MAVIS

PNTL

Hybrid Multi-Cloud PAM Platform

Challenges

Asset Management

In the process of providing internal and external network services, companies inevitably need to establish corresponding servers to meet service requirements. Under the company's policy choices, cloud services with virtual machines may be used, or on-premises data centers may be built, or even a hybrid multi-cloud approach may be adopted. Any of these methods will require IT stuffs to maintain additional records and manage user permissions. This not only increases the workload but also increases the likelihood of errors due to cross-platform, cross-machine operations, and the need for third-party tools. Furthermore, if these records are not encrypted, it increases the risk of the company being exposed to vulnerabilities. This could lead to significant losses for the company due to lack of identity control or data leakage.

Identity and Permissions

Identity and permission management pose significant security risks for the information systems used by companies. Achieving comprehensive management usually requires a considerable amount of manpower and thorough planning to meet both the requirements of the company and the operational settings suitable for the operators. Without regular maintenance by the company or administrators, it is easy for system identities or permissions to exceed the requirements of business processes. Under these circumstances, if these accounts are stolen or leaked, they could be used to steal confidential information, causing irreparable damage to the company. Successful hacker attacks often involve the misuse or destruction of privileged accounts, highlighting the importance of protecting identity and privileges, which are crucial aspects for companies to focus on.

Operation Logs

Current operations in both on-premises data centers and cloud services are hindered by tool limitations, making it difficult to effectively record operation logs and the processes of using operations. Consequently, more tools are needed to assist in recording or capturing, which may lead to omissions and ineffective management of some files. This includes the need for additional storage space for file storage management, as well as significant retention periods to properly utilize record files, enabling retrospective and search capabilities in the event of a crisis. In addition to the preservation of logs or operation records, auditing or management is also hindered by time or operational management issues, making it difficult for personnel to effectively review past recorded operation logs. Under such circumstances, significant time is usually required to locate the actual files or records that need to be reviewed.

Features

- **Compliance and Security Standards**
  - **Compliant with ISO 27001 international certification requirements**, including A.9 Control and A.12 Logging.
  - **References NIST CSF standards**, specifically PROTECT (PR.AC) and Data Protection (PR.DS).
  - **Compliant with PCI DSS standards**, covering items 2, 7, 8, and 10 across three major areas.
  - **Adheres to the IEC 62443 international standard**, including IEC 62443-2-1 and IEC 62443-3-3.
- **Authentication and Security Mechanisms**
  - **Two-factor authentication (TOTP RFC 6238)**: Strengthens system login security by requiring time-based one-time passwords.
  - **Certificate management**: Manage and update platform certificates for secure, encrypted data transmission.
  - **Encryption protection**: Uses AES-CBC 128-bit encryption and supports HTTPS/TLS to ensure the protection of sensitive data both at rest and in transit.
- **User and Role Management**
  - **Role-based access control (RBAC)**: Precisely control user access to assets and services, ensuring that only authorized personnel can access specific resources.
  - **User management**: Monitor and manage user account statuses in real-time, allowing immediate account setup or deactivation.
  - **Group management**: Streamlines the assignment of permissions by managing user groups and syncing with LDAP systems.
- **Just-In-Time Access**
  - **Optimized approval process**: Accelerates request processing and improves accuracy.
  - **Flexible application management**: Supports advance submission and modification of requests.
  - **Transparent history records**: Easily view and export historical operation data.
  - **Quick re-apply feature**: Expedites new requests by reusing previous data, saving time.
  - **Customizable notifications**: Enhance security with tailored notification conditions, especially for repeated requests.
- **Resource, Asset, and Connection Management**
  - **Agentless cloud integration**: Reduces cybersecurity risks by eliminating the need for agent software, minimizing maintenance costs.
  - **Cloud credential management**: Rapidly import and manage cloud credentials for AWS, GCP, Azure, and private cloud platforms like VMware.
  - **Project management**: Efficiently manage multiple assets with an all-in-one framework, allowing for easy editing and deletion while maintaining full records.
  - **Access service management**: Securely manage device connection information, preventing users from directly accessing sensitive credentials.
  - **Device management**: Simplifies server management with manual and batch import options, enabling quick and direct connections through a web interface.
  - **Web application management**: Centralize control of AWS, GCP, Azure consoles, and GitHub with automatic login features and domain whitelisting.
  - **Database management**: Manage and monitor popular databases (e.g., PostgreSQL) to ensure data security and integrity.
- **Real-Time Monitoring and Logging**
  - **Real-time monitoring**: Monitor live session activity and command usage, allowing for immediate termination of risky connections.
  - **Log management**: Comprehensive logging of user actions, including access logs, retention policies, and privileged actions. Supports Syslog format and seamless integration with SIEM systems. Provides video logging for user sessions, ensuring full activity tracking.
- **System Management and Backup**
  - **System Management**: Authorize, manage, and view system version information. Backup mechanisms ensure resilience in case of system failure or data loss. High availability (HA) design enhances system reliability by providing redundancy and automatic failover capabilities to minimize downtime.
  - **Connection Settings**: Ensure stable and secure system connections, with the ability to adjust regional settings to meet the needs of multinational enterprises.
  - **SIEM Integration**: Enhance system security monitoring and response capabilities.

MAVIS
Hybrid Multi-Cloud PAM Platform

Solutions

Core Values

MAVIS Hybrid Multi-Cloud PAM Platform - Combining four core functions to effectively enhance enterprise security levels, assist management users, and alleviate management burdens.

Identity Access Monitoring and Management

MAVIS utilizes a zero-trust architecture for real-time access management, ensuring the security and compliance of privileged access. By integrating Just-In-Time Access, it further enhances asset management efficiency and protection.

Hybrid Multi-Cloud Resources Integration

MAVIS centrally integrates and manages all IT assets across clouds.

Comprehensive Record

MAVIS records all connection operations comprehensively and facilitates easy content search.

Web Applications Integration

A single interface accommodates commonly used applications to address issues related to shared account responsibilities.

Asset Access Management

- MAVIS allows connection to devices that permit SSH connections, such as network management devices and Linux, as well as RDP devices like Windows servers.
- Apart from servers imported via cloud credential management, servers can also be manually added by users, requiring only the IP address and relevant settings for uniform management within the platform.
- After importing or manually adding cloud machines, connection settings need to be added to access service management. These settings include the account password or key of the connection device. Once configured, connection devices can select to connect directly to the target machine. Through secure vault mechanisms, asset connection sensitive information is protected.
- MAVIS connects to target machines via proxy servers, offering direct file upload or download via SFTP, in addition to SSH-enabled or RDP connections. This reduces the familiarity requirement with third-party tools and differences in tools.
- Furthermore, user can manage web applications within the system. Along with account and password management, user can log in through the system, eliminating the need for recording access information for related web pages. Connections are recorded by MAVIS.
- After connecting through MAVIS, all operation records are fully recorded and the operations are easily traceable. user can replay the connection's operations via video playback or view command details in the log, achieving rapid traceback and search purposes.
- All devices managed by MAVIS do not require additional agent software installation, ensuring the most secure management for enterprises without installing any unfamiliar software on important assets.
- In addition to operation log records, MAVIS also fully records all personnel operations in the system, categorizing them based on project or system permissions for easy retrieval.

Modules

Cloud Credential Management

- MAVIS offers multi-cloud integration functionality, including management of the three major public clouds: AWS, Azure, GCP, and the private cloud VMWare. This is achieved through importing cloud certificates or via API, enabling swift management of company assets.
- In addition to managing cloud credentials, user can also use MAVIS's management processes to select and manage the necessary servers, avoiding the inclusion of excessive and unused machine information, which can cause management troubles.
- When user chooses machines for import and management, MAVIS automated processes synchronize the status of the machines managed by MAVIS with the cloud, enabling personnel to achieve multi-cloud management through a single platform.

Identity and Access Management

- MAVIS enables real-time account control, allowing management personnel to create and configure accounts instantly, which facilitates efficient login and operations. Multi-factor authentication mechanisms provide multiple layers of protection for account security, effectively safeguarding enterprise assets and access permissions.
- MAVIS also offers specific permissions control, allowing assets to be assigned different permissions for each account or identity. This responsibility-based approach ensures meticulous control over identity and asset permissions while reducing risks associated with configuration errors.
- The project-based asset management feature organizes assets according to project structures, enabling easy classification and tagging, thereby simplifying the management of numerous devices. Management personnel can efficiently oversee current login accounts; if any harmful activities are initiated, they can swiftly address these issues through a system interface that prevents ongoing dangerous operations.
- Finally, the Just-In-Time Access Integration feature enhances connection management by allowing users to submit connection requests in advance and modify them as needed. This ensures a transparent approval process and facilitates quick resubmission, streamlining overall access management.