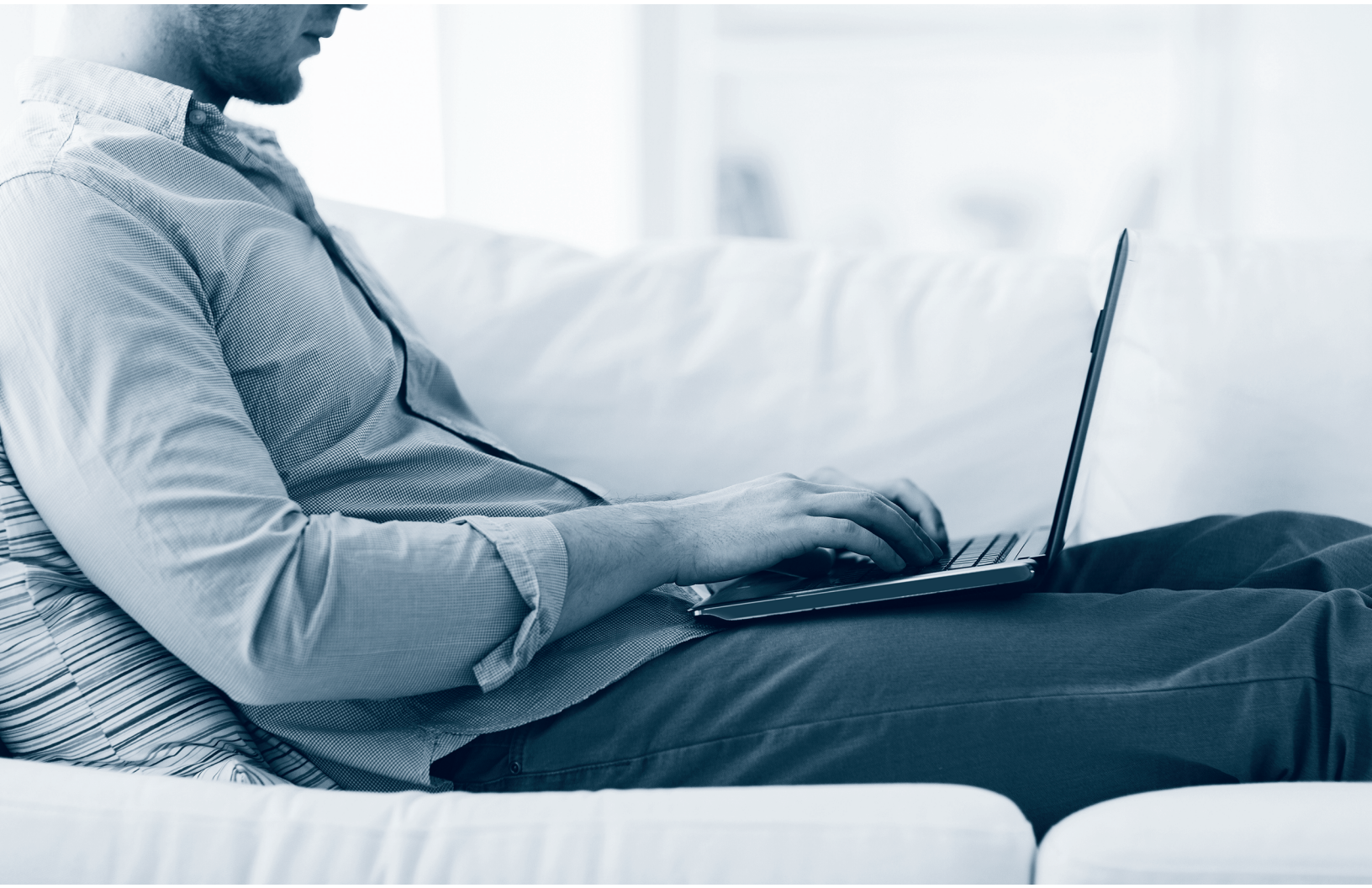
Centrify®

WHITE PAPER

Best Practices for Privileged Identity Management in the Modern Enterprise



Contents

Abstract

Data breaches continue to be top of mind for organizations large and small. Three key dynamics are making that challenge much harder — the cloud, the growing sophistication of attackers, and dramatic growth in outsourced services.

In this paper, we explore the modern enterprise — a hybrid organization with infrastructure spread across on-premises data centers as well as hosted in the cloud and one where IT functions are split between internal and 3rd-party administrators. We look at these and related trends impacting our data security and specifically, best practices on how to manage and govern privileged user access to mitigate these risks.

Introduction

"We're incredibly thankful to have a PIM solution that gives IT, Risk and Compliance the data breach protection and auditing they demand and the ease of use our end users and admins expect, all while supporting our corporate goal of progressive business growth in the cloud"

That's the kind of "I'm able to finally sleep soundly at night" statement that every C-Level IT, Risk or Compliance manager dreams of making.

The sad reality, however, is that the current generation of Privileged Identity Management (PIM) solutions are still incredibly myopic to the evolution of business and, especially, IT. They continue to approach IT security as exclusively orbiting the traditional data center; a collection of servers that store lots of sensitive information for the organization and network devices that keep the infrastructure available, all managed on-premises by internal IT. When they need a solution for cloud deployments and hybrid use cases, their typical approach is to retrofit older on-premises technology, simply putting the same code on a virtual appliance and hosting it in a cloud IaaS.

They continue to use designs for the previous generation of IT, effectively ignoring the thousands of workloads migrating to the cloud at an increasing rate and a new set of business and operational dynamics that come into play as a result.

In today's economy, trying to find an IT organization that has NO presence in the cloud, NO sensitive data residing there, and NO privileged accounts shared amongst administrators is impossible. It's an exercise in futility. The **modern enterprise** is a hybrid one, and a hybrid enterprise needs modern solutions to protect it from the growing sophistication of cybercriminals who know how to exploit it.

The cloud is here to stay — the jury is no longer out. A new approach to PIM is required, an approach aligned with the modern enterprise. Just as the cloud was hailed for its elasticity — its ability to adapt to the changing needs of the business — PIM must equally adapt to the challenges of IT infrastructure hybridization, administrative teams comprising internal and 3rd-party outsourced users, and requirements for local and remote access across on-premises and cloud-hosted resources.

This paper describes PIM best practices that take into consideration this new dynamic for the modern enterprise.

Trends

The macro trends really haven't changed in the past several years, but they have accelerated. Outsourced services, cloud (*aaS), Mobile, Big Data, BYOD — they're all growing in adoption and investment. Even the relative newbie — Big Data — is, according to analyst group Gartner, over the proverbial Peak of Inflated Expectations.

Digital business is a top imperative. It's continuing to drive massive, fundamental shifts in technology, buying behavior and delivery/consumption of business services. Providers of application services, infrastructure and support, and business process services are reinventing to satisfy these needs and to ensure their own sustainable, profitable growth.

From the perspective of security in general, and Privileged Identity Management (PIM) specifically, data breaches are still top of mind. They continue to trend up and grab headlines, and are a leading culprit in C-level insomnia. Traditional network-centric approaches are proving to be insufficient by themselves. Companies and government agencies are refocusing efforts around identities to help better combat such threats. Their new mantra is that ***Identity is the New Perimeter***.

Data Breaches

PIM is vastly more important in this new, hybrid world of distributed resources and administration. Historically, not many companies looked at PIM as a "must solve it" problem. The thinking was, "so long as I have a vault for my root and admin passwords, as well as my passwords for service accounts, I'm good". But peel back the Band-Aid™ and you find fundamental security problems, as evidenced by breach attacks exploiting both end user and privileged user accounts, bypassing proxy-based password vaults, and compromising servers directly. This requires a modern, holistic solution, rather than a one-size-fits-all approach.

Cybercrime is now a highly organized and professional criminal activity; often government-sponsored. The U.S. Government has recognized the importance, categorizing cyberspace as the 5th domain of warfare, after the traditional land, sea, air, and space.

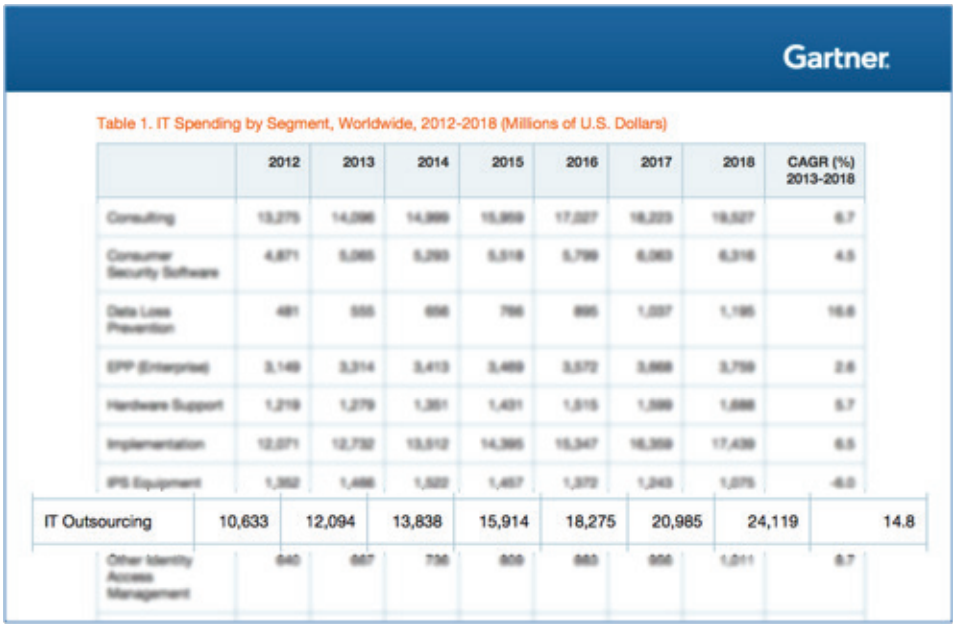

Gartner

Table 1. IT Spending by Segment, Worldwide, 2012-2018 (Millions of U.S. Dollars)

	2012	2013	2014	2015	2016	2017	2018	CAGR (%) 2013-2018
IT Outsourcing	10,633	12,094	13,838	15,914	18,275	20,985	24,119	14.8

Figure 1: Gartner IT spending — IT Outsourcing is on the rise and securing and auditing their access to our most privileged accounts is a top priority

To some degree, modern hybrid organizations are unintentionally playing into the hands of cybercriminals. By spreading infrastructure across on-premises and cloud, and outsourcing administration, operations, and development to 3rd parties, they are exposing a greater attack surface and driving up risk. *Verizon, in its annual Data Breach Investigations Report, warns us of a higher business impact from data breaches involving external contractors than those involving internal employees.*

Privileged identities are clearly the main target of professional cybercriminals. When you compromise root or administrator accounts on a key server, you have the keys to the kingdom. You're easily able to exploit anything on that server, and can use that server as a base from which to wage a more extensive campaign to hijack privileged identities across the entire network.

Big Data

As an example of the explosion of identity silos that exacerbates this situation, let's take a quick look at Big Data. Organizations are aggressively moving their Big Data lab experiments into production. What does this mean for identity-related risks to the organization?

The kind of computing scale required for an enterprise Big Data deployment can be off the charts. A simple lab cluster with 4 or 5 nodes can easily morph into dozens of clusters with hundreds or even thousands of nodes required for full production.

From a security perspective, Hadoop distributions from MapR, Cloudera, HortonWorks and others default to no security for identity and authentication. Enabling secure mode for Hadoop means having to configure a Kerberos infrastructure to authenticate the hundreds of business and service users/accounts in the system. This is no small undertaking, which is why most organizations choose to defer this until after the lab has proven the concept. Of course, this results in a rush job to get it implemented for a fast production roll out, with the potential consequence of substantial new security risk to the business.

The time and effort required to enable secure Hadoop is significant. Given the complexity of setting up a Kerberos realm, Key Distribution Center (KDC), identity store, managing keytab files, etc., production is not the time to be figuring all this out.

Adding to the complexity, Hadoop environments by nature have a security and trust model that's subtly different from most traditional server infrastructures. Analytic jobs are spread across multiple nodes for execution. Other nodes are responsible for mapping and reducing functions, orchestrating and tracking. They all talk to each other and must perform their combined duties on behalf of the user submitting the job. Given the potential for sensitive information, it's imperative that proper role-based access controls are in effect for administration, analyst access, and auditing.

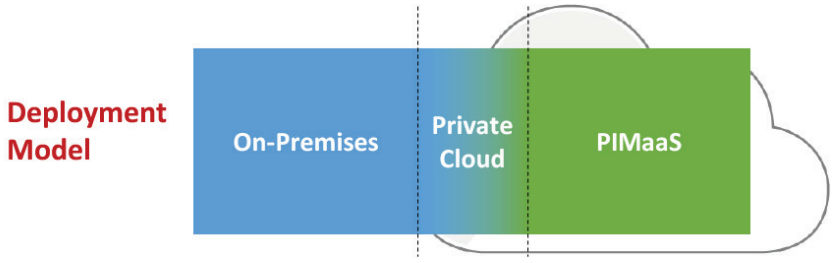
In any Big Data deployment, you have major security, risk, and compliance challenges to overcome, especially in relation to identity. Take all this outside your on-premises data center into the cloud, outside the purview of even your traditional PIM and IAM solutions, and the risks become very serious, indeed.

The Modern Hybrid Enterprise

"Users are no longer exclusively inside the firewall, nor is your infrastructure."

Organizations are migrating existing applications, taking them off antiquated, underperforming on-premises hardware and putting them onto brand new gear at Amazon, CenturyLink/Savvis, Azure and other IaaS providers. Migrating applications is not a simple matter of forklifting software from one server to another. There are many considerations including identity management and privileged access. The problems look similar to those on-premises except you can't generally use your on-premises PIM technology in the cloud.

So, you need a PIM solution that is also hybrid; a solution designed to secure hybrid IT deployments. Depending on your circumstances, cloud-tolerance, and perhaps regulatory constraints, a vendor needs to offer you a choice of deployment options — on-premises or private cloud deployment (managed by the customer) or PIMaaS (managed by the vendor).



Both deployment options should be driven off the same code base, built from the ground up as a multi-tenant service capable of exploiting cloud infrastructure and easily accommodating the more traditional on-premises data center architectures.

Privileged IT admins need access to the cloud service admin UI (e.g. AWS Console) to access and manage their infrastructure and servers. This isn't just about administrators, however. The servers are there to support applications — how do we secure access to the applications? Will you want SAML-based login from your corporate (or outsourced) IDP? Will you want to use Active Directory groups to control the role and entitlements the admin gets after logging into AWS?

There's also a line between OS security and application security that organizations need to consider. With more and more sensitive data being stored in SaaS applications and organizations creating enterprise-shared login accounts to apps such as Facebook and Twitter, every user must be considered a privileged user — it's just a matter of degree.

IT must ensure that privileged and regular users can get access to their infrastructure, servers, and applications and that both have secure access from any location and from any device.

Best Practices

To get the mind around the many moving parts of a comprehensive PIM implementation, it's useful to break it down into functional subsets. For this paper, our breakdown is:

- **Identity Consolidation** — centrally managing identities, roles, privileges and local accounts across heterogeneous resources
- **Privileged Access Request** – employing a workflow-based request and approval mechanism for privileged access

- **SuperUser Privilege Management (SUPM)** — the privilege elevation tools that enable a "least privilege" access model with granular administrative tasks for authorized users
- **Shared Account Password Management (SAPM)** — for legacy and emergency "break glass" scenarios where you can't elevate privilege and have to permit direct login as (e.g.) root
- **Privileged Session Management (PSM)** — the service that manages the privilege session and the video recorder keeping watch over it
- **Secure VPN-Less Remote Access** — remote access to resources on-premises and in cloud IaaS without a VPN
- **Application to Application Password Management (AAPM)** — replacing plain text passwords embedded in scripts with an API call to a secure password store
- **MFA Everywhere** — enforcing the use of a 2nd factor for user login, password checkout requests, and step-up authentication

In the following sections, we'll review best practices for each function. While it may be valuable for you — based on your current PIM maturity — to look at gaps in specific areas and cherry pick, it is highly advisable to assess your current state across them all.

Identity Consolidation

"Give users a single identity and get them to login as themselves"

Users are at the heart of both the challenges and the solution; more specifically, managing user identities and their associated roles and entitlements. The objective here is straightforward — **unify identity across all business platforms** (Windows, UNIX, Linux, and Mac), reducing silos and overall complexity.

This aspect of PIM is often neglected. As one of the inaugural capabilities in the PIM macrocosm it's now considered "table stakes" for any viable PIM solution. It's not ignored per-se; it's just not leveraged to maximize risk reduction and not given the attention it deserves.

By definition, Active Directory Bridging allows a PIM solution to act as a bridge from a non-Windows environment to Active Directory. Why? To leverage the many benefits that Active Directory offers in regards to identity management, Kerberos-based authentication, and true role-based privilege management that spans all your platforms. At a basic level, this means consolidating your identities across UNIX, Linux, Mac, and Windows in Active Directory, thereby avoiding the huge administrative effort as well as the security risks of managing identity silos (e.g., /etc/passwd) at every endpoint. Arguably more important is to give users a single, unique identity and get them to log in as themselves (i.e. their Active Directory IDs) vs. log in with a shared account, thereby ensuring better accountability from all your OS and application log and auditing systems.

Choosing Active Directory as your central repository makes sense for the majority of enterprises who already have big capital and human investments in the technology. It avoids standing up a parallel silo of identities (e.g. Oracle OID or CA Directory) with the challenges inherent in synchronizing them and their passwords with the new silo, installing agents on domain controllers, changing schema, and often changing user behavior by forcing them to reset passwords in a new tool instead of their laptop login screen.

Best Practice: Consolidate UNIX, Linux, and Mac identities under a single unique ID in Active Directory for centralized identity, role, and privilege management and Kerberos-based authentication.

Data breaches are about compromising existing privileged accounts and using them to jump around the network from server to server looking for data to monetize. So before this consolidation and in preparation for host-based SuperUser privilege management (see below) it's a good initial best practice to disable as many privileged accounts as possible thereby simplifying administration and limiting the attack surface.

Best Practice: Delete or disable as many privileged accounts as possible to reduce the attack surface.

Of course, not every account can be disabled or migrated into Active Directory. E.g., accounts such as Local Admin, and accounts associated with OS-specific daemons, application services, and application network and batch scripts. These accounts are also prime targets for attack since they often have admin-level privileges associated with them or if not, may allow an attacker to move laterally in the network to other servers that have admin credentials exposed in a similar way.

But while these accounts must remain local, they can still be brought under the same Active Directory-centric control for consistent lifecycle management. They can then be centrally created, provisioned to the right set of end-points, modified, deleted and subject to the same auditing and role-based access control governance.

Best Practice: Don't ignore local accounts or treat them as silos. Manage their lifecycle similarly, via Active Directory.

Following this advice, the next logical step is to have these local account passwords automatically synchronized with your incumbent password management repository (see SAPM below). In this way, the passwords can be immediately brought under management and rotated for security. Those local accounts supporting IT login are then accessible remotely through your SAPM portal.

Best Practice: As part of Local Account Provisioning, automate the synchronization of these account passwords into your SAPM solution for stronger password management and to enable remote access for internal and outsourced IT.

Active Directory's benefits should not stop there. Look for solutions that can enable centralized management of computers as well as users. By extending Active Directory's Group Policy model, you can further leverage your investment in Active Directory and Active Directory administration skill sets by applying group policy to UNIX, Linux, and Macs. Examples of such policies include host-based firewall rules (iptables), network access policies (openSSH) or computer certificate management (auto-issuance/renewal) for use by the applications running on it.

Best Practice: In addition to managing identities in Active Directory, look for a solution that supports machines and that can extend group policy to non-Windows servers.

But there's more! Squeezing yet more out of Active Directory's object management framework can give you the ability to bring machines, users, and roles together more effectively, enabling delegation, segregation of duties, and temporary support for multiple user UNIX profiles on the road to a best practice rationalized single profile. This hierarchical "zoning" capability can greatly improve productivity and compliance (e.g., securely isolating a collection of "PCI" machines and constraining access to a subset of trusted administrators).

An ideal Identity Consolidation solution would enable all this without being invasive to Active Directory, i.e. no changes to schema and no software dependency on domain controllers.

Best Practice: Look for advancements that extend Active Directory's model to bring more IT efficiencies and security such as hierarchical zones without requiring Active Directory schema changes or agents on domain controllers.

A final word. When exploring Identity Consolidation see if the vendor solution can support application login as well as user login across non-Windows platforms. For example, if your UNIX developer is building an app, a typical approach might be to build user authentication and authorization logic right into the code and maintain identity information in a separate silo (such as Oracle OID). Then there's the issue of password change and syncing between the two; putting an agent on each Domain Controller to sync a password reset from the user workstation.

Instead, look to leverage what's already in place as an authoritative store. Join the server to Active Directory and the code can ask the OS to authenticate the user and avoid that entire overhead. You can extend this model to UNIX, Linux, even Mac apps via PAM, LDAP, GSSAPI, or SAML.

Best Practice: Provide application developers with a centralized (Active Directory) means of externalizing user authentication, authorization, and identity management logic.

Privileged Access Request

"Reconcile who has approved access with who accessed resources"

There are situations where — even with the appropriate role — a user's action requires an extra layer of control and governance.

Perhaps, due to the extra sensitivity of certain actions and resources, it's desirable to add an additional layer of control in the form of a request/approval mechanism for additional security, governance, and compliance. The user must then explicitly request access and an approver would assess the request, granting or denying as appropriate.

Since IT activities vary in duration, it's important to provide the approver with the means to either grant permanent or time-based access (e.g., for 30 minutes) after which the permission grant is automatically revoked and the password rotated. Since best-practice dictates that superuser accounts such as root and administrator should be used only in exceptional "break glass" situations, limiting their use based on time is essential. So ensure the Privileged Access Request capability covers both login requests and password checkout requests.

This request/approval mechanism along with time-based grants will reduce your attack surface by only exposing access to more sensitive resources on an as-needed basis. Also for these more sensitive activities and resources, accountability and reconciliation is improved. With

users having a single identity (see Identity Consolidation on page 8), we can quickly and easily reconcile who has approved access with who has accessed resources, and for how long with contextual rationale.

Best Practice: Ensure your solution supports workflow-based privileged access request across both SUPM and SAPM components for stronger security, governance, and compliance

Privileged Session Management (PSM)

"Trust but verify"

Session recording is a critical element of any PIM deployment. Given the power of privileged accounts and the sensitivity of the systems, applications, and data they can access it's vitally important to audit and monitor their activities. Session recording involves the actual recording of the session as well as playback for compliance and data breach investigations.

Like any set of security controls in a complex environment, there's always the question of what to deploy first. Your individual circumstances will, naturally, vary but note that PSM has been deployed first by some organizations as initial intelligence into their PIM project plan. Compared to other PIM capabilities, it can be relatively simple to deploy and quick to value. So while (e.g.) your core SuperUser privilege management implementation is underway and you're cleaning up and consolidating your user identities, putting session recording on your privileged servers can give you immediate visibility into what your privileged users are doing in your environment and quickly support your audit and compliance activities.

Best Practice: PSM deployed first can provide valuable insights. Consider the potential benefits to your organization of deploying PSM first for a quick win.

Vendor options typically fall into two camps: centralized session recording on a gateway or proxy, and session recording on each host machine. Best practice dictates the latter as the most effective and secure option. As an analogy, if you put a security camera only on your front door but I creep around the back and manage to break in through a bedroom window, I've gained access to your house without you knowing. For remote or outsourced staff, the front door is the only way they can come in (legitimately). But malicious attackers — they'll find ways to bypass a central monitor. Hence the best practice is security controls (SUPM below) and a video camera on every sensitive asset.

In addition, while both methods capture session information, more detailed and comprehensive information can be captured on the host versus a gateway (especially when combined with a least-privilege approach to SuperUser privilege management that ties activities to a real user instead of a shared/anonymous user ID). At the host, you're able to faithfully capture the commands and actions performed to a very detailed level. This enables a very accurate transcription of the session producing accurate metadata that allows you to search recordings and pinpoint activities quickly. On a gateway, you don't have such access, which means you typically can't get the same rich metadata as a host-based auditing agent.

Be aware that some solutions "snapshot" data at relatively low resolutions, making it difficult to audit session activity or, in the worst case, missing important screen information. The best solutions capture video for every change in pixels, effectively capturing differences in frames more accurately than "snapshot" solutions.

Best Practice: Use a PSM solution based on "change in pixels" for maximum coverage, maximum resilience, and finer detail. Host-based PSR, where appropriate, can give you more information, better search and indexing, and a richer activity audit trail.

SuperUser Privilege Management (SUPM)

"Assign rights where you can; share accounts where you must"

SUPM refers to the practice of constraining the amount of privilege for a given account to the least amount possible to perform your job function. As mentioned, attackers are laser focused on attacking highly privileged accounts so they can own the machine and, from there, spread out to find even more highly privileged accounts across the network. If accounts have little privilege by default, they provide cyber attackers with much less leverage.

Security vendor approaches tend to fall into two main camps. One camp advocates keeping the privileged accounts in place and simply governs access to their password. This does little to reduce the attack surface. Implemented on a central gateway or proxy, it can log a user into a server but is unable to control individual privileged actions on that server. Once you're logged in, you're in with all the privileges of (e.g.) root. As such, all your activities on that server are logged anonymously — as root, resulting in zero accountability unless you find a way to correlate the local host events back to the original user login to the SAPM system. Even with privileged shells or white listing, it only protects the server if accessed through the proxy. Arguably the biggest challenge with this approach is when admins find a way to bypass the proxy and go straight the server, losing any protection the solution would otherwise offer.

The other camp advocates for a "least privilege" approach at the host-level wherever possible, and a password management approach at the gateway where a least privilege approach simply can't work. It enforces no direct login with highly privileged accounts (removing or disabling them — thus reducing the threat surface). You log in as yourself with a low amount of privilege. When you need to perform a privileged task (such as installing a software package), you explicitly ask for additional privilege. If granted (by role), that task will run as (e.g.) root, but audit trails will tie back to the real user ID for full accountability. Even better, the account can't be hijacked by malware and used to "land and expand" across the network. This is consistent with regulatory guidance such as PCI and NIST SP 800-53 that recommend least access to the set of servers based on need to know and least privilege to govern what you can do when you're on the machine.

Any approach to managing passwords, server login, and session recording centrally on a gateway is potentially vulnerable to the "front door" bypass we discussed in Session Recording, above. Host-based solutions don't suffer from this potential breach point.

Best Practice: Minimize the number of shared accounts. Reduce/disable the number of privileged accounts. Use host-based SUPM for least privilege login with unique ID and explicit privilege elevation wherever possible, and use SAPM for accounts where you can't use SUPM as the EXCEPTION not the RULE.

Almost as a corollary to this is that by implementing true SUPM, you can eliminate knowledge or usage of privileged account passwords, granting broad rights to start and gradually reducing those rights over time as you learn specific rights required for a specific job function.

Best Practice: Leverage SUPM to fine-tune your entitlements model.

Best Practice: Tying this to Identity Consolidation in Active Directory will provide further economies, allowing you to centrally manage the roles and entitlements for these users and effect global changes quickly and consistently across Windows, Linux and UNIX.

Whatever your approach, when users need access to privileged accounts and critical systems, look for a solution that supports contextual identity assurance. This involves Multi-Factor Authentication (MFA) and user context to assess risk and provide stronger identity assurance. E.g., a mobile phone can report GPS location in addition to generating a one-time password for greater assurance. Note that this can also be a highly effective counter to "pass the hash" attacks that are used to compromise servers without the need to use brute force to try to guess passwords.

Best Practice: Look for solutions that login using a second factor when authenticating privileged users. For greater identity assurance, look for a solution that considers context as well.

MFA should not stop at the point of login/authentication to a server, however. It should also be available during password checkout and privilege elevation (step-up authentication). After all, a command executed with admin-level privileges (during elevation) has the potential to do harm if the person elevating is not the legitimate user.

Best Practice: Ensure your solution also supports step-up authentication after login, when potentially powerful actions are performed during privilege elevation.

All the above is very relevant to resources inside your firewall. But as we know, the modern hybrid enterprise has servers on the outside. One method is to stand up an Active Directory domain in your cloud environment and join your non-Windows servers to this via your SUPM solution. Then you can manage all hybrid users from the same authoritative identity store. The leading IaaS vendors such as Amazon Web Services and Microsoft have documented guidance on how to deploy Active Directory there and trust internal Active Directory.

Similarly, you can deploy a virtual private cloud at a managed service provider (MSP), or with an IaaS hosting vendor such as Azure or AWS. Connected to your data center with a dedicated high-speed VPN, a private cloud functions as an extension of your existing data center and leverages your existing Active Directory, making it an excellent place to deploy a SUPM-based solution on servers.

Best Practice: Use a SUPM/Identity Consolidation solution in the cloud to join non-Windows servers to a local Active Directory Domain and manage identity. Use SUPM on servers within a virtual private cloud connected to your on-premises Active Directory.

Shared Account Password Management (SAPM)

From a security perspective, keeping sharing highly privileged accounts is the easiest way to introduce risk — which is the exact opposite of what we want. Ideally, then, we would eliminate all these accounts reducing the attack surface for attackers. However, there are situations where you have to login with such accounts. In that case, as security and risk practitioners, we should be limiting those situations to the absolute minimum possible.

So what are these situations? These are occasions where you cannot delete or disable a privileged account such local admins, root, administrator, legacy application administrative accounts or network device accounts. You must limit their use to only very infrequent or emergency situations, such as software installations/updates and the classic "break glass" situation where (e.g.) the network is down, a critical Linux machine has crashed, and it's only accessible via the console with a "root" login.

Best Practice: Data breach mitigation is most effective when reducing the attack surface — reducing the number of privileged accounts as close to zero as possible and only using SAPM for emergency login scenarios such as "break glass".

Modern SAPM solutions, however, should give customers a choice in deployment options: customer managed (on-premises or private cloud) and vendor-managed (PIM as-a-Service).

Best Practice: Pick a SAPM vendor with both customer-managed and vendor-managed deployment choices.

Such solutions will be able to accommodate modern hybrid cloud infrastructures and use-cases that traditional on-premises SAPM can't. These use-cases include anytime, anywhere remote access to on-premises and cloud-based resources, secure VPN-less resource access (see below), outsourced IT and contractor login, ubiquitous MFA consistent across the entire hybrid enterprise, and multiple Identity Provider (IDP) support. In the classic break-glass explained above, the legacy on-premises SAPM solution is inaccessible if the network is down. PIMaaS is resilient to your network outages, accessible to every valid user, anytime, from any device.

With that said, be careful of solutions calling themselves cloud. Some so-called PIMaaS products are not architected for the cloud; they are simply legacy code put on a virtual appliance and made accessible via a browser. This "cloud washing" is not only misleading, it will cost you more without inherent SaaS efficiencies and economies of scale.

Ensure your vendor has a single code base for both deployment options, built organically from the ground up for multitenancy.

Best Practice: A SaaS-based PIMaaS solution designed specifically for the cloud is best practice to support modern hybrid enterprise infrastructures and remote use-case scenarios. Avoid solutions that have been developed initially for on-premises and then fork-lifted to the cloud as this will result in major performance, scalability and license cost challenges.

For organizations using Active Directory, it's not best practice to mix employee identities with external identities. In fact, such organizations would rather not have to manage external identities at all. The SAPM solution you choose should support multiple directories to accommodate this. For internal users, this can mean Active Directory exclusively. However, a merger, acquisition or custom application may require authenticating some users against an additional, separate user store, and it may not be practical to enable trust relationships between them. For external users who are not federating (i.e., you are the IDP managing their accounts in your SAPM solution), then it's best practice to store those identities in a SAPM cloud directory separate from your enterprise directory.

Best Practice: Ensure your SAPM solution supports multiple directories such as on-premises Active Directory and LDAP, and a SAPM cloud directory.

As your remote and outsourced workforce grows,[1] [2] you will want a solution that is capable of supporting SAML-based federated login. With both sides being part of a pre-established business-to-business (B2B) federated trust and with SAML not transmitting any passwords over the wire, this approach significantly reduces your attack surface.

From a productivity perspective, your IT group no longer needs to manage identities for these outsourced partners. When outsourced users leave, your IT doesn't need to be concerned with cleanup or the risk of orphaned accounts, especially critical if regulated systems (such as PCI) are involved. This approach is also a productivity gain for the partner, giving its users single sign-on to your SAPM portal.

Best Practice: Ensure your SAPM solution supports multiple B2B federations to reduce your attack surface and bring productivity gains to both parties.

With IT functions being outsourced to 3rd party contractors, we need to be very careful about how to enable their access to our critical resources. The rule of thumb here is to NEVER give them root login to your servers! This may not be possible for routers, hubs, and switches, however.

For servers especially, only allow them to login via SAPM with a unique user ID and least privilege. Then, on the target server, they can request privilege elevation for specific admin tasks via host-based SUPM controls. Host-based auditing and session recording will tie every activity back to the real user for bulletproof auditing.

Many organizations disable remote SSH login with the root account. So, look for a SAPM solution that supports this and allows configuration of an alternative "proxy" account to login with least privilege and then privilege elevation on the server.

[1]According to Gartner, IT outsourcing will be a $335 billion industry by 2019 (Gartner, Forecast: IT Services, Worldwide, 2013-2019, 4Q15 Update, December 17, 2015)

[2]According to a December 2015 commissioned study conducted by Forrester Consulting on behalf of Centrify, 100 percent of organizations surveyed are outsourcing at least one IT function and at least one application development function

Best Practice: For outsourced IT, enable least-privileged login to servers via SAPM, then use SUPM to elevate privilege based on roles, record the session on the server, and leverage multi-factor authentication for identity assurance.

Of course, not every user who gains access to your resources is going to be legitimate. E.g., a "trusted" employee may go rogue. Having tools available to help in these situations can be invaluable. One such capability is Monitor and Terminate. For a user with the appropriate entitlements, it permits real-time monitoring of another user's activities along with the ability to terminate the remote login session if activities are deemed inappropriate.

Best Practice: Look for SAPM solutions that support watching a user's activities in real-time with the ability to terminate a session if necessary.

Secure VPN-Less Remote Access

A PIMaaS solution is a natural fit when supporting a remote IT workforce — a situation becoming all too common with IT resources travelling, working from home or being outsourced to 3rd party organizations. But of course, remote access introduces the challenges of securing such access. Traditionally this has been accomplished with a VPN. Implementing the VPN server and VPN clients on user machines, managing them, adjusting firewall rules, and opening ports is costly, exposes the network to risk, and impacts end user behavior.

A best-practice alternative is to establish a secure VPN-less connection to the end-point. In this way, the user and session are connected directly to the end-point without exposing the broader network to the user.

Best Practice: Ensure your SAPM solution does not expose the whole network by requiring a VPN for remote resource access but implements a secure VPN-less mechanism that puts the user right into the target server.

With this ability, note that you can extend this service to all users — privileged or not. SAPM would then manage the passwords for privileged shared account access while providing non-privileged users with an interactive login — with the convenience of a SaaS service through a highly secure VPN-less access mechanism.

Best Practice: Ensure your SAPM's secure VPN-less remote access can extend to both privileged and non-privileged users.

Application to Application Password Management (AAPM)

Plain text passwords embedded in script files pose a big potential threat. Attackers, bots, malware — they routinely trawl through such files looking for passwords to elevate their existing privileges and/or login to other systems on the network to expand their attack surface.

Following the SAPM advice above, store these passwords in a secure repository and give the script developer an API to fetch the password in real-time. All the attacker sees is an API call instead of a plain text password.

An added benefit to the script developer is lower maintenance and higher availability. The developer no longer needs to change script code whenever a password changes. The API call will always deliver the current password. This also means that the script will not break when the dependent password changes resulting in higher availability.

Many times passwords used in this way are rotated infrequently, if at all. This is due in part to the manual effort for an already busy IT. It's also due to having to update all the dependent script files with the new passwords and potentially breaking some business-critical service if a password was omitted. Putting these passwords under SAPM control obviates this issue.

Best Practice: Replace plain text passwords embedded in scripts with an API call to your SAPM service for better security and reduced IT administrative overhead

MFA Everywhere

Our best practices, if followed, will reduce your attack surface considerably by disabling login to accounts with privilege. Or, for those accounts that can't be disabled, placing them in a secure password store or authenticating with Kerberos credentials instead of passwords.

However, passwords will still proliferate and it's a matter of time before one is compromised. So another way to minimize your identity-related risk is by introducing multi-factor authentication. This should be a common service available for login to servers and cloud services, password checkout and privilege elevation. Then an attacker, bot, or piece of malware can be prevented from logging into a server since a 2nd factor will be sent to the legitimate user. This should be equally applied when checking out a password or elevating privilege to run a sensitive command on a resource.

Best Practice: Ensure MFA is available across all your environments for login to servers (especially for IT admins), password checkout, and privilege elevation.

Look for a solution that goes beyond MFA being a binary yes/no policy. It should be contextual, factoring in things like time of day, anomalous user behavior, or use of a trusted device. Don't force users down a path of 2nd factor authentication if (e.g.,) they're device is trusted, they're coming from a trusted domain/IP, and their behavior is consistent with established norms.

Best Practice: Ensure your MFA policy engine can factor contextual data into consideration to avoid forcing an extra factor on users where the risk is not sufficiently high.

Finally, your choice of MFA solution should be predicated on its ability to span on-premises as well as cloud environments. Vendors with a platform of common services that can be shared across solutions will provide you with a consistent MFA experience, centralized configuration and easier management.

Best Practice: Ensure your MFA, like your PIM, is sourced from a single vendor developed organically as a shared platform service that can consistently span all PIM solutions.

Solution Integration

It's even more important today with a hybrid environment to have a fully integrated solution that covers all the aspects of PIM described above. These capabilities will be layered throughout your extended IT infrastructure and as such, need to blend and integrate seamlessly, present consistent interfaces to operators and administrators, and consistently deliver on the promise of security, IT efficiencies, and sustainable compliance. With most PIM vendors partnering to complete their portfolio, you need to pay close attention to this.

Some key benefits from a single source are:

- **Minimal compatibility issues:** the vendor architects and designs their PIM solutions to work together, ideally off a consistent identity platform that bridges cloud and data center. Benefits include lower integration issues, more cross-application features, and faster feature update cycle
- **New features, sooner:** you have the infrastructure already in place to implement new products and features quickly from that vendor. For SaaS applications, this can be as quickly as 4-6 weeks
- **Short procurement:** finding a vendor you can trust makes it easier to onboard new products developed by them. Even if they license/OEM 3rd party technology to round out their portfolio, you're not guaranteed that same degree of quality
- **Faster time to value:** software from the same vendor provides consistencies—in UI experience, product integration, design approach, vendor interface, staff training, and licensing
- **Vendor accountability:** the old adage "one throat to choke" is incredibly important. One vendor, one phone number, one invoice, one trusted partner. The PIM vendor will never be as proficient with 3rd-party technology as the original developers. There will be painful dependencies for updates, integrations, support, and maintenance

Look for solutions from a single vendor, organically developed. They should be built off the same cloud-based identity platform, one that centralizes common capabilities and makes them consistently available to the solutions that build on it. Should you start with one and then adopt additional capabilities over time, they should all fit like pieces of a single puzzle, without incurring dramatic changes to operations, user behavior, or maintenance/support contentions.

Best Practice: Obtain your PIM solutions from a single vendor, one who has developed it organically versus a patchwork of homegrown + 3rd-party offerings to fill out their portfolio. Evaluate to ensure consistency, strong integration, and both on-premises + cloud support.

Conclusion

Organizational boundaries are perforating. Infrastructure and applications are balancing out across on-premises and cloud IaaS. New operational models are expanding, involving internal IT and outsourced services. The modern enterprise is a hybrid and will remain in that state for the foreseeable future.

Combating data breaches by securing access to your sensitive resources and data requires an equally modern approach to governing privileged identity usage and monitoring such use. Legacy on-premises solutions that simply manage passwords are insufficient. "Responding" to customers by fork-lifting such tools into a virtual appliance in the cloud does not satisfy all these modern requirements and exposes you to unnecessary risks and costs.

Best practices, a cohesive blend of host-based and gateway-based architectures, and new, innovative cloud-based technologies are fundamental requirements that enable IT and the business to succeed in a hybrid on-premises/cloud world where the attack surface is bigger than ever. They are the fundamental requirements of a PIM solution for the modern enterprise.

SANTA CLARA, CALIFORNIA	+1 (669) 444-5200
EMEA	+44 (0) 1344 317950
ASIA PACIFIC	+61 1300 795 789
BRAZIL	+55 11-3958 4876
LATIN AMERICA	+1 305 900 5354
EMAIL	sales@centrify.com
WEB	www.centrify.com