ACDS
ADVANCED CYBER DEFENCE SYSTEMS

Privileged Access Guard

Protect the “keys to the kingdom” of your sensitive information.
Manage the access of all privileged and admin users.

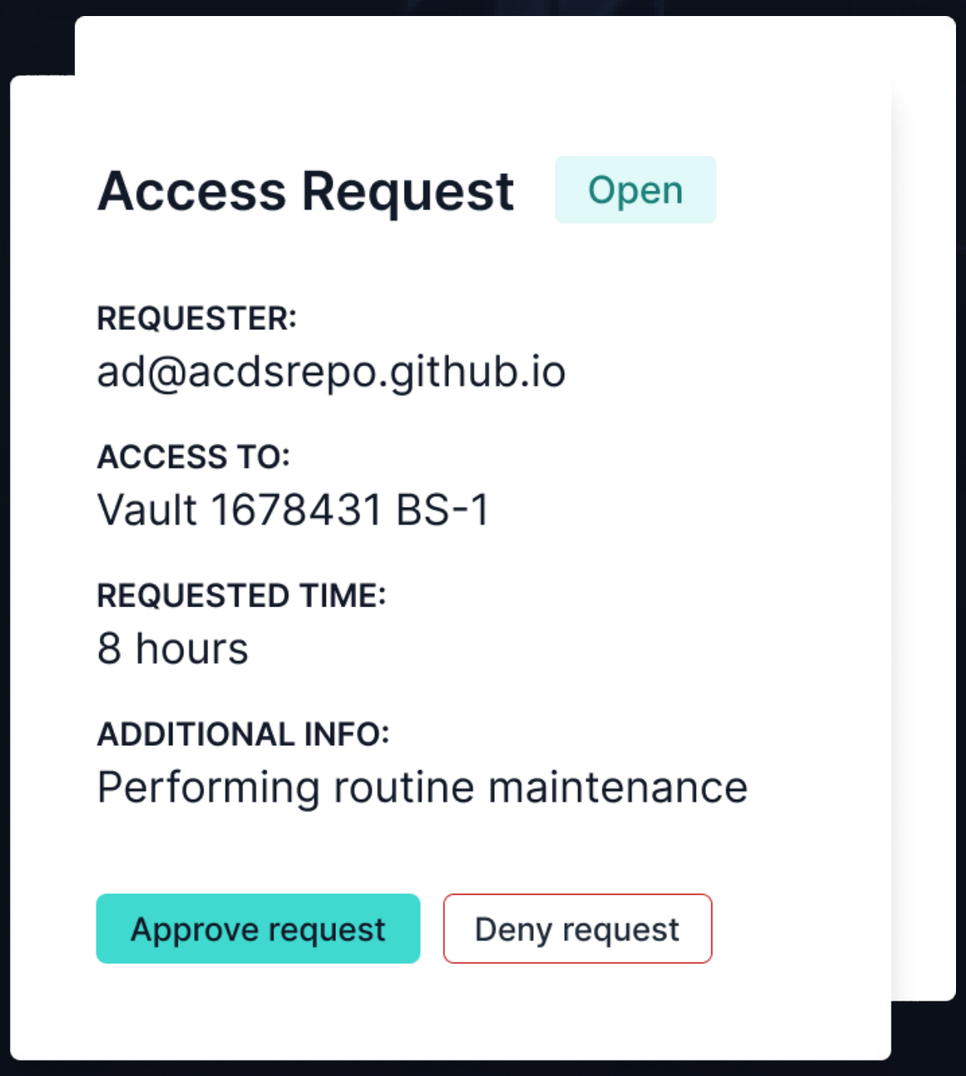
The increase in sophisticated, targeted security threats by both external attackers and malicious insiders have made it extremely difficult for organisations to properly protect critical and sensitive information. The task of protecting these assets has only grown harder as IT environments have become more complex and widely distributed across geographic locations and in the cloud.

Many recent high-profile breaches have one thing in common: They were accomplished through the compromise of credentials.

277 days

Average length of time that an unauthorised access can go undetected, allowing cybercriminals to see and steal information at their convenience.

Control access to critical systems.



Privileged Access Management (PAM) is an additional security measure that you can place in front of your system administration interfaces making it more difficult for an attacker to access critical systems and, at the same time, providing an audit trail, making it easier to identify misuse of administration interfaces.

Privileged Access Guard is a workflow tool for system administrators to grant users limited time-bound access to elevated permissions in an auditable manner. We’ve built Privileged Access Guard to make the protections of PAM accessible to a much wider audience at a fraction of the cost and time to deploy.

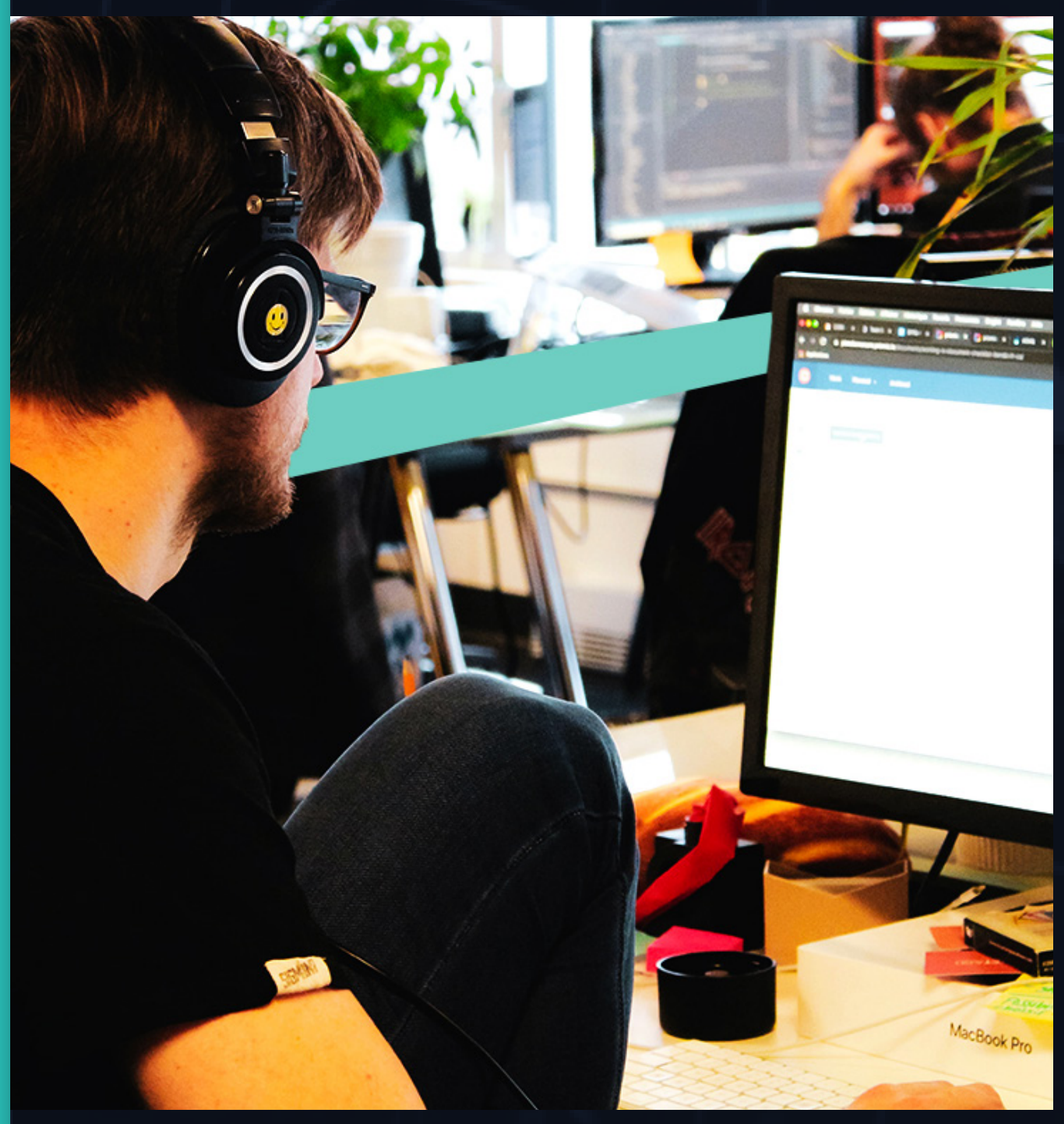
Privileged Access Guard is built on the core principles of PAM: Just in Time (JIT) Administration, Principle of Least Privilege (PoLP) and Lightweight and Protective Administration. These are proven methods to protect IT assets and ensure that the right user has access to the right resources, for the right purpose and for the right time frame. Grant privileges only as and when needed to reduce the attack surface, minimise insider threat, and implement a robust security policy to protect sensitive IT resources.

Key Features:

- Credential management for privileged accounts
- Delegation of access to privileged accounts
- Time-bound privilege elevation
- Full logging for comprehensive audit trail
- Supported credentials include passwords, password vaults, SSH keys.

Future capabilities include:

- Secrets management for applications, service and devices
- Fully integrated with Keycloak (others coming soon).
- Privileged task automation (PTA)



Benefits:

- Protects internal staff members as well as external contractors and ensures any account that is breached can be traced immediately.
- As a system administrator, Privileged Access Guard removes the burden of securing and protecting your privileged administration credentials. The access provided is temporary in nature.
- As a system risk owner, Privileged Access Guard provides you with confidence that the privileged management interfaces of your systems are being used and accessed as intended. You have visibility into what requests are being generated by whom.
- Privileged Access Guard makes it more difficult for attackers to use stolen administration credentials.

ACDS
ADVANCED CYBER DEFENCE SYSTEMS