MAVIS PNTL

Hybrid MultiCloud PAM

The challenge

Asset management

Nowadays, most organizations may need to set up servers such as cloud service virtual machines, local information data centers, and even hybrid multi-cloud solutions to respond to internal or external services, especially the ones linked to multiple environments. In fact, avoidable access to cross-platform, cross-machine, or third-party tools can lead to excessive data traffic or even over-complicated privileges, raising error rates or maintenance costs. Besides, if files or data is unencrypted, exposure to potential lack of identity or file leakage may also result in a loss too high to take.

Identity privilege

When an organization requires full executive control, it usually requires a lot of staffing and planning to meet both business needs and an easy-to-manage environment. If the organization or the administrator does not maintain this on a regular basis, identity accounts or privileges in the system may exceed work process requirements. Under this premise, if an account is stolen or leaked, it can be used to steal confidential and sensitive information, which could cause irreparable damage to the organization.

Operation record

Whether operating a local information data center or a cloud service, it’s difficult to efficiently record the entire process, from operation logs to screen recordings, due to tool limitations. Not only is it easy to overlook all operation log records, but some files cannot be effectively managed. Storing these recording files requires additional storage space and proper use of the recording files requires considerable years of protection. In addition to leaving logs and operation records, there is a high possibility that operation logs recorded in the past cannot be viewed effectively during inspections and management due to time and operational management issues.

Function description

Encryption protection mechanism
- AES-CBC 128-bit

Two-factor authentication
- TOTP RFC 6238

Complies with the requirements of the international certification ISO 27001

Agentless local-cloud integration
- Reduce security risks and management costs

Project management
- Manage asset and corresponding access role permissions through the project structure

Dashboard
- Projects, asset information and user usage records can be viewed at a glance through analytics dashboards

Device management
- Provide import or manual add to manage servers in a unified way
- Direct connection to the target device through the web interface

Web Application Management
- Mavis allows for the onboarding of web applications such as AWS Console, GCP Console, Azure Console, and Github. By enabling automated login, users no longer need to manually record access information. They can simply connect to these applications and have their activities automatically recorded.

Cloud credential management
- Manage three public clouds, AWS, GCP and Azure, and private cloud VMWare to manage

Project
- Manage access to project member’ roles and composition to enhance privilege management and asset maintenance

Access service management
- Add device connection information and prevent project members from receiving that directly through privilege settings
- Provide Linux operating system, Windows operating system and file upload and download services

Log
- Record all user operation in the system
- Record user’s connected device operation log

User management
- Through user account status management, real-time setting enable and disabled user login access

Project management
- Existing projects can be edited, deleted and full record kept

System information
- Allow authorized management and view system version information

System log
- Record operations with higher authority, such as project or user settings

MAVIS
Hybrid MultiCloud IT PAM

The solution

Core Values

Mavis - A dashcam for ITOps that integrates three core functions to empower administrators and reduce the administrative burden.

PAM privilege management

Mavis provides secure and complete IT maintenance management based on zero-trust architecture and privilege access management

Hybrid multi-cloud, cross-cloud centralization

Mavis centrally integrates and manages all your organization’s IT assets through cloud providers like AWS, GCP, Azure and VMWare or local information data centers.

Full operation records

Mavis fully logs all connection operations, making it easy to find the content you need.

Four modules

Cloud credential manager

■ Mavis provides multi-cloud integration capabilities including management of three major public clouds: AWS, Azure, GCP, and private cloud: VMWare, by importing cloud credentials or APIs to quickly manage corporate resources.

■ Users can not only manage their cloud credentials, but also select and manage their desired servers through the management processes provided by Mavis. This avoids adding too many unnecessary machine information and causing administrative problems.

■ After selecting a cloud server to import into management, through Mavis’ automated process, the cloud server managed by Mavis can be synchronized with the state of the cloud, allowing users to perform multi-cloud management and manage multi-cloud through one platform.

Resource access manager

■ As long as devices that support SSH or RDP connections, such as network devices, Linux operating systems, and Windows servers, can be connected through Mavis.

■ Besides managing imported servers via cloud credentials, users can also add servers manually, simply configuring the connected machine’s IP address and related information to manage the resources into Mavis.

■ After manually adding a server or importing a cloud resource, you need to add the connection settings in Access Service Management. This parameter includes the password or access key of the connected device. Once installed, you can directly access and log in to the target device according to the configuration and the sensitive information will be protected by the secret vault.

■ Mavis also provides the SFTP protocol with which you can directly upload and download files to reduce error rates when using a variety of third-party tools.

■ In addition, users can also onboard web applications into the system, and the system can handle the login process with username and password on their behalf. This eliminates the need for regular operators to manually record access information for web pages. With Mavis, they can simply connect to the applications and have their activities recorded.

■ Mavis will fully record the operation logs by screen recording, the operator can easily find the record through the session recording.

■ To help secure the organization that manages all Mavis managed resources, the target device does not need to install any agent applications.

■ Except for session recording, Mavis will also log all the logs of the user’s operation in the system based on the user’s permission.

Identity & privilege manager

■ Managers can manage all the login sessions to control the system security by creating user accounts or configuring account access status.

■ Multiple factor authentication to protect an organization's important assets.

■ Organizations can manage assets with Mavis, and in addition to helping them categorize assets efficiently, they can also quickly subdivide assets through tags regardless of the number of devices they need to manage.

■ Each account can also be managed individually, and identities are granted different permissions for each project. Mavis provides role-based access control to achieve separation of privileges and responsibilities.