Defending Against Insider Threats in the “Snowden Era”

Get started

Understanding Insider Threats and Their Stakes

From Bradley Manning to Edward Snowden, insider threats are becoming all too commonplace and damaging.

The three major types of insider risks involve threats from:

- **Malicious insiders**, who deliberately steal information or cause damage.
- **Exploited insiders**, who may be "tricked" by external parties into providing data or passwords they shouldn't.
- **Careless insiders**, who may simply press the wrong key, accidentally delete or modify critical information or lose devices with sensitive information.

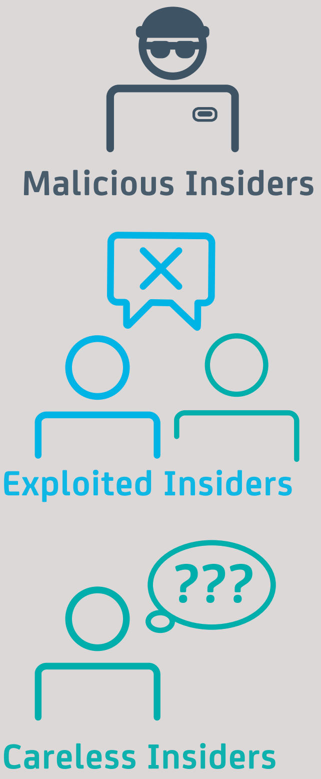
Most potential to cause significant harm

Why should organizations take insider threats seriously? Because the stakes have never been higher, especially given the value enterprises place on intellectual capital and trade secrets.

With the rise of Big Data analytics, businesses now store vast quantities of information to uncover important patterns and gain actionable insights. And in many cases, this data contains highly sensitive information—such as customers' personal data, credit card numbers and transactions, private communications and even locations.

The cost of security breaches averages $5.4 million per year.[1] Other consequences include broken privacy laws, class-action lawsuits and reputational damage that can lead to substantial loss—including business closures. And since employees and other insiders have the easiest access to this data—and often little accountability—they perhaps pose the most risk to cyber-security.

> "The U.S. economy has changed over the past 20 years. Intellectual capital, rather than physical assets, now represent the bulk of a U.S. corporation's value. This shift has made corporate assets far more susceptible to espionage."[2]
>
> — Protecting Key Assets:
> *A Corporate Counterintelligence Guide*, The Office of the National Counterintelligence Executive (ONCIX), 2013.



[1] Ponemon Institute, 2013 Cost of Data Breach Study.
[2] Ocean Tomo Intellectual Capital Equity, Courtesy Office of the National Counterintelligence Executive.

The Real and Substantial Threat of Insider Attacks

Using such tools as email, collaboration software, cloud services, FTP, USB drives and mobile devices, malicious insiders can attempt the following:

- **IP theft** – Stealing intellectual property from the organization
- **Espionage** – Uncovering classified information, trade secrets and intellectual property to gain national, strategic or competitive advantage
- **Fraud** – Using unauthorized modification, addition or deletion of an organization's data for personal gain
- **IT sabotage** – Leveraging IT to direct specific harm at an organization or an individual

What makes insider threats particularly dangerous is that they are usually the most difficult to detect. The 2013 *Verizon Data Breach Investigations Report* found that 62 percent of insider security breaches took months (or even years) to be discovered.[3]

And to make matters worse, once the problem has been identified, the data has often landed in the worst possible place. About 65 percent of employees who committed insider IP theft had already accepted positions with a competing company or started their own company at the time of the theft. About 20 percent were recruited by an outsider who targeted the data. And, more than half steal data within a month of leaving.[4]

[3] Verizon, Verizon Data Breach Investigations Report, 2013.

[4] Behavioral Risk Indicators of Malicious Insider IP Theft: Misreading the Writing on the Wall, Eric D. Shaw, Ph.D., Harley V. Stock, Ph.D.

Knowledge is the First Line of Defense – Test Your Misconceptions About Insider Threats

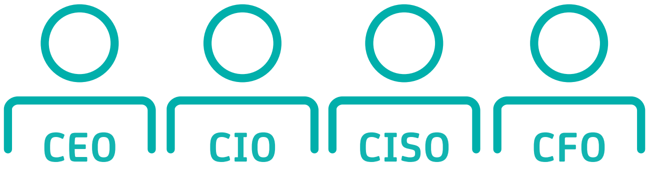
The first step to managing insider threats effectively is to understand the reality of the threat environment and the best ways to defend against it.

Test your knowledge with this quick quiz

Quiz

How can you identify high-risk individuals within your organization? Review this chart and **find out**.

There should be no exceptions to the principle of least privilege access.



Understanding Insider Threats
Real and Substantial Threats
Test Your Misconceptions
Defending Against Insider Threats
Striking the Right Balance
The Problem with Privileged Identities
Capabilities of PIM Solutions
Mitigate Insider Risks
What to Look for
About the Solutions from CA Technologies

The Challenges of Defending Against Insider Threats

Understanding the insider threat landscape is the first step to decreasing risks. But reducing insider security breaches can be easier said than done. Organizations commonly face the following challenges:

Difficulty managing trust

- Insider resistance to new security controls

Ineffective management of privileged users

- Privileged users with total access to key systems, applications and information
- Widespread sharing of administrator passwords
- Inability to identify specifically who performed which action on what system

Poor overall identity governance

- Inadequate controls over user identities, access and information use

Inadequate information classification and policy enforcement

- Lack of knowledge as to the location of sensitive information
- Poorly defined and communicated policies for confidential data handling
- Ineffective controls to detect and prevent inappropriate transmittal or disclosure of private information

Reactive response

- Lack of analytic and predictive capabilities to help prevent insider attacks, or at the very least, identify “at-risk” insiders

Insufficient auditing and analytics

- No way to continuously audit access
- An overwhelming volume of log data generated, making auditing time-consuming and complex

No comprehensive, written acceptable-use policies

- Lack of detailed acceptable use policies for all employees

Trust and Security – Striking the Right Balance

"Trust" does not mean giving employees unrestricted and unnecessary access to information. The key is to find the right balance between employee enablement and control by:

- Deterring security breaches by enforcing accountability — To make malicious insiders think twice before acting
- Implementing least-privilege access — To deny actions and limit the damage done by all types of insider attacks (including inadvertent, but crippling, actions)
- Controlling sensitive data — To prevent security breaches using tools as simple as USB drives or email

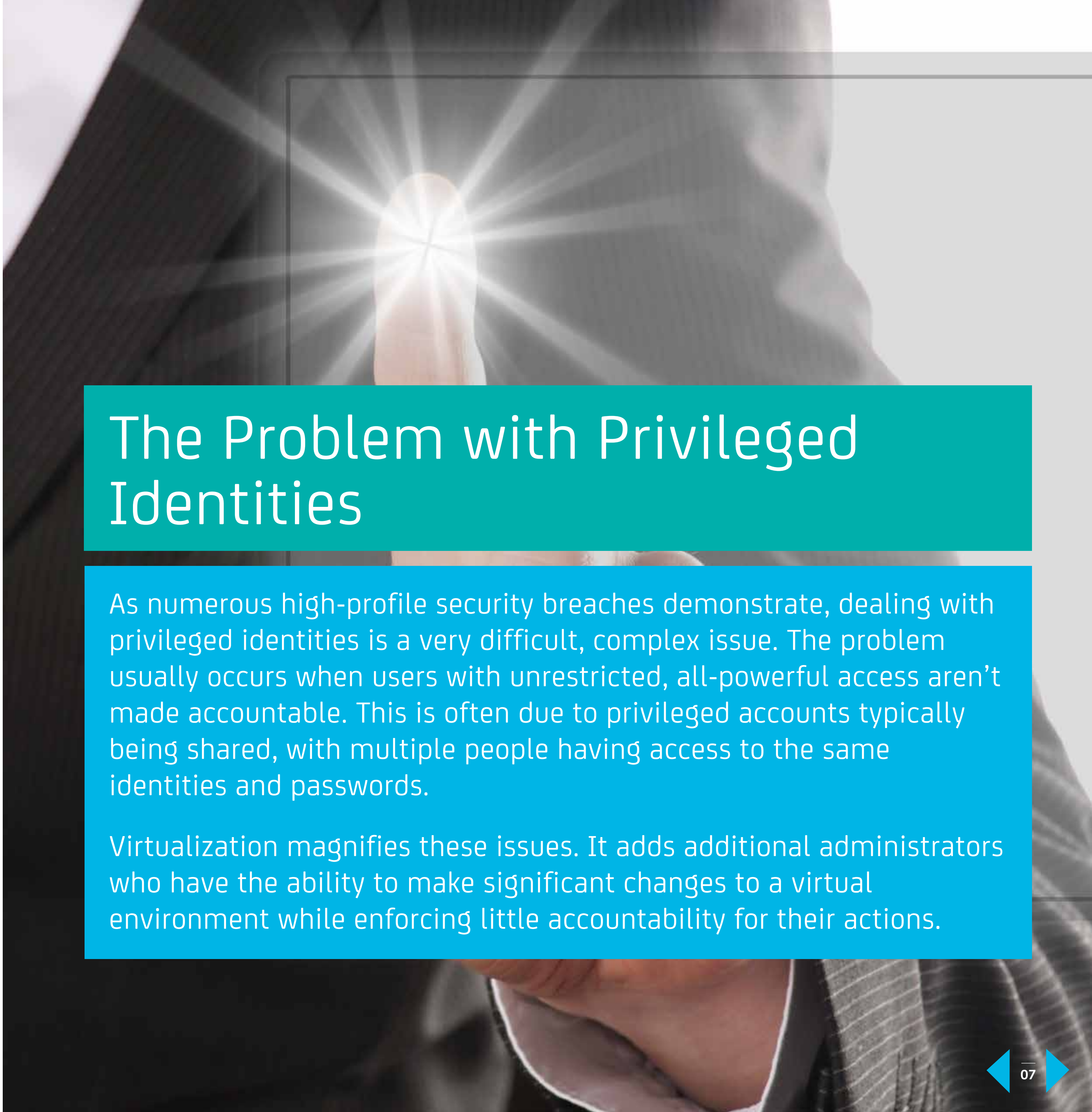
These actions can help companies reduce insider threats and improve compliance. And, they can be implemented via:

- Data Protection Solutions
- Privileged Identity Management Solutions

Let's take a closer look at these options.

Quiz

Test your data loss and theft exposure - **take the quiz**



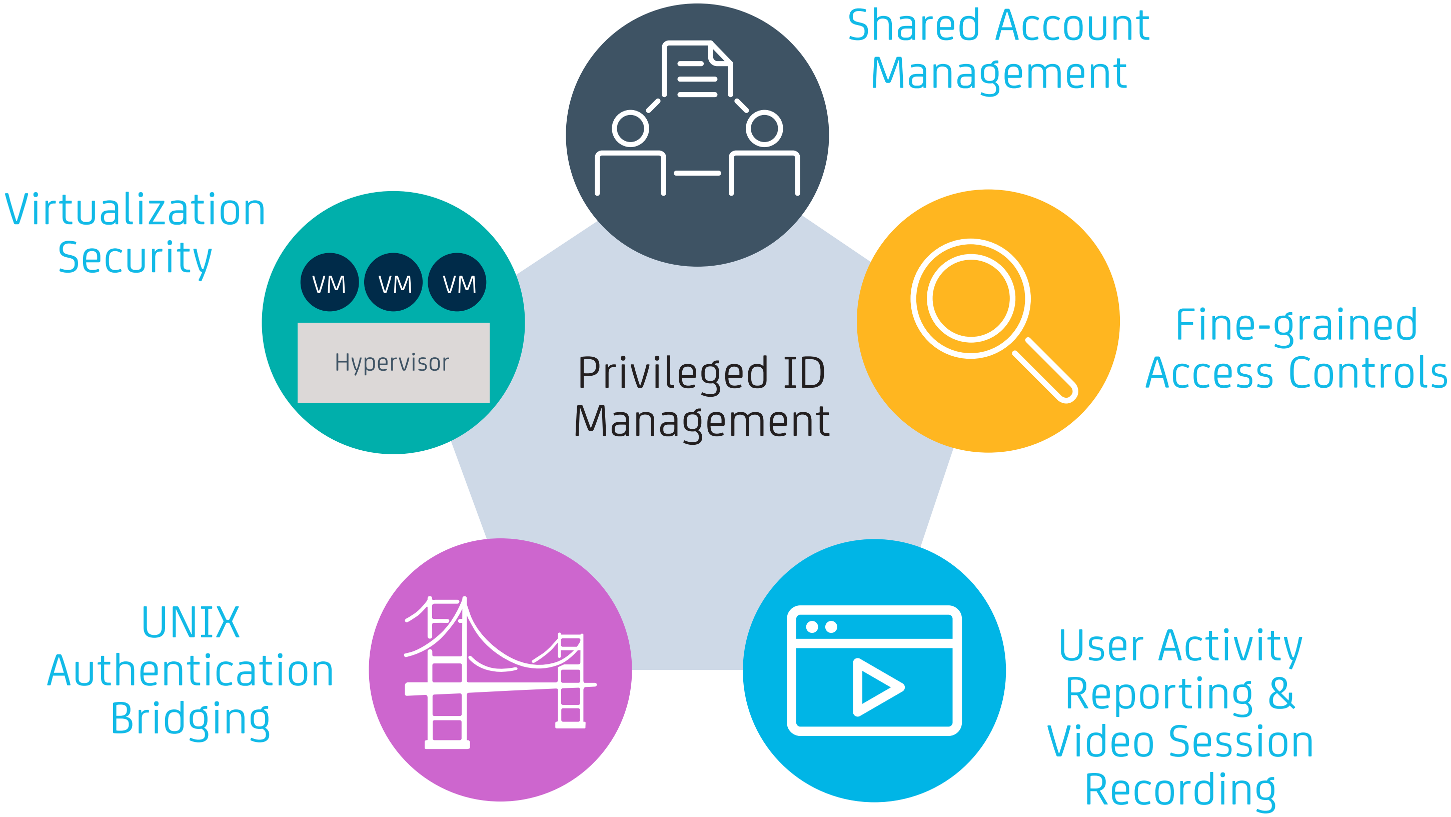
The Problem with Privileged Identities

As numerous high-profile security breaches demonstrate, dealing with privileged identities is a very difficult, complex issue. The problem usually occurs when users with unrestricted, all-powerful access aren't made accountable. This is often due to privileged accounts typically being shared, with multiple people having access to the same identities and passwords.

Virtualization magnifies these issues. It adds additional administrators who have the ability to make significant changes to a virtual environment while enforcing little accountability for their actions.

The Five Essential Capabilities of Privileged Identity Management (PIM) Solutions

An industry-leading privileged identity management solution should be comprehensive and include:


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

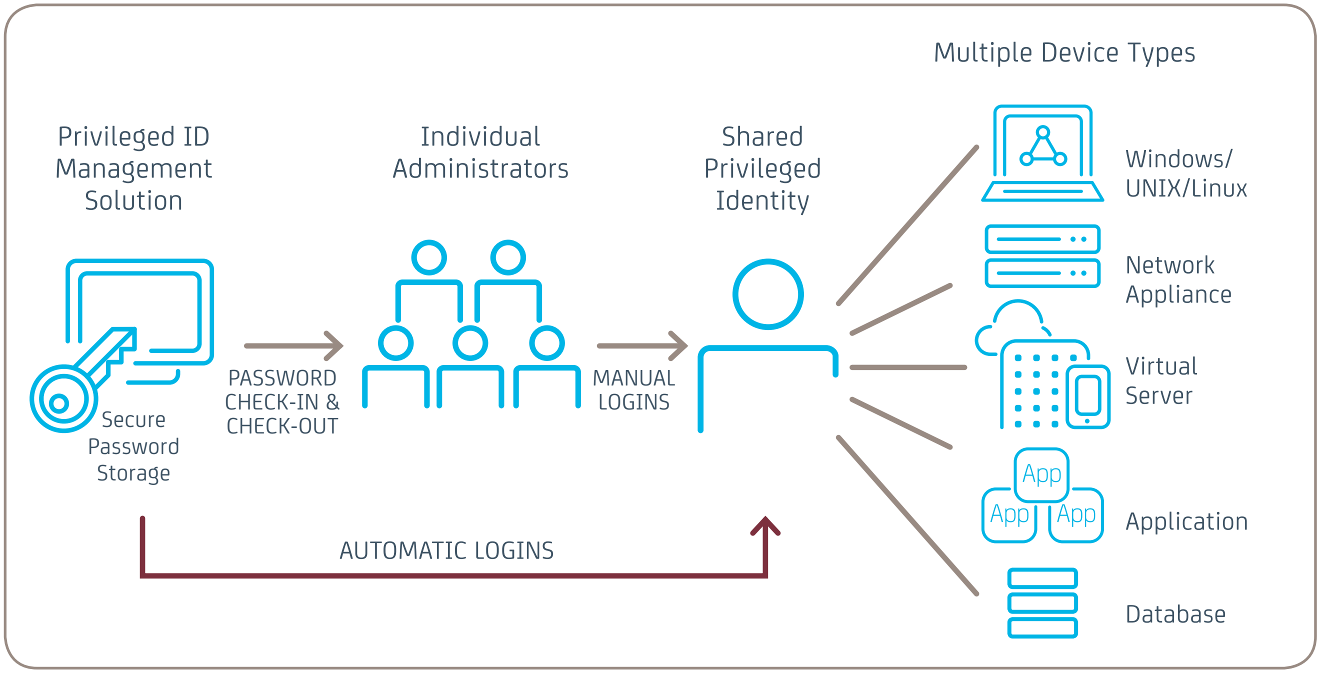
PIM Capability 1:
Shared Account Management

Shared Account Management helps organizations control access to privileged, administrative accounts (including "break glass" functionality) with password storage and automatic login capabilities.

This is the starting point for most privileged identity management solutions.

Benefits include:

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



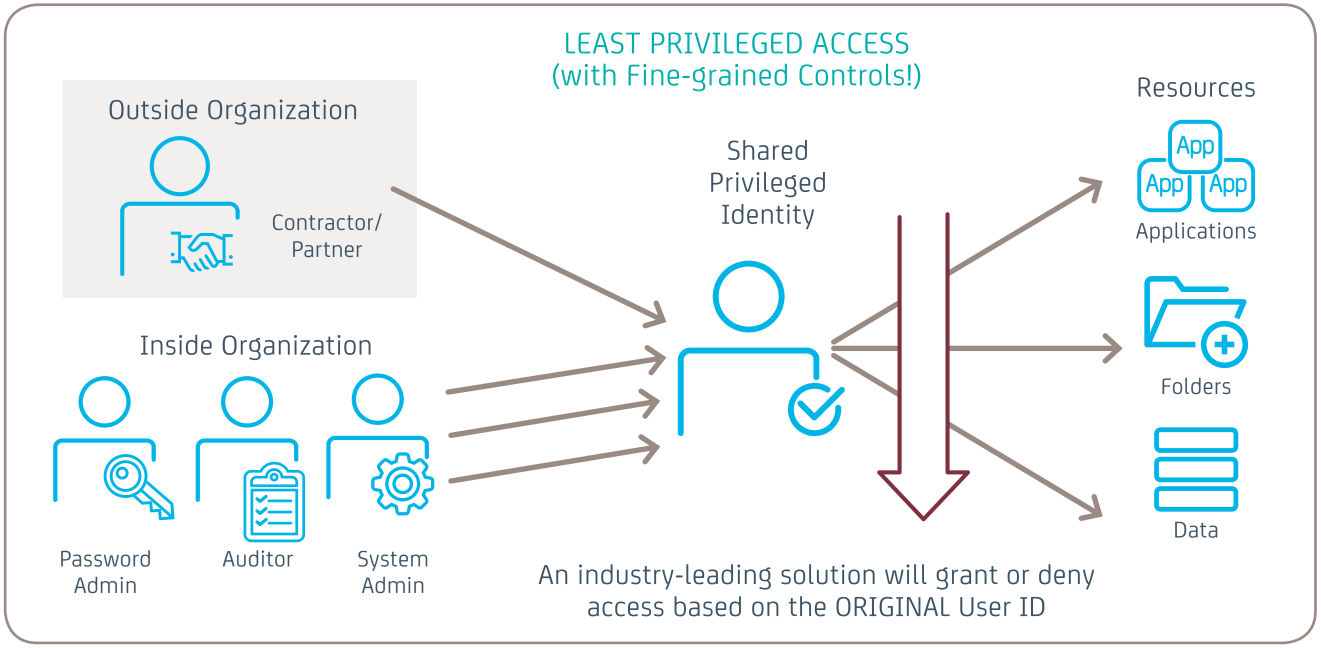
PIM Capability 2: Fine-grained Access Controls

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.

Benefits include:

- Reduced risk by providing administrators with only the minimum privileges they need to do their jobs

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.

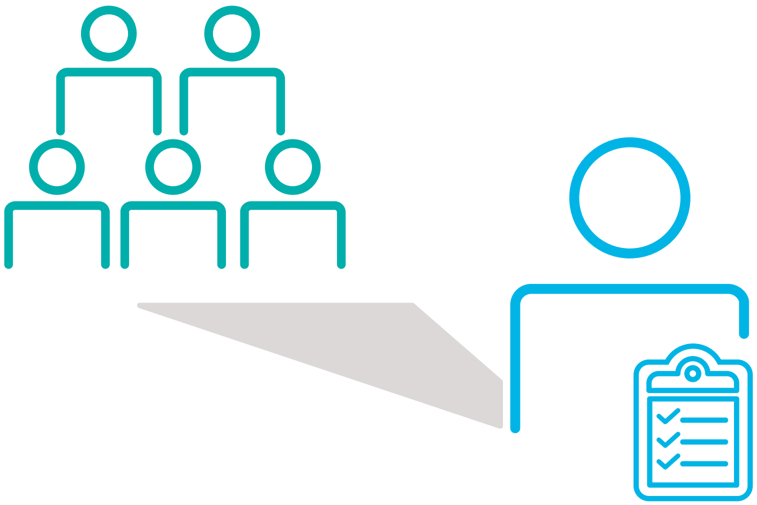

LEAST PRIVILEGED ACCESS (with Fine-grained Controls!)
Outside Organization
Contractor/ Partner
Inside Organization
Password Admin
Auditor
System Admin
Shared Privileged Identity
Resources
App
App
App
Applications
Folders
Data
An industry-leading solution will grant or deny access based on the ORIGINAL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

PIM Capability 3:
User Activity Reporting & Video Session Recording

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.

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
- Enabled accountability for users of IT systems
- Authorized logs for applications that do not natively produce logs



Logs must capture all actions based on the original, individual identity!

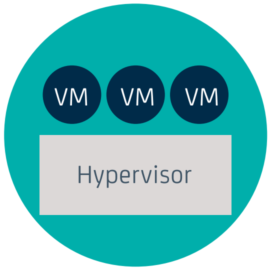
PIM Capability 4: UNIX Authentication Bridging

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.

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

PIM Capability 5: Virtualization Security



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.

Benefits include:

- Improved compliance
- Reduced risks of virtualization, including hypervisor administrators

Mitigate Insider Risks with Data Protection Solutions

Data Protection solutions are designed to:

- Track and control how authorized users handle sensitive and protected information
- Help organizations protect private data
- Assist in behavioral profiling of employees
- Serve as an effective training tool for security awareness
- Integrate with other security and compliance solutions to prevent unauthorized access to critical data

Enterprises can leverage Data Protection solutions to protect four critical types of data:

- Data at access—Sensitive information that individuals in inappropriate roles are attempting to access
- Data in use—Private data handled on a local workstation, laptop or mobile device
- Data at rest—Data on shared folders, document repositories, public folders, ODBC sources and collaborative systems
- Data in motion—Data communicated over the network

Understanding Insider Threats
Real and Substantial Threats
Test Your Misconceptions
Defending Against Insider Threats
Striking the Right Balance
The Problem with Privileged Identities
Capabilities of PIM Solutions
Mitigate Insider Risks
What to Look for
About the Solutions from CA Technologies

What to Look for in a Data Protection Solution

An industry-leading Data Protection solution should protect:

1 Data at access by classifying content, enabling fine-grained access controls. Ideally, it should:

- Include a web service API that enables external commands and integration of classification data
- Support IAM, storage, file servers and collaboration software

2 Data in use through implementation of a highly scalable endpoint agent, enabling enterprises to protect data at the source via:

- Controls for email, web, printing and data saving
- Scans for sensitive data on the endpoint
- Online and off-line enforcement
- Incident-appropriate response upon detection of a violation
- Education of end-users (educational popup windows to explain company or regulatory policy)

3 Data in motion through implementation as a network appliance or an integration directly with ICAP servers and MTAs, enabling organizations to monitor data at network egress points (including web, email, instant message and FTP protocols).

4 Data at rest through implementation of a local server or network scan, enabling scans for structured and unstructured data across various database, file and document repositories. Capabilities should include:

- Discovery and scanning tasks that can be executed on-demand or on a specified schedule
- Options to delete, copy, stub or move to another location
- Integration with file encryption and rights management technologies

What to Look for in a Data Protection Solution Continued

What to Look for in a Data Protection Solution Continued

An industry-leading Data Protection solution should also:

5

Provide a wide variety of monitoring and control options, including:

- Monitoring for violations
- Blocking improper use
- Quarantining for approval
- Delivering warnings to educate users about potentially improper data usage
- Encrypting valid use
- Assigning digital rights
- Provoking justification for potentially “improper” use
- Replacing sensitive data with links
- Moving stored data

6

Classify when files are created to eliminate costly discovery processes.

- Traditional Data Protection discovery solutions can help with asynchronous discovery of sensitive content and consolidation of data, but content verification, classification and remediation of access controls remain a costly, resource-intensive effort.
- By leveraging fine-grained access controls, an effective Data Protection solution should classify data and enforce access and other file handling rules as content is being written to file shares and collaboration sites. This can eliminate the need to maintain costly manual discovery and remediation processes.

Understanding Insider Threats
Real and Substantial Threats
Test Your Misconceptions
Defending Against Insider Threats
Striking the Right Balance
The Problem with Privileged Identities
Capabilities of PIM Solutions
Mitigate Insider Risks
What to Look for
About the Solutions from CA Technologies

About the Solutions from CA Technologies

CA Privileged Identity Manager

CA Privileged Identity Manager is a comprehensive solution for privileged identity management in both physical and virtual environments. They help to mitigate risk and facilitate compliance by controlling how privileged users access and use enterprise systems and data across the IT environment to achieve a higher level of security, reduced administrative costs and easier audit/compliance processes.

CA Privileged Identity Manager helps organizations:

Enable privileged users' accountability.
Control and monitor how privileged users access and manage enterprise data, enabling accountability and segregation of duties.

Secure both physical and virtual environments.
Control privileged users on physical systems, virtual machines and the hypervisor.

Facilitate compliance (including the virtual data center).
Address regulatory compliance by proactively reporting on the status of key compliance policies, through hypervisor security controls and privileged identity management.

Reduce IT costs through automation.
Increase automation, including password management, on both physical and virtual systems.

Improve security through automation.
Use policy-based automation to reduce human error, enabling required changes to occur in real-time and improve security.

Expedite adoption of virtualization.
Control privileged user actions in virtual machines and the hypervisor, enabling virtualization of critical servers.

Prevent password theft and sharing.
Prevent password sharing and "over the shoulder" password theft, while also eliminating the need to cut and paste passwords.

Create a secure multi-tenant environment.
Use network zoning and hypervisor hardening capabilities to enable secure multi-tenancy.

Reduce UNIX and Linux administration costs.
Reduce the cost of UNIX and Linux account management by authenticating users to Microsoft Active Directory and providing single sign-on capabilities.

Get an overview of how CA Privileged Identity Manager can help reduce risks.

About the Solutions from CA Technologies Continued

About the Solutions from CA Technologies

Continued

CA Data Protection

CA Data Protection allows organizations to control information in use, in motion, at rest and at access. CA Data Protection delivers these capabilities through CA Data Protection Endpoint, CA Data Protection for Networks, CA Email Supervision, CA DataMinder Protection for Stored Data and integration with CA Identity & Access Management (CA IAM) solutions. CA Data Protection is an information protection and control solution that helps minimize the accidental, negligent and malicious misuse of data while helping to comply with various data protection standards and regulations. Through the delivery of broad information and communication coverage, precise policy enforcement through identity context and content-aware identity and access management (IAM), organizations are able to take a comprehensive approach to reducing risk to their most critical assets while enabling critical business processes to continue.

Learn how CA Data Protection can safeguard your critical data.

CA Data Protection delivers:

Broad information control.
CA Data Protection delivers broad control of information across the enterprise. Not only does CA Data Protection control information at the endpoint, over the network, on the message server and in the repository, but it also controls access to information.

Identity-centric data protection.
CA Data Protection leverages identity across policy, user entitlements and delegated remediation. Through the application of identity, organizations are able to precisely enforce policy, enable persistent protection and protect employee privacy.

Content-aware IAM.
CA Data Protection's ability to accurately classify content enables IAM technologies to make more informed and intelligent decisions. For example, CA SiteMinder® is able to consume content classification information to make fine-grained authorization decisions.

Appendix

What is a High-risk Individual?

Personality Traits

- Immature
- Amoral/Unethical
- Prone to fantasizing
- Lacks conscience
- Emotionally unstable
- Low self-esteem
- Superficial
- Restless/Impulsive
- Manipulative
- Evidence of personality disorders

Vulnerable Lifestyle & Circumstances

- Demonstrates poor work attitude—doesn't follow procedures,
- Shows signs of being stressed—loses temper, apathetic, memory problems
- Exploitable/vulnerable lifestyle—financial, alcohol, gambling, drug problems
- Exploitable or vulnerable work profile—has access to sensitive assets
- Recent negative life events—problems at work resulting in loss of status, personal injury, death, relationship break-up, etc.

Workplace Behavior

- Engages in unusual copying activity—extensive use of equipment, covers or removes protective markings, use of various offices to perform copies
- Engages in unusual IT activity—conducts key-word searches in a sensitive database, shows an unusual pattern of usage prior to foreign travel, etc.
- Unauthorized handling of sensitive material
- Commits security violations

Previous page

Understanding Insider Threats
Real and Substantial Threats
Test Your Misconceptions
Defending Against Insider Threats
Striking the Right Balance
The Problem with Privileged Identities
Capabilities of PIM Solutions
Mitigate Insider Risks
What to Look for
About the Solutions from CA Technologies

Misconceptions Quiz

#1

Most people behind insider threats are “hackers.”

True

False

Most people behind insider threats are “hackers.”

False:

You are correct.

Insiders are very rarely hackers. They are individuals who:

- Have access to sensitive data or know where sensitive data resides
- May have privileged access to private systems
- Have been entrusted with all the tools they need

Next question

Most people behind insider threats are "hackers."

True: **This is a misconception.**

Insiders are very rarely hackers. They are individuals who:

- Have access to sensitive data or know where sensitive data resides
- May have privileged access to private systems
- Have been entrusted with all the tools they need

Next question

Understanding Insider Threats
Real and Substantial Threats
Test Your Misconceptions
Defending Against Insider Threats
Striking the Right Balance
The Problem with Privileged Identities
Capabilities of PIM Solutions
Mitigate Insider Risks
What to Look for
About the Solutions from CA Technologies

Misconceptions Quiz

#2

Insider threats are primarily a technical problem.

True

False

Insider threats are primarily a technical problem.

False: You are correct.

While technical issues may influence security breaches, organizational factors that contribute to insider-driven attacks include inadequacies in:

- Management practices (especially a lack of awareness of high-risk individuals within the enterprise)
- Auditing functions
- Security culture
- Role-based, personnel security risk assessments
- Pre-employment screening
- Communication between business areas
- Corporate governance

Next question

Insider threats are primarily a technical problem.

True: **This is a misconception.**

While technical issues may influence security breaches, organizational factors that contribute to insider-driven attacks include inadequacies in:

- Management practices (especially a lack of awareness of high-risk individuals within the enterprise)
- Auditing functions
- Security culture
- Role-based, personnel security risk assessments
- Pre-employment screening
- Communication between business areas
- Corporate governance

Next question

Misconceptions Quiz

#3

Organizations must blindly trust their administrators.

True | False

Organizations must blindly trust their administrators.

False:

You are correct.

Applying the principle of "least privilege access" to all employees and administrators is a safer way to manage trust. The principle of least privilege access:

- Restricts access to the minimum a user needs to do his/her job
- Limits the ability for damage to be done by a malicious or exploited insider
- Prevents careless mistakes

Next question

Organizations must blindly trust their administrators.

True:

This is a misconception.

Applying the principle of "least privilege access" to all employees and administrators is a safer way to manage trust. The principle of least privilege access:

- Restricts access to the minimum a user needs to do his/her job
- Limits the ability for damage to be done by a malicious or exploited insider
- Prevents careless mistakes

Next question

Misconceptions Quiz

#4

Detection of security breaches is the most important part of an insider threats defense program.

True | False

Detection of security breaches is the most important part of an insider threats defense program.

False:

You are correct.

Deterrence is more important than detection. Organizations can prevent security events from happening in the first place by:

- Deploying data-centric (vs. system-centric) security
- Crowd-sourcing security
- Using positive social engineering to constantly remind insiders of proper data usage policies

Next question

Detection of security breaches is the most important part of an insider threats defense program.

True:

This is a misconception.

Deterrence is more important than detection. Organizations can prevent security events from happening in the first place by:

- Deploying data-centric (vs. system-centric) security
- Crowd-sourcing security
- Using positive social engineering to constantly remind insiders of proper data usage policies

Next question

Understanding Insider Threats
Real and Substantial Threats
Test Your Misconceptions
Defending Against Insider Threats
Striking the Right Balance
The Problem with Privileged Identities
Capabilities of PIM Solutions
Mitigate Insider Risks
What to Look for
About the Solutions from CA Technologies

Misconceptions Quiz

#5

Analyzing massive amounts of data is the solution.

True

False

Analyzing massive amounts of data is the solution.

False: You are correct.

Organizations should analyze the *right* information. It's most important for enterprises to:

Know Their People

- Work hours
- Network use patterns
- Devices they use
- Recent position changes
- Ambitions

Know Their Data

- Data that would cause the most long-term damage to an organization, if exposed
- Data that, if breached, would cause the most short-term damage
- Data that must be protected, according to laws and regulations

Know Their Enemy

- Potential targets of insider attacks
- High-risk individuals within the organization

Return to presentation

Analyzing massive amounts of data is the solution.

True:

This is a misconception.

Organizations should analyze the *right* information. It's most important for enterprises to:

Know Their People

- Work hours
- Network use patterns
- Devices they use
- Recent position changes
- Ambitions

Know Their Data

- Data that would cause the most long-term damage to an organization, if exposed
- Data that, if breached, would cause the most short-term damage
- Data that must be protected, according to laws and regulations

Know Their Enemy

- Potential targets of insider attacks
- High-risk individuals within the organization

Return to presentation

Identifying Exposure to Data Breaches

Quiz

1. Do you know where all of your sensitive data is?
2. Is your sensitive data properly classified and tagged?
3. Do the right people have access to the right data and ONLY the right data?
4. Are you able to keep track of all of your organization's newly-created data?
5. Do your users understand your organization's policies and procedures for handling data and are they following them?
6. Can you identify users that might pose greater risk to the organization based on their data usage patterns and/or behavior?

If you answered "**no**" to three or more of these questions, your organization may be vulnerable to (or has already experienced) data theft or exposure. Read the rest of the e-book to learn how to reduce your risks now and in the future.

If you need more assistance, ca.com/data-protection go to learn more about our capabilities.

Previous page

For more information, visit ca.com/data-protection

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com.**

This document is for your informational purposes only and does not create any warranty of any kind. Some information and results illustrated here are based upon CA or customer experiences with the referenced software product in a variety of environments, and may perform differently depending on the actual usage and type of environment and is not indicative of the future performance of such software products.