SOLUTION BRIEF • ENTERPRISE IAM

ca technologies

How can I counter the insider threats within my organization?

Learn how an Enterprise IAM approach offers an effective countermeasure.

Employing a zero-trust model with layered, defense-in-depth enterprise identity and access management solutions from CA Technologies offers your organization a comprehensive strategy against ever-evolving threats, regardless of whether they are internal or external.

Executive Summary

Challenge

Data is the lifeblood of an organization, used to make decisions and tell us how things are running. Apps are driving digital transformations across every industry, but these apps are just new interfaces to connect users with data. Data has value—both to the organization and to modern-day pirates, who seek to steal this digital bounty. Enterprises must work diligently to secure their data from external attacks; however, increasingly the threats are originating from within the organization. How do you defend against malicious insiders who wish to exploit sensitive data for financial gain or the accidental insiders who inadvertently click on a phishing email and have their credentials stolen?

Opportunity

CA Technologies provides a layered, defense-in-depth enterprise identity and access management (EIAM) approach. Privileged access management (PAM) solutions from CA combat insider threats and targeted breaches by preventing unauthorized access and usage of privileged accounts. CA Single Sign-On enforces similar access controls across all online applications. CA Threat Analytics for PAM incorporates machine learning and risk analytics to establish baseline behavior in order to identify anomalous behavior. CA Advanced Authentication strengthens the login process by adequately verifying the identity of a user before granting access to sensitive information, reducing the risk of the accidental insider. Lastly, CA Identity Suite provides a unique approach to governance that helps ensure that least privilege is enforced, while providing a rich, yet easy-to-use experience for both requesters and approvers.

Benefits

A modern EIAM solution strikes the right balance between enterprise data security and convenient user access. It provides a comprehensive strategy against ever-evolving threats, regardless of whether they are internal or external. Traditional identity and access management (IAM) technologies are enhanced and supercharged with user behavior analytics, which further reduces friction and automates mitigation processes when risk is elevated. Simply put, the CA Technologies EIAM suite of solutions offers the best foundation to manage and control access to enterprise IT apps, data and infrastructure, minimizing risk and improving compliance.

Background

Large, successful, targeted data breaches are what make the headlines, but external attackers are not the only threat to the organization. Enterprises must also work diligently to secure their data from malicious insiders who wish to exploit sensitive data for financial gain or the accidental insiders who inadvertently click on a phishing email and have their credentials stolen.

A recent survey by Cybersecurity Insiders found that 90 percent of respondents felt vulnerable to insider threat. The survey also discovered that insider threat is more widespread than most people believe, and that it is growing. In fact, 53 percent of respondents reported that they had experienced an insider attack against their organization in the last 12 months and 20 percent reported six or more attacks in 12 months. In addition, 27 percent reported more frequent insider attacks during this period.[1]

Moreover, Verizon's 2017 Data Breach Investigations Report states that "malicious insiders are not always the people snarfing up vast troves of data and packing it off to WikiLeaks tied up with a bow. Those breaches are the ones that get the headlines, the glory and, potentially, land the actor in a prison cell. What is more common is the average end-user absconding with data in the hope of converting it to cash somewhere down the line (60 percent). Sometimes employees let their curiosity get the better of them and they engage in some unsanctioned snooping (17 percent)."[2]

Given all of this, what can enterprises do to tackle the insider threat and protect their organizations? The good news is that the survey reported that 73 percent of respondents felt that they had appropriate controls in place to detect and prevent an insider attack. The bad news is that only 33 percent felt that these controls were very effective. How confident is your enterprise with the controls you have in place? What can be done to improve your existing controls?

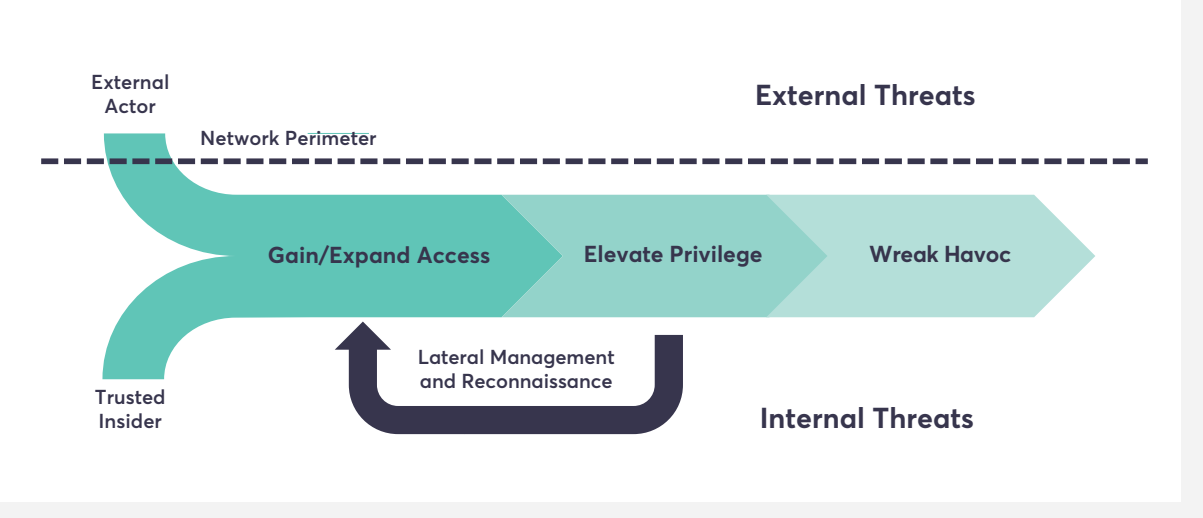
This solution brief will look at the nature and impact of insider threat and ways to mitigate potential attacks using a comprehensive approach to privileged access management from CA Technologies.

The Kill Chain and the Dilemma of Insider Threat

Cybersecurity teams at Lockheed Martin first identified a common data breach attack vector and coined the term "kill chains" because disrupting the attack sequence at any point can "kill" the attack. The kill chain is comprised of a consistent and predictable series of steps an attacker must accomplish to successfully achieve their goal. While the articulation of some kill chains can be quite complex, it's possible to summarize the key steps associated with the typical data breach kill chain in a simplified manner.

As shown below, the steps are surprisingly simple: An attacker gains access either by exploiting the credentials and access they already have (trusted insider) or compromises these credentials (external

FIGURE 1.
The Data Breach Kill Chain Process



actor). Once the attacker has gained access, one of the first steps is to elevate privileges, typically by compromising other privileged credentials. Unless the attacker is remarkably lucky, the first system compromised is unlikely to be the ultimate target, so the next step is to conduct reconnaissance of the network and move laterally to systems and servers closer to their ultimate goal. This process is repeated until the attacker reaches their goal and steals the data they are seeking to wreak havoc.

The Cybersecurity Insiders survey found that confidential business information (financials and customer data) was the most vulnerable (57 percent), but privileged account information (passwords, credentials, etc.) was the second most vulnerable data (52 percent). Unfortunately, these two are interrelated because stealing the second can lead to stealing the first.

Identity is the most frequently exploited attack vector; the 2017 Verizon Breach Report found that 81 percent of all breaches utilized lost, stolen or weak credentials. Therefore, the most common approach to breaking the kill chain is to monitor access and protect against stolen login credentials. However, this approach is significantly more difficult when one considers insider threat. How does one determine when an internal user is using their access for legitimate or illegitimate purposes?

But more important than identification is prevention, and unfortunately, only 22 percent of respondents stated that they could detect an attack in minutes, and even fewer—only 17 percent—felt that they could detect and prevent an attack in minutes. This means that the majority of organizations cannot detect or stop an attack until hours after it has begun—by which time, the majority of damage may already be done. One of the primary reasons for this is that many of the traditional insider threat technologies are based on static rules, which can be ineffective against today's attacks. Enterprises not only need to secure privileged accounts, but also need a way to automate the detection of compromised accounts or malicious insiders and thwart these attacks in real time, before any damage is done.

The strategic solution to these challenges is a modern privileged access management technology that incorporates machine learning and risk analytics and integrates with the larger enterprise identity and access management framework to provide full privileged identity lifecycle management and governance.

Combatting Insider Threat and Targeted Breaches

To guard against costly breaches by insiders, enterprises must manage and control access to privileged accounts across physical, virtual and cloud-based applications and systems. Employing a zero-trust model with a layered, defense-in-depth EIAM approach offers your organization a comprehensive strategy against ever-evolving threats, regardless of whether they are internal or external.

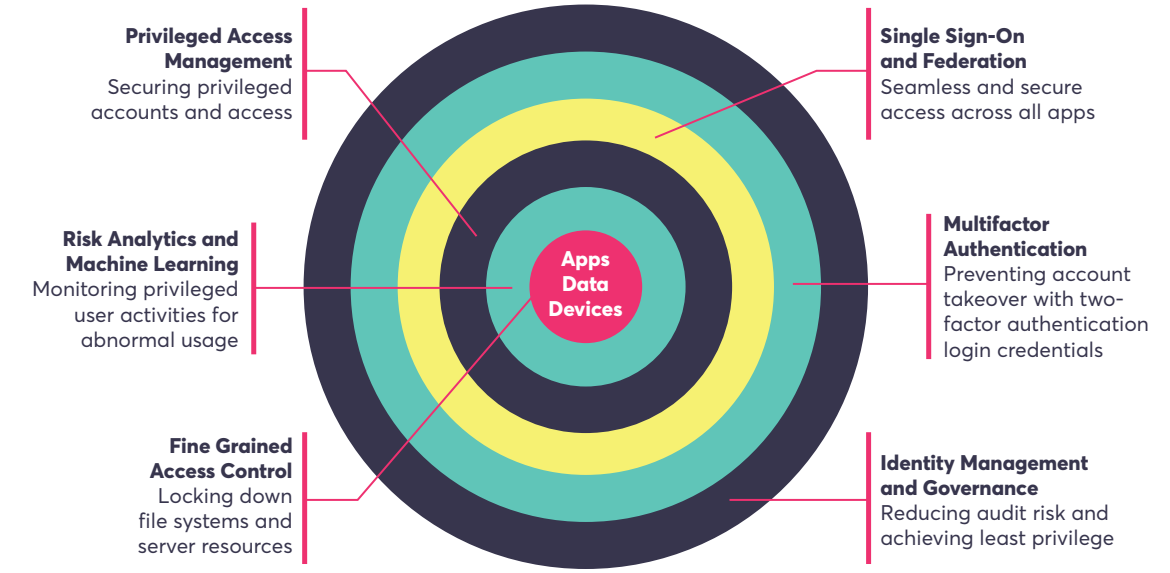
In Figure 2, the modern EIAM solution consists of multiple layers of protection. Let's look at each of them.

Privileged Access Management

The starting point for most organizations is privileged access management (PAM). Privileged account information is the second-most targeted data according to Cybersecurity Insiders, which is not surprising as these accounts often have access to the sensitive data that insiders and hackers want to steal.

Privileged accounts comprise not only employees with direct, hands-on responsibility for system and network administration, but also vendors, contractors, business partners and others who have been granted privileged access to systems within your organization. In many cases, privileged accounts aren't even people—they can be applications or configuration files empowered by hard-coded administrative credentials. A PAM solution provides multiple means of breaking the kill chain, stopping attackers and preventing breaches by preventing unauthorized access to privileged accounts; limiting privilege escalation, reconnaissance and lateral movement; and monitoring, recording and auditing privileged activity.

FIGURE 2.
Comprehensive Enterprise Identity and Access Management



CA Technologies provides two complementary privileged access management solutions:

- **CA Privileged Access Manager (CA PAM)** defends and controls privileged users and the credentials they use to access and manage your digital infrastructure. It proactively enforces security policies and role-based limits on privileged user access—all while monitoring and recording privileged user activity across virtual, cloud and physical environments. CA PAM is a password vault—a proxy-based gateway that issues and manages passwords for privileged accounts. This solution can help to address compromised credentials, because it takes the passwords from privileged accounts out of the hands of the end users and vaults and manages them. In addition, it can also control what users can do with those accounts once they have checked them out.
- **CA Privileged Access Manager Server Control** provides localized, fine-grained access control and protection over operating system-level access and application-level access on physical servers. CA Privileged Access Manager Server Control is an agent-based solution that provides an extra layer of security for your most critical infrastructure.

For more information, see the recently published Gartner Market Guide for Privileged Access Management (ID: G00315141), which highlights the trends that are shaping the cybersecurity market and provides some recommendations for choosing the right solution[3].

Single Sign-On

As mentioned previously, the Cybersecurity Insiders survey found that both regular employees and privileged IT users pose the biggest insider security risk to organizations; however, what defines or differentiates a regular user from a privileged one? Is it based on the privileges that have been granted to the user, or is it based on the access and activities that are being used at a specific moment in time? In fact, as organizations have pushed more and more enablement out to the business users, many regular employees have elevated access rights, which could be arguably considered "privileged access." For this reason, a single sign-on solution should also be considered as part of an insider threat program.

As enterprises rapidly expand the ways they provide online services to employees, contractors and partners, they need to make convenient "anywhere, anytime" access and "any-device" options the new standard. The use of traditional single sign-on (SSO) in Web access management (WAM) has been critical to controlling access to resources, including access to PAM solutions. It provides a seamless and secure experience for users, enabling them to readily move from one web-based application to another, or in the case of partners, the ability to federate from their domain to yours. These types of solutions also offered the means to enforce access controls across all web-based apps.

CA Technologies provides two market-leading access management solutions:

- **CA API Management** centralizes and manages security at the API layer while meeting the most stringent regulatory and compliance standards. It extends access management to apps, mobile, and IoT, and integrates with CA Advanced Authentication and CA Single Sign-On to provide a consistent and convenient user experience across all access channels.
- **CA Single Sign-On (CA SSO)** provides secure and flexible access management for mobile, Web and SaaS applications, regardless of where they're hosted or how they're accessed. Highly scalable and proven in mission-critical deployments at hundreds of sites, CA SSO enhances security by identifying who the user is and what they're attempting to do and enforcing appropriate access policies using a standards-based framework that can be shared by IT and application developers.

Risk Analytics and Machine Learning

Access management technologies such as CA PAM and CA SSO are very good at managing and controlling access to the IT resources that they are protecting; they can grant or deny access or prevent specific actions based on security policies.

However, compromised accounts, especially privileged accounts, are the most common source of security breaches today. They also have the highest impact. Once attackers gain access via a legitimate user identity, they can access all the data and systems to which that identity has access. Often, these attacks go unnoticed for weeks, or even months, while the perpetrator is traversing the system horizontally and vertically. Traditional access management solutions must adapt to this new reality.

Organizations need to adopt an automated mechanism for addressing this threat. That mechanism is user behavior analytics (UBA), which monitors identities to establish baseline behavior in order to identify anomalous activity. Advanced algorithms continuously assess the behavior of privileged identities and compare their actions to historical observations and the behavior of other identities. The algorithms then assess risk and quickly detect malicious activity.

While legitimate user behavior is subject to change, it usually changes gradually. Machine learning algorithms adapt accordingly, by learning from changes and emerging patterns. This is also used to reduce false positives. Thus, a UBA tool uses automated analytics to continuously monitor identities and quickly detect attacks, high-risk activities and breaches.

CA Technologies provides two UBA solutions:

- **CA Threat Analytics for PAM** enables the enterprise to continuously access risk and quickly detect malicious activity among privileged users. This is a value-add component to CA PAM that provides user behavior modeling and analytics. It can model normal behavior for a privileged user and detect when the behavior patterns change. This component addresses insider threat in a new way. Before an internal user turns malicious, they will have a normal usage pattern, but as they go rogue, this pattern will change as they seek out ways to do harm. A user behavior analytics engine can detect these changes and take action. Similarly, if a legitimate user account is compromised, the external hacker will exhibit a different usage pattern than the legitimate user and this will also be detected.

- **CA Risk Authentication** is an integral component of CA Advanced Authentication; it detects and protects against high-risk login attempts or other sensitive access by analyzing a wide set of factors, including user behavior, device characteristics, geolocation and velocity data, without requiring any direct input from the end user. And when deemed too risky, the user can automatically be prompted to submit additional credentials or information to further prove their identity.

Multifactor Authentication

While a malicious insider is simply a good user who has been lured to the dark side of the force, the accidental insider is usually one who has had their account compromised by an external hacker. How are these accounts compromised? The biggest factors are falling for phishing attempts (67 percent), weak/reused passwords (56 percent) and shared passwords (44 percent), according to Cybersecurity Insiders. To reduce this risk, most security experts recommend the replacement or enhancement of simple username/password combinations with stronger authentication and several regulations recommend, or require, multifactor authentication. Factors can include the following:

- Something you know (such as password or PIN)
- Something you have (such as smartcard, digital ID or one-time password (OTP) generator or mobile device)
- Something you are (a biometric factor such as fingerprint or voiceprint or user behavior)

Strengthening the login process and adequately verifying the identity of a user before granting access to sensitive information reduces the risk of the accidental insider.

CA Technologies provides a comprehensive authentication solution:

- **CA Advanced Authentication** provides a secure, user-convenient and cost-effective way to protect many sensitive corporate resources, including cloud-based services, privileged accounts, remote access, virtual desktops and Web resources. It provides a wide variety of software-based, multi-factor authentication credentials and also can evaluate real-time risk based on user behavior, device characteristics and geo-location data. Together these capabilities enable an intelligent, layered security approach to protect user identities and organizational data.

Identity Management and Governance

Managing privileged users is a continuous and critical process. First, you must discover where your admin accounts are and eliminate improper privileges and orphan accounts. Next, you must enforce your least-privilege policies for these users and eliminate shared accounts—this is called PAM. Lastly, you must govern privileged access to avoid entitlement creep and to ensure that each user still needs any elevated privileges that they have. If any one of these essential capabilities is weak or missing, your overall risk of breach or insider threat rises significantly.

However, what is the definition of a privileged user? Is it just those users who have access to admin accounts? A recent Ponemon study found that 71 percent of respondents say that they have access to data that they shouldn't and 80 percent of IT professionals stated that their organization were not enforcing "least privilege" policies[4]. This begs the question—at what point does a regular user become a privileged user? One definition could be that a "privileged user" is any user who has been given access right or entitlements that, if misused or compromised, could cause unacceptable damage or loss to the organization. This is alarming, as we may have a far larger pool of "privileged users" than we thought.

For this reason, an identity management solution should be considered the final layer of protection against insider threat and targeted breaches.

CA Technologies provides a market-leading identity solution:

- **CA Identity Suite** provides a unique approach to governance that helps ensure that least privilege is enforced, while providing a rich, yet easy-to-use experience for both requesters and approvers. It also provides automated provisioning and deprovisioning of access to both regular and privileged accounts, along with role and group management of all users.

The CA Technologies Advantage

In today's world, where breaches are the norm, information is everywhere and personalized experiences drive digital transformation, identity is the key. Identity is the foundation of trust in a zero-trust online world. At CA Technologies, we understand how important it is to strike the right balance between enterprise data security and convenient user access. And, we have adopted three strategic initiatives to differentiate our IAM solutions:

- **Hybrid Cloud:** As your application environment moves to a hybrid model, we believe the modern EIAM solution should do so as well. Your EIAM infrastructure is mission-critical, and it's critical to protect, monitor and audit all access across virtual, cloud and physical environments to prevent lateral motion and secure critical infrastructure and sensitive data.
- **Behavioral Analytics:** Gaining visibility into what users and their accounts are doing is key for two reasons: First, you can detect anomalous activity either for a malicious insider or to identify an account that has been taken over. Second, you can simplify the user experience and reduce friction by positively identifying legitimate users from fraudulent ones. Our strategy is to apply advanced analytics into our security products to make PAM and IAM processes more effective.
- **Total Cost of Ownership:** An EIAM solution can reduce the attack surface and provide extremely fast time-to-value, which is what really matters when your organization is in danger of being breached. A comprehensive solution provides all the capabilities needed, and makes long-term financial, business and productivity sense.

Next Steps

The rise in malicious and negligent insider attacks is alarming. Organizations need to consider their options and select a vendor that offers a layered, defense-in-depth approach to combatting insider threats and targeted breaches. The EIAM solutions from CA Technologies offer a comprehensive strategy against ever-evolving threats, regardless of their origin. To learn more about insider threats and the solutions discussed in this brief, visit https://www.ca.com/us/products/insider-threat.html.

For more information, please visit **ca.com/pam**

Connect with CA Technologies

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**.

1 Cybersecurity Insiders, Crowd Research Partners, "Insider Threat – 2018 Report", December, 2017, https://www.ca.com/us/collateral/ebook/insider-threat-report.html

2 Verizon, "2017 Data Breach Investigations Report," July 2017, www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

3 Felix Gaehtgens, Anmal Singh and Dale Gardner, Gartner, "Market Guide for Privileged Access Management," August, 2017, www.gartner.com/doc/3789663/market-guide-privileged-access-management

4 Ponemon Institute, "Privileged User Abuse & The Insider Threat," May 2014, www.raytheon.com/capabilities/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf

ca technologies

CS200-343242_2018