SSH

Break-Glass Access: When Traditional PAM Tools Fail (To Do What They Are There For)

Traditional PAM tools offer the capability to create and manage break-glass emergency access, but this functionality is highly dependent on the tools' operationality. Traditional PAM tools do not offer emergency access in case of PAM tool failure.

In this paper, we discuss how to manage break-glass access in a modern way, even during PAM tool failure.

Index

Introduction

In modern IT environments, protecting an organization's secrets and access to them is everything. Businesses are offered a variety of approaches to access and secrets management to choose from, and often, the more thorough and secure they want to be, the more complex their environments get. As a result, organizations manage their secrets and access with a combination of tools – some of them deployed on-premises, some in the cloud, and some tools are hybrid – usually, the organization's Privileged Access Management (PAM) tool is at the center of their access management.

Unfortunately, more complexity means more potential points of failure. For that reason, when deploying an access management solution, like a PAM tool, businesses often require a "back-up" capability that would allow users to preserve their access rights even if the PAM tool fails or breaks down. This type of emergency access is called break-glass access.

What is break-glass access?

Break-glass access refers to a procedure used in critical emergencies or exceptional cases, when a user with insufficient access is granted elevated access rights to bypass normal access controls. The user then gains immediate access to accounts or targets that they wouldn't normally be authorized to access with the aim of performing emergency tasks, which they wouldn't perform during regular, day-to-day operations.

Break-glass access is granted through a dedicated break-glass account which is traditionally created in advance. The account is typically highly privileged and allows access to the most critical systems, like root accounts. For that reason, break-glass accounts are well monitored, documented, tested, and managed to avoid any misuse. The related break-glass credentials that allow access to the account are typically quickly available to prevent unnecessary delays and have a time duration limit, which helps to control and reduce the account usage to certain tasks only.

When might you need break-glass access?

An emergency break-glass access should be used only in situations when normal procedures are insufficient or unavailable. For example:

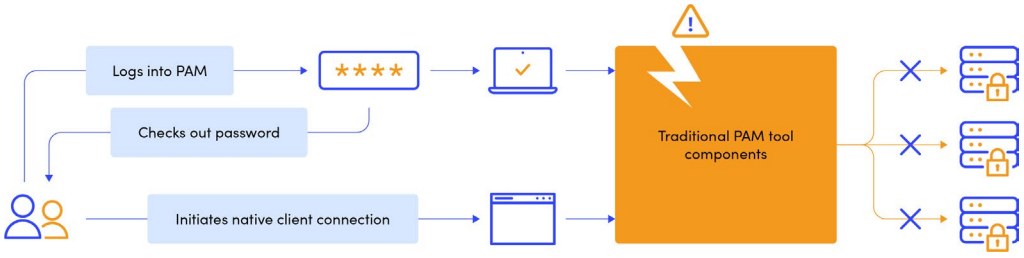
- The deployed PAM tool is unavailable due to excessive downtime or maintenance.
- PAM tool failure – the authentication process fails due to the server being down.
- Multi-factor authentication (MFA) is required but unavailable due to network outage.
- Account problems due to a cyberattack – access to all accounts was removed.
- Account problems due to a locked password – the password was typed incorrectly too many times.

The traditional way of managing break-glass access

The traditional way to manage break-glass access is via a PAM tool. Traditional PAM tools offer the functionality to create, monitor, and manage break-glass accounts. However, their capabilities are limited and dependent on the operationality and availability of PAM tools.

Traditional PAM solutions operate one or more access strongholds and password vaults through which all access is managed, including break-glass access. Typically, in an emergency situation when break-glass access is needed, a user checks out a system account password from a password vault in order to bypass the normal access controls.

In most scenarios, managing break-glass access through a PAM tool is enough. However, the problems arise during a PAM tool failure or unavailability – when one of the PAM tool components, either a stronghold or a password vault, becomes inoperable. This results in the inability of the PAM tool to provide regular as well as break-glass access. Like this, the deployed PAM tool basically becomes a single point of failure.



A traditional PAM tool needs to be operational at all times to provide access, including break-glass access. During a PAM tool failure, availability disruption prevents any access to targets.

Additionally, there is no way to make a traditional PAM tool "bullet-proof" - there is no system that can keep the tool operational at all times. However, there are modern solutions that offer another way to manage and operate break-glass access even during PAM tool unavailability.

The modern way of managing break-glass access

The solution to the PAM failure problem is implementing an access management solution that is capable of utilizing several ways to access targets, even when break-glass access is needed. One such solution is, for example, SSH's Zero Trust Suite.

This is how SSH's Zero Trust Suite implements the modern way of managing break-glass access:

Use encryption keys to ensure access

Traditional PAM tools do not offer comprehensive encryption key management, thus utilizing SSH keys for break-glass access is not possible.

On the other hand, Zero Trust Suite offers full-on encryption key management, including discovery, management, and automation of the entire SSH key lifecycle as well as the possibility to migrate to keyless access.

When break-glass access is needed but the deployed PAM tool is not available, Zero Trust Suite can utilize SSH keys to ensure access to the system. For example:

- The PAM tool is unavailable due to downtime or maintenance. It is possible to schedule provisioning and de-provisioning of SSH keys before the expected downtime.
- PAM tool failure or unexpected downtime. New access keys can be provisioned within seconds upon request for a specific time duration, utilizing existing ticketing tools or through a dedicated user portal. The procedure is fully documented and audited and allows the implementation of approval flows.

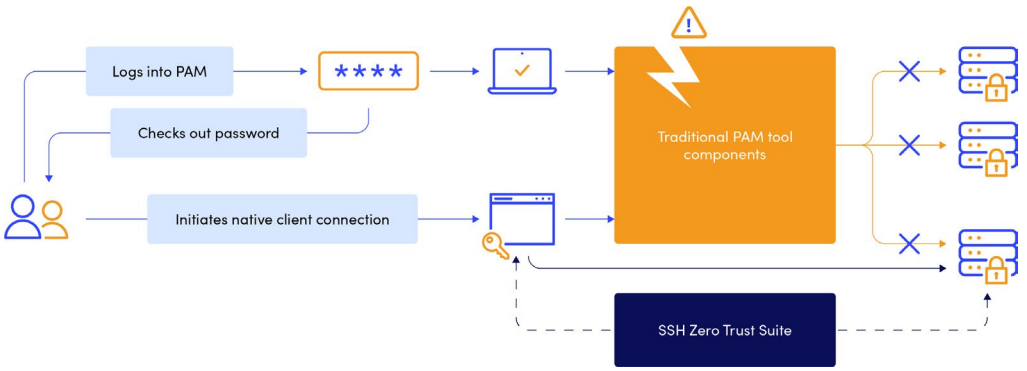
Eliminate passwords and password vaulting

Traditional PAM tools use password vaults, which are a potential point of failure. When a password vault is unavailable, the break-glass access password cannot be checked out. Thus, the entire system is unavailable.

Our modern Zero Trust solution offers passwordless (and keyless) access using ephemeral certificates, eliminating the need for password vaulting entirely. In this model, access is granted just-in-time for the session, and all the secrets needed for authorization are inside the certificate which automatically expires once the authorization is done. Users do not see or handle any secrets during the session.

In effect, this approach also eliminates the password vault's point of failure.

Additionally, ephemeral certificates provide the option of break-glass access without involvement of third-party tools or applications. In other words, if necessary, the connection between the native client and a target could be established directly, without the involvement of a PAM tool or even SSH Zero Trust Suite.



SSH Zero Trust Suite offers the option to schedule provisioning and de-provisioning of break-glass SSH keys in advance of a PAM tool downtime. It also enables immediate provisioning of SSH keys upon request and within seconds. Once the credentials are deployed access to targets is available without the involvement of any third-party applications or tools.

Zero Trust Suite also offers the option to use ephemeral certificates that allow break-glass access to targets, with the ability to implement approval flow processes when granting access. Like that, it is possible to gain full visibility into SSH sessions via searchable audit trails.

Approval workflows

SSH Zero Trust Suite has built-in Approval Workflow which could be selected to enforce the approval process even during a break-glass period.

When integrated with an existing ticketing system, it is also possible to align the workflow with enterprise-wide processes.

Audit trails

With Zero Trust Suite, detailed audit trails are available to keep access records of break-glass accounts.

The records contain information on who used the accounts (interactive users or machines), when the accounts were used, and what targets were accessed during the break-glass period.

Session recording is optional if video recording is required to see what actions were performed.

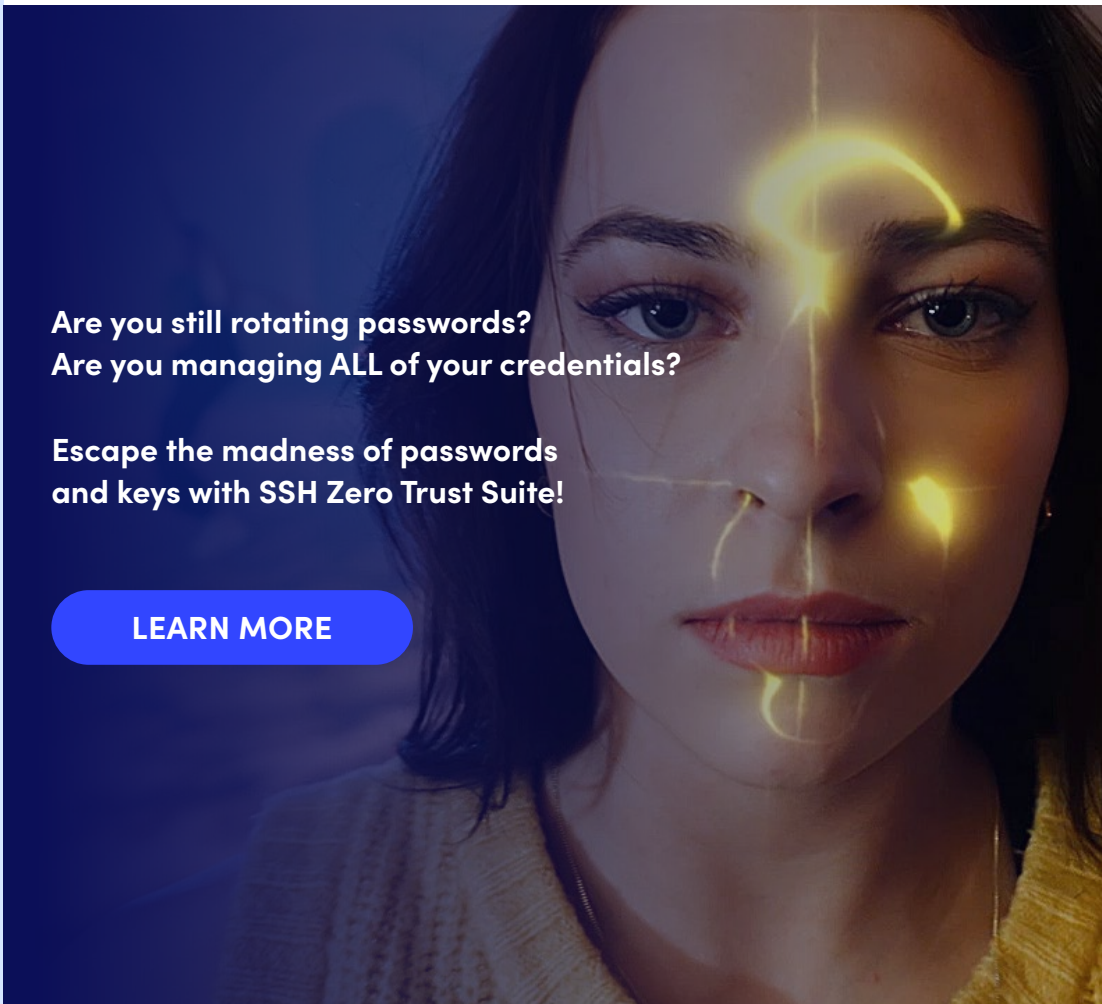
Keyless and passwordless access and secrets management with SSH Zero Trust Suite

SSH Zero Trust Suite can help you stop managing, rotating, and vaulting credentials and implement modern access and secrets management suitable for modern hybrid IT environments.

Zero Trust Suite combines management of passwords, keys, and other credentials into a single centralized solution. It also allows you to plan your path and migrate to passwordless, keyless, and credential-less access management at your own pace.

Less is more applies even to access and secrets management. Your IT environment is already complex enough. But with Zero Trust Suite, you can simplify, streamline, clean up, and lean up your environment and processes. The reduced cost of managing your access is only a cherry on top.

Credential-less is simply more.



SSH

We'd love to hear from you!

Get in touch with our experts around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH COMMUNICATIONS
SECURITY CORPORATION
Karvaamokuja 2b, Suite 600
FI-00380 Helsinki
Finland
+358 20 500 7000
info.fi@ssh.com

US HEADQUARTERS

New York City

SSH COMMUNICATIONS
SECURITY, INC.
434 W 33rd Street, Suite 842
New York, NY, 10001
USA
Tel: +1 212 319 3191
info.us@ssh.com

APAC HEADQUARTERS

Hong Kong

SSH COMMUNICATIONS
SECURITY LTD.
35/F Central Plaza
18 Harbour Road
Wan Chai
Hong Kong
+852 2593 1182
info.hk@ssh.com

SSH

Let’s get to know each other

Want to find out more about how we safeguard mission-critical access for leading organizations around the world? We’d love to hear from you.

REQUEST A DEMO

SSH