PRIVILEGED IDENTITIES - THREAT TO NETWORK AND DATA SECURITY

Dunja Pešić[1],
Mladen Veinović[2]

[1]OmnitechIT,
Belgrade, Serbia
[2]Singidunum University,
32 Danijelova Street, Belgrade, Serbia

Abstract:
Privileged accounts represent the biggest threat to enterprises. The number of cyber-attacks in which privileged accounts and insiders are involved directly or indirectly, has significantly increased in recent years. All-powerful access with the lack of accountability creates a risk which can certainly cause damage of immense proportions. The widespread use of virtual environments enhances the risk. The problem with the lack of accountability due to the use of shared accounts and passwords, little separation of duties and principle of "least privilege" not being followed is a massive occurrence in the use of virtual environments. Privileged identities are classified into groups of malicious insiders. They are involved in IP theft, espionage, fraud and IT sabotage.

Along with the argumentative idea of the technical approach towards the solution of the problem, other mentioned issues will be processed, because Insider threat is a people-centric issue. People are complex beings, hence the approach to a solution must be versatile.

Attention will be given to the positive practices of Identity based security, host based security, end-to-end security and compliance for cloud and virtual environments. Likewise, we will observe the negative practices and possible approaches to the problem of organizational factors contributing to insider attacks, with the aim to introduce environment where being an insider is not easy.

Key words:
IT security, insider threat, privileged access.

1. INTRODUCTION

Insider threats are becoming all too subtle, and the damage they can create is becoming greater. One of the major dangers of insider threats lies in the fact that they are usually the most difficult type to detect, due to their subtlety, or get detected after irreparable damage is done. Exercising an approach of remediation to this type of vulnerability is not effective because the theft of information or assets has already been done, making the approach of prevention and enablement the best possible choice.

Most organizations believe that the implementation of infrastructure security is enough to be protected of cyber-attacks, but the weakest link in the security of an organization is the user, for external or insider threats. When breaching a network perimeter, external attackers mainly seek to gain access to privileged accounts.

Insider threats can be classified into three groups: malicious insiders (which are the focus of this study), who deliberately steal information or

Correspondence:
Dunja Pešić

e-mail:
dunja.pesic@omnitechweb.it

DOI: 10.15308/Sinteza-2016-154-160

cause damage; insiders who are unwittingly exploited by external parties and insiders who are careless and make unintended mistakes. Whichever the case from the foregoing, negative practice of social engineering is part of the issue. Better part of mitigation strategies is user awareness training. It can be argued that this necessary step is the ideal theoretical solution in general, but hardly widely feasible in practice. Mainly, because even if an organization funds training for employees, there is no guarantee that they will be highly motivated to embrace and implement knowledge of data protection. The risk of all three types can be reduced by ensuring accountability and implementing least privilege access.

For this reason, the subject of research in this study is privileged identity and access management solution, because it protects against both external and insider threats. During the research, an overview was performed of the best commercial solution.

The paper is intended for all those who care about the security of their data and applies equally to private and business users.

The scientific objective of this paper is to analyze the solution that offers:

- enablement of compliance for privileged identity access and virtualization security,
- greater control over superuser actions through fine-grained controls,
- support to both physical and virtual environments,
- reduction in costs and improved efficiency through virtualization - aware and automated security controls,
- proven scalability in some of the largest and most complex IT environments in the world.

2. OVERVIEW IN THE FIELD OF RESEARCH

The research in the field of threat to network and data security from privileged identities selected the best solutions on the market: Privileged Identity and Access Management by CA Technologies. From this point forward, the challenges of defending against insider threats and the problem with privileged identities will be presented. Privileged Identity Management lies at the core of any program to reduce insider threats [1]. Privileged Identities can be classified into two groups:

- High risk profile by position in the hierarchy of the organization *e.g.* CEO, CIO, CISO, CFO, etc. It is unlikely to refer this group as potential malicious insiders. Assuming that by harming the organization, they are directly harming themselves, their main goal is the success of the company. They can be defined as privileged users who may be targeted and exploited by malicious attackers, due to their lack of awareness, vulnerable lifestyle and circumstances. Perhaps the rule that there should be no exceptions to the principle of least privilege applies to this subgroup of super users chiefly. Almost without exception, they have access to sensitive data of the organization.
- High risk profile by employment in the IT department of the organization *e.g.* administrators of various parts of the system and network. Some of the individual factors that should be considered in this subgroup are personality traits and workplace behaviour, which are exceptionally important but are not the key problem in IT departments. The greatest risk is when users with unrestricted, all-powerful access are not made accountable. This is usually because privileged accounts are typically being shared by several people. Virtualization magnifies these issues. In addition virtual environment is dynamic in nature, therefore it is difficult to control access to virtual machines. This subgroup of super users can be labelled as paradoxical. Their purpose is to maintain the network and system and to protect the organization from threats that could breach IT security, but evidently there lies the weakest link for possible insider threats. In the environment where all-powerful accounts are shared, one malicious person is enough to make irreparable damage. It would be superficial to incriminate IT department as the source of the problem. The situation there is the result from the organization ratio towards IT department, such as corporate governance, lack of awareness or communication between business areas.

Classification of insider threats as primarily a technical problem or as mostly hacker activity is a common misconception. This is a large part of the security breaches issue. Awareness is necessary, technology has become a dominant instrument in every aspect of everyone's everyday life, which is why the awareness of possible risks and exploitations should not be observed as knowledge principally reserved for IT professionals, but rather, it should become a matter of general education of individuals.

Organizations that belong to the private or state sector need to demonstrate maturity, considering that if security breaches do occur, their members, managers or responsible people and the organization itself are not the only victims: customers and clients suffer financially, emotionally, mentally due to oversight of possible threat. And even if the attack is remediate, the trust of clients will be difficult or impossible to restore. Consequently, prevention and enablement is the best solution.

Before securing privileged identities, an organization needs to understand the types of accounts that exist, as well as their unique purposes and requirements. Classification is shown in the table below. [7]

Privileged Account Type	Description	Used By	Security Focus
Default Local Administrative Accounts (*e.g.*, root, administrator	"All powerful" accounts used to manage the system or device by administrators	Multiple types of administrators, often shared	Ensure accountability by individuals.
Named Administrator Accounts	Accounts for individuals that have administrative privileges	Named individual administrators	Ensure least privilege access.
Service Accounts	Accounts used by operating system services and applications that require privileged access, often used by web servers, e-mail servers, databases, *etc.*	System services and applications	Ensure unused accounts are removed or disabled and that passwords are changed regularly.
Domain Administrator Accounts	Accounts used to administer a domain instead of a local system	Domain administrators	Apply extra controls and monitoring.
Emergency Accounts	Accounts used only in the event of an emergency that requires temporary privileged access	Backup administrators	Ensure all emergency use is authorized and monitor all use.
Application Administrator Accounts	Application accounts with elevated privileges that are used to administer an application	Application administrators	Apply risk-appropriate controls, dependent on the nature of the application.
Hypervisor Administrator Accounts	Accounts used to administer virtual environments, such as VMware	Virtualization administrators	Applying best-practice controls to this class of administrator

Table I.

3. OVERVIEW OF THE PROPOSED SOLUTION

CA Technologies has been a leader in the field of Identity-centric Security for several years.Awards and recognitions are persuasive confirmation. As well Forrester Wave Report Names CA Technologies as the only leader in Privileged Identity Management [4].

From this point forward, the authors shall present their solution for Privileged Identity and Access Management.

CA Privileged Identity Manager is a comprehensive and mature solution for privileged identity management in both physical and virtual environments. CA Privileged Identity Manager is a highly scalable solution that provides privileged access and account management, including: shared account password management, fine-grained access controls, user activity reporting and UNIX Authentication Bridging across servers, applications and devices from central management console. CA Privileged Identity Manager for Virtual Environments brings privileged identity management and security automation to virtual environments from infrastructures to virtual machines. CA Privileged Identity Manager is the only privileged identity management solution that enforces access controls at the OS kernel level. Because of this, it is uniquely suited to protect your most critical systems and most sensitive data. [5]

Figure 1 shows how Privileged Access Management (PAM) helps to address five primary challenges [2] in the Organization, while Figure 2 displays the five essential capabilities of Privileged Identity Management (PIM) Solutions [3].

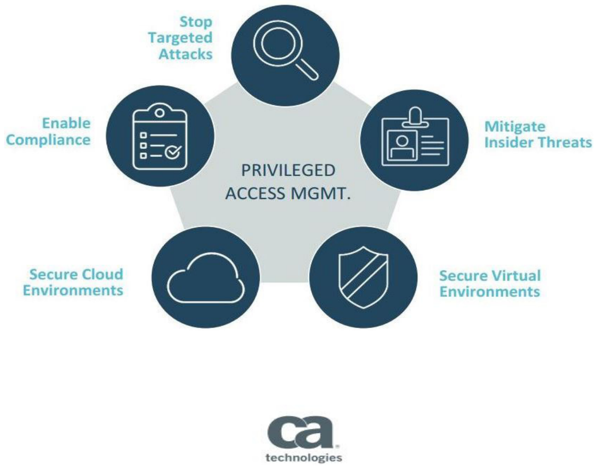


Figure 1. Five primary challenges

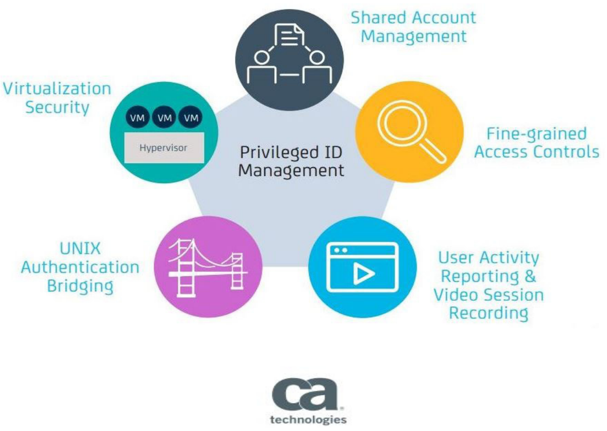

Shared Account Management
Virtualization Security
VM
VM
VM
Hypervisor
Privileged ID Management
Fine-grained Access Controls
UNIX Authentication Bridging
User Activity Reporting & Video Session Recording
ca technologies

Figure 2. The Five essential capabilities of PIM

PIM Capability 1: Shared Account Management

Shared account password management controls access to privileged accounts. It stores passwords in a central location and helps provide accountability for user actions through secure auditing. Shared passwords must be stored, changed and distributed in a timely and secure manner in order to comply with corporate security policies. Additionally, many applications also use hard-coded passwords in shell scripts and batch files. These passwords are static and can be stolen by anyone who gains access to the script file, including malicious intruders. [5]

A solution should be able to make access to shared accounts simple, without compromising security. Features such as those preventing the user from seeing the password during an automatic login are essential. [5]

Shared Account Management helps organizations control access to privileged, administrative accounts (including "break glass" functionality) with password storage and automatic login capabilities (Figure 3). This is the starting point for most privileged identity management solutions. [3]

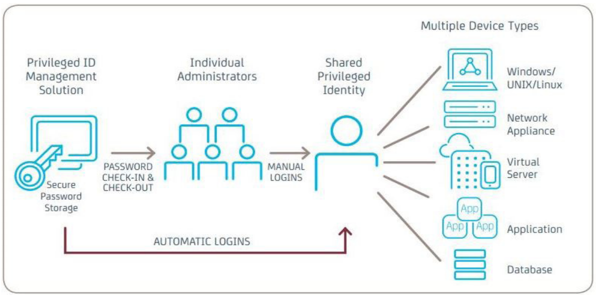


Figure 3. Shared Account Management

"Benefits include:

- A reduction in the risk of unauthorized users gaining access to privileged accounts
- Improved accountability via prevention of password sharing." [3]

PIM Capability 2: Fine-grained Access Controls

The use of shared accounts (such as "root" and "Administrator") 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. These capabilities are required to help ensure that administrators have only the privileges they need to do their job and nothing beyond that. [5]

Fine-grained access controls allow enterprises to control what access users have based on their individual identities, even when they're using a shared administrative account (Figure 4). [3]

"Benefits include:

- Reduced risk by providing administrators with only the minimum privileges they need to do their jobs."[3]

This capability essentially enables two or more users to be logged into the same administrative account, but have different access rights based on their original user ID and role. [3]

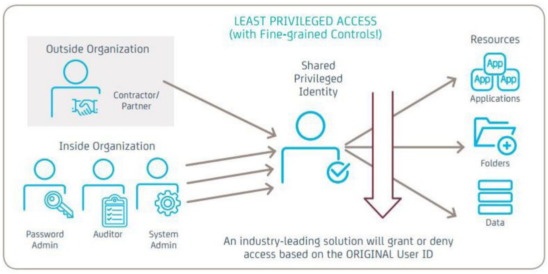
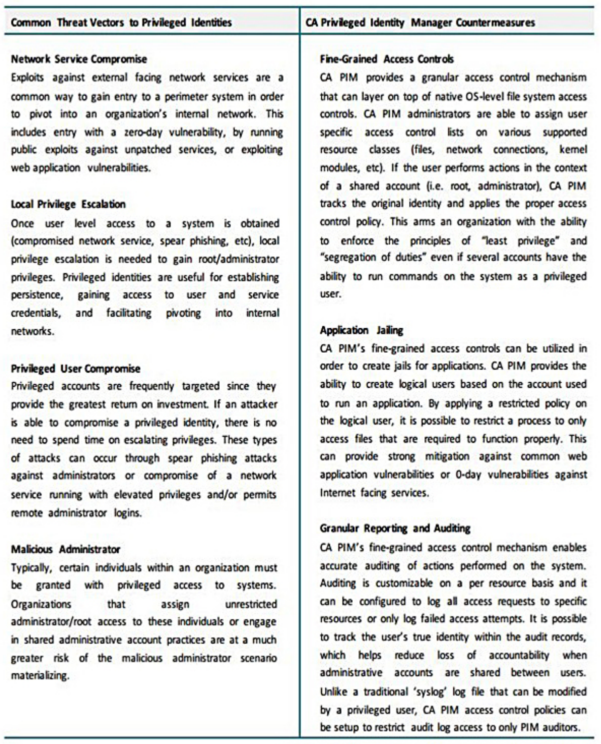

LEAST PRIVILEGED ACCESS (with Fine-grained Controls!)
Outside Organization
Contractor/ Partner
Inside Organization
Password Admin
Auditor
System Admin
Shared Privileged Identity
Resources
App
App
App
Applications
Folders
Data
An industry-leading solution will grant or deny access based on the ORIGINAL User ID

Figure 4. Fine-grained Access Controls

Figure 5 provides a summary of the common threats that affect privileged identities and relevant CA PIM countermeasures within the scope of the research project conducted by GDS Labs Security Research. [6]



Common Threat Vectors to Privileged Identities	CA Privileged Identity Manager Countermeasures
Network Service Compromise Exploits against external facing network services are a common way to gain entry to a perimeter system in order to pivot into an organization's internal network. This includes entry with a zero-day vulnerability, by running public exploits against unpatched services, or exploiting web application vulnerabilities. **Local Privilege Escalation** Once user level access to a system is obtained (compromised network service, spear phishing, etc), local privilege escalation is needed to gain root/administrator privileges. Privileged identities are useful for establishing persistence, gaining access to user and service credentials, and facilitating pivoting into internal networks. **Privileged User Compromise** Privileged accounts are frequently targeted since they provide the greatest return on investment. If an attacker is able to compromise a privileged identity, there is no need to spend time on escalating privileges. These types of attacks can occur through spear phishing attacks against administrators or compromise of a network service running with elevated privileges and/or permits remote administrator logins. **Malicious Administrator** Typically, certain individuals within an organization must be granted with privileged access to systems. Organizations that assign unrestricted administrator/root access to these individuals or engage in shared administrative account practices are at a much greater risk of the malicious administrator scenario materializing.	**Fine-Grained Access Controls** CA PIM provides a granular access control mechanism that can layer on top of native OS-level file system access controls. CA PIM administrators are able to assign user specific access control lists on various supported resource classes (files, network connections, kernel modules, etc). If the user performs actions in the context of a shared account (i.e. root, administrator), CA PIM tracks the original identity and applies the proper access control policy. This arms an organization with the ability to enforce the principles of "least privilege" and "segregation of duties" even if several accounts have the ability to run commands on the system as a privileged user. **Application Jailing** CA PIM's fine-grained access controls can be utilized in order to create jails for applications. CA PIM provides the ability to create logical users based on the account used to run an application. By applying a restricted policy on the logical user, it is possible to restrict a process to only access files that are required to function properly. This can provide strong mitigation against common web application vulnerabilities or 0-day vulnerabilities against Internet facing services. **Granular Reporting and Auditing** CA PIM's fine-grained access control mechanism enables accurate auditing of actions performed on the system. Auditing is customizable on a per resource basis and it can be configured to log all access requests to specific resources or only log failed access attempts. It is possible to track the user's true identity within the audit records, which helps reduce loss of accountability when administrative accounts are shared between users. Unlike a traditional 'syslog' log file that can be modified by a privileged user, CA PIM access control policies can be setup to restrict audit log access to only PIM auditors.

Figure 5. Common threats and CA PIM countermeasures

Example of Privileged User Compromise and Application Jailing is shown in Figure 6.

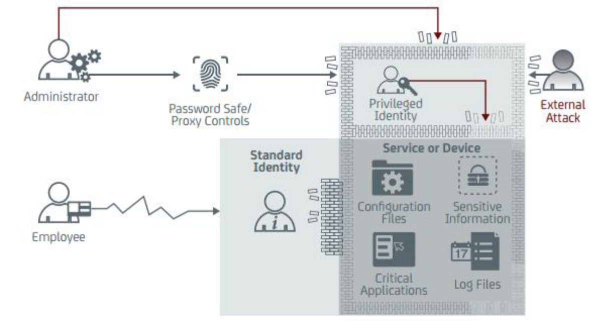


Figure 6. Application Jailing [5]

PIM Capability 3: User Activity Reporting & Video Session Recording

Video session recording can provide a deeper understanding of what actually happens on corporate servers and desktops. Video replay provides clear-cut evidence of precise user actions. Unlike system logs, video records can show exactly which applications were run and what files or URLs were accessed. This can eliminate blind spots that currently exist for applications that do not produce their own logs, including many of the most common desktop and cloud-based applications. Video logs supported by deep analytical capabilities can be essential in forensic investigation. [1]

Session recording for proxy activities enables Security Administrators to be able to record privileged sessions accessed through the proxy server. The solution records all screen movement in full resolution and Super-Administrators can then search and playback the sessions with DVR-like playback controls. Recordings are stored in an encrypted fashion and made available as soon as the privileged session ends. Advanced policies allow you to specify the endpoints that can be recorded. [9]

User activity reporting records all user actions-tracking by individual, even when a shared account is used. Ideally, this capability should trace an IT system in a video-like format, ensuring that all users can be held accountable for their actions (Figure 7). [3]

"Benefits include:

- A simplified way to determine "who did what" in a forensic investigation, via an easy visual record instead of the need to search through incomprehensible log files [3]
- Enabled accountability for users of IT systems [3]
- Authorized logs for applications that do not natively produce logs."[3]

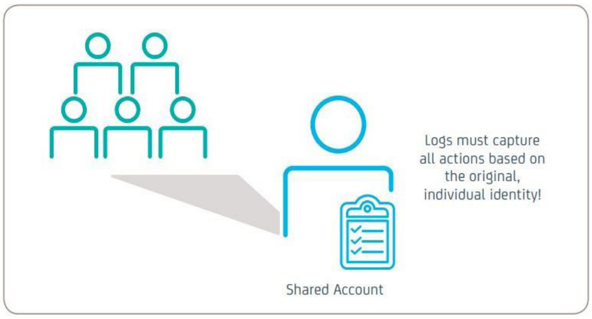


Figure 7. User Acitivity Reporting & Video Session Recording

PIM Capability 4: UNIX Authentication Bridging

„UNIX authentication bridging authenticates users on UNIX and Linux systems to the Microsoft Active Directory, thus providing a single place to determine access instead of a set of distributed password files."[3]

"Benefits include:

- Consolidated authentication and account information in Active Directory, as opposed to the need to manage UNIX credentials locally on each system
- Decreased administrative overhead."[3]

PIM Capability 5: Virtualization Security

In this diverse environment, it's important to enforce a consistent policy and enable consolidated logging across servers. An explosion in the number of servers and devices being managed has compounded these issues. Virtual machine sprawl means that there are many more servers to manage, and since it's irrelevant to hypervisors which operating system is a guest, this exacerbates the heterogeneity problem. Yet, maintaining the security of this expanded, virtualized data center is largely overlooked. Virtualization also creates a new class of hypervisor privileged users that can create, copy, move or otherwise manage these guest operating systems, further stressing the need for adequate separation of duties to prevent the data and applications running in these guests from compromising in addition to audit capabilities. [8]

Virtualization security requires a Privileged Identity Management solution that controls privileged users on the hypervisor, while providing virtualization-aware automation of security controls on virtual machines. It also tracks and audits access to the host operating system and supports auditability across all virtual machines to ensure compliance. [3]

"Benefits include:

- Improved compliance,
- Reduced risks of virtualization, including hypervisor administrators."[3]

CA Privileged Access Manager for VMware NSX

It is important to mention an addition (CA Privileged Access Manager for VMware NSX), which is a great boost to virtual environments security.

CA Privileged Access Manager for VMware NSX (Fig.8.) enhances VMware NSX's native security capabilities and adds fine-grained access control. Automatically discovers and protects ESX/ESXi hosts and guest systems. Automatically establishes and enforces policies across dynamic virtual resources by adding policy protections and access permissions in real-time, as virtual instances are created. Automatically define highly restrictive, micro-segmented, secure network access to NSX-based resources. Using synchronized security settings that are core of NSX Security Groups, automatically providing with short-term administrative access to select systems - or deny access and terminate sessions in response to security incidents. Monitor, react and record everything, including NSX REST APIs interactions. Delivers full audit and response logs of all user events, including interactions with the powerful NSX Manager APIs. Captures continuous, tamper-evident logging and recording of administrative sessions. Generates alerts, warnings or even terminate sessions. Analyses logs using VMware vRealize Log Insight or other log managers. Manages privileged user credentials and simplify with single sign-on. Stores credentials in an encrypted credential safe. Gain faster access and productivity improvements with single sign-on. [10]

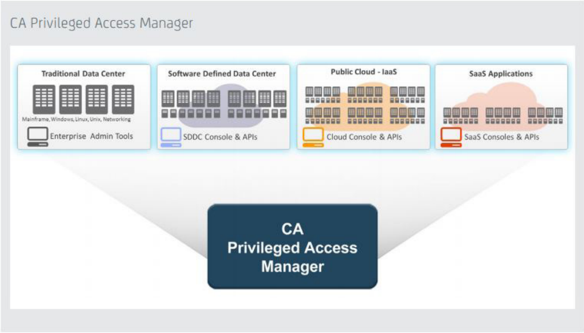


Figure 8. CA PAM for VMware NSX

Compliance challenge of PIM

Regulations and industry standards often require strict controls over privileged identities. Organizations must have correct policies in place, have those policies successfully deployed but also provide proof of being compliant with both corporate policies and regulatory standards, while accounting for any deviations from the policy. Privileged identities are a unique compliance challenge, as requirements for "least privilege access" and "segregation of duties" often conflict with traditional approaches of administrators having unrestricted access to systems and data. Shared accounts also present a compliance challenge, as all user activities must be tracked to individuals. When multiple administrators can log into a single account simultaneously, powerful tools are needed to track "who did what" at the individual level. [5]

4. CONCLUSION

This study mainly presents the challenges of defending against insider threats and the problem with privileged identities. Risks from insider threats by privileged identities were analyzed, and the best available commercial solutions were presented.

CA Privileged Identity Manager is a comprehensive and highly scalable solution for privileged identity management in both physical and virtual environments. It provides a proactive approach to securing sensitive information and critical systems without impacting normal business and IT activities. CA Privileged Identity Manager helps mitigate risk and facilitate compliance by controlling how privileged users access and use enterprise systems and data across the IT environment in order to achieve a higher level of security, reduce administrative costs and allow for easier audit/ compliance processes. [7]

CA Privileged Identity Manager is the only solution to implement access controls at the OS kernel level that is significantly harder to bypass than competing "sudo" and proxy-based solutions. It has a highly scalable architecture that has been tested to run on over 100,000 endpoints. [7]

It is important that the business environment can operate efficiently and to be protected from threats concurrently. This is a transparent solution to a very complex issue.

REFERENCES

[1] Russell Miller, Security Management / CA Technologies - Beyond Passwords: A Fine-Grained Approach to Privileged Identity Management, January 2013

[2] Mike Dullea Product Management / CA Technologies - CA Privileged Access Management Product Roadmap, March 9, 2016

[3] CA Technologies - Defending against Insider Threats in the "Snowden Era", http://www.ca.com/

[4] Forester Research Inc; https://www.forrester.com

[5] CA Technologies - Privileged Identity Management Buyer's Guide, http://www.ca.com/

[6] Gotham Digital Science (GDS) - CA Privileged Identity Manager (PIM) GDS Labs Security Research Whitepaper

[7] CA Technologies – Best Practise for Securing Privileged Identities, http://www.ca.com/

[8] CA Technologies – Privileged Identity Manager with CA Contol Minder, http://www.ca.com/

[9] CA Technologies – Why Upgrade to CA Privileged Identity Manager 12.9? Capabilities and Benefits, http://www.ca.com/

[10] CA Technologies - CA Privileged Access Manager for VMware NSX, http://www.ca.com/