergencies, may be entirely legitimate, while even the best personnel make errors. Others may be less so, when personnel (and not just technical IT staff) take matters into their own hands. Regardless, all these factors should cause organizations to re-think how they manage IT change. The sheer complexity of IT makes it difficult to anticipate every possible control scenario – but constraints on the administrative privilege required in almost any case can help organizations identify concerns, place granular controls on IT change when warranted, and maintain high visibility into administrative activities that support more accurate root cause analysis of IT problems.
- **Authorized personnel, authorized change…but unanticipated consequences:** This is perhaps an even more common scenario. Authorized administrators and technicians evaluate and deploy changes as expected – but the outcome of change has an unintended effect. Configuration changes and patch deployment are frequent examples. Changes may be tested, but the nuances of

production environments may vary from target to target. The scope of change targeting may not be aligned with intentions, resulting in changes made to systems unintentionally or outside the expected scope of change. Even when all is tested and anticipated well, some changes may not deploy as expected. Deployment may be incomplete, or a breakdown in a sequence of dependencies may occur. These are significant contributors to IT costs, when performance or availability takes a hit, or when changes must be backed out and re-evaluated. Privileged access control can help contain these through granular definition of access targets, limits on administrative activity, or containing the scope of privileged accounts and users authorized to perform administrative tasks. Granular visibility into privileged activity supports the ability to identify specific causes of problems in these cases as well.

EMA research supports these values. In one study of more than 200 enterprises worldwide,[1] approximately one-fourth of all respondents achieved all four "Plan – Do – Check – Act" (PDCA) IT change management milestones of:

- Defining change management objectives (Plan)
- Actually implementing those objectives in practice (Do)
- Monitoring adherence to those objectives and detecting deviations (Check), and
- Responding to deviations when warranted (Act)

When compared to all others in this study, these high performers had:

- Half the median incidence of security events requiring an unplanned response
- Fewer incidents of unsuccessful IT change requiring remediation
- Larger server-to-sysadmin ratios
- More IT projects completed on time, within budget, with expected features

Privileged access management can do more than help foster these values. Access control can *enforce* them as well. When access is granted, visibility into privileged access can identify when administrative actions are the root cause of IT performance, availability or resource integrity problems – particularly when change "goes south."

When a common method to manage and enforce policy for auditing, authorization, and authentication deployable for both on- and off-premises data centers can be employed, IT operational costs can be further reduced through more consistent control of administrative actions, with comprehensive visibility into those actions that speeds problem solving.

When a common method to manage and enforce policy for auditing, authorization, and authentication deployable for both on- and off-premises data centers can be employed, IT operational costs can be further reduced through more consistent control of administrative actions, with comprehensive visibility into those actions that speeds problem solving.

Characteristics of an Effective Solution

What should an effective solution to these problems entail? And how can privileged access management technologies help capitalize on the opportunity to reduce IT operational costs through improved IT reliability?

[1] IT Risk Management: Five Aspects of High Performers that Set Them Apart, EMA Advisory Note, July 2011

A comprehensive approach should:

- Enable organizations to define a number of flexible parameters for controlling administrative access, such as time windows, restriction to specific individuals or access targets, or limiting access to specific utilities or functions necessary for a task.
- Link role-based control of user access to critical systems, applications, and services with specific user identities. This supports the linkage of administrative accounts – which are often shared among a group of qualified professionals – to individual accountability, and improves the granularity of both visibility and control.
- Support efficiency through leveraging existing identity resources commonly used to define both individual users and administrative accounts. Microsoft Active Directory is one of the most widely adopted examples of such an identity resource. The ability to extend these resources across a variety of access targets to unify user identity across the heterogeneous enterprise is a distinct advantage.
- Provide a scalable, searchable, and comprehensive audit solution for user activity on critical systems, including the ability to replay both command-line and graphical user sessions ("video replay").
- Centralize privilege visibility and control through a "single pane of glass" for management, policy, and reporting across all servers and users. This increases efficiency (which further helps to reduce costs) and unifies a consistent approach to management throughout an environment.
- Integrate user activity auditing such as syslog and Windows Event Log data with other centralized monitoring and reporting technologies such as SIEM (Security Information and Event Management).

EMA Perspective

It is often said that "with great power comes great responsibility." High-privilege IT access is no exception. Administrative accounts have the power to have the greatest impact on business-critical IT. And this, in turn, can have a direct impact on the business itself – and perhaps on many others that may be affected, such as customers or stakeholders affected by incidents from IT service disruptions to the compromise of highly sensitive information.

Privileged access management constrains exposure to these risks, with granular controls on who, what, when and how individuals can exercise administrative rights. Privilege audit documents how that power has been exercised. When used responsibly, it details how IT interactions may have led to service issues. When used maliciously, privilege control helps to minimize risks, while privilege audit can document actions to help contain incidents and support fair and responsible enforcement.

The impact of high-privilege access to IT – even when used responsibly – cannot be overlooked. With modern approaches to privilege management and visibility, organizations can support more comprehensive compliance, help assure business integrity, and tackle security risks – while simultaneously realizing the cost benefits and other advantages of improved IT reliability.

The impact of high-privilege access to IT – even when used responsibly – cannot be overlooked. With modern approaches to privilege management and visibility, organizations can support more comprehensive compliance, help assure business integrity, and tackle security risks – while simultaneously realizing the cost benefits and other advantages of improved IT reliability.

About Centrify

Centrify provides Unified Identity Services across data center, cloud and mobile — resulting in one single login for users and one unified identity infrastructure for IT. Centrify's software and cloud services let organizations securely leverage their existing identity infrastructure to centrally manage authentication, access control, privilege management, policy enforcement and compliance across on-premise and cloud resources. More than 4,500 customers have deployed Centrify across millions of servers, applications and mobile devices to optimize costs and increase agility and security. Visit www.centrify.com to learn more.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
2685.061213