Sheaf
IT & CYBER SECURITY

OUT-OF-OFFICE
WORK FROM ANYWHERE, ANYTIME

Get secure and seamless remote access to corporate networks and resources

USAM

Universal Secure Access Management

VARIA

Multi-Factor Authentication Platform

FALCON

Enterprise Monitoring & Dashboards

POWERFUL ALL-IN-ONE TASK TOOL FOR REMOTE TEAMS

WORK FROM ANYWHERE, AT ANYTIME WITH AN EASY-TO-USE INTERFACE ON A SECURE INFRASTRUCTURE

ARION, an enterprise-class solution, designed with cyber security in mind, offers reliable network access for the modern and decentralized workforce by providing just what is needed.

“Empowering the modern and agile workforce to ensure business continuity at all times”

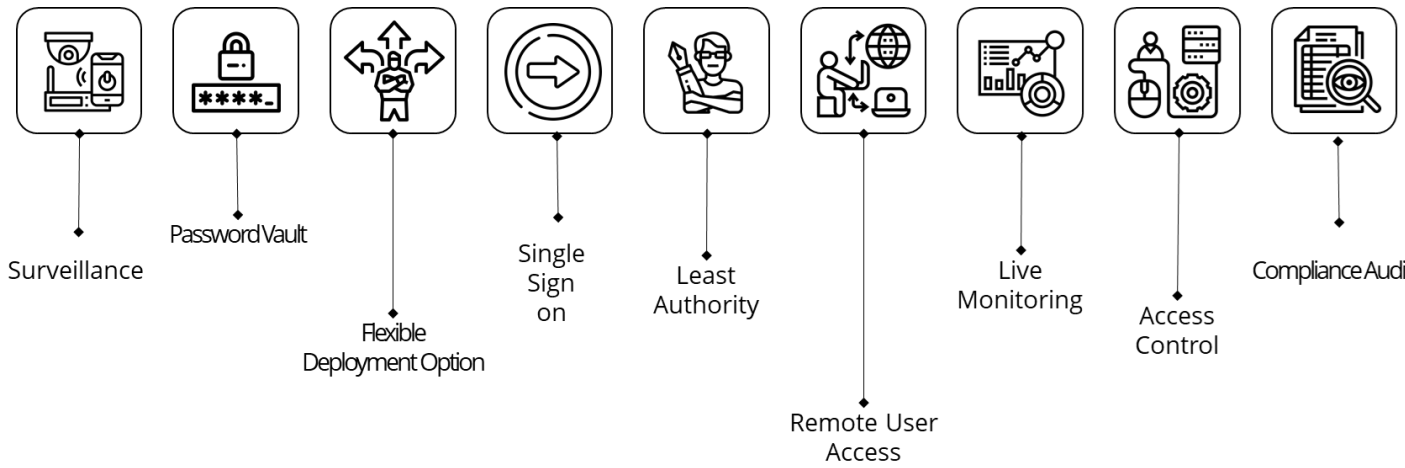
ARION FACILITIATES THE NEW NORM

‘OUT-OF-OFFICE’

Increasingly, organizations are experimenting with the ‘work-from-home’ or ‘work-from-anywhere’ practice as part of ensuring business continuity or productivity or cost-efficiency and so on amid unforeseen challenges that inhibits our ability to operate in a desired operational model for an organization.

ARION offers a range of functions for such out-of-office access while enforcing stringent policy and control over remote access, as part of **cybersecurity management plan.**

ARION is integrated with three cyber security and monitoring solutions, namely USAM, VariA and Falcon.

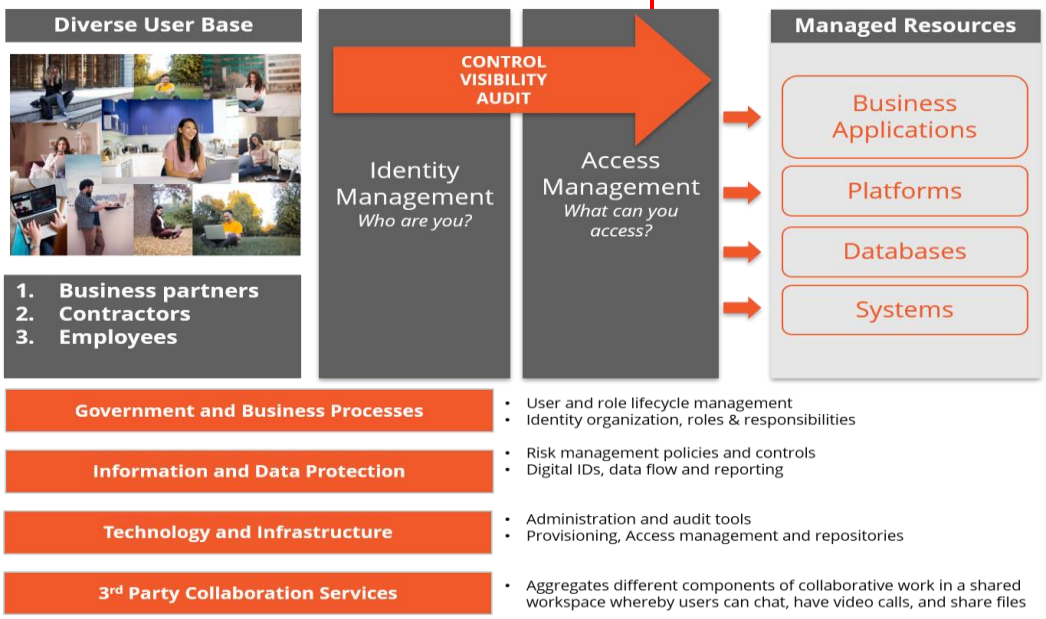


A key enabling technology to work-from-anywhere operational model

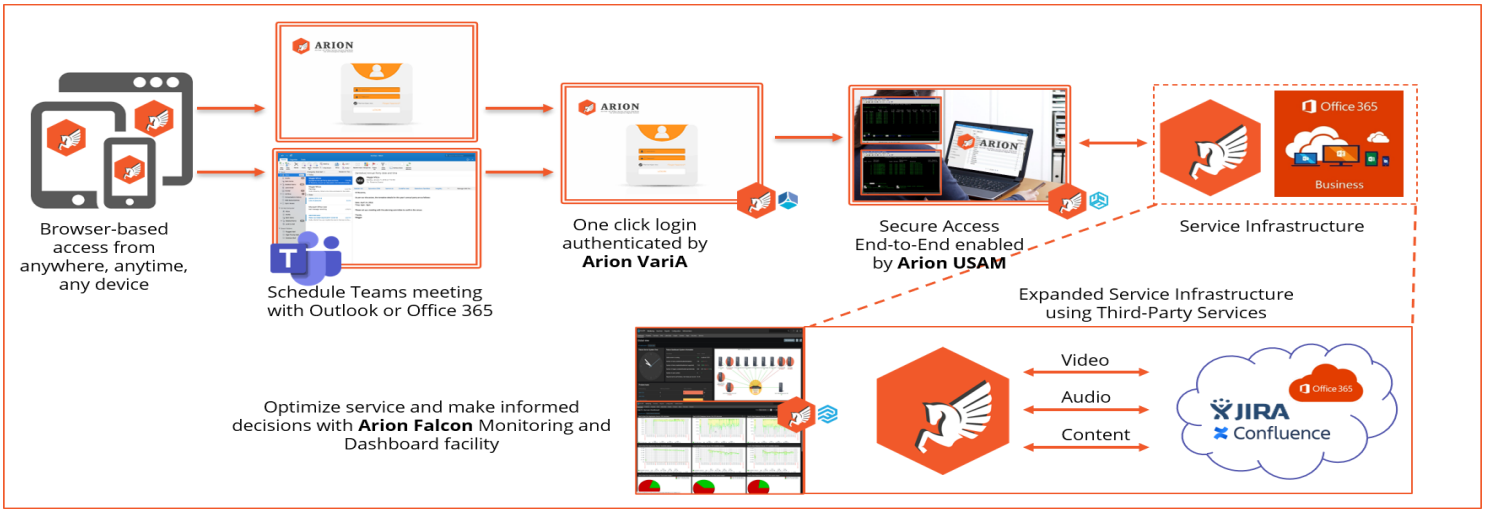
ARION platform is one of the key enabling technology drivers to implement the work-from-anywhere operational model.

The user base for ARION are broadly the business partners, contractors and employees. While answering questions such as Who are you and What you can access, it can constructively strive to manage access, control and audit of access to business applications, platforms, databases and systems.

ARION, a robust work-from-anywhere solution can fully automate the provisioning and de-provisioning process, giving Arion Administrators full power over the access rights of employees, partners, contractors, vendors, and guests. Automated provisioning and de-provisioning speed the enforcement of strong security policies while helping to eliminate human error.



ARION is a vendor-agnostic platform that can deliver 3rd party services such as Microsoft Office365 including Microsoft Teams and Atlassian Confluence collaboration tools that aggregates different components of collaborative work in a shared workspace where users can chat, have video calls, and share files.



PROVIDING THE RIGHT AND SECURE ACCESS INFRASTRUCTURE

ARION MANAGES AND PROTECTS ENTERPRISE SENSITIVE INFORMATION AND AUDITS EVERY USER ACTIVITY AND EVENT

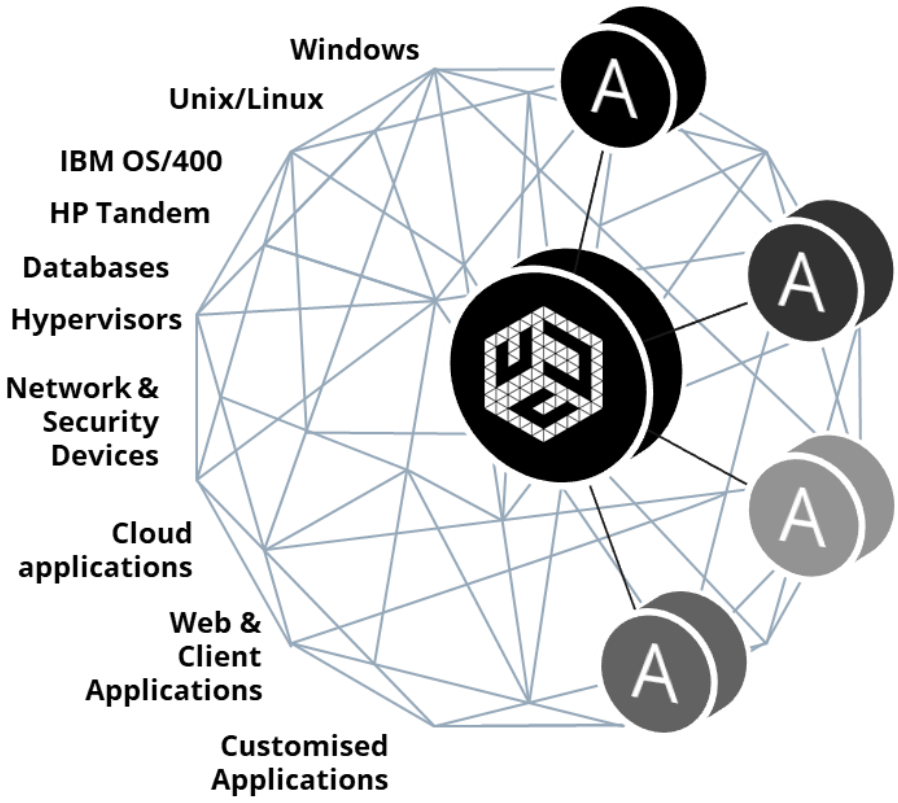
The challenge landscape is further complicated with the increase in the distributed applications, that we see in today's IT landscape.

With the increase of distributed applications comes an increase in the complexity of managing user identities for those applications. Without a seamless way to access these applications, users struggle with password management while IT is faced with rising support costs from frustrated users.

However, with ARION, integrated with USAM, access to multiple applications, is straight-forward, managed and secure.

ARION ADOPTS THE COMPREHENSIVE PRINCIPLE TO MANAGE YOUR OUT-OF-OFFICE ACCESS

ARION ADHERES TO A HOLISTIC APPROACH IN SECURE ACCESS MANAGEMENT



Authorization

- Only the right accesses that is actually required.
- Authorized Access Matrix
- Comprehensive Workflow

Authentication

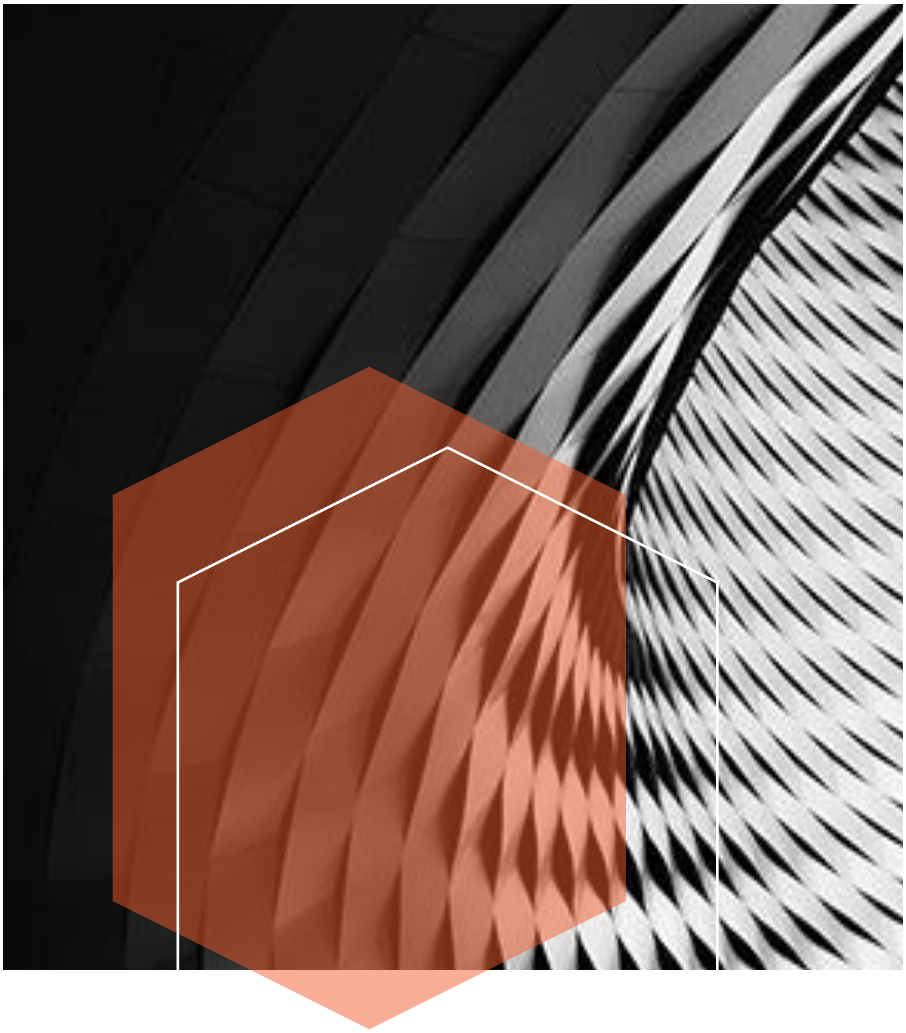
- Username & Password
- AD/LDAP
- One time password, Mobile Apps Token, Hardware Token, SMS, Email, etc.

Access

- Role based access control
- Session Management
- Credential Management

Audit

- Session Recording & Monitoring
- Audit Trails
- Reporting & Audit



WITH ARION, SECURITY AND ACCESS CONTROL IS UNCOMPROMISED AT ALL TIMES

UNDOUBTEDLY SECURE

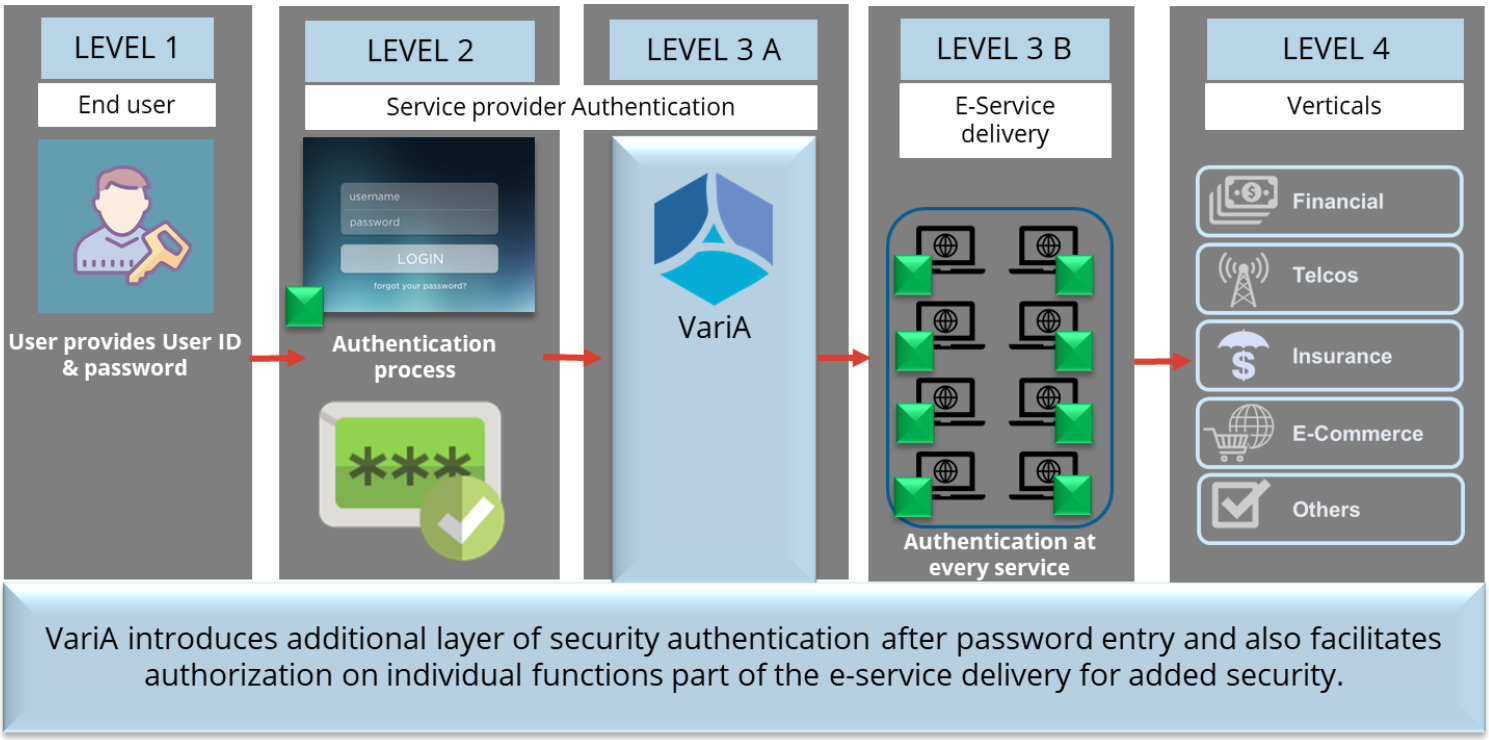
ARION facilities are those of necessity for today's secure environment for out-of-office access. Its fundamental design is based on the following core implementation as shown below, which defines that Secure Access Management is not to be done in isolation. It needs to be tightly integrated with Access control and Surveillance.

With this core design philosophy among many other functions, ARION offers:

Surveillance	Password Management	Access Control & Workflow	Single-Sign-On (SSO)
• Real time 24x7 monitoring for each user access • Screenshot capturing capability – NOT Video • Only capture interactive user activities • Real time transfer of recorded data	• Store and manage password in secured vault • Password reset (Manual/Auto) • Password verification & reconciliation • Split password control • Enforce strong password complexity policy	• Restrict access for only authorized user based on entitlement & approval • Comprehensive & customizable workflow • Provide emergency access during break-glass scenario	• Leverage organization existing identity directory – AD, LDAP, Oracle • *ONE* ID to remember • Centralised access portal for all managed systems • Remove direct server access

ARION PROVIDES EXTRA LAYER OF SECURITY

ARION PLATFORM USES SILVERLAKE VARIA TECHNOLOGY FOR ITS MULTI-FACTOR AUTHENTICATION SERVICE PLATFORM (MFASP) - A PURPOSE BUILT GENERIC MULTI-FACTOR AUTHENTICATION THAT PROVIDES AN ADDITIONAL LAYER OF AUTHENTICATION.



Over the years, passwords and password encryption methods have become more complex, but so have the dexterity of hackers. Passwords can be obtained through phishing, brute forcing, or legally by being shared by their owners for the sake of convenience. This way, organizations are largely clueless when a password was compromised and access is granted to unauthorized parties. In today's threat landscape, relying on just a username and password is no longer sufficient.

VariA is a multi-factor authentication electronic service platform that provides an additional layer of authentication for ARION users. Once registered, end users have the choice to log in with SMS OTP, Time-based OTP (TOTP), Push Notifications, or QR code. Availability of the Push Notification and QR code option is subject to configuration of VariA to allow inbound and outbound traffic to the Internet.

An Android or iOS mobile application secured with biometric or PIN can be issued to end users, simplifying their management of multiple credentials. And it is a more cost-effective solution compared to hardware tokens. With QR code, end users can enjoy instant log-in without the need to key in anything.

ARION THWARTS RISKS OF DATA BREACHES

VARIA
MULTI-FACTOR AUTHENTICATION SERVICE PLATFORM

BENEFITS

- Future MFA mechanisms easily applied without upgrading of target systems
- Centralized MFA for ease of management and enterprise-wide visibility
- Single MFA touch point for end users to access multiple target systems within an organization
- Supports virtually every type of web application
- Variety of authentication options to suit your needs, offline or online, with or without mobile application
- Easy one-time configuration of target systems

Over the years, passwords and password encryption methods have become more complex, but so have the dexterity of hackers. Passwords can be obtained illegally through phishing, brute forcing or legally by being shared by users for convenience. This way, organizations are largely clueless when a password was compromised and access is granted to all who enter it. In today's thread landscape, relying on just a username and password is therefore no longer sufficient or advisable.

ARION'S Enterprise class MFA offers multitude of security features

MOBILE APPS AUTHENTICATION FACTOR

Mobile apps equipped as the most cost-effective solution, supporting various authentication methods such as Push, TOTP and QR code and the apps are secured with password, PIN and fingerprint

ACCESS CONTROL

Single point of control to disable a user's access instead of having to disable access in all applications

FUTURE-PROOF

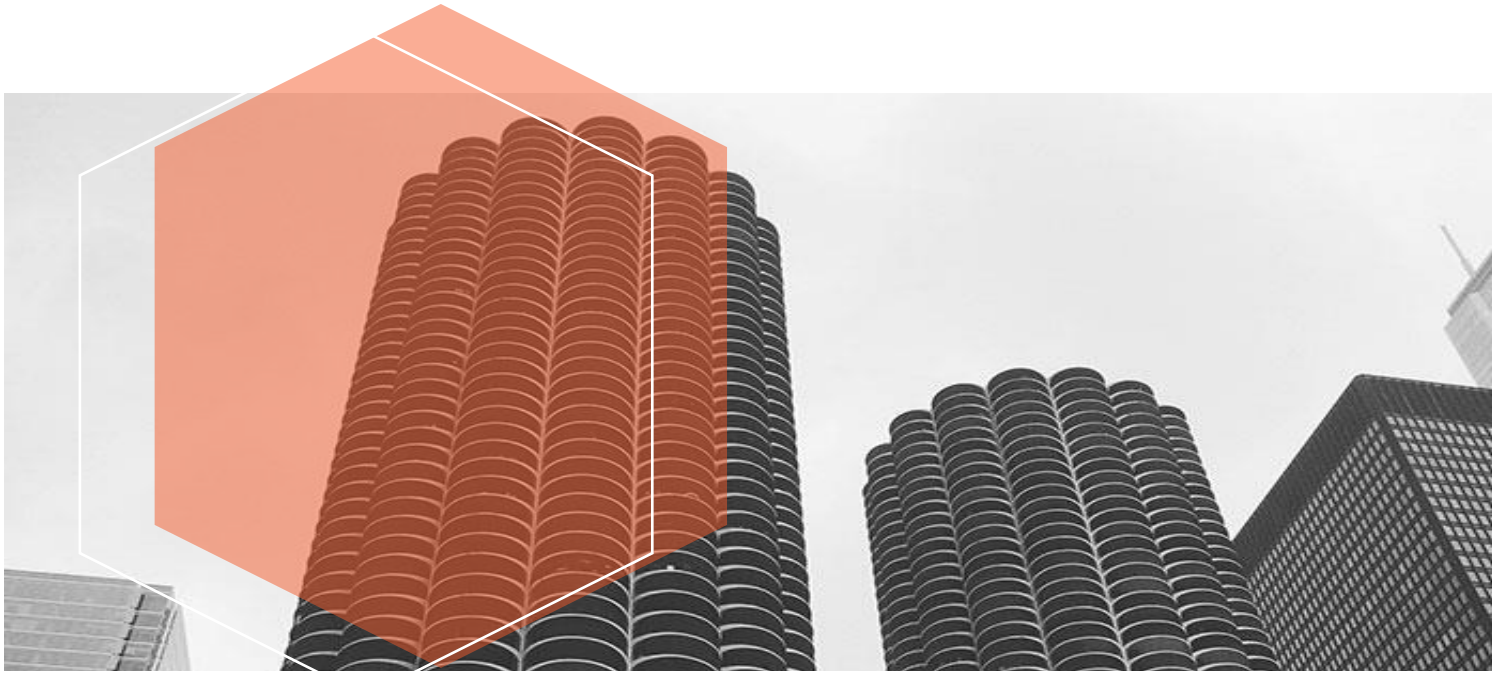
Any new MFA mechanisms (e.g. Facial recognition as MFA) or technology (more secure cryptography algorithms) need only be upgraded in VARIA rather than in all applications

ANYTIME AND ANYWHERE

Based on latest TOTP mechanism that is trusted and used by major companies like Google, Microsoft, Facebook, Amazon, LastPass, etc. VARIA does not require any mobile or network connectivity between device and server, so it can be used even travelling or when mobile connectivity is limited

APPLICATION SUPPORT

Supports both web-based and client-based applications. Simple integration using RESTful APIs



ARION MITIGATES WORRIES ON DOWNTIMES

ENTERPRISE MONITORING AND DASHBOARD SYSTEM FACILITY FOR ARION IS PROVIDED BY SILVERLAKE FALCON

Falcon is a powerful and affordable enterprise-level real-time monitoring system to gather and analyze events from servers, virtual machines, cloud and network devices enabling the user to quickly detect, diagnose, and resolve problems and service outages.

Falcon offers its users the perfect balance of simplicity and depth. Being able to monitor your enterprise network is all dependent on your perspective. Falcon technology delivers a comprehensive view of the connected network (including all your digital assets) which is critical especially when you are working out-of-office.

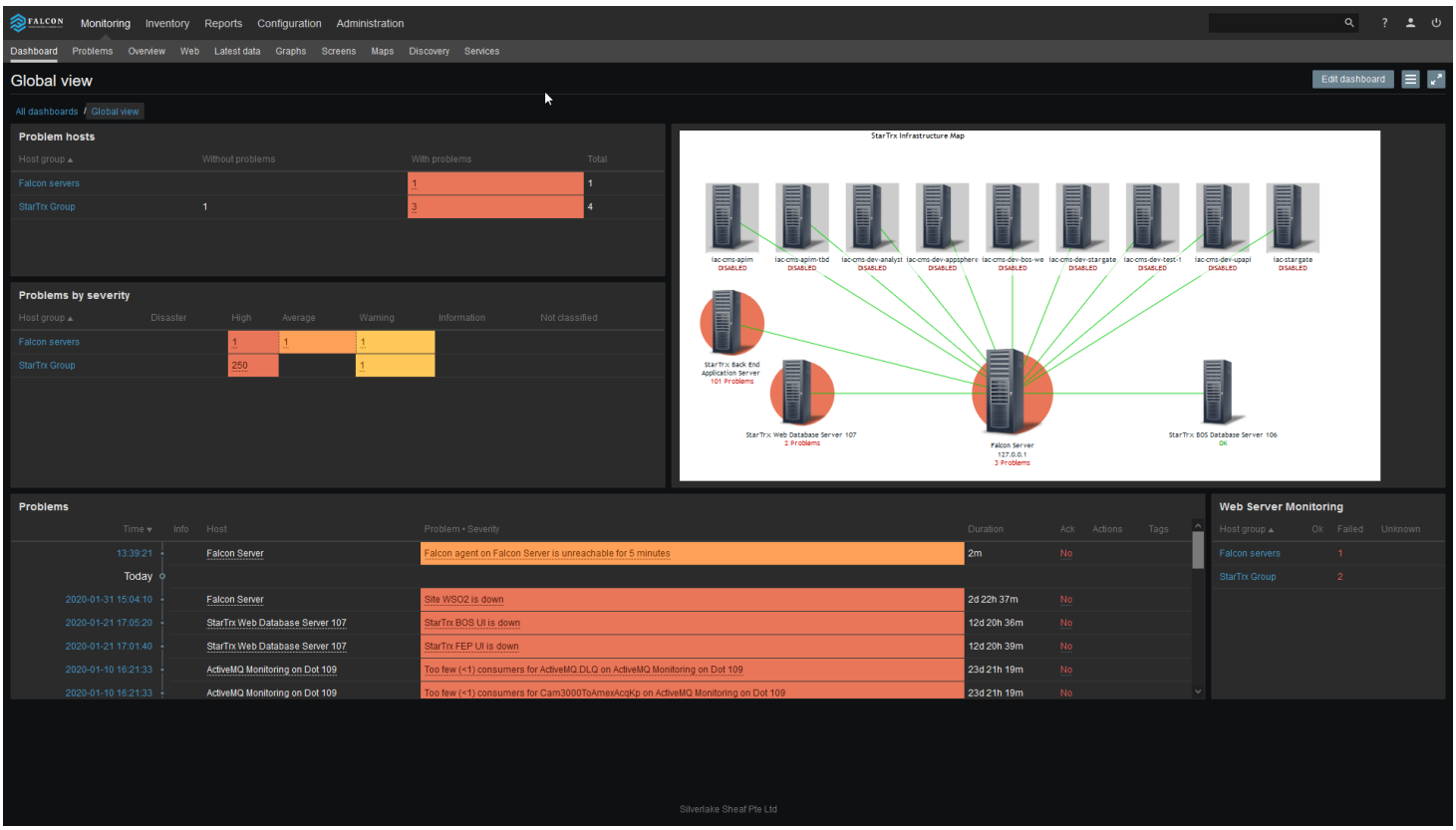
- Speed troubleshooting, increase service levels, and reduce downtime
- Improve the quality of services and reduce operating costs by avoiding downtime
- Monitor resource usage trends and plan capacity increase in a timely manner
- Modular and highly scalable
- Monitor performance and availability of networks, applications and cloud resources
- Send notifications or execute remote commands in case of current or potential problems
- Rich visualization capabilities, customizable dashboard, custom graphs and network maps
- Provide distributed monitoring options
- Improve operational efficiency with out-of-the-box dashboards, alerts, and reports

Falcon Server is a perpetual subsystem of ARION platform that performs monitoring, interacts with Falcon agents, calculates triggers, sends notifications and acts as a central repository of events/data.

The server is the central repository in which all configuration, statistical and operational data is stored, and it is the entity in Falcon that will actively alert administrators when problems arise in any of the ARION monitored sub-systems.

Falcon Agent is native software module deployed on monitoring target digital assets to actively monitor local resources and applications (storage drives, memory, processor statistics, network, file systems, etc.).

The agent gathers operational information locally and reports data to Falcon server for further processing. Falcon agents are extremely efficient because of use of native system calls for gathering information.



"SECURE, TRANSPARENT, UNINTERRUPTED SERVICE LEVELS – NO REASON WHY ONE CANNOT WORK OUTSIDE THE PHYSICAL ENTERPRISE"

About Silverlake Sheaf (Company No. 200002357N)

Founded in 2017, the Silverlake Sheaf Group (Sheaf) is a subsidiary of the Silverlake Group of Private Entities (SPE). Headquartered in Singapore, Sheaf specializes in two core business activities:

- Wholesale of Cyber Security software, hardware and peripheral equipment including development of software in areas of payment, enterprise integration, cyber security; and

- Information Technology Consulting services related to Cyber Security and Digital Transformation.

Sheaf has an office in Malaysia; and representative offices in Thailand, Vietnam and India. Sheaf is an authorized reseller/distributor for Silverlake MasterSAM worldwide. Sheaf offers a spectrum of market-ready solutions ranging from cyber security, payment and enterprise integration.

For enquiries please visit **www.silverlakesheaf.com/nebula** or write to **sheaf_sales@silverglobe.com**

Do connect with us on LinkedIn for more updates: **https://www.linkedin.com/company/silverlake-sheaf**