sbPAM

# STEALTHBITS PRIVILEGED ACTIVITY MANAGER

Secure, task-based privileged access management

stealthbits

Data breach has become commonplace and typically spread through the overabundance of privileged access rights to systems that attackers exploit. Most Privileged Access Management (PAM) vendors focus on controlling access to managed privileged accounts. While this approach can provide just-in-time access for administrators, the accounts still retain their privileges while not in use (aka standing privileges) resulting in a widespread attack surface that attackers use for lateral movement. This problem is compounded as organizations assign more managed accounts to each administrator.

## Just-in-time PAM while reducing attack surface

Stealthbits Privileged Activity Manager (SbPAM) facilitates secure administrative access using third generation technology that is both intuitive and easy to deploy. SbPAM automatically generates ephemeral accounts for each administrator then dynamically provisions and deprovisions just-in-time permissions that are appropriate for the requested activity. This action removes the 'standing privilege' attack surface when accounts are at rest and removes the overhead of maintaining complex access control groups.

- **Ensure Authorized Access** - Adaptive Zero Trust security architecture with multi-tier approval capability ensures all privileged access is authorized.
- **Zero Standing Privileges** - Rights dynamically provisioned at the time required, and then removed on completion.
- **Meet Best Practices** - Support the separation of privileged access accounts for admin vs. productivity tasks.
- **Gain Proof** - Record and playback all administrative activity (e.g. accidental or malicious) over RDP and SSH.
- **Just-in-Time Access** - permissions can be dynamically provisioned to single user, dual (ephemeral or namesake) and shared service accounts.
- **Reduce Future Attacks** – Auto-purge Kerberos tickets after session access to mitigate pass-the-hash and golden ticket attacks.
- **Real-time Service Account Management –** See updates and status changes as they happen. Immediate alerting if issues discovered with options to pause and roll-back changes.

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

**GOLD WINNER**

**Privileged Access Management by Cybersecurity Excellence Awards**

## KEY FEATURES

### Zero standing privileges (ZSP)

Permissions to perform a requested activity are allocated at the time it is required and then immediately removed on activity completion for Zero Standing Privilege.

### Ephemeral account support

Use SbPAM "Activity Tokens" to provide temporary permission and access that are auto-provisioned when needed and de-provisioned when not.

### BYOV-Bring your own vault

Stealthbits Privileged Activity Manager contains a built in vault for credential management, but can uniquely map to vaults from other vendors in order to capitalize on exiting PAM investments.

### Access certification

Gain the unique ability to certify user entitlements for compliance. Why perform in another system? Built-in workflow and exportable data.

### Session recording & playback

Enforce accountability or gain evidence during investigations with recorded sessions. Live monitoring with lock, block and remote terminate functions.

# THE POWER OF ACTIVITIES

## Attack surface reduction

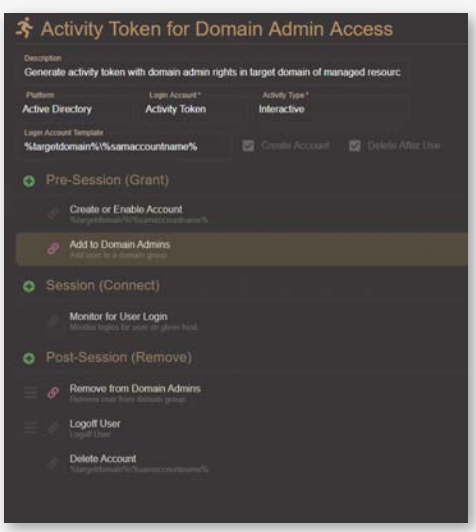
Until now, organizations have been faced with the burden of ever-growing privileged accounts and the attack surface they represent. Traditional methods of threat mitigation have centered around the management of the accounts, but have not addressed the root of the problem.

SbPAM dynamically assigns and removes permissions to accounts as they are being used through Activities. When accounts are at rest, they have no privileges, rendering them harmless.

## What are activities?

An Activity is a structured set of steps

- Pre-Session (Grant permissions to user)
- Session (Connect user to resource)
- Post-Session (Remove permissions from user)




During the Pre-Session phase, an account might be created/enabled and roles assigned. The Session phase determines the nature of the activity (e.g. interactive server logon, application launch). The Post-Session phase ensures that accounts used for the activity have their permissions reset, and optionally, the accounts can be disabled or removed.

# Simple configuration

Compared to traditional PAM tools, STEALTHbits Privileged Activity Manager policy management is designed to be straightforward and easy to configure. Access Policies are made up of three (3) basic elements:

- Users - administrators requiring privileged access
- Resources - systems or applications
- Activities - steps to setup, monitor, and reset

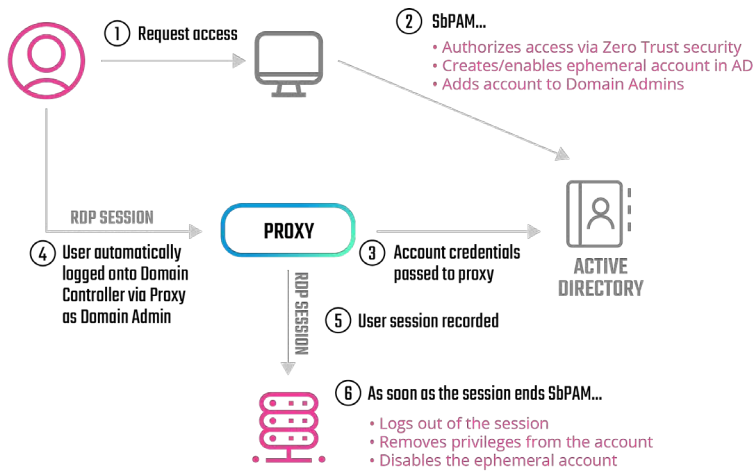
Reduced complexity is key to enabling operational security. Critical infrastructure access requires policies that are clear and unambiguous, but flexible enough to deal with the nuances of each environment.

# Proxy - The critical element

Logging directly onto managed systems from desktops leaves artifacts that can be compromised and inevitably requires ports to be opened into secure networks.

A critical element of any PAM solution is a proxy that is able to securely broker the connection between security zones and provide recording and playback capability for administrator accountability.

## Just-in-time domain admin permissions




As a tier-1 component, the proxy has been designed with self-healing redundancy and the capability to scale using an architecture supported on both Windows and Linux.

- Launch directly from native SSH/RDP clients
- 2FA authentication fully supported for all connection types

## Schedule a Demo

stealthbits.com/demo

## Download a Free Trial

stealthbits.com/free-trial

## Contact Us

info@stealthbits.com