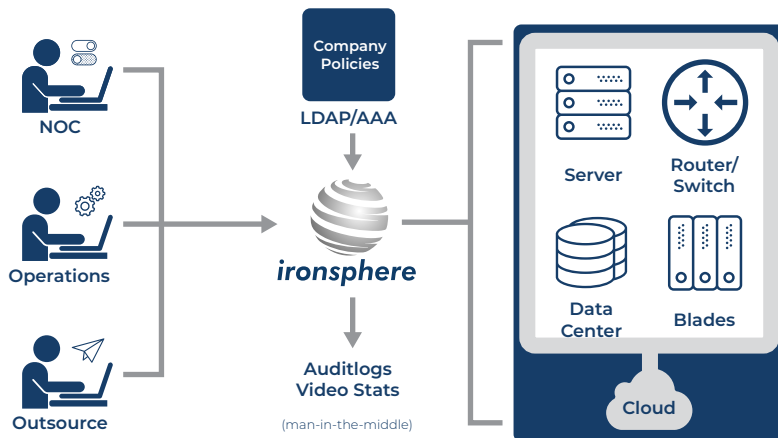


Unified Management of Privileged Access Accounts



An agentless, man-in-the-middle approach

Ironsphere Addresses:

- Regulatory Compliance
- Risk of Insider Threats
- Malware that targets privileged accounts
- Security of Outsourced IT operations (contractors and vendors)
- Audit Trails and On-demand reporting

Ironsphere unifies multi-vendor environments with pre-integrated modules, managing numerous vendors and hundreds of network elements with a single, universal system.

Unified Access Manager

Protocol-based security software unifies AAA, Active Directory, LDAP & TACACS+.

Session Manager

Logging and recording of all sessions, including command and context-aware filtering.

Data Access Manager

Securing Data Access with logging, policy enforcement, and real time data masking.

Privileged Task Automation Manager

Virtual & Physical Network Automation Suite for Telecom Service Providers and Enterprises.

Dynamic Password Controller

Takes control of device and database passwords, providing security while sustaining efficiency.

MFA Manager

Additional layers of authentication integrating mobile device, geolocation, and time.

Public Cloud PAM

Security and enhanced capabilities for users of Cloud IaaS platforms like AWS, Azure, Google and others.

Admin Management API

Lifecycle management of configurations, inventories and policies.

- » Man-in-the-middle scenario for SSH/HTTP/RDP proxy
- » Session management and dual control
- » Logging and Session Recording
- » Object Character Recognition (OCR) for RDP, RDP session recording
- » Internal TACACS+ and RADIUS Support
- » Single-Sign-On (SSO)
- » Password management, changing password in configurable interval, password history

- » Break Glass
- » Linux/Windows/Network Element Password Management
- » Limit/filter command (proxy)
- » Multitenancy
- » Advanced Policy
- » Context Aware Policy
- » Multi-Factor-Authentication (MFA) with GeoFencing