WHITE PAPER

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

What is Privilege Management and Where Do You Start?

A Non-Vendor-Speak Guide to Privileged Access

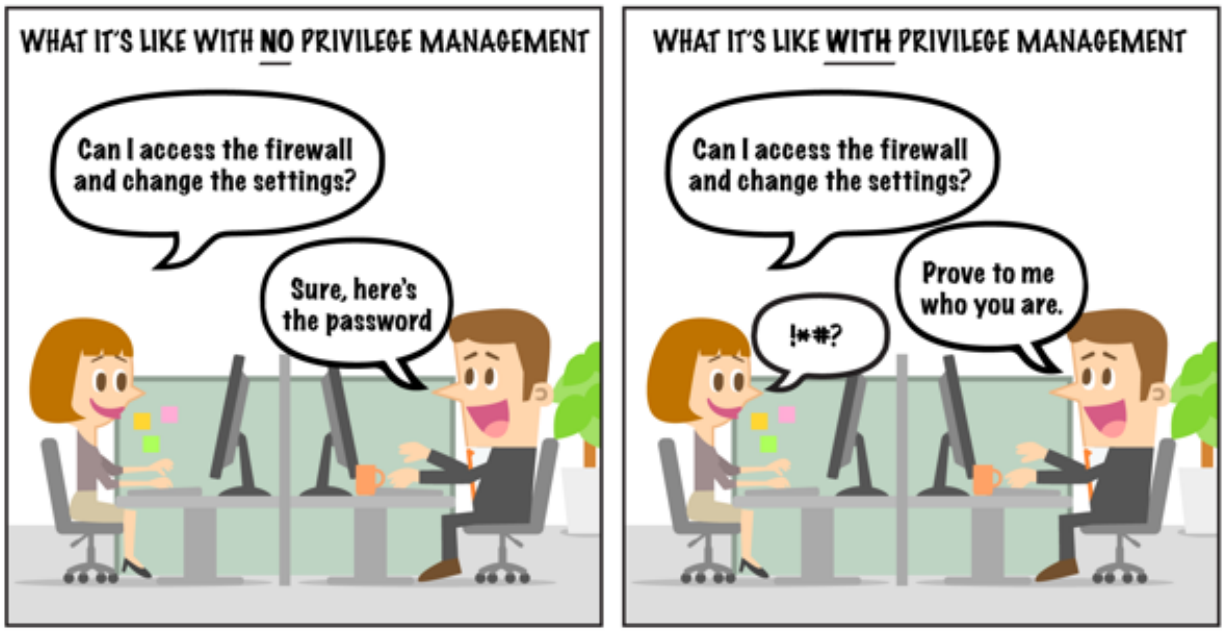
Scott Carlson, Technology Fellow, BeyondTrust

Contents

Protecting Your Company's Secrets

Before we start, let's get something straight: I work for a cyber security vendor. Now, I haven't *always* worked for a vendor; in fact, I have extensive experience designing and running privileged access management and identity management programs for several companies. So, I promise I won't try to sell you anything here. Just had to get that out.

It's probably a safe presumption for me to make that we all have possessions and stuff that we consider important – our residences, our personal details, and our money, for example. And, because this stuff is important, we should be keen on controlling who has access to it.



Thinking about the concept of "privileged access," within the context of company is no different. Directly relating it to personal decisions, you should ask four questions:

1) What is my stuff, and who do I trust to have special/privileged access to my company's stuff?
2) Why should I trust them?
3) How do I make sure that they can maintain my trust?
4) What action should I take if that trust is broken?

HOW PRIVILEGED ACCESS MANAGEMENT RELATES TO DATA BREACHES

The size, scope, and impact of security breaches continues to escalate. Through the media, we seem to learn of a continual stream of data security incidents so that it now seems almost routine when we hear that hundreds of millions of user accounts have been stolen, or that hundreds of organizations have had their data breached. The reality is that the government has even lost information equal to the size of the population of the United States. Everyone is

touched by these breaches in some way, and, at the very least, it feels quite unsettling. The average person doesn't know how to stop a data breach and, honestly, many companies don't know how to stop a data breach either.

In many data breaches across 2015 and 2016, attackers exploited the login accounts of employees or contractors to gain unauthorized access to sensitive data. Clearly, data exfiltration, or other damage incurred due to theft of login accounts and other break-in events, is unacceptable. However, despite the pervasiveness of such breaches, sensitive login accounts, credentials, passwords, and detailed access patterns can be largely controlled if you take a few steps to understand your corporate environment and then design/build an appropriate privileged access methodology/process framework/security framework/workflow/tool deployment/script tailored to it. At the end of the day, you need to do SOMETHING, and that SOMETHING is likely unique, but considerably "pattern like", between different types of entities.

This white paper will introduce ways that will help you control the privileges that users have within your environment, reduce the surface area against which you can be attacked, and educate you on tools and methods that can help you protect your critical assets from all but the most sophisticated attacks. Let's get started.

Remember:

There is no silver bullet.

But, there IS a way to quickly make progress

Roles at Your Company

Within your company, you have people and computer systems that have a normal operation, operations that are special/privileged, have the ability to change things important to you, or are important to the continued operation of your company. Within each of these layers, there are jobs people are supposed to do, a job that people have the ability to do--but shouldn't, and special roles and responsibilities that have "special purpose" to your business or computer operations. These special roles and responsibilities are considered "privileged," and some examples are:

- Your security guards have privileged access to every room in the building for monitoring purposes.
- Your security team has privileged access to the server environment in order to conduct forensic operations against your servers, with employees, or against external attackers.
- Your HR department has privileged access to employee data so that they can help employees with their life events, such as getting paid, having a child, or obtaining insurance.
- Your server team has privileged access to create, destroy, and make servers function.
- Your data/database team has privileged access to your most sensitive data.
- Your finance team has privileged access to your banking application to execute wire transfers to other people or companies.

CRITICAL QUESTIONS TO ASK WHEN "TRUST, BUT VERIFY" ISN'T ENOUGH

So, how do you safeguard your company and its data when there are so many people who enjoy special/privileged access to the organization's most critical data? You could put blind faith in them, or you could periodically check-in on what they have done. But, when money or data has been stolen, following up on activity months later is simply inadequate. Best security practice calls for enforcement of least privilege to manage access, protect against inappropriate privileged operations, and immediately act against abuse. You understand the best practice, but how do you accomplish all of that?

Let's start to slice your company into a few keys layers that you as a leader should understand. It doesn't matter if your IT operations are insourced or outsourced, you must be able to answer these questions and point at an accountable person in your company that, "has this under control."

As we unveil the layers, you need to consider these questions:

- Do I roughly know where my most critical business information is?
- Do I know when someone doing work for me switches from being a normal user to a privileged user, and do I know where he/she is performing this action?
- Do I know that administrators of my systems have the minimum access required to do their jobs and that their managers have assured/attested to that fact?

- Do I know how many computer systems we have, and who manages each of them?
- Do I know what, "normal operation," within my environments is? What network paths can users follow into my company, what network paths leave my company, and where does data flow during normal business processes?
- Even if it is a manual process, do I know that my teams can quickly create or remove an account from my networks or systems?
- Is it "too easy" to leave my network with our data?
- Is it "too easy" to access systems that have critical data on them?
- Is it "too easy" for systems to get infected with malware and begin full compromise of the entire network?
- Would my team detect when accounts are acting erratically?
- Is anyone showing me data that isn't so high level that it's actually telling me what my risk is?
- What does, "Red Alert," mean to me if someone were to break in and misuse account information-- does my team know how to react to this?
- Do my employees understand what they need to access versus what is convenient to access?
- Do my human resources personnel have the minimum access they need to perform their jobs?
- Do I know what I am monitoring, and what I am NOT monitoring?

If you already know the answers to these questions, you are probably in the most mature 1% of companies in the world with regard to information security governance. Congratulations!!!!!!!!! Those 1% of you can stop reading and go play some golf. The rest of you… stay with me here.

Moving on, lets segment your environment into some conceptual areas and walk through the areas that you should consider when building out a privileged access management (PAM)—also known as Privileged Identity Management (PIM)-- program and layering it on top of your systems, business operations, and data center.

Building Out a Privileged Access Management Strategy

In the industry, we call building and executing on your strategy a PIM/PAM project. No matter what you call it, it is still the concept of developing definitions, implementing rules, and executing the ongoing management of the privileged decisions, rights, roles, groups, entitlements, and passwords that some users in your environment have.

We will break down a sample environment into four major swaths so that we can conceptually explain what types of PAM/PIM use cases you need to work through to build your program out and execute it for real. Most companies on the planet have these types of roles and they should all agree with the concept that they are trying to implement so that they can use tools to enforce controls which enable behavior.

In my view, REQUIREMENTS define CONTROLS you need, and TOOLS enforce those CONTROLS where they need to be enforced, but monitor them where they just need to be monitored, but not directly enforced.

Control Layers

At any large enterprise, there are likely tens of thousands of employees, tens of thousands of computers, hundreds of applications, and thousands of different employee roles.

If you go into your privilege management project with the thought that you need to figure out how to map thousands of roles into tens of thousands of assets, you will lose before you even start.

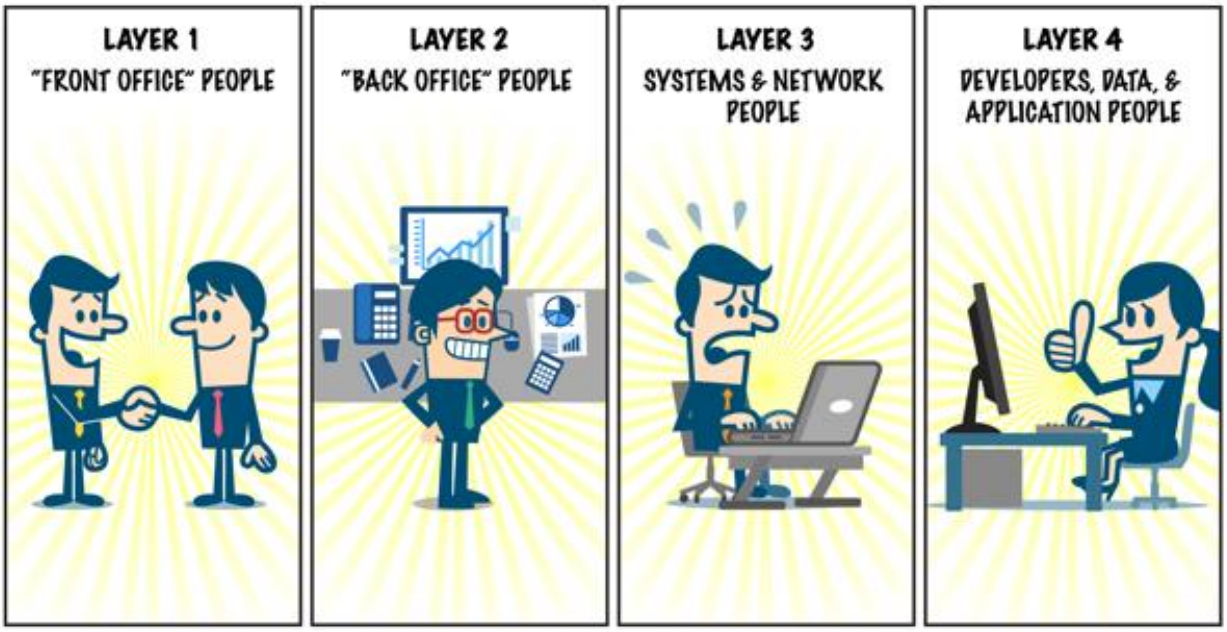
This is why it is more useful to break down a first phase of this project into a few major layers of the environment, and a few major layers of job functionality. I do not believe that doing an extensive role mapping exercise is the place to start. When you run out of actual security work to do, you can go back and re-map roles to see what you might have missed to tighten it up a bit.

This documents' philosophy on privilege management is that you should always start by covering the widest swath of the 85% right away, work hard to do the next 10% as soon as possible, and then continuously work to close the last 5% while maintaining the first 95%.

It is crucial to show progress on a project like this in order to keep the attention of management. **Privilege management is NOT a project; it is a journey**… it is a future way of life. Once it works, you must maintain it forever. This forever maintenance is why you should consider tools and technology to help you, otherwise you could simply hire people to execute a project against a timeline and be done.

Let's now break down the people into four representative groups:

- Layer 1 – The "Front Office" people
- Layer 2 – The "Back Office" people
- Layer 3 – The Systems and Network people
- Layer 4 – Developers, Data, and Application people



Throughout this section of the paper, I'll provide a checklist of items by layer for you to consider. Evaluate yourself on these items; they will reveal your gaps.

LAYER 1 - THE "FRONT OFFICE" PEOPLE

In the, "Front Office," are folks who provide customer service, answer the telephones, or provide a set of services that change only when you want a business process to change. For the front office, your goal is to provide a set of standard computer systems and applications allowing people to do their jobs. These workers should never have permissions to change their systems or applications, or to install software. This group follows a defined set of processes and procedures, and if they access customer data, they likely only touch one or two records at a time. Sometimes these front office workers run reports, but the data is in a read-only form and, in almost every case, large data extracts are not permitted. From a privilege management standpoint, you would want technology that implements the following concepts:

- ☐ Remove all administrative rights from the workstations for these resources or replace workstation with a thin client.
- ☐ If there are legacy software solutions in play that require administrative rights within the operating system, add local software agents that allow the escalation of the privilege of those programs, while giving the user full administrative rights to the rest of the system.
- ☐ Remove the ability to install or modify software, especially from the internet.
- ☐ Remove the ability to log-in via VPN, remote email, remote geographies, or to your data center via administrative ports, depending on the makeup of the workforce.

- ☐ Enable screen or keystroke recording for any system or application target where users would need to connect and perform operations that are considered privileged. This is most often done via local software, or by having users connect to a reverse-proxy or jump host in front of the target system or application.
- ☐ Within applications, apply least privilege—that is reduce the rights of the employee to the minimum possible entitlements for them to execute their given job. Work toward a model allowing people to run single privileged actions, commands, or updates without opening up every privilege.

Total: _____

LAYER 2 - THE "BACK OFFICE" PEOPLE

In the "Back Office," are folks who may provide advanced financial analysis, perform business process work, conduct money transfers, write checks, or work with large data sets. These employees might lack access to the systems themselves, but they likely have access within applications. These are the experts in business processes, and the people and application administrators you trust enough to give them rights within that application, as well as to supervise others who have access to the data or financial transactions that can impact your company. From a privilege management standpoint, you would want technology that implements the following concepts:

- ☐ Remove all administrative rights from the workstations for these resources – see above.
- ☐ If there are legacy software solutions in play that require administrative rights within the operating system, add local software agents that allow the user to escalate privileges to run those programs--but not have full administrative rights to the rest of the system.
- ☐ If there are custom "fat clients" needed by the users that require updating, or must be installed individually, use privilege management software to give users the ability to install software from a trusted repository, or to download software from trusted web sites on the internet. You could choose to trust a directory, application, or certificate authority.
- ☐ Remove the ability to install or modify software, especially from the internet on the local workstation unless that software is validated as safe by publisher or by security scan.
- ☐ On target applications where the user is executing highly privileged operations, deploy session recording and monitor for inappropriate behavior, such as conducting a transaction that is unexpected, or working with applications the user has not accessed before. You want to track the source, destination, time of day, operation executed, and file movement operations.
- ☐ These users should have two or more accounts. Each individual should have an unprivileged / standard user account that he / she uses to log into his / her workstation, and the user should also have an application administrator account to perform highly privileged operations. In the case where a single sign-on solution is used, you might want to consider

using multiple authentication providers to hide the fact that the user has multiple accounts. But, in reality, a user might have one account per system that he or she is accessing.

- ☐ If these users have privileged access to download large data sets onto their workstation, you must add other technologies to ensure that these data sets do not leave the workstation.

Total: _____

You can see from the first two layers that we have focused primarily on business users who need to consume and work with data, or directly execute against business processes. They almost never need to directly change the technology that they are given to do their job, which is why we can remove the need to have system level administrative rights in almost every circumstance. There's a great side effect here, in that helpdesk costs may be reduced significantly because users are unable to harm their system by pretending to be IT people or by installing software that THEY like better.

LAYER 3 - THE SECURITY, SYSTEMS, AND NETWORK PEOPLE

Your systems and network people provide a specific function--they perform critical administrative functions against your computer systems, desktops, networks, and data centers. These workers possess the "keys" to your data center and must obtain the highest level of administrative rights on the technology they are supporting during build operations, break-fix operations, and, for your security team, forensic operations. Even though these users have full access to system resources, they very likely should never need to look at the actual data present, so they likely do not perform the same business level functions as the front-office and back-office job roles.

From a privilege management standpoint, you would want technology that implements the following concepts:

- ☐ Remove all administrative rights from the workstations for these resources.
- ☐ If there are custom "fat clients" needed by these users that require updating or that must be installed individually, use privilege management software to enable users to install software from a trusted repository, or to download software from trusted web sites on the internet. You could choose to trust a directory, application, or certificate authority.
- ☐ If these users must test new software solutions, prohibit them from performing tests on their corporate workstations. In many cases where an environment is in-scope for PCI compliance, these administrator workstations are also in-scope due to their ability to "touch" the systems within the data center. Allow these users to perform testing and proof-of-concept installations within a development lab or in a segmented cloud environment.
- ☐ These users must have multiple accounts per environment. Best practice would dictate that they need accounts per environment with special/segmented administrative rights different than their normal account.

- ☐ Insert a jump host between these users and any privileged device or network segment they need to access, especially within a regulated environment. Use this jump host to log them into target systems and record all of their activity so that you can report on it and track their actions. Screen recording isn't enough, you should also record the keystrokes and clicks so that you can do micro-analysis of the behavior.
- ☐ Rotate the passwords of these accounts and ensure each account has a unique password.
- ☐ Do not let any of these users share accounts with their peers. If a shared administrative account needs to be used, only access the account through a password manager that manages and rotates the password when done.
- ☐ In highly-secure environments, limit the server and network targets that these users can access and utilize localized agents to limit the commands that can be executed on the host itself. It is not sufficient to just limit who can get to root, sometimes you want to execute what root itself can type without secondary approval.

Total:_____

LAYER 4 – DEVELOPERS, DATA, AND APPLICATION PEOPLE

Developers, data, and application staff provide administrative functions to your business software, and almost always need direct access to real customer data or program source code. They need access to this data to provide business reports, write better systems, update incorrect data fields, or write software. While it's likely that these users lack access to the underlying servers, they can modify software or change the way software functions. They nearly always have access to critical data to do their job.

In the case of developers and other folks who can change the actual software, you have to consider the environment in which they build, deploy, and then release the software to be used by the end user. For data scientists and other types of data people, there are multiple environments where the data warehouse might live, and then parallel environments where mathematical and operational models are developed against a subset of the data. You always want these people to work against a representative data set, but not have the ability to leave WITH the data set.

From a privilege management standpoint, you would want technology that implements the following concepts:

- ☐ If these users must test new software solutions, create code, or run data analytics, best practice dictates that you should create a development or testing environment from which users perform these actions, rather than on their workstations. A workstation (especially mobile) is an untrusted environment that is vulnerable to hacker or malware threats. If you absolutely must allow the users to do things locally, lock down the machine in such a way that users can only install software from trusted web sites, or trusted repositories. You can acknowledge that these users must download the latest libraries, but make sure that you

scan them and authenticate the most trusted repositories, OR, have a master internal repository where someone scans and validates software that is to be used by many.

- ☐ For each of the actions that require moving data in bulk, or where repeated automated actions are taken by these users, store passwords for robot accounts in a password safe and require your users to code operations by checking in and out the passwords necessary to do this movement. This way, you can always ensure that access does not leave with your user.
- ☐ When accessing data or moving code to production, require these users to utilize a separate administrative level account and track their operations through use of a jump host or session recorder (similar to what you should be doing with system administrators).
- ☐ In the scenario where development folks are also on-call following the release to production of their code, the developers could end up with a regular account, development account, and then a privileged production account that only has access to a specific set of servers that they need to access as a support tech.
- ☐ In the case where data analysts need to spin up and down environments or access a data warehouse, ensure that they have separate analytics accounts that access the data through a jump host so that you can track their activity against the data. Your main objective is not to obstruct the users from looking at the data or performing their duties, but to prevent data theft or leakage. You may want to create a production-like environment for the purpose of developing new operational models that is not exactly the production data itself, but is supported in the same meaningful way.

Total:_____

INFRASTRUCTURE AND DATA CENTER GEAR

We've talked a lot about people and the privileged access they have to the environment through their various accounts, but what about the systems and data center gear residing within your facility or your cloud environment? While not necessarily a "role" per se, these systems require the same controls. This gear comes with administrative built-in accounts, and physical access to this gear often gains access to a direct console. This gear might not have access to the data itself, but a comprehensive program must also protect against availability threats and destructive events. As information security gets better at monitoring operations, attackers may just choose to shut down your entire data center because you didn't adequately protect the UPS or the power strips As the use of internet-connected (IOT) devices increases, your devices may have embedded things that are uncontrollable. With that said, apply the following set of practices against the infrastructure itself:

- ☐ Always change the default passwords of everything.
- ☐ If you connect your power strips, UPS, lights-out, consoles, and other management gear to your network, connect it in such a way that it can only be accessed through a multi-factor jump host that records all sessions.

- [ ] Never allow the internet to connect directly to any devices that provide controls or management infrastructure within your data center without appropriate multi-factor controls and effective network security controls.
- [ ] Physical access to gear should always be camera-recorded and appropriate physical access barriers should be in place.
- [ ] A network connecting any console-type devices should always be on a separate management network that is air-gapped from the regular production network.
- [ ] A separate set of accounts should be used to access consoles. The device passwords should be managed and operated out of a password safe that controls who has access and when they can access, and automatically rotates the passwords. For highly secure operations, a session manager can be used to automatically enter the password (while never revealing it) for the user. This allows you to leverage very long and nonsensical passwords.

Total:_____

What to Do Next

You can see some patterns to each of these use cases, including:

- Always remove administrative rights from user accounts on operating systems.
- Always change default passwords--**always**.
- Require administrative users to use a second account to access privileged systems or privileged applications.
- Always use a jump host or session recorder that users rely on to access privileged environments to remove the ability for an attack or malware to compromise your whole company.
- Always record behavior against a highly privileged application, database, or system.
- Always prohibit the installation of software that hasn't been certified, especially on critical systems, or systems of staff that perform critical business operations.
- Use a password safe to store the password to your critical systems.
- Remove access to systems or applications when the user does not need it.
- Limit the commands that can be typed on highly sensitive/critical systems, especially when multiple types of users need to directly access the system.
- Centralize administration of all of this!

Throughout this paper, we've discussed a number of concepts to consider as you build your privileged access management program. Remember that this is a lengthy journey, and unless you are building a company from scratch, you will need to communicate to people, purchase software/hardware products, and change behavior. This all comes after careful planning, use case development, and following best practices. As you start to lock down your environment, you will make it incrementally more difficult for insiders and external attackers to perform improper operations against your company. You will never be 100% secure, but by employing these strategies, you can mature your security posture to the point where attackers will have to try harder than ever--expending considerable resources and energy---to break in… or just move on to the next target.

Good luck in your journey.

Appendix: Glossary of Terms

Here is a list of terms and definitions I referenced in this paper (and many related to PAM and IAM that I didn't reference.)

A

Access Management – Access management is the process of managing a user's login and access across a wide range of applications, systems, and resources belonging to an organization. Most IAM solutions manage user access to resources, but leave access authorization decisions to the application owners.

Attribute – Small pieces of information that make up a digital identity. Attributes may include name, phone number, group affiliation, etc.

Authentication (AuthN) – Authentication is the process of validating an identity, whether it be the identity of a user or, as in the Internet of Things, a device. The classic method of validation is the username/password combination.

Authorization (AuthZ) – Authorization is the process of determining whether or not a user has the right to access a service or resource, or to perform an action.

Authorizer – An individual responsible for approving changes in user authorizations and privileges.

B

C

Compliance – In IT and data storage terminology, compliance refers to organizational compliance with government regulations regarding data storage and management and other IT processes.

Credential – A credential is an item, such as an ID card, or a username/password combination, used by persons or entities to prove themselves.

D

Data – Any information stored by a computer.

De-provisioning – The removal of an individual's organizational digital identity, access, and privileges.

E

Event – An action, or the result of an action. Events are often logged and monitored for security purposes.

F

G

Group – In identity management, a group allows the management of multiple entities i.e. employees or customers) within a single category. Groups are used to define roles and simplify access control.

H

I

Identification – Identification is the process by which an entity's information is gathered and verified for accuracy.

Identity and Access Management – Identity and Access Management (IAM) is a system, solution, or service that addresses an organizational need for a system-wide solution that manages user's access and authentication into external and internal applications, databases, or networks.

J

K

L

Least Privilege –Least privilege is a cornerstone IT security concept that pertains to restricting access rights for users, accounts, and computing processes to the minimal amount necessary to perform authorized activities.

Log Files – Log files are files that record either events that occur in an operating system or software, or messages occurring on communication software. For example, when a failed login to an E-mail system occurs, a log file is created to record that event.

Logging – the act of keeping a log for an extended period of time.

M

Multifactor Authentication – Multifactor authentication adds an additional step (or factor) to the authentication process, typically by pairing something the user knows (such as username and password) with an action, or something the user has(such as an SMS message to their phone, an email, or a token).

N

O

Off-boarding – The process by which a user is removed (with access revoked) from an organization's IAM system.

One Time Password (OTP) – A password that is valid for one use or session.

P

Password – A word or string of characters used to prove one's identity, or authorize access to a resource. Usually, but not always, paired with a username.

Password Safe – A mechanism for the secure storage, rotation, and monitoring of privileged credentials (passwords). Formerly known as a "store," or "vault."

Password Reset – The process by which a user changes their own password.

Privilege – A privilege is a construct that allows certain users within an organization to have a number of powers based on their credentials and identity attributes.

Privileged Account Management (PAM) – See privileged identity management.

Privileged Access Management (PAM) [also Privileged Identity Management (PIM)] – Privileged access management is a process or technology focused on managing, monitoring, and protecting powerful privileged user accounts within the IT infrastructure of an enterprise.

Privilege Management – Privilege Management is the process by which the owner of a network can modify or assign privileges for applications and resources.

Privileged User – A user possessing specific security privileges and entitlements.

Provisioning – A process that enables users to use their privileges to access applications and services.

Q

R

Requester – A person who requests a change in user profiles, privileges, or entitlements, either by an automated or manual process.

Role – An identity attribute that gives users automatic privileges when assigned. Roles may take the form of groups wherein all members of a group have the same set of privileges.

Role-Based Access Control (RBAC) – A model in which users are assigned "roles" that give them a certain level of access to resources and systems. Assigning a role to a user grants that user a certain set of privileges and entitlements.

S

Self-Service Password Resets – A self-service password reset is a process that allows users who have forgotten their passwords to use an alternate process to authenticate themselves, and thus, reset their passwords without the assistance of help desk personnel.

Session – A session is an interaction between two or more entities on a network, generally consisting of an exchange of information. In the context of identity management, the most

important information exchanged is the credentials of each entity and the time-out information for the session.

Single-Factor Authentication – A method of authentication that relies on a single factor, such as username and password, to verify a user's identity.

Standard User – This is a non-privileged user in computing environments (Windows, Mac, Linux, Unix, etc.) with basic access rights. This type of account/user, has limited ability to access resources and settings, as opposed to a privileged or superuser account (such as root or admin), which may have vast administrative rights.

T

Termination – The process by which user or customer credentials or privileges are de-provisioned and removed.

U

User – Users are people whose access to systems and identity information must be managed.

User Provisioning – Technologies or processes that create, modify, and deactivate user accounts, privileges, and profiles across IT infrastructure and business apps.

V

W

X

Y

Z

About BeyondTrust

BeyondTrust® is a global security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Access Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.