From Access to Actions:

How Zero Trust PAM Defines Modern Enterprise Security

strongdm

Table of Contents

Executive Summary

Traditional security measures focusing on controlling access at the "front door" are no longer sufficient in today's complex IT environments. Simply validating privileged users and managing entry points overlooks the critical aspect of monitoring user activity within applications and data repositories. The future of security lies in applying fine-grained permissions to control user actions on critical resources, and continuously assessing the risk profile of those users.

This necessitates a shift towards a Zero Trust model for privileged access management (PAM), where permissions are evaluated in a continuous fashion, and every action is evaluated in real-time against policies. Zero Trust PAM is the most effective way for organizations to adapt to the evolving threat landscape while ensuring operational agility and productivity.

The Actions Loop of Modern Enterprise Security

Since the advent of the modern internet, enterprise security measures have focused on controlling access in the form of ***who, what and from where***. The idea has been to validate users and manage their entry points, with the hope that that initial check at the entry point will be enough to secure an organization's vast IT environment.

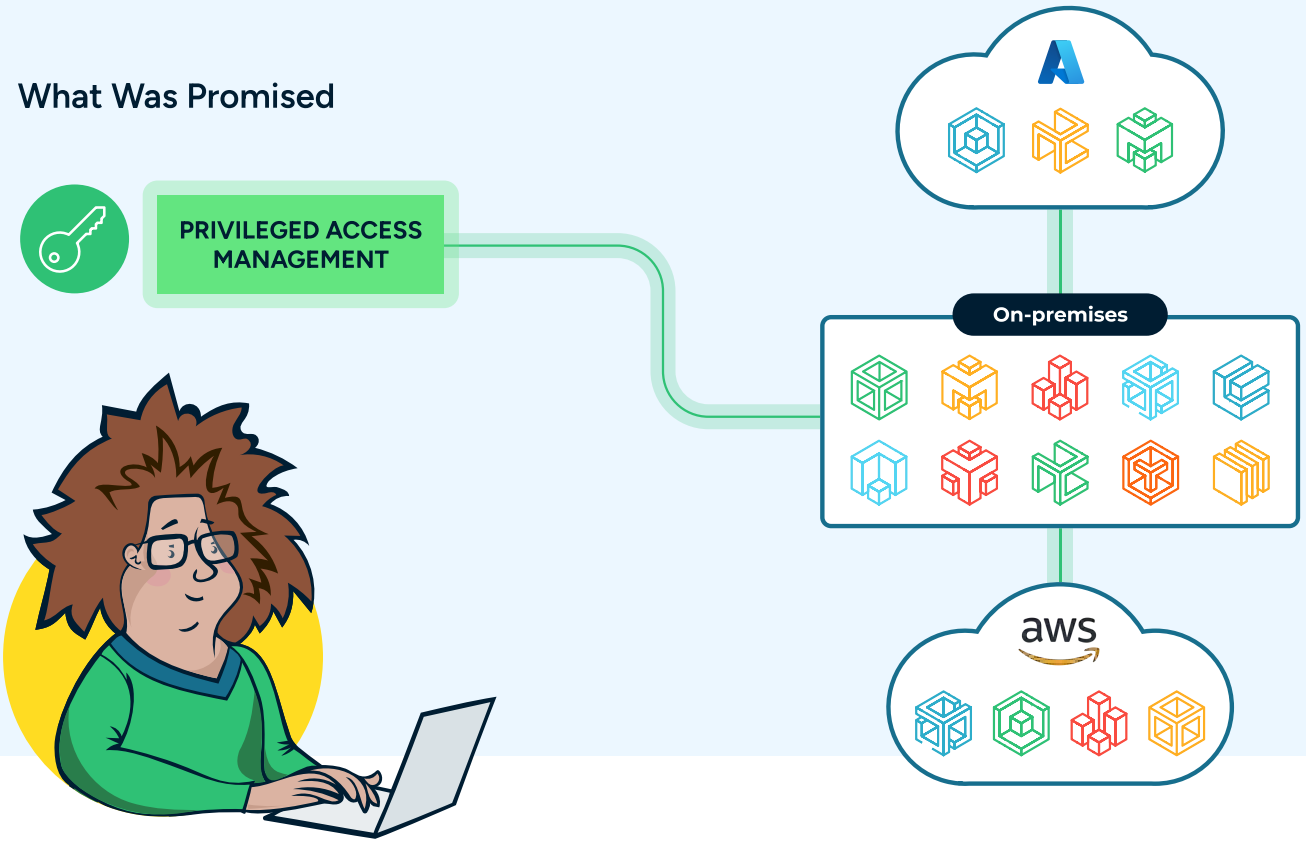
When organizations had simple tech stacks of just a handful of databases and ERP applications, this approach worked. It relied on the "front door" theory that sought to eliminate risk by preventing access to unknown users.

This approach was predicated on the idea that a security issue presented itself specifically and definitively as a security issue, and that it could be stopped before it created an even bigger issue. But this doesn't work for today's environments. In fact, it's risky. It overlooks a critical aspect of security:

What happens after access is granted?

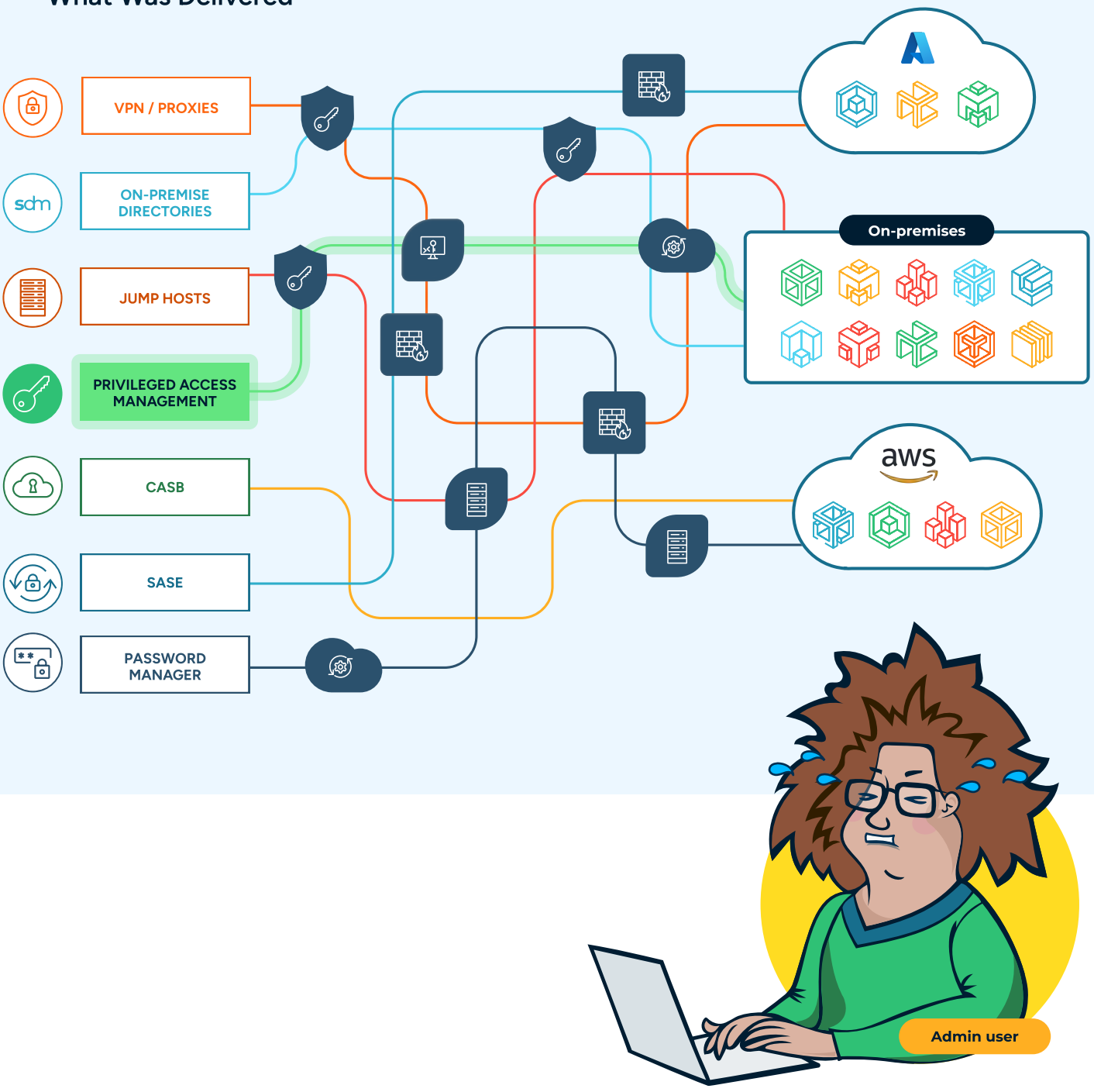
What is a user actually doing with the access they have? And as organizations apply more policies to establish and manage security and compliance guardrails, being blind to activity within applications and data repositories poses major risk. This oversight leaves a gaping hole in security postures, as managing access alone is akin to securing the perimeter of a house but ignoring what happens inside.

It demands that PAM goes beyond simply identifying who is accessing an environment. It has to manage ***who*** can access ***where, what, and how*** and that requires continuous assessment of risk and controlling what users do once they're inside of an IT environment.



Today's infrastructures are complex, for sure, but they are more than that. Some parts are static and rely on legacy applications that aren't easily adaptable to modern policies and compliance standards. Others use dynamic, ephemeral systems to scale up, down, in, and out, as needed, and that creates a continuous stream of new resources to manage. And irrespective of the organization's size, there are always an assortment of new tools being added and integrated.

What Was Delivered



Why PAM Needed to Evolve

Privileged Access Management (PAM) plays a critical role in securing environments by managing and monitoring privileged accounts, which have elevated access to systems and sensitive data. However, modern security challenges demand that PAM goes beyond simply identifying who is accessing an environment. Here's why:

Beyond Identity: Contextual Awareness

Knowing who is accessing an environment is important, but it's not enough. Modern security threats require a comprehensive understanding of the context in which access is being attempted. For example, is the user accessing the environment from an unusual location? Are they performing actions outside of their normal behavior pattern? By analyzing these contextual factors, PAM solutions can detect anomalies and prevent potential security breaches before they occur.

Move Past "Having" the Data: Real-Time Decision Making

Traditional PAM solutions focus on collecting data about user access but often fail to utilize this data effectively. It's crucial to move beyond simply having the data to actually using it for real-time decision making. For example, if telemetry data shows that a user is accessing sensitive information during odd hours or from a suspicious IP address, PAM solutions should have the capability to flag or block such activity immediately. This shift from passive data collection to proactive decision-making enhances security and reduces risks.

Telemetry Context: A Valuable Resource

Telemetry context, which includes data such as user behavior, device information, and network activity, is often underutilized or hoarded by organizations. This valuable resource should be leveraged to enhance security measures. For example, if telemetry shows that a user is suddenly downloading large amounts of data or attempting to access unfamiliar systems, this could indicate a compromised account or malicious insider activity. By incorporating telemetry context into PAM, organizations can proactively detect and prevent malicious activities

Telemetry Data is Compounding: Analyze and Adapt

Telemetry data is continuously growing, and if not properly managed, it can overwhelm organizations. However, this compounding data also provides valuable insights into evolving threats and user behavior patterns. PAM solutions should utilize this data to adapt security policies and improve threat detection over time. For example, if multiple users are falling victim to a phishing attack, PAM solutions should recognize this trend and adapt security measures accordingly.

That's a lot to manage and secure. Consider that when these changes are taken together, they begin to compound. This creates a profusion of security concerns because every tool, every integration, each configuration change, and hundreds of other factors that happen in a perpetually changing state have the potential to increase security risk. Enabling users – even privileged ones – to simply be verified once and then be able to operate without additional verification isn't logical. And it certainly isn't safe.

Imagine a world where every action, no matter how minor, is governed by the principles of Zero Trust – where each command, query, or configuration change is evaluated in real-time against policies that adapt to the context of the user, the sensitivity of the action, and the prevailing threat landscape.

Static, perimeter-based security models no longer work. Granting standing access to privileged users reduces security posture. Session recordings and after-the-fact remediation is not viable.

Dynamic, action-oriented security is required for today's enterprise environments. Control based on adherence and behavior around policies transforms not just how organizations protect their assets but also how their IT organizations operate. It paves the way for a new era of operational agility where security measures no longer hinder productivity but enable it. This gives developers and IT professionals an operating model within a seamless environment that offers both the freedom to innovate and the assurance that every action is safe by design.

Where Legacy PAM Falls Short

LACK OF VISIBILITY & CONTROL

Lack of visibility, **poor user adoption**, and **lack of audit trails** to all resources, on-premise and in the cloud.

EVER-INCREASING RISK

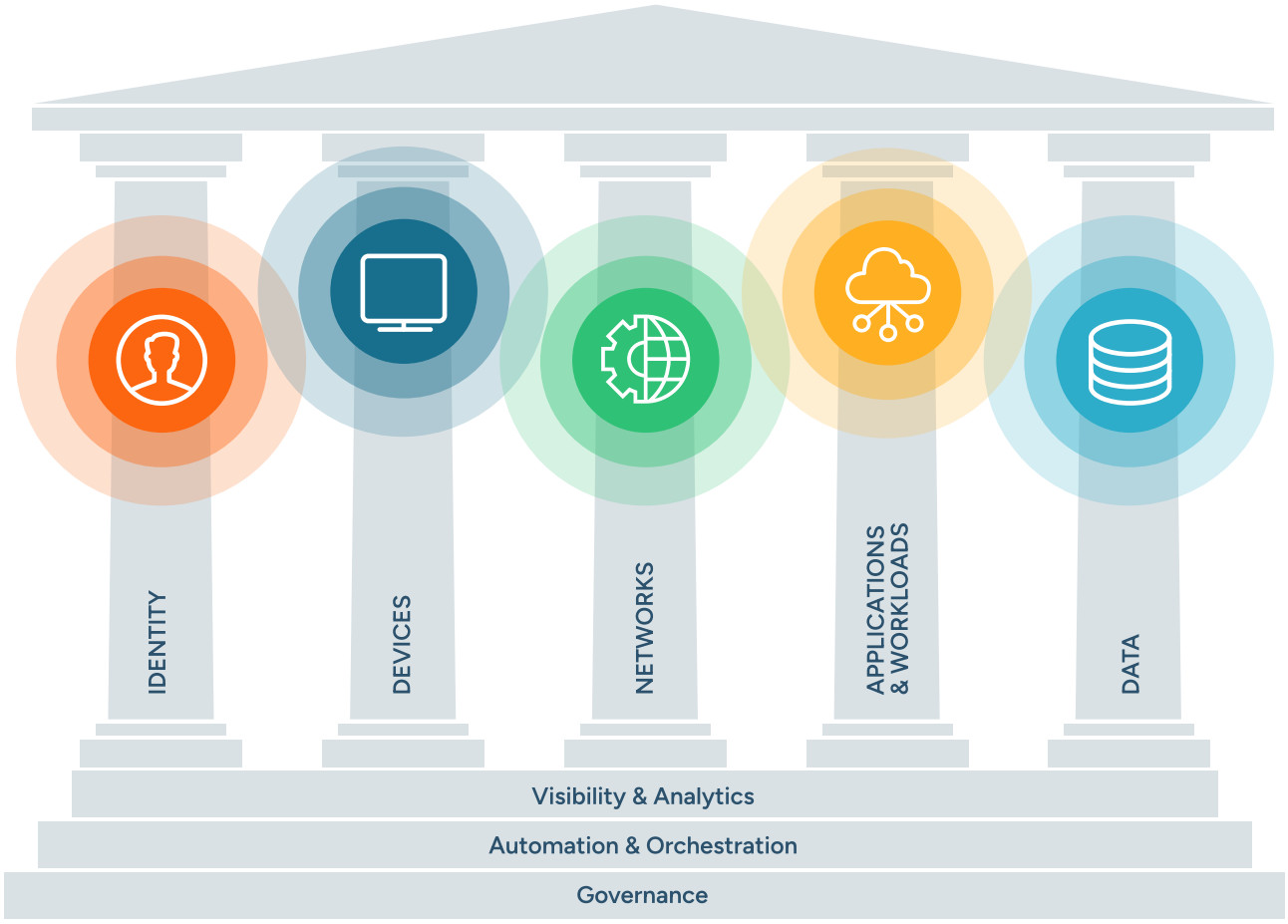
Increased attack surface with standing access, **over-provisioned users, local storage of credentials**, and unused privileges. Completely exposed cloud infrastructure.

INCOMPLETE DEPLOYMENT

Admins have **stalled deployments** of their PAM. End users are unable to get access to the tools they need to do their jobs.

Zero Trust Pillars in Action

Zero Trust PAM is the new model. It enables enterprises to improve security controls for critical infrastructure and resources through micro-authorizations, contextual awareness, and enforcement of policies. The result is multidimensional protection of managed enterprise resources through granular, continuous assessment and authorization for privileged users.



Source: CISA

IDENTITY

Continually authenticate, assess and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

DEVICES

Understand the health and status of devices to inform risk decisions. Real time inspection, assessment and patching informs every access request.

NETWORKS

Segment, isolate and control (physically and logically) the network environment with granular access controls.

APPLICATIONS & WORKLOADS

Secure everything from applications to hypervisors to include the protection of containers and virtual machines.

DATA

Data transparency and visibility is enabled and secured by enterprise infrastructure, applications and standards, robust end-to-end encryption, and data tagging.

Defining “Zero Trust”

John Kindervag, a former analyst at Forrester Research, is credited with developing the concept of "Zero Trust" security architecture. He introduced this idea in 2010 in response to the evolving cybersecurity landscape and the traditional perimeter-based security model's inadequacy in protecting against modern threats.

The core principle of Zero Trust is to eliminate the assumption that anything can be trusted implicitly. Instead, it advocates for a model where trust is never granted by default, irrespective of who made a connection, or where it was made. Every user, device, and network flow is verified and authenticated before access is granted to any resource.

Kindervag emphasized the need to move away from the perimeter-based security model, which relies on the idea of a trusted internal network and focuses on defending the perimeter from external threats. Instead, he proposed a model where security measures are applied at every level of the network, from the user and device level to the application and data level.

The original Zero Trust model promotes the following key principles:

Verify identity	Authentication of users and devices is crucial before granting access to resources.
Least privilege access	Users and devices should only be authorized to access to the resources necessary to perform their tasks.
Assume breach	Instead of assuming that the network is secure, Zero Trust assumes that threats are already present inside the network and implements measures to mitigate them.
Micro-segmentation	Network segmentation is used to create zones and boundaries, limiting the lateral movement of threats within the network.
Continuous monitoring	Continuous monitoring of network traffic and user behavior allows for the detection of anomalous activities and potential security breaches.

In August 2020, the National Institute of Standards and Technology (NIST) published Special Publication 800-207, titled Zero Trust Architecture, which modified the concept of Zero Trust to align it with the needs of modern environments, especially those that make use of cloud-based assets.

The way NIST defines it, there is no time constraint placed on monitoring. Rather than assessing risk only at the point of access (even if the assessment is done at the point of access for each individual asset a user is interacting with), NIST 800-207 recommends continuous monitoring.

Zero Trust must be absolute, pervasive, and applied to actions, not access. That means using context signals to make real-time assessments of every action that occurs with the users and resources that touch an enterprise’s environment. StrongDM has taken the concept a step further by making a distinction between continuous monitoring and real-time monitoring. Continuous monitoring is essential, but evaluating without end is not necessarily effective unless the monitoring aligns with policies that dictate what is and is not secure behavior.

In our view, Zero Trust means that every action must be evaluated in real-time against dynamic policies.

Infrastructure Changes Should Not Require Security Retooling

There is a narrow specificity to what legacy security tools can accomplish. They are designed to address a unique set of issues and to work in specific environments. That approach was adequate when infrastructures were on-prem and resources were typically added according to regimented planning.

But today's environments do not recognize timelines or scaling limitations. Cloud environments enable easier application integration and rapid adoption. Containerization and ephemeral storage capabilities create computing and processing power on-demand. It's a perverse, but effective way of torturing complexity into simplicity.

But what gets lost in all of this is security efficacy. This technology democratization means more people want access to more resources and they want that access with zero friction. We've created a continuous situation where access is considered a foregone entitlement.

Legacy tools can deliver the necessary access, but not with the accompanying security rigor required for today's security landscape. At issue with these tools is that the policies that govern have to be rewritten into the tools with every change. In other words, policies have to be rewritten to address a new application or even a new user. And that has to happen **every time** there is a change.

And think about how many changes your environment encounters every day…or for that matter, every hour. Changing that means retooling your security infrastructure continuously. Why not just have your security infrastructure dynamically – and continuously – adapt to the environment it serves?

For today's environments, you must define what you enforce **today** but then seamlessly grow into **tomorrow** without redesigning the system of roles, attributes, and policies. The core of what is needed is effective access control and authorization management that meets today's needs and it must have:

- **Dynamic Policy Management:** Enterprises require a policy management system that can adapt to evolving business needs, regulatory requirements, and technological changes without necessitating frequent manual updates. A dynamic policy engine enables organizations to enforce access controls in real-time based on the current context, reducing the risk of unauthorized access and security incidents.
- **Adaptability and Flexibility:** As organizations grow and their IT environments become more complex, the ability to adapt access control policies becomes essential. Static policies that require constant rewriting are inefficient and prone to errors. An adaptable system allows for seamless integration of new resources, changes in user roles, and modifications to access requirements without disrupting existing operations.
- **Granular Access Controls:** Enterprises need granular control over access permissions to ensure that sensitive resources are only accessed by authorized individuals. Fine-grained access controls enable organizations to define access policies at a detailed level, restricting access to specific data or functionalities based on user roles, attributes, and contextual factors.
- **Real-time Enforcement:** Real-time enforcement of access policies is critical for preventing unauthorized access attempts and minimizing the impact of security breaches. By evaluating access requests in real-time and enforcing policies accordingly, organizations can ensure that only authenticated and authorized users can access sensitive resources at any given time.

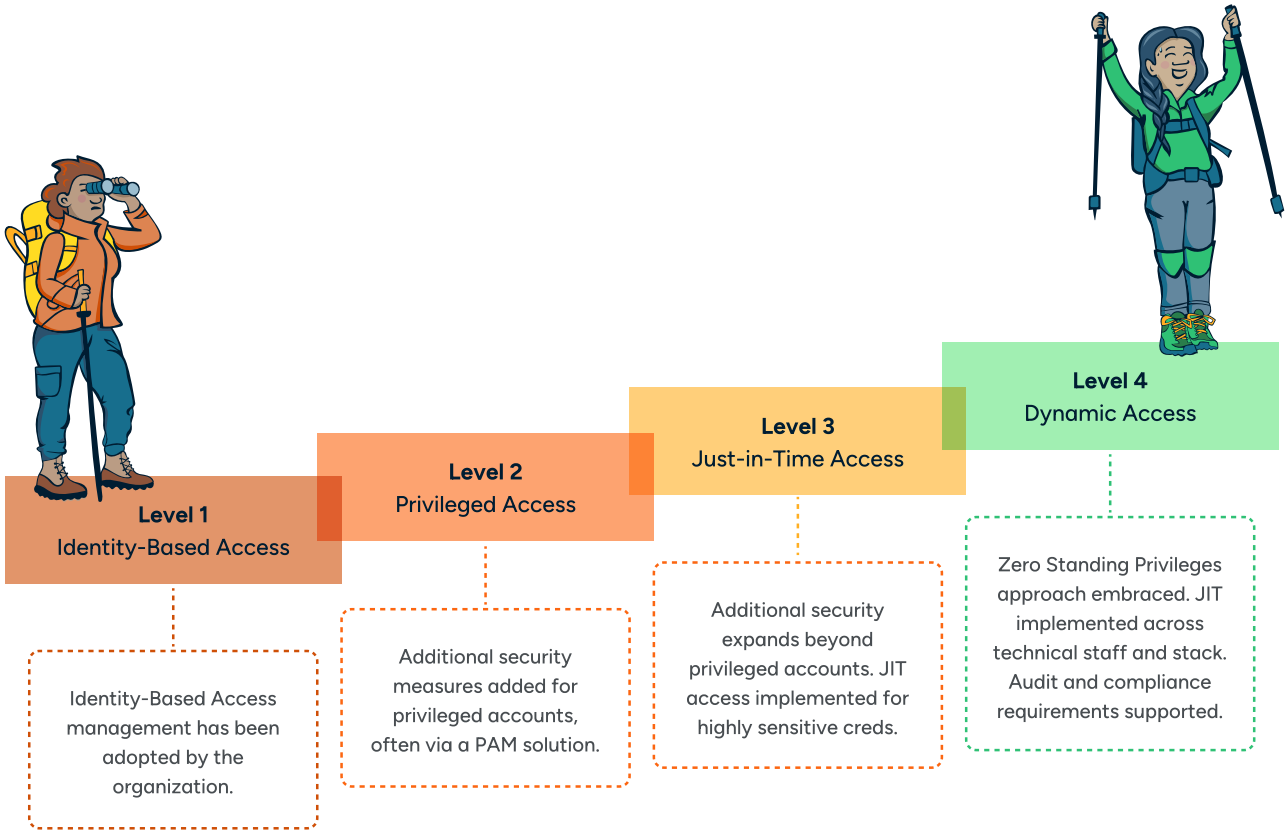
Scalability: With the rapid growth of data and increasing complexity of IT infrastructures, scalability is paramount. A scalable access control solution can accommodate the expanding needs of an organization, supporting the onboarding of new users, integration of additional resources, and expansion into new markets or business areas without sacrificing security or performance.

Modern enterprise security requires a comprehensive access control and authorization management solution that offers dynamic policy management, adaptability, granular access controls, real-time enforcement, and scalability. This type of solution enables organizations to effectively protect their sensitive data and resources while supporting business growth and innovation.

The Foundation for Modern Security is Zero Trust

Traditional privileged access management (PAM) provided the foundation for access control measures. It girded the entire concept of "front door" security and worked effectively until the advent of cloud computing and the rapid adoption of tools needed to support remote work culture. The attack surface of modern environments also grew and changed rapidly due to adding new applications and data repositories. Ten years after the cloud became a viable option for enterprises, legacy PAM providers are still struggling to fully support those environments in a way that doesn't frustrate users or admins.

As a result of all this change, cyber threats evolved, ranging from data breaches to ransomware attacks, exploiting constant credential leaks and weak access management. Instead of brute force attacks and other forms of "breaking in," bad actors now use valid keys, credentials, and session tokens to gain legitimate-looking access through a growing number of entry points and diversified attack vectors. The challenge now lies in securing a continuously changing and expanding digital ecosystem rather than protecting a fixed perimeter.



In response to this shifting landscape, the Zero Trust model has become the default cybersecurity strategy for modern security teams. Zero Trust operates on the principle of "never trust, always verify," rejecting the assumption that everything within a network is inherently trustworthy. In short, Zero Trust says “Don’t trust anyone or any machine until they’ve been verified.” It requires all devices and users to be authenticated, authorized, and regularly validated before being granted access, regardless of whether they are inside or outside an organization's network. Zero Trust mandates continuous verification of access requests, regardless of origin or destination, providing a dynamic and adaptive security framework.

This approach is increasingly vital as organizations face advanced threats, the dissolution of traditional network perimeters, and the adoption of remote work and cloud-based resources. Zero Trust is a fundamental, and necessary, shift from conventional security models, offering a more comprehensive and adaptable approach to safeguard critical assets and data.

The Role of Privileged Access Management (PAM) in Enterprise Security

The security approach that is based on Privileged Access Management (PAM) certainly plays a critical role in modern security practices. Privileged accounts are prime targets for attackers due to their elevated permissions, granting access to sensitive data and systems. PAM solutions help mitigate this risk by controlling, monitoring, and auditing privileged access, ensuring only authorized users can access critical systems while maintaining accountability and compliance.

As organizations embrace the Zero Trust approach, managing privileged access takes on another dimension. In simplest terms, PAM serves as a gatekeeper, rigorously authenticating and authorizing every request for privileged access based on predefined policies and context. Integrating PAM into the broader Zero Trust architecture bolsters defense against both internal and external threats, safeguarding critical assets amidst the rapidly evolving digital landscape.

Evolution of Privileged Access Tools

Level of Maturity	Identity-Based Access	Privileged Access Management	Just-in-Time Access	Zero Trust PAM
Shared Accounts	✓	✓	Eliminated	Eliminated
Always-On Access	✓	✓	Mostly Eliminated	Eliminated
MFA in Use	✓	✓	✓	✓
SSO Adopted	✓	✓	✓	✓
IdP Adopted	✓	✓	✓	✓
Privileged Accounts Protected		✓	✓	✓
Time-Bound Access			✓	✓
Full-Stack Secured			✓	✓
Granular Auditing				✓

However, legacy PAM systems are incapable of fully meeting the demands of the Zero Trust model. They were primarily developed for on-premises environments and are closely intertwined with Active Directory (AD), a conventional identity and access management system widely utilized in Windows settings. These solutions are ill-suited for the Zero Trust model due to several key factors. Firstly, they were constructed before the widespread adoption of cloud computing, lacking native support for cloud-native architectures like microservices and containerization, which are pivotal to Zero Trust principles. Secondly, traditional PAM solutions struggle to dynamically scale to meet the demands of cloud environments, hindering consistent access controls across hybrid or multi-cloud architectures. As a result, their architectures are not capable of supporting new resource and infrastructure types that have been built to take advantage of the cloud.

Deploying legacy PAM solutions can pose significant challenges because of inherent design and functionality limitations. First, legacy systems are typically complex and monolithic, making them cumbersome to install, configure, and integrate within existing IT infrastructures. Their rigid architectures often lack flexibility, making customization and adaptation to unique organizational needs a daunting task.

Legacy PAM solutions are incredibly difficult to deploy and typically have an onerous, friction-filled user experience, and as a result, they are underutilized by technical staff. These systems frequently rely on outdated technologies and architectures, making them incompatible with modern IT environments characterized by cloud-based services, mobile devices, and dynamic workloads. This compatibility gap necessitates extensive customization and integration efforts, leading to prolonged deployment timelines and increased costs. Designed for a different cybersecurity era, they focus on a narrow range of high-privilege accounts and resources within the corporate network perimeter. This approach doesn't align with Zero Trust's need for comprehensive visibility and control over all access points. In today's distributed IT environment, legacy PAM's scope is too restricted to provide effective protection across cloud services, remote servers, and various endpoints.

Scalability, or lack of it, is a common obstacle in deploying legacy PAM products. As organizational requirements evolve and the number of privileged accounts and users grows, legacy PAM solutions struggle to accommodate the increased workload efficiently. Scaling these systems often requires costly hardware upgrades or the implementation of complex clustering solutions, further adding to the deployment complexity and cost.

There is also the increasing issue of poor alignment between the PAM approach and the needs of modern security teams. PAM systems can pose usability challenges, hindering adoption and utilization by technical staff. Their complex interfaces impede efficient access rights management, leading to security gaps and heightened vulnerability. In a Zero Trust framework, where dynamic and context-aware access decisions are crucial, legacy PAM systems' inflexibility and limited coverage hinder the organization's ability to adapt to evolving threats and protect critical assets comprehensively.

Legacy PAM solutions are built to operate with general guardrails. But today’s systems are governed by more than just who gets in the front door. **Adherence to policies and permission granting can no longer just happen once; that level of blind faith presents a dangerous proposition for security teams.**

Today’s security and compliance teams must have continuous enforcement and real-time evaluation of policies to facilitate prompt detection and remediation of deviations from the defined access control policies. This is the Zero Trust PAM approach; it is detailed and thinks small to operate big. It gives today’s teams a well-structured framework that achieves both regulatory and internal compliance objectives and provides a level of security rigor that is unmatched.

Too Big to NOT Fail

Enterprise security teams can no longer afford to focus solely on coarse-grained user authentication and authorization at the front door of the enterprise systems. This broad approach fails to identify user actions, which is where vulnerabilities occur.

Enterprises face a range of challenges beyond basic user authentication and authorization, which include inadequate authorization controls and the manual adjustment of controls to enforce policy compliance. Traditional authentication and authorization mechanisms often fall short due to their reliance on multiple tools, frequently operating on a point-in-time basis. This approach lacks the necessary granularity to discern anything beyond an initial validation. As a result, it becomes challenging to accurately identify and mitigate potential security threats or enforce compliance standards effectively.

Coarse-grained access controls prove inadequate, hindering enforcement based on real-time conditions and operation-specific granularity. They may serve as a foundational layer of security, but are insufficient for addressing the complex and dynamic nature of modern cybersecurity challenges. Both legacy and modern applications face hurdles in universally embracing Zero Trust access controls without undergoing significant rewriting. Resolving these issues is critical for users to safeguard sensitive data, mitigate overexposure, and maintain compliance.

Security teams are faced with three critical issues:

1 The Complexity of Access

One of the primary challenges in current enterprise access control solutions involves the tendency to either over-grant permissions or manage an excessive proliferation of roles. This issue arises when organizations struggle to balance providing sufficient access for employees to perform their duties effectively while ensuring that access is not unnecessarily broad or unchecked.

Accurately tracking access granted for specific purposes, such as resolving a customer issue, is also tricky. In these instances, questions may arise regarding whether individuals accessed data belonging to a different customer, potentially leading to privacy concerns or compliance breaches. Actions are not evaluated independently or against policies, so there is still no authorization beyond the first entry point.

The increasing adoption of multi-cloud and hybrid environments introduces complexities in access control management. Organizations require controls that seamlessly operate across various cloud platforms and on-premises systems. However, achieving this level of compatibility and consistency poses a significant challenge, as different environments may have distinct access control mechanisms and requirements. As a result, organizations face the dilemma of ensuring uniform access controls across disparate IT infrastructures without compromising security or efficiency.

2 The Complexity of Compliance

Current solutions to enterprise compliance and regulatory challenges grapple with various issues stemming from various government and industry regulations. Each sector may have its own compliance requirements, governance standards, and security protocols, further complicating the landscape for organizations striving to adhere to these regulations.

One significant challenge arises from the manual translation of regulatory controls into actionable enforcement points within an organization's systems and processes. This process often involves painstakingly mapping regulatory requirements to specific operational procedures and technical configurations, a time-consuming task and prone to human error.

Additionally, the manual audit of compliance controls can be a laborious and protracted endeavor, sometimes spanning weeks to months. Organizations must meticulously review their adherence to regulatory standards and internal policies, often relying on manual assessments and documentation reviews. This manual audit process can impede efficiency and agility, delaying identifying and remedying compliance gaps or issues.

3 Explosion of Point Solutions

Modern security teams face the daunting task of managing many point solutions, each catering to specific identity and access management aspects. This multifaceted landscape often includes platforms such as SSO/ Identity Management tools, Identity Governance and Administration (IGA), Privilege Access Management (PAM), Secret Vaults, and individual applications and infrastructure components. Despite the vision of Zero Trust security frameworks, many security and compliance teams face the complexities of effectively integrating and optimizing these disparate solutions.

The reality for most security teams is navigating through the uncertainty created by a lack of observable actions and enforceable policies. While the concept of Zero Trust promises a paradigm shift towards a more resilient and proactive security posture, the practical implementation often proves challenging amidst the labyrinth of point solutions. Budget constraints compound this challenge, with security teams tasked to achieve more with limited resources. Flat budgets necessitate a strategic approach to maximize the efficacy of existing security investments while seeking innovative solutions to bridge gaps in the security infrastructure.

The Problem Isn’t Access, It’s Actions

What we’re seeing isn’t so much that access is a bigger or more complex issue. Instead, access is no longer the only issue; it’s the actions of users and how those actions are authorized that form the foundation for the most effective approach to enterprise security.

Zero Trust PAM uses fine-grained authorization policies that maintain perpetual vigilance over every action within an organization's digital ecosystem. It depends on a robust engine capable of seamlessly enforcing policies across all facets of infrastructure and applications. This unified approach ensures that access controls remain consistently applied, transcending mere connectivity to exert control over every operation.

Trust the user (who)

- IDP(s) integration
- StrongAuth

Trust the Device (on what)

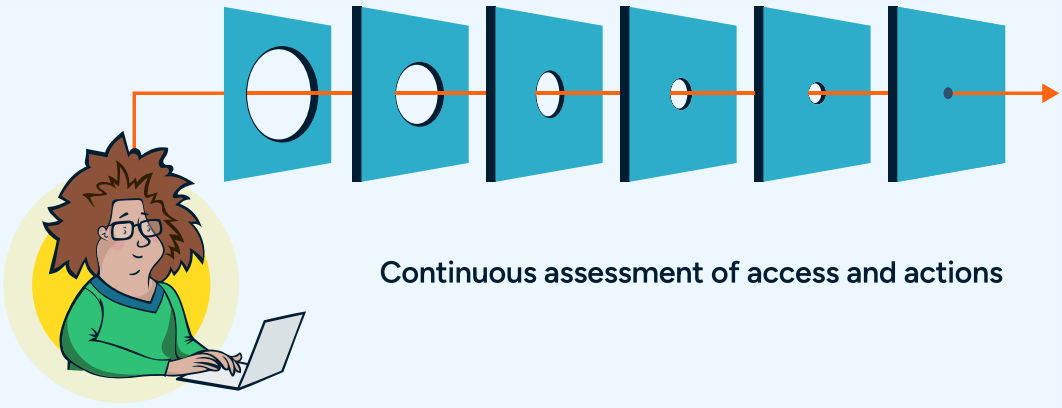
- Endpoint verification
- EPP/EDR integration

Trust the Context (where, when)

- IP Address
- Time

Trust the action (what)

- Is the action okay?



The extension of Zero Trust into a continuous operation reinforces the notion of granular access controls for every action and operation undertaken within the system. This comprehensive framework bolsters security and fosters heightened trust and accountability throughout the organization.

The most important outcome of Zero Trust PAM is enabling organizations to mitigate risks preemptively. By leveraging real-time context-based risk assessments and user behavior analytics, access controls can be dynamically adjusted to adapt to emerging threats swiftly. This bolsters defense mechanisms, making security infrastructure more adaptable and resilient, fortifying organizations against an increasingly complex threat landscape.

With Zero Trust PAM, policies are ultimately the critical element that integrates security controls across complex environments that use on-prem and cloud resources. Policies operate with a principal attribute that delineates the identity or identities a policy applies—this could be a user or a machine within the system. The operation attribute specifies the actions and executions permitted on a particular system, outlining the range of activities authorized under the policy. Then, the resource attribute defines the specific data or tool that the principal and action will access, ensuring clarity and specificity in permissions. The context attribute encompasses both inherent and dynamic factors. Inherent context factors, such as IP address, ID, geographical location, time, and multi-factor authentication, provide static parameters for policy enforcement.

Zero Trust PAM evaluates dynamic context factors, external signals, and computed attributes, such as endpoint risk scores, data loss prevention (DLP) insights, and threat analyses, to enable policies to adapt and respond to changing security conditions in real-time. By comprehensively considering these attributes, organizations can develop robust and adaptive policies that effectively mitigate risks and safeguard critical resources.

How Thinking Small Enables Operating Big

Thinking small in the context of cybersecurity involves closely examining the myriad of small actions and behaviors of users within an IT environment. Organizations can significantly enhance their security posture by focusing on the granular details of user actions, resources, and policies. Continuous monitoring of small actions allows for quickly detecting anomalies or deviations from normal behavior, enabling swift response to potential threats.

When organizations "think small," they implement granular access controls, which restrict user access to only the resources and information necessary for their roles. This minimizes the attack surface and reduces the risk of unauthorized access or data breaches. No more checking credentials at the front door once and allowing broad access. User validation never stops, and every action is evaluated for its compliance and policy adherence.

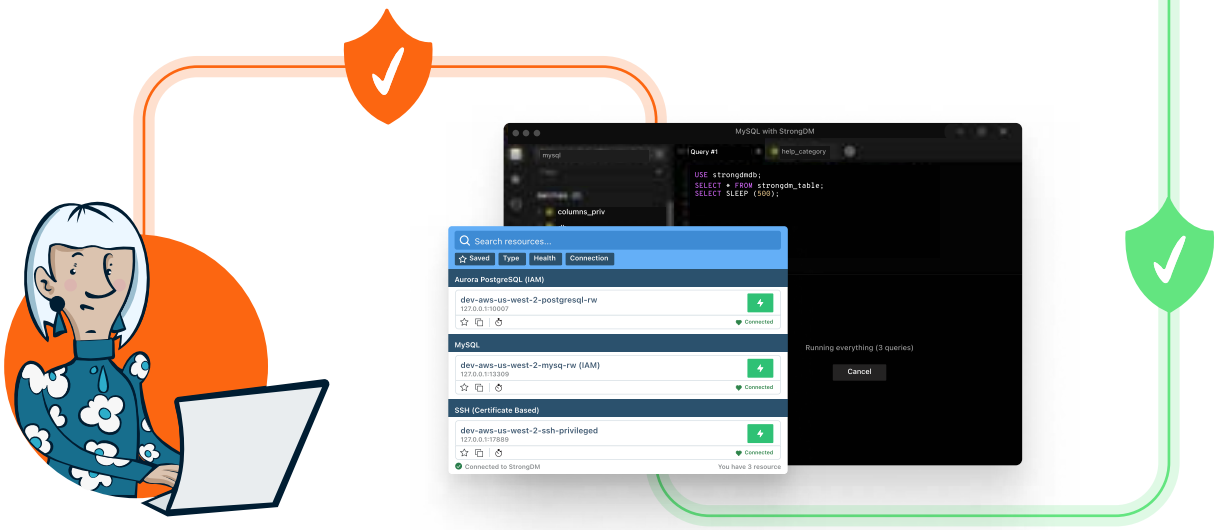
By analyzing actions and behaviors, both big and small, security and compliance teams gain insights into patterns and trends that may indicate security risks or vulnerabilities. For example, assessing context signals such as login times, file access patterns, and resource usage can help identify signs of compromised accounts or insider threats.

Additionally, addressing fine-grained actions and behaviors facilitates compliance with regulatory requirements by providing detailed records of user activities and access permissions. This ensures transparency and accountability in data handling practices, mitigating the risk of non-compliance penalties.

Thinking small – in the form of policies in cybersecurity strengthens the organization's defenses by paying attention to the smallest details of user actions and behaviors. This proactive approach enables organizations to effectively identify and mitigate security risks, fortifying their overall security posture.

Access is Once and Done, Actual Security is Continuous

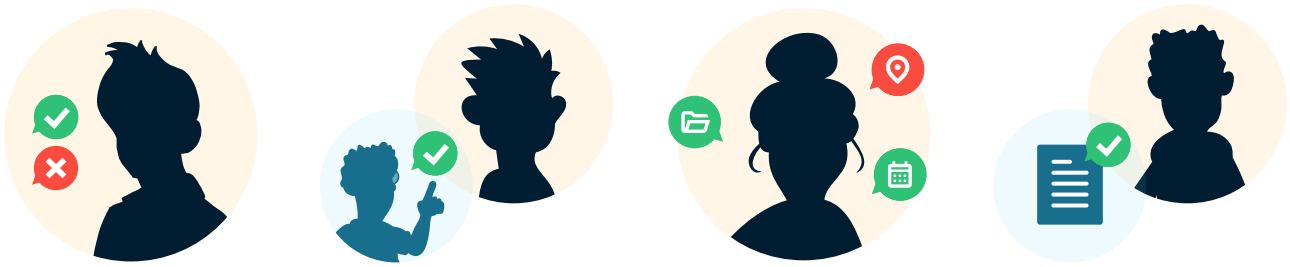
Continuous monitoring of user actions in an IT environment mitigates risks across the entire environment by quickly detecting and responding to suspicious or anomalous behavior. With Zero Trust PAM, you can identify and address suspicious behavior in real-time, ensuring continuous compliance with data security regulations and minimizing insider threats. Granular access controls detect signs of compromised accounts, while real-time response capabilities help contain security incidents. These measures are vital for proactive risk management and maintaining regulatory compliance in a continuous authorization security strategy.



Zero Trust PAM delivers continuous, contextually aware, and finely-grained authorization and control over access within an organization's digital ecosystem. At its core lies a policy engine facilitating distributed enforcement of centralized policies across various systems and applications. This decentralized enforcement model ensures access controls remain consistently applied, regardless of the specific operational context. And, as policies need to evolve to address changes in the business or regulatory environment, they can be quickly and easily rolled out and deployed everywhere.

One of the key advantages of the continuous authorization model is its ability to enable elevated permissions for granular operations. This means that organizations can provide users the necessary permissions to perform specific tasks for only the time needed. This fine-tuned control over access is made possible through the implementation of *BAC (Anything-Based Access Control) policies, which support a range of access control models, including Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control (PBAC). Additionally, organizations have the flexibility to define custom actions and parameters within these policies, empowering them to align access controls with their unique security requirements and operational workflows.

By leveraging Zero Trust PAM, organizations can establish a robust security framework that adapts to the dynamic nature of modern digital environments. This approach enhances security posture and fosters a culture of compliance and accountability, where access decisions are made based on real-time context and risk assessments.



***BAC**
Anything-Based

RBAC
Role-Based

ABAC
Attribute-Based

PBAC
Policy-Based

It's Now About Preventing Breaches, Not Access

The Zero Trust PAM approach is a paradigm shift in security protocols, offering greater accuracy for dynamically controlling privileged actions across managed resources. This approach ensures that access permissions are tailored with precision, granting users the necessary privileges to perform specific tasks without compromising overall security. Using a robust policy-based action control mechanism, organizations can establish a finely-grained security framework that adapts to the evolving threat landscape.

One of the primary objectives of Zero Trust PAM is to provide frustration-free access to users, enabling them to securely access the resources essential for their job functions without encountering unnecessary obstacles. This seamless access enhances productivity and creates a positive user experience, thereby promoting greater efficiency within the organization.

Zero Trust PAM enables enterprises to implement on-demand access protocols, and organizations can significantly reduce their attack surface and eliminate excess privileges, thereby mitigating the risk of unauthorized access and potential security breaches. The continuous aspect means that detection and mitigation are informed in real-time through persistent evaluation of actions.

In addition to enhancing security measures, Zero Trust PAM ensures continuous compliance with regulatory standards and organizational policies. Through policy-based action control, organizations can enforce real-time, verifiable Zero Trust compliance, which minimizes the risk of non-compliance penalties and maintains a robust security posture. This approach to compliance management not only safeguards sensitive data but also instills customer confidence regarding the organization's commitment to security and regulatory adherence.

By applying Zero Trust PAM, enterprises achieve critical security and compliance fortification with these capabilities:

- **Zero Trust Anywhere:** This empowers organizations to implement continuous, contextual, and granular authorization and control across their entire technology stack. This includes Software-as-a-Service (SaaS) platforms, custom applications, and infrastructure components, ensuring that access permissions are dynamically tailored based on real-time context and user behavior.

- **Access Visibility:** With Zero Trust PAM, organizations gain enhanced visibility into access requests and user activities across their digital environment. This visibility enables proactive monitoring and detection of potential security threats, allowing organizations to respond swiftly and effectively to mitigate risks.

- **Fine-Grained Action Control:** Zero Trust PAM extends beyond traditional access controls to precise control over specific operations and actions within applications and infrastructure. This fine-grained control ensures that users are only granted permissions necessary for their designated tasks, reducing the risk of unauthorized activities or data breaches.

- **Zero Trust Architecture Without Rewriting Apps:** This capability enables organizations to adopt Zero Trust principles without the need to overhaul or rewrite existing applications. By implementing Zero Trust architecture, organizations can strengthen security measures within their current infrastructure, mitigating risks associated with legacy systems or complex application environments.

- **Cloud Native Authorization for Non-Cloud Native Systems:** Zero Trust Authorization provides cloud-native authorization capabilities even for applications not designed for cloud environments. This enables organizations to leverage modern security protocols and controls, enhancing security posture across cloud-native and legacy applications.

- **Bringing Ever More Fine-Grained Control to SaaS Applications:** Zero Trust Authorization offers finer-grained control over access and permissions within SaaS applications, surpassing the capabilities of native controls. This ensures that organizations can enforce consistent security policies across their entire application portfolio, regardless of the platform or provider.

- **Centralized Policies Enforceable Across Distributed Infrastructure and SaaS:** With Zero Trust PAM, organizations can enforce security policies consistently across their entire IT infrastructure, including on-premises infrastructure and cloud-based SaaS applications. This unified approach to policy enforcement simplifies security management and ensures compliance with regulatory requirements.

Importance of Context

With the introduction of Zero Trust Contextual Policy-Based Control, solutions like the StrongDM® Dynamic Access Management Platform empower enterprises to elevate their security controls for critical infrastructure and resources. This is accomplished through micro-authorizations, contextual awareness, and robust enforcement mechanisms.

Micro-authorizations allow security teams to define and enforce access permissions at a highly granular level, ensuring that users only have access to the specific resources, data, and functionalities required for their tasks. This fine-grained control minimizes the risk of unauthorized access and unsanctioned actions and reduces the potential impact of security breaches.

Contextual awareness enhances security posture by considering various factors such as user behavior, device attributes, and environmental conditions when evaluating access requests. Organizations can better identify and mitigate potential security threats by contextualizing access decisions based on real-time data.

Strong enforcement mechanisms ensure that access policies are consistently applied and enforced across the entire infrastructure, regardless of the user's location or device type. This ensures uniform compliance with security policies and helps prevent unauthorized access attempts.

Ultimately, Zero Trust PAM uses policy-based contextual controls to enable greater precision and contextual awareness for enterprise security teams by providing a comprehensive framework for access management. By implementing micro-authorizations, leveraging contextual awareness, and enforcing strong security policies, organizations can enhance their security posture and better protect their critical assets against evolving cyber threats.

Policies, Context, and Continuous Security Efficacy

The vision of Zero Trust PAM is a shift in cybersecurity that continuously scrutinizes and evaluates a user's actions in real-time against dynamic policies. StrongDM uses this approach to ensure that each command, query, and resource configuration change is assessed within the user's context, the action's nature, and the evolving threat landscape.

With the StrongDM platform, security and compliance teams can establish a robust security framework that adapts to emerging risks and safeguards critical, managed assets across the enterprise. Trust is never assumed using this approach, and security measures are continuously enforced, enabling technical teams to mitigate threats and maintain the integrity of their systems and data.

Learn how the Zero Trust PAM approach provided by StrongDM can help your organization enhance their security posture and foster a culture of vigilance and resilience that will enable you to achieve the security rigor required in today's security landscape.

What StrongDM Delivers

TOTAL CONTROL

Access is **100% auditable**. Understand who, what, when, where, and why.

REDUCE RISK

Implement **Zero Standing Privileges**, access exists only when it is needed. Eliminate credential exposure and reduce attack vectors.

COMPLETE DEPLOYMENT

High **Return on Investment**. Low total cost of ownership and increased productivity for administrators and users.

strongdm

StrongDM provides a dynamic access platform that gives every business secure, dynamic access controls that people love to use. Trusted by the Fortune 500 to fast-growing businesses like SoFi, Chime, Yext, and Better, StrongDM gives businesses the control and visibility they need at the speed they want, with one platform that works for every environment. Connect with us on LinkedIn, Twitter, Facebook, YouTube or head to www.strongdm.com to learn more.