WALLIX
CYBERSECURITY SIMPLIFIED

A Beginner's Guide to Access Security

A Beginner's Guide to Access Security

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This is the comprehensive beginner's guide for anyone looking to understand the basics of access security.

Access security is a framework of policies and technologies that combine to manage the access that users have to an organization's sensitive IT assets. Strong access security brings a number of benefits, including stronger cybersecurity, better compliance with regulations, and more control over external devices accessing an organization's network and data.

A modern business needs to protect itself from threats that exist both inside and outside its walls. Access security gives businesses the tools they need to see exactly who is accessing their resources, and then control those users' privilege levels. Three processes are key to this: identification, authentication, and authorization.

The Zero Trust model and the principle of Least Privilege are two concepts that are vital to strong access security. There are a number of specific systems that businesses can employ to apply these concepts across their IT infrastructure: Identity Management, Privileged Access Management, and Endpoint Privilege Management.

Access Security

Introducing Access Security

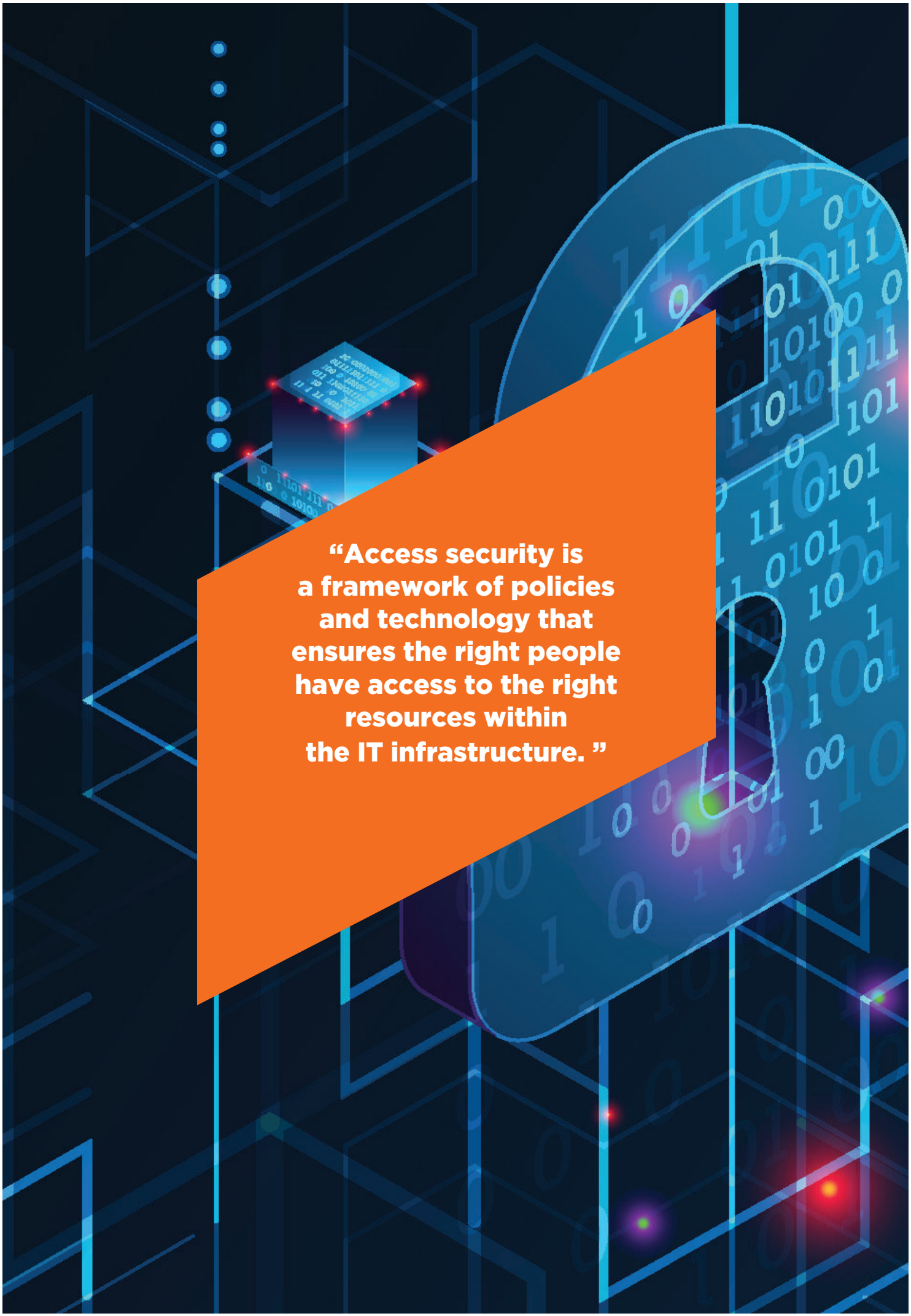
What is access security?

Businesses have physical security procedures in place to make sure that outsiders cannot simply walk into their buildings and do whatever they like. Every day, checks and structures are used to make sure that only the right people can access areas that contain sensitive information. These physical controls could include access passes, physical checkpoints, keycodes, or facial recognition technology. Today, sensitive information and customer data are stored in IT infrastructures. Surely then it makes sense for businesses to apply the same level of scrutiny to their IT networks?

We all have a physical identity – and now we have digital identities too. It can be easy to spot an on-premise intruder based on their physical identity, but digital identities are harder to track. At all times, organizations need to know who users are and what level of access they should have within an IT network. They need to ensure that their employees and business partners have the appropriate levels of access to their IT resources and conversely, do not have access to resources they do not need. It wouldn't make sense to let people have unrestricted physical access within an organization's building, and it's the same with IT networks.

Businesses need to have one digital identity per individual person using their system. These identities must be maintained, modified, and monitored throughout each user's 'lifecycle'. For example, an employee's role may change, or they may leave the company, meaning their level of digital access needs to be amended or rescinded entirely.

Effectively, access security is a framework of policies and technology that ensures the right people have access to the right resources within the IT infrastructure. It establishes rights and restrictions for every person who needs to use a network. When hundreds of users are active within a network, it's vital that a business can tell who is who, what they've done, and when. There are three processes that work in concert to do this: identification, authentication, and authorization.


“Access security is
a framework of policies
and technology that
ensures the right people
have access to the right
resources within
the IT infrastructure. ”

Identify, authenticate, authorize

These processes work in unison to verify who users are and what level of access privileges they have within a network. On the face of it, the meaning of these three words appear similar. However, there are some important differences between these key aspects of access security.

Identification

Access security starts with identity. In order to control what users can or can't do within an IT network, firstly we need to know who is who. Each user within a network has a digital identity attached to a unique username or email address. These virtual identities have a specific relationship to a unique corresponding person in the real world.

Access and privileges within the IT network are granted according to these unique identities, ensuring people have access to the applications that they need to do their jobs. When organizations deploy an identity management process or system, their primary motivation is to grant the appropriate privileges to users via their identities.

However, a user ID alone should not be used to presume someone's identity. Unique user IDs are nowhere near enough to verify users in a modern IT environment. After all, someone could simply type in another person's username and begin accessing files from their account. This is why it's important to authenticate.

Authentication

There needs to be a way to prove, or authenticate, that a user truly matches their digital identity. This comes in the form of a separate piece of confidential information, usually something you know, something you own, or something that's a part of you.

- **Something you know:** The most common example would be a password. If a username is your identifier, then your password is your form of authentication. A password is the most basic form of access security, one that is open to risks such as password sharing or theft.
- **Something you own:** This could be a physical item such as an access card or a fob/RSA token that generates a temporary passcode.
- **Something you are:** These are biometric authentication factors. They authenticate your identity by using part of the user's body, such as an iris scan, facial recognition, or fingerprint scan. Behavioral biometrics can also be used, such as typing, voice, or signature recognition.

Pairing a user identity with a method of authentication creates a set of user credentials – their keys to the IT kingdom.

Requiring additional forms of authentication on top of a password greatly increases the likelihood of accurate identification. It is harder for a hacker to steal two (or more) of the above factors – lending greater credibility to logins to sensitive IT assets. Using two or more of these authentication methods is known as multi-factor authentication (MFA).

Authorization

Authorization is the process of giving somebody permission to have or do something. In a computer system with hundreds of users, this is a vital security step. A user might have the credentials to log into a network, but what are they allowed to do there? Authorization grants levels of privilege and protects sensitive corporate assets by ensuring that only certain, approved individuals may access them. Once we can uniquely identify every user and verify that they are who they say they are through authentication, IT admins can grant the correct levels of privileged access to resources for each user's role and needs.

This step is important, as not all users need to have the same level of access. One user may need to only use the internet and a small number of applications – while another may need to access and modify important servers and databases. It wouldn't make sense for those two users to have the same level of systems access.

A strong access security framework relies on a business being able to identify users, authenticate them, and authorize them for the appropriate levels of access. Businesses that implement this effectively can enjoy the range of benefits that strong access security brings.

The benefits of strong access security

Managing privilege levels

It's never good for user credentials to be stolen by a malicious actor. However, the amount of damage that can be done depends on – and can be mitigated by – the level of access granted to that specific identity.

Strong access security allows organizations to manage privilege levels and control the visibility that users have.

Not all users need the same privileges to do their jobs. Having an access security framework in place to manage privilege levels helps a business to avoid overprivileged users with access to too many sensitive resources within their IT networks. This lowers the risk of privileged credentials falling into the wrong hands and opening the business up to a breach.

Access security solutions also help to streamline the actual management of privileges. They allow IT admins to grant or revoke privileges to any and all resources from a centralized hub. This makes the process more organized and manageable from an IT admin perspective, and enables simplified oversight.

Protection from cybersecurity threats

Gartner predicts that worldwide spending on cybersecurity will reach $133.7 billion in 2022. Modern organizations of all shapes and sizes are taking sensible measures to protect themselves from cyberattacks – and access security is an integral part of this. Privileged Access Management (PAM) was named as the number one cybersecurity priority by Gartner for 2019.

When threats can come from inside or outside an organization, it's never been more important to know:

- Who is accessing your system?
- What privileges do they have?
- What they are doing with their access?
- When they are accessing the system?

This is relevant to 'insiders' such as on-site employees and 'outsiders' such as third-party contractors or remote employees. Compromised user credentials are often the entry point to a network for malicious activity such as ransomware, malware, or phishing making control of access security a priority.

Securing the perimeter

In the past, a business' IT security perimeter ended within its walls. Now businesses have endpoints all over the world, as both employees and contractors can access networks remotely from their own devices. The Internet of Things (IoT) is expanding, opening up more avenues than ever into a network. It is also creating routes into industries that were previously sheltered from the wider connected world.

These factors mean that endpoints outside of the corporate network are not protected by traditional perimeter security. Businesses therefore need an additional layer of security for endpoints that can access sensitive assets from anywhere. An access management solution can authenticate users from a variety of different endpoints, meaning those users can verify their identities remotely without any impact on their productivity.

Compliance with regulations

It's a sensible policy to know exactly who is entering and exiting a network – and what privileges they have. But it's not just nice to have – it's an obligation. This is reflected in compliance regulations such as ISO 27001 and GDPR which require businesses to have strong control, transparency, and audit logging of privileged users' sessions. Having a strong access security framework is the best way to stay on the right side of regulations such as these, as well as avoiding any penalties for not respecting regulatory standards.

Businesses shouldn't wait for a data breach to protect themselves with robust access security. The right solutions allow IT teams to support compliance without overburdening cybersecurity resources or overcomplicating business tasks. A well-run access security solution can help to streamline and speed up the implementation of compliance rules across a whole organization.

Access security brings a number of benefits to an organization. But before exploring the specific systems that put access security into action, it's important to understand some of the concepts behind it; concepts such as insider threat, zero trust, and Least Privilege are critical to keeping networks secure.

Understanding Access Security

Insider Threat

An insider can be defined as anyone who has legitimate access to a business's sensitive data. This makes all full-time employees, part-time employees, and 3rd-party contractors insiders, as they all have access rights to an organization's infrastructure at various times. In the age of cybercrime, this also makes all insiders a potential avenue of attack for hackers.

It may seem strange to consider trusted and valued employees as 'threats', but the reality is that a significant proportion of data breaches are linked to insider access credentials. This does not mean every insider is treated as if he or she has malicious intentions, but in terms of access security, each set of access credentials, no matter how trustworthy the user, represents a new point of vulnerability. Even though the vast majority of employees would never deliberately jeopardize their company's security, their credentials could be lost, stolen, or inadvertently shared with someone less trustworthy.

How big of a problem is insider threat?

Insider threat is the leading cause of cyberattack. According to a 2020 report from The Ponemon Institute, the number of cybersecurity incidents caused by insiders has increased by 47% since 2018. The report also states that 62% of incidents were caused by negligence, as opposed to criminal actions.

According to a 2020 report from The Ponemon Institute, the number of cybersecurity incidents caused by insiders has increased by 47% since 2018. The report also states that 62% of incidents were caused by negligence, as opposed to criminal actions

Insider threat is a risk because even trustworthy employees can inadvertently cause a serious data breach through email phishing scams, sharing account credentials and root passwords, or simply accessing critical assets from endpoints outside the corporate network. The Ponemon Institute's research claims that organizations are spending on average 60% more on insider threat today than three years ago. More businesses are taking steps towards protecting against this vulnerability.

How do we protect against it?

People will always need access to IT resources in order to do their jobs. Organizations must protect their assets from accidental misuses that create vulnerabilities. As more exposure and vulnerabilities are created, the likelihood of a malicious attack increases.

Here we'll explore two principles which a business can apply to protect itself against data breaches. Firstly, by using a Zero Trust policy of identification and authentication to ensure they know who is accessing their network. And secondly, by authorizing insiders with the least amount of privileges that they need to do their jobs.

The Zero Trust Model

It's an unfortunate truth that any user can be considered a threat when it comes to access security – even trustworthy insiders. That's why it makes sense to implement a Zero Trust approach for users accessing the corporate network. This doesn't mean that everyone should be treated with suspicion, or as though they're an accident waiting to happen.

It simply means that nobody is trusted implicitly

when it comes to accessing an organization's sensitive data. Instead of assuming that all activity is legitimate until proven otherwise, a Zero Trust security model proactively requires proof of identity before allowing access. Users need to prove that they have both the need and the authorization to access a network resource before entry is granted.

How can we trust users?

Using a Zero Trust approach to access management does not eliminate insider threat, but it does help to mitigate it. Trusting a user solely based on their possession of a username and password login is not enough protection.

This is where multi-factor authentication (MFA) comes in. As detailed above, MFA requires more than one form of verification to prove that a would-be user is who they say they are. It is far less likely (though not impossible) that a hacker gets hold of two forms of verification than one. For example, a hacker would need to steal both a user's password and their security token, as opposed to just the password. The more factors of authentication used, the more trust in a user's identity.

Is multi-factor authentication enough?

Employees are trusted – and that's a good thing. However, when it comes to access security, trust by default is a dangerous policy. Nobody should be implicitly trusted when serious data breaches are at risk.

Zero trust is the first line of defense when it comes to preventing hacks from stolen credentials. An important part of a Zero Trust model is the Principle of Least Privilege. This ensures that if credentials are stolen, the impact that a hacker can have is kept to a minimum.

The Principle of Least Privilege

Least Privilege means granting users access only to the minimum applications and files they need to do their jobs. Limiting access rights to only the bare minimum of what is required – no more, no less – eliminates overprivileged users and the risks they bring with them. A hacker can do greater damage with far-reaching admin rights than with a small amount of user privileges attributed to a compromised user. Least Privilege can also be extended to the times and places that people need access to certain resources. For example, employees may only be permitted to access files during specific working hours and from specific locations.

With Least Privilege policies in place, the potential 'attack surface' a hacker can exploit is reduced. Consider this physical analogy for a system without Least Privilege. It would be like visiting a hotel and being given an access card that unlocked any door in the building for as long as you wanted it for. Instead, we get a card that works only for communal areas and our own room – and only for the duration of our stay.

Why is Least Privilege so important?

Least Privilege limits users' visibility of resources they don't need or are unauthorized to view. Therefore, if a hacker did steal a user's credentials, they only gain

access to a limited number of resources and can therefore inflict a limited amount of damage. The hacker would not be able to bounce between any resource that they liked. By limiting the access that users have, we limit the exposure in the event of their credentials being compromised.

For example, a third-party provider contracted to carry out administrative maintenance on a specific piece of equipment does not need the same levels of access and permissions as the head of IT. He/she would only need access to the assets required in order to do the job. All it would take would be for an overprivileged contractor to click on a phishing link that downloads malware – and then you have a hacker with admin rights to the organization's most sensitive assets. If an insider did need to have elevated access to a sensitive area of the network, this can always be requested and granted as needed, per task.

How can we implement Least Privilege?

Least Privilege is simple in theory. However, it might need to be applied across hundreds or even thousands of users in an organization – all of whom may have different roles and access needs over time. There would be plenty of leavers and joiners to consider, too. In order to successfully, and sustainably, implement the Principle of Least Privilege, businesses need a clear understanding of:

- What assets are considered sensitive resources?
- Who genuinely needs to access these sensitive resources?
- Which regulations does the business needs to comply with?

Least Privilege applied in tandem with a Zero Trust approach comprise is a powerful access security methodology. Identifying users and administering privilege rights is much easier when managed through a centralized access security solution. Now, for a more detailed look at the management systems that allow the Zero Trust and Least Privilege principles to be put into action.

Managing Access Security

Identity and Access Management (IAM)

Cloud environments, remote working, 'bring your own device' policies (BYOD), and the Industrial Internet of Things (IIoT) have made IT networks more complex than ever. This can make it even more challenging to manage digital identities. Not having a centralized system to monitor and manage user access leaves organizations open to unnecessary risk.

We have seen how verifying the identity of a network's users is an integral part of access security. Identity and Access Management is an umbrella of solutions which identify and authenticate any user who needs access to an organization's system. These systems allow businesses to define who each user is and what they can do within a network.

What are the key features of IAM?

IAM systems include a variety of tools which facilitate the 3 pillars: identify, authenticate, authorize. With

the right selection of solutions, an organization can establish a robust defense to protect identities, access, and corporate data.

What is required of the solutions comprising this IAM ecosystem? An identity management solution needs to be able to verify users, preferably through multi-factor authentication (MFA). This allows organizations to enforce a Zero Trust policy whenever anyone attempts to access their network.

The digital identities within an organization's infrastructure can change over time and thus need to be flexibly managed as users move through their 'lifecycle', allowing for identities to be easily added, removed, or amended. Effective Access Management therefore allows super-admins to enable and disable accounts, grant and revoke access rights, and store user information in databases. The system needs to be easy for IT admins to manage. If the administration of the system is complicated or spread across several different resources, it won't be as effective.

Similarly, the most effective security solutions provide a seamless user experience. If connecting to resources is complicated, users will look for loopholes which defeats the purpose of the solutions and puts the businesses further at risk. Simplifying authentication through Single sign-on (SSO) and centralizing access through a single platform streamlines user experience and encourages user adoption of proper security processes.

IAM is an umbrella term for managing all of an organization's digital identities and their accesses. Thus, a strong IAM framework should include a Privileged Access Management (PAM) solution. PAM solutions provide a robust layer of security by facilitating the implementation of Least Privilege and Zero Trust for elevated user access rights.

Privileged Access Management

Privileged Access Management, or PAM, is a solution that helps organizations monitor and audit all actions taken by privileged users. Identity solutions and MFA authenticate and authorize any user who needs access to a system, after which PAM is focused on streamlining management and oversight of elevated users' access rights, keeping organizations safe from the accidental or deliberate misuse of privileged access.

The dangers of unconditionally trusting any user are clear due to insider threat, and the Zero Trust approach to security requires that every attempt at privileged access be validated and monitored. It is risky to give even super-admin users root privileges such as the ability to change system configurations, to install software or access secure data. Privileged credentials could be lost, shared, or stolen. A malicious user with admin rights can not only make far-reaching changes to a system, but they would also be in a position to hide their actions. Not to mention the occurrence of negligence and mistakes, where privileged rights are accidentally misused.

A PAM solution mitigates this threat by facilitating precise control over exactly who has admin privileges to which resources, and when. It monitors users' actions, leaving an audit trail that can be

checked in the event of a security breach. The most effective PAM system validates privileged attempts to access resources against the following criteria:

1. Can the user prove who they are?

2. Does the user have the necessary privileges to access the resource in question?

3. Are there appropriate circumstances for the privileged access?

4. Is all user activity being monitored and logged for tracing and audit purposes?

5. Can the session be terminated (either automatically or manually) if the activity is unauthorized or suspicious?

PAM solutions can vary in their architecture, but most feature three main components:

- **An access manager**
- **A password manager**
- **A session manager**

These modules work in tandem to ensure the above questions are always answered in the affirmative before privileged access is granted.

Access Manager

The access manager componenet governs access to privileged accounts. It enables an organization's IT security team to map user's roles and access, granting, revoking and modifying user privileges to any and all assets from a unique console. It provides the tools needed to provide all users (internal, external, and 3rd party) with the access they need to do their job, as well as a way for super-admins to manage authorizations and track users.

The access manager centralizes access and management to all resources within one single platform, with no separate logins or disparate systems. Users only see the resources that they have the rights to access; no more and no less. They cannot see other IT assets on the network, even if they can guess that the resources are there.

Using an access manager gives administrators a clear picture over who is using and accessing resources across their organization. And it makes connecting to resources simple for internal and external users, streamlining access to all authorized resources through one platform. The access manager is especially important for large organizations who need to provide external access to contractors, service providers, and remote employees, offering an additional layer of security for these "insiders" connecting from outside the corporate network.

Password Manager

The goal of an effective PAM solution is to prevent privileged users from knowing the actual passwords to critical systems. The password manager stores all password SSH keys within a secure vault, meaning that users need never know or share the root passwords. Employing an advanced password management tool in a PAM solution significantly

reduces the risk of an organization's passwords falling into the wrong hands. Passwords are enforced for complexity and automatically rotated, meaning credentials become invalid even if they are breached.

A password manager is more than simply a vault. While it does securely store and encrypt passwords, it also helps to enforce robust password policies and improve best practices within an organization. The password manager is a key part of the PAM solution, allowing organizations to reduce risk exposure and meet a variety of compliance requirements.

Session Manager

The session manager is the core of a robust PAM solution, monitoring privileged access in real time, checking whether actions taken in a privileged session are both legitimate and authorized. It also creates an unalterable audit trail of all sessions, the logs of which can be searched, making it easier to meet compliance regulations. And if attempts are made to access sensitive resources without authorization, they can be automatically terminated. This is the Zero Trust principle in action: 'better safe than sorry'.

The session manager gives complete visibility over privileged user actions, reducing the risk of deliberate or accidental abuse of privilege. It records clicks, typing, and all other actions to allow organizations to see exactly what a privileged user did during a session. This includes actions a user may be trying to hide, whether on another screen or with key commands. The recording of sessions can also help to catch legitimate mistakes in real time and lead to them being reversed. Recordings are particularly useful in case the information needs to be reviewed during a future audit or training.

A comprehensive PAM solution is the best possible way to optimize security against the potential risks posed by privileged users.

Endpoint Privilege Management

In addition to PAM, Endpoint Privilege Management (EPM) is a critical component of an effective IAM strategy that can be used to secure the devices that users are accessing an organization's network from and other "terminal" equipment. Endpoint Privilege Management applies the Least Privilege principle to these endpoints, enabling organizations to define privileges beyond the user level to allow or block applications and processes. This helps to protect the network from threats such as ransomware or malware. Whether it's a phone, computer, or point of sale terminal – all devices need to comply with specific criteria before being granted access to network resources.

Why should we protect endpoints?

The days when employees only accessed a network from their fixed workstations are long gone. Modern organizations can have hundreds or thousands of endpoints – and this number will only increase as the Industrial Internet of Things (IIoT) connects even more devices to networks. The average modern employee can access an organization's network from a desktop PC, a work laptop, work phone, and their personal devices, too, and from anywhere. The more

endpoints, the more potential avenues hackers have to infiltrate IT infrastructure.

It's important that the correct security measures are in place to prevent unauthorized devices from accessing a network. However, it would be impractical to apply these measures to every device individually. Endpoint Privilege Management allows for control and compliance with regulations such as GDPR, NIS, and PCI-DSS – without penalizing user productivity.

How does Endpoint Privilege Management work?

Endpoint Privilege Management offers a centralized software approach that enables administrators to identify and manage end users' device access to the corporate network. EPM eliminates the risks associated with overprivileged users, applying privileges at the application and process level, rather than at the user level. Admins can set access permissions so that even personal devices outside the network perimeter cannot pose a risk to corporate assets. They can also enforce Least Privilege by setting policies where endpoints are granted precise, granular access permissions to ensure that IT infrastructure is protected without impacting user productivity.

With controls set at the process level, IT can whitelist, blacklist, or even grey-list specific applications or actions. Users' daily tasks are not disrupted – no need to call IT to download a tool important for work productivity – but endpoints remain secured with restrictions placed on processes those applications can carry out, even for users with elevated privileges.

Summary

Consider this example of access security coming together. A contractor needs to access an organization's database to perform some work, so she attempts to log on to the corporate network through her personal tablet. The organization's IAM procedure ensures she authenticates her identity using MFA: a temporary password she has been supplied with as well as the code from an RSA token.

The PAM system authorizes her access to the server she needs, then monitors and records her session as she works. If she needs access to further resources, elevated privileges can be requested and granted by the IT team for a specified period. At the end of the task, once her work is completed, the PAM system automatically checks in and rotates the resource password, and revokes her elevated privileges. The PAM system removes her access privileges from the company's network when the need expires. The Endpoint Privilege Management system ensures that the device being used to modify the database has the appropriate security settings and allows her to download and work from whitelisted apps.

This scenario shows how an organization with strong access security can use PAM and EPM in tandem to keep critical systems and data secure as part of an overarching IAM strategy.

about WALLIX

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED