DATA SHEET

STEALTHbits Privileged Activity Manager

ZERO TRUST PRIVILEGED ACTIVITY MONITORING AND MANAGEMENT

Data breach has become commonplace, and despite significant investments in perimeter and endpoint security, breach typically begins at the desktop and server layers of an organization's IT infrastructure and spreads through the overabundance of privileged access rights to each system and other misconfigurations and vulnerabilities attackers exploit.

While most Privileged Access Management (PAM) vendors technically supply the capability to solve the privileged access problem at the root of every data breach, existing PAM solutions focus on controlling access to accounts and their passwords, not on the activities the administrator needs to perform. The result is minimal reduction of an organization's attack surface because the accounts still exist on the endpoint and can still be compromised using modern attack techniques.

JUST-IN-TIME, SECURE AUDITED ACCESS CONTROL

STEALTHbits Privileged Activity Manager facilitates secure audited administrative access to servers and desktops using third generation PAM technology that is both intuitive and easy to deploy. The solution securely authenticates every user and adds just-in-time permissions that is appropriate for the requested activity and removes them when the activity is complete; this removes the attack surface when accounts are at rest and removes the administrative burden of maintaining access control groups.

- Zero Trust security architecture to ensure that all privileged access is authenticated at all times.
- Just in time access ensures that the user is granted rights to perform the activity at the time it is required, and until the activity is complete.
- Just enough permissions are assigned to the activity for true least privilege delegation.
- Advanced proxy architecture with self healing and elastic scalability allows access to be granted across security zones.
- Flexible distributed architecture ensures consistent performance across the largest, most complex installations.

KEY FEATURES

Attack Surface Reduction

"Remove rather than manage". STEALTHbits Privileged Activity Manager only applies privileges to accounts when they are being used. This reduces the overhead and attack surface of traditional privileged account management.

Just-in-Time Access / Just Enough Privilege

Only enough permissions to perform the requested activity is allocated, at the time it is required. True delegated access—no more broad admin-level permissions.

Activities

Rather than map users to accounts that have persistent privilege, STEALTHbits Privileged Activity Manager dynamically adds and removes privileges as users require them.

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.

Built-in Proxy

Security best practices dictate that user workstations should be segmented from critical server infrastructure. Transparent proxies allow secure administrative connection.

THE POWER OF ACTIVITIES

A New Approach

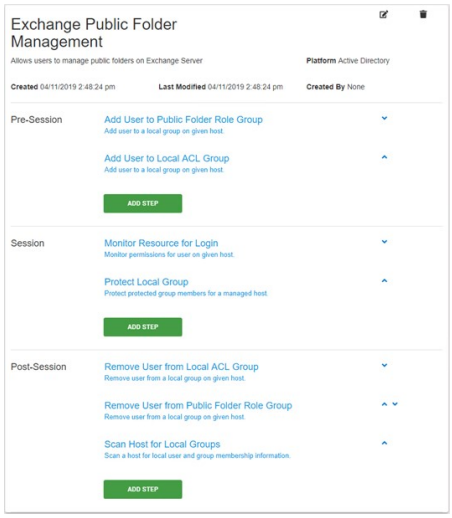
Until now, organizations have been faced with the burden of ever-growing privileged accounts and the attack surface they represent. Traditional methods of threat mitigation have centered around the management of the accounts but not addressed the root of the problem.

STEALTHbits Privileged Activity Manager 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 made up of 3 phases:

- Pre-Session
- Session
- Post-Session



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 3 basic elements: Users, Resources, and Activities.

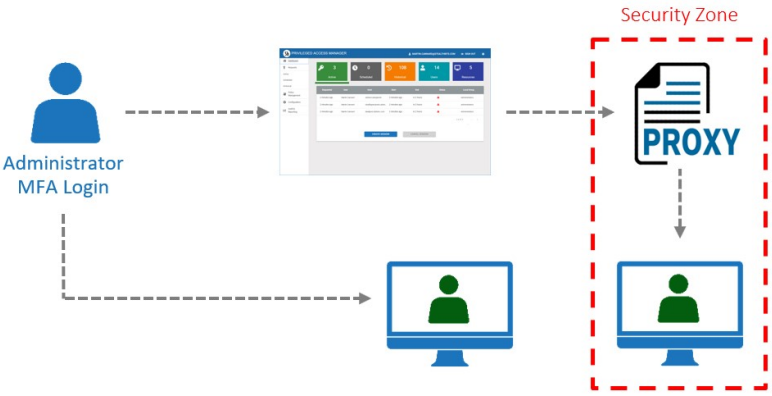
- Users - administrators requiring privileged access.
- Resources - systems or applications.
- Activities - steps to setup, monitor and reset.

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 broker the connection between security zones. STEALTHbits Privileged Activity Manager includes an advanced session proxy out of the box for automatic connection to privileged sessions.



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.
- Countdown timer and session extension options.

Schedule a Demo

stealthbits.com/demo

Download a Free Trial

stealthbits.com/free-trial

Contact Us

info@stealthbits.com