CORE SECURITY

Privileged Access Management

Technical Overview

CORE SECURITY

Table of Contents

Introduction:

The number of Request for Proposals (RFPs) for Privileged Access Management (PAM) solutions are increasing exponentially. Privileged credentials cannot be administered efficiently when most companies are having to manage them manually. Companies have been searching for a new automated way to manage privileged credentials, such as admin, root, SYS, and others, to ensure that these special accesses are properly protected. With the growing number of accounts, environments, and devices, manual managing is not enough anymore. PAM controls are in going from a "nice to have" to a necessity because of new corporate governance requirements, security regulations, and the need to eliminate "top threats".

Privileged Account Password Management Challenges:

Enterprise networks are constantly evolving. Employee access roles change often, making it difficult for your IT staff to keep all privileged accounts under control. Privileged credentials, computer operating systems, databases, and network devices are highly regulated, causing more confusion and obstacles when managing these accounts. In order to comply with mandatory regulations provided by SOX, PCI-DSS, HIPAA, FISMA, BASEL III, and others, your IT staff must have the proper tools to secure and monitor these accounts. Privileged identities must be detected and tracked at all times. Service and application account passwords must be safely secured and recorded. These passwords must be able to change on a set schedule without disrupting the productivity of the company. User access to privileged logins must be audited to meet corporate requirements. All of these steps are very difficult to accomplish effectively without an automated solution.

Lack of Controls vs. Manual and Automated Methods:

When recording privileged passwords, most organizations use Post-It notes, print outs, verbal or emailed passwords, and spreadsheets. Often, these spreadsheets are kept in file shares or drop boxes that are not properly restricted or secured. Having this information in a position where it could be easily infiltrated is a major security risk for the company and its accounts. Many companies use manual programs to manage privileged accounts. But without an automated program, full discovery and management is impossible. Manually managing these accounts takes away precious time from IT employees, and it fails to account for excess vulnerabilities that are easy for modern hackers to exploit. It is also increasingly more difficult to locate which privileged accounts are still accessible. Having a manual system for managing these accounts wastes both time and money while simultaneously exposing your company to excess security risks.

System Architecture:

A solution for an automated privilege account management solution should automatically detect and secure current hardware and software assets while still having the flexibility to handle not only mainstream hardware and applications, but also legacy and in-house applications that you support. It should also be able to handle changes on your network without having to use staff intervention or outside support.

Database:

All privileged account passwords and information should be encrypted and stored in a secure database. Ultimately, your database platform will determine the performance and reliability of your PAM solution. An industry-standard database can not only help lower your outgoing cost, but it will also make it easier for your IT employees to configure, secure, and maintain the PAM solution as a whole. Commercial databases like SQL Server and Oracle allow your staff to have several cost-effective programs. Use of these highly popular and well-documented database designs helps to eliminate “security by obscurity” risks, assuring that your IT staff has the proper resources and information to keep the application and network secure while still giving you options to deploy the latest encryption solutions. Utilizing these databases allows you and your staff to manage your PAM solution with your own in-house personnel.

Business Continuity and Disaster Recovery:

PAM software controls access to the most sensitive and important accounts. Because of this, it is crucial to configure both a solution for business continuity and disaster recovery. Search for a solution that has the ability to support clustered and mirrored deployments for higher availability. You should choose a deployment option that can support reliable database failover, and a PAM software architecture that minimizes single points of failure. For example, if the system hosting the PAM administrator were to disconnect or go offline, users should still be able to have access to their passwords. The most important thing is to choose a PAM product that is able to document the mechanisms that it uses to assure reliable access and operation.

Performance and Scalability:

PAM software has the ability to scale economically over many departments and systems to provide large cost savings should your company ever need to change. Also, your PAM solutions performance will not be impacted, no matter how much your organization grows. Ideally, you would want a multi-threaded application. This way your company is able to simultaneously change passwords on multiple machines in a reasonable amount of time. Also, it should be able to process simultaneous requests without decreasing productivity. To make sure that these needs are met, you must pick an architecture that can prevent and size-up fail-over and still increase performance. This architecture should be an n-tiered architecture. This way you have the option to deploy the password database, management console, web server, and reporting database on multiple machines. Your PAM solution should have the ability to deploy individual zone processors on remote machines to reliably handle password changes at distant locations and on multiple isolated (DMZ) networks. It should also have a console design and password change architecture, including a back-end database and highly tuned, multi-threaded password change algorithm. This should provide increasingly responsive console interaction and reporting even when processing large password changes across multiple devices and accounts.

Discovery of Systems, Accounts, and Services:

If your PAM solution fails to successfully discover your privileged accounts, this will quickly burden the IT staff and lead to expensive professional service contracts or another inefficient manual process. More importantly, lapses in coverage leave accounts exposed, including logins present in legacy software and applications, and make your network vulnerable to today's sophisticated and advanced hacking techniques.

Managed Targets:

When picking out a PAM solution, make sure that you look for in depth coverage of your present-day devices and applications, as well as a comprehensive list of popular management targets that help you scale for the future. Particularly, the solution you should look for would be able to reliably discover and change the largest range of privileged accounts. Good solutions include ones with Windows accounts such as named accounts, built-in administrator and guest, database accounts such as Microsoft SQL, midrange and mid-range and mainframe accounts on Linux, UNIX, Open VMS, OS/390, OSX, TN3270, and Network devices with privileged logins on Cisco, Foundry, HP, Juniper, NetApp, and others. It should also have privileged logins on out-of-band server management cards found on HP, Dell, and other IPMI compliant servers. Active Directory and LDAP-Compliant directory service accounts, privileged accounts used in web services, interdependent process and service accounts, and shared account passwords should be able to be maintained as well. Vendors who offer more thorough and out of the box coverage as part of their core PAM offering prove that their solution is designed for good adaptability and will be able to support a rapidly growing list of targets with each new release.

Discovery Techniques:

PAM solutions that can reach a broad range of system and account discovery techniques can give your company the flexibility to fix the solution once, with a minimum of interaction thereafter. Look for a solution that both adds and automatically tracks systems found in domain systems lists, network browse lists, active directory/other LDAP-compliant directories, scanned IP address ranges, and ODBC query results from configuration management database. Also, the solution should aid you in the process of importing many system lists from text files and in making ad-hoc entries through a management console.

Password Management:

Regulatory mandates like PCI-DSS, SOX, FISMA and HIPAA, and standards like IOC/IEC 27002, COBIT and BASEL III provide detailed instructions about password complexity, reuse, age, and other requirements. Your privileged accounts must follow these requirements in order to comply with corporate policies and industry or government regulation.

Password Change Policies:

With a PAM solution, you have the option to change passwords to static or random values that meet the general conditions you set. If you choose random values, they typically need to comply with corporate policy or regulatory mandates. Because of this, there should be easy to use settings that specify password length, the use of special characters, upper or lower case letters, and numbers. It is imperative to realize that different management targets such as hardware, databases, and applications can have varying requirements for secure passwords. It is very important that your PAM solution accommodates these differences and makes it easy to select the right settings. Your PAM software should also support the correct grouping of target systems so that it's easy to configure specific policies for different types of target systems and account designs. There is one area of password management that does not have many PAM solutions: password correlation and propagation. One of the most important characteristics of an effective PAM solution is its ability to automatically discover every location throughout the company where a privileged account is being used or referenced. This auto-discovery is critical for privileged credentials to be secured and maintained. PAM software should have the ability to manage simultaneous password changes to targets across your network to avoid potentially having any service disruptions or lockouts when changes are made.

Password Change Jobs:

A PAM solution should help make password changes more convenient for all team members. Also, it should handle situations in which failed passwords are reported or addressed. Basing your password changes off of systems, as opposed to accounts, allows you to upload new passwords on multiple machines at a time. This can help prevent the chance of with system failure. Once the new password changes have been set, the system routinely replaces them without operator intervention. A good PAM software has the ability to reset individual passwords or groups of passwords on demand. It should also have the ability to schedule automated checks to ensure that each password stored in the database matches the current login for each target account.

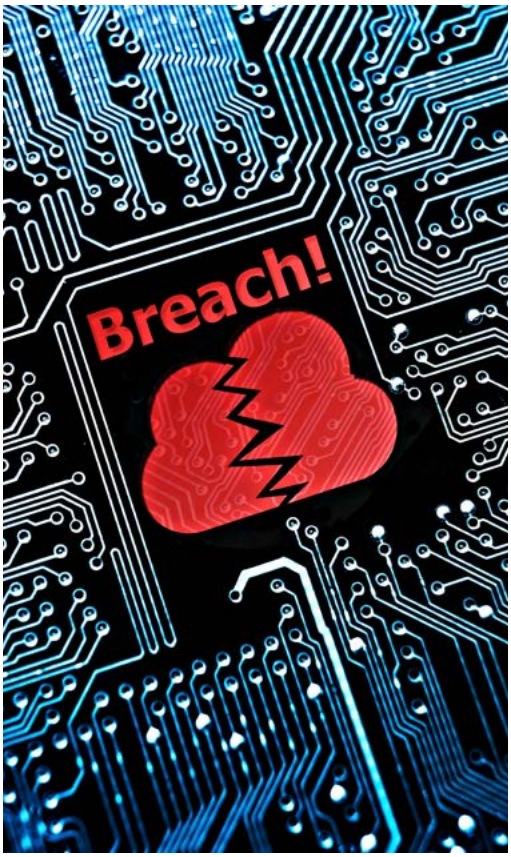
Password Encryption:

A great thing about PAM software is that it encrypts passwords in a backend database. Encryption options should include military-grade AES encryption, a FIPS 140-2 software encryption module, higher levels of FIPS 140-2 compliance, and support for Hardware Security Modules (HSMs) that use PKCS#11. The PAM solution should also be capable of providing for SSL encryption between its distributed modules, and between the web application and user machines, to protect passwords and other sensitive or private information.

Account Pooling:

Ideally, most PAM solutions have at least one to two failback mechanisms to prevent account lockouts should a password changes be delayed or prevented because of system downtime, network latency, maintenance events, and other conditions that prevent updating of all credentials in the proper order. Account pooling is a PAM feature that helps to assure reliable password changes. This particular feature gives you the ability to configure an account pool with any number of accounts when configuring a password change. Now whenever the job runs, it advances through the accounts in the pool in order. This leaves the previous passwords in the pool unchanged until it is their turn to be randomized and propagated again. Once these systems are configured, the systems that cannot be reached during one or more password change jobs can still have the ability to reference previous valid credentials from the account pool. This prevents service disruptions and lockouts that are triggered by network and system issues, even if target systems are unreachable on several tries.

Security Double Tap:



Pass-the-Ticket attacks can allow hackers to breach networks by copying tickets from the memory of a compromised end-user machine, or from a delegated authorization server. The moment an attacker gains sufficient lateral movement to steal the password hash of the krbtgt account on a domain controller, they could create unlimited Golden Tickets. These tickets, with virtually unlimited lifetimes. Fortunately, advanced PAM solutions have the tools and resources to remove Pass-the-Ticket access from compromised machines. One of these tools is called the Security Double-Tap feature. This changes passwords twice on potentially compromised machines, either on schedule or on-demand. This forces quick replication of the changed credentials within the domain to block the use of compromised accounts. Along with this process, administrators are able to optionally configure an automatic chained reboot of target systems to wipe out memory of hashes and passwords after a user escalation period is completed and after changes to the systems have been made using escalated credentials. These specific features now are able to rapidly remediate many different Windows systems, including end-user machines, delegated ticket servers, and Key Domain Controllers (KDC's).

SSH Key Management:

A very crucial feature for IT Security are SSH keys. These are used to identify individuals and applications on UNIX and Linux systems throughout corporate networks. Many datacenters are home to large numbers of SSH key pairs that never expire and can be reused in many ways. Because of this, SSH key management is critical for IT. Advanced PAM solutions need to have the ability to discover SSH keys present on UNIX and Linux systems, change the keys, and store away the new private keys in a secured repository. This solution provides automated workflows to connect authorized users to machines using the stored SSH keys. This gives users immediate and audited SSH access without ever disclosing a private key that could be handled or exchanged improperly.

Secure Application Launcher:

Advanced PAM solutions should always include a secure application launcher that allows users to have fast, audited access to any corporate application hosted on premise, in the cloud, or on any website. A good application launcher can grant immediate access to critical applications without disclosing passwords that could be shared among users or unknowingly disclosed to hackers. Having a secure application launcher allows administrators to always be aware of who has accessed corporate applications and at what time. The result is that the PAM solution can eliminate anonymous, shared access to in-house and cloud-based applications, corporate social media administrator logins, and other critical assets. If the application launch feature is designed properly, it also allows administrators to configure an unlimited number of new commercial, cloud, and in-house applications more easily. This assures that IT staff will not be locked into a fixed set of applications that were previously configured by the PAM vendor.

Access Management:

Any quality PAM solution includes role-based access controls. These map user roles (defined by your directory services) to groups of IT resources. Your personal PAM access rules can closely mirror your organization's policies. Whenever changes occur in your directory, your access rules should update in real time. Also, you are immediately alerted when you have activities that warrant your attention. An example is that you can configure an explicit account inside your PAM solution for subcontractor personnel, without providing these outside employees with domain credentials. This allows your subcontractors to access a small subset of your systems. Also, you should be able to grant access through a Remote Desktop/SSH connection that does not disclose any passwords. There should also be an option to grant your staff immediate, audited access to a particular group of servers for required departments or individuals to get explicit management approval before access is allowed.

Directory Authentication:

Your PAM solution should authenticate with trusted Windows domains, popular standards-based directories such as Oracle Internet Directory and Novell directory, and other LDAP and RADIUS servers in real time. It should also provide you with the flexibility to grant access to members of Windows groups, Individual Windows users, roles (as defined by your directory services), RADIUS users, or independent, explicit use rlogins that you configure in the product. As mentioned earlier, PAM solutions should be able to grant each role the ability to access all crucial resources, groups of systems and accounts that you define, or individual systems or accounts. Because you typically have the ability to create many levels of delegation within the PAM product, your best practice, in most cases, is to make permissions that are applied at the global level more restrictive, while granting broader permissions with rules that apply to explicit accounts being recovered. This will help ensure that data is secured. PAM solutions also allow for time-bound password retrieval that can force check-in and a password change after each access. This is especially critical for answering the question on "who had access at what time". And, this is also extremely essential for reliable logging, auditing, and controls.

Multifactor Authentication:

Having a privileged account fall into the wrong hands could ultimately end in disaster. Because of this danger, many of today's regulatory mandates (such as the Audit Guidelines) require people to use multifactor authentication when they request access. Look for a PAM solution to support all of the time and event based methods that your organization might adopt. These include out of band authentication, such as Time-based One-Time Password (TOTP), that requires nothing further for your organization to buy. Other methods that your organization might adopt include OATH authentication using third-party tokens or out-of-the-box support for proprietary tokens including RSA SecureID and YubiKey. Using multi-factor authentication can aid you in safeguarding your organization from common hacker exploits. An example of this would be an organization that recently fell victim to a hacker posing as an executive. This could have prevented data loss by purchasing an inexpensive out-of-box multifactor authentication using email or SMS delivered to IT staff cell phones.

Workflows:

It should be easy to configure workflows that quickly provide authorized users audited access to privileged credentials, from any location or time, while simultaneously automating the approval steps to increase the efficiency of your team. Your new solution should make sure that you can configure checkout rules for each user role. For a group of critical accounts, take accounting for example, you might want to be notified if their specific IT manager requests access. You might want to require all other personnel to get explicit approval before gaining access. Workflow capabilities should always allow all users to be able to request access and for managers to grant access within the system that is both easy to use and easily monitored.

Help Desk Integration:

In order to augment security and save staff time, your well-integrated PAM solution works in concert with your Help Desk software. Help Desk integration should prove that all privileged password check-out requests originate from valid trouble tickets, guarantee that all requestors have been configured for the requested level of privileged access, and automatically update trouble tickets to reflect activity within the PAM product. These solutions will help to create Help Desk tickets from within the product when unexpected events such as failed logins occur. Search for a PAM solution to help major Help Desk systems such as HP Service Manager, BMC Remedy, Microsoft System Center Service Manager and others.

Usability:

Your PAM solution should have the ability to raise the productivity of IT staff, Help Desk personnel, and anyone else who uses the product by being able to access privileged accounts for routine administrative duties and emergency repairs. In order to reach this goal, the software should have:

- An effective and intuitive user interface that is able to quickly authenticate users with their domain logins or other credentials
- Present privileged passwords to authorized employees in very few clicks, and allow access on the go in an encrypted Web Session.
- The ability to provide varying views and options depending on the user's role.

For example, displaying only those systems and accounts configured for access to each end-user, and presenting delegation and reporting features only to those administrators who are allowed access. It is also important that it has the ability to present systems and accounts in ways that make it easy for users to drill down to the resources that they want to access and the ability to make it easy for contractors who may not have the domain logins to access the solution.

Auditing:

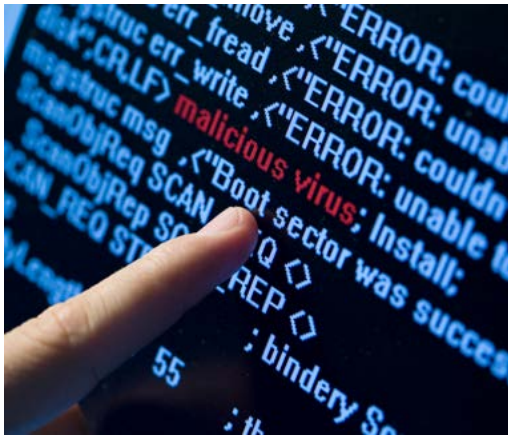
It is very important to have reliable auditing coverage with any PAM solution so that the software can support a variety of methods to record and audit any action that it performs. These actions include text-based application logs, an internal auditing database, application Syslogs, email notifications, and integration with outside frameworks using tracks for SNMP, Triggers for Microsoft System Center Operations Manager, and others. The system should record access to the Web console for password requests, approvals, check-out delegation changes, reporting and other tasks.

Alerting and Integration:

The main goal of your PAM alerting features is to make sure that you and others are allowed to take appropriate action as soon as important events occur. The solution must be configurable. This ensures that events can trigger email alerts, run specific programs, and communicate with trouble ticketing applications, SIEM solutions, and other frameworks. It should be capable of alerting on actions such as password requests and check-outs, password changes, failed password change jobs, console and web application activities, and others. Along with the out-the-box integration with popular Help Desk and SIEM frameworks, look for the solution to provide an easily configurable process for integrating with virtually any provisioning database, security framework and other security applications. Any integrations that are not provided out-of-the-box should be easy to implement with minimum effort.

SIEM Integration:

Alone, SIEM applications lack the ability to correlate security events with human and automated actions that use privileged credentials. Because of this, the integration of your PAM solution and your SIEM framework can eliminate a critical blind spot in your security framework by tying individuals and processes that have privileged access to the security events that they can trigger. Out-of-the-box integration with leading SIEM frameworks such as HP ArcSight ESM, RSA envision, and Q1 Labs QRadaris are an important consideration when choosing a PAM solution, as is the ability to easily integrate with other platforms.



Reporting:

An ideal PAM solution should provide a large range of preconfigured reports that help you monitor the performance of the application, ensure that security and compliance requirements are met, and supply business intelligence to assist with your daily operations. The solution should also allow you to create custom reports using popular third-party reporting tools such as Crystal Reports and SQL Server Reporting Services.

Reporting Architecture:

Use of separate data warehouses, whether configured as an additional database on the same server as the PAM solution or as a database on a different machine, can help insure responsive reporting regardless of the complexity of the report or the size of the PAM installation. When you configure a separate data warehouse, you can assure that archial, data segmentation, replication, and reporting data growth can be more easily accommodated over a period of time. Most importantly, a data warehouse model allows for structured, minable data that remains completely segmented from encrypted account passwords.

Compliance Reports:

PAM solutions should provide already configured reports that make it simpler to prove compliance with important mandates such as SOX, PCI-DSS, HIPAA, CAG-12, BASEL III, and many others. Your PAM solution should allow ad-hoc reporting and the collection of reporting data that follows a schedule that you can customize. When using either the administrator console or the application web client, authorized personnel should always have access to these reports. These reports present the PAM solution's activities as a whole are often used for compliance reporting. These have the ability to include reports of all systems that are managed and unmanaged, reports of stored passwords and their status, reports of all passwords changes, reports that show activities done by selected accounts, and reports that show activity for selected users.

Operational and Business Intelligence:

Your PAM solution should provide the reports you need in order to meet your compliance requirements while also giving you other actionable business intelligence. You are able to gain business insight from reports that tell you about password requests, password check in and check out, delegation change requests, and others. When combined with information from preconfigured compliance reports, your PAM solution should be able to answer questions such as:

- "What were an employees actions in the 30 days before he left his job?"
- "Which of our systems had the most administrative login activity over the last 30 days?"
- "Which of our systems have highly privileged, orphaned accounts that may be present because of personnel changes or other activities?"
- "Which of our systems have privileged accounts that may use vulnerable default logins?"

Ease of Deployment and Operation:

While the need for a PAM solution is clearly evident, is it hard to justify the cost of a month's long implementation. You should have the ability to deploy well designed PAM software in a matter of days, with minimum outside professional services intervention. Also, your ongoing market burden for the PAM solution should also be minimal. The operation of your PAM solution should be self-sustaining, requiring very little administrative involvement.

Configuration vs. Customization:

Your PAM solution should be as easy to configure as it is to implement. You should expect drop-down menus and dialog boxes to enable easy configuration at all places in the product. The same vender-supported code base should be sent to every customer and it should be able to be simply configured for your specific, even complex purposes. You should not have to customize your PAM solution as a one-off implementation since this could multiply your future costs and complexity of updates and security fixes. Also, configuration should not require expensive professional services. Expect your PAM solution to only take days or hours to configure. To prove that your organization achieves a positive return on its software investment, look for a PAM vendor who can:

- Provide references with deployments that are comparable in size to your own.
- Has a detailed, written analysis of your organization's business goals
- Has a detailed documentation of your needs with respect to systems, applications, and lines of control
- And has a statement of work that details the time and cost required to bring unsecured privileged accounts present in your target systems and applications under control.

Implementation Plan and Project Timetable:

Your PAM vendor should provide a firm cost proposal and definitive, realistic project timelines for your implementation services. These services should include any specialized preparation of your host systems and network environment needed for the deployment, configuration of disaster recovery and high availability options, planning and configuring workflow and role-based access controls to align with your organization, and help to create any specialized reports that may be needed to meet compliance or operational objectives. You should always expect your full project to be completed, and the PAM solution should secure all of your required management targets, within a few weeks.

Proof of Concept:

As a part of your selection process, you should consider your PAM software's vendor and you should make sure it includes proof of concept that covers all of your hardware platforms and a realistic sampling of your essential applications. For each platform and application, you must make sure that you document what capabilities your staff can deploy unassisted out-of-the-box, what capabilities need a vendor's professional services, and what capabilities are not delivered at all. You must be aware that marketing checkbooks often lie. This is essential to remember when proceeding with your evaluation. Cleverly written marketing pieces can suggest that a product's capabilities extend to all areas where the vendor claims coverage, and salespeople often believe this false hype. Make sure that you ask very explicit and specific questions, both of vendor's engineers and reference customers, about how individual target platforms, managed applications, and use case scenarios are configured and deployed. In each case, was the vendor's capability delivered out-of-the-box, only through custom development, or never at all?

SDK:

Because every IT environment is considerably different, an important consideration to make is the ability of your PAM solution to manage and operate reliably with the systems, applications, and devices that are unique to your enterprise. Your PAM solution should offer a Software Development Kit that can address corner cases, using API's available for virtually all platforms to allow real-time, programmatic access to passwords. The SDK allows applications and individuals to access the password store independently, without using the product's original interface. The main uses for the product are its ability to:

- Improve the security of your in-house applications and scripts
- Programmatically update account information in the password store
- Programmatically enroll systems in the PAM without waiting for group updates
- Replace clear-text passwords embedded into applications with secure retrieval from the encrypted data base
- Programmatically manage the entire Privileged Access Management lifecycle via any language or platform.

Maintainability:

Look for a PAM solution that has open documentation. This means that it is open to everyone online. This saves long-term costs for your organization because it includes product upgrades with your cost of support, and upgrades that install quickly.

About Core Security:

For more information on how Core Security can help with your Privileged Access Management needs, contact us.

Core Security

678-304-4500

info@coresecurity.com