Silverlake Appliance (SIA) Universal Secure Access Management (USAM) X Series

White Paper

CONTENTS

DISCLAIMER

Silverlake MasterSAM Pte Ltd. ("Silverlake") does not make any representation or warranty, express or implied, as to the accuracy, timeliness or completeness of this document or the information contained herein and none of such parties shall have any direct or consequential liability for the information contained in, or any omissions from, this document.

The information contained herein is subject to change without notice. Silverlake reserve the right to amend or replace the information at any time, and undertake no obligation to update or correct the information set forth herein or to provide the recipient with access to any additional information. This information may not be modified, redistributed or reproduced by the recipient whether such information is in electronic or hard copy form.

The information contained herein is preliminary and does not purport to contain all the information that interested parties may desire. Neither the receipt of this information by any person, nor any information contained herein constitutes, or shall be used or relied upon as constituting, the giving of advice by Silverlake to any such person.

By downloading / receiving this document, the recipient acknowledges and agrees that the recipient will not modify, distribute or reproduce the document in whole or in part and will use this document solely for the purpose of evaluating the recipient's interest in the Products.

1 EXECUTIVE SUMMARY

In process of formulating a typical proposal for the provision of an enterprise Universal Secure Access Management (USAM) system, solution architects / consultants must identify products and services that address the key success factors for an implementation. However, the completeness of the technical solution is only one aspect of the USAM challenge; equally important are the management of the initial project delivery risk and the ability to continue to support the enterprise's evolution as it grows and changes over time.

Objective of this process is to have identified key appliance (hardware, software) – choose from SIA USAM X3, X5, and X7 Series - to start the initiative on a full function USAM platform, to provide a means to manage it into the future and at the same time maintain cost efficiency. The SIA USAM X Series is the first appliance developed based on Intel® technology, a new cyber security line that combines best of both technologies to bring unprecedented level of "edge-to-cloud" and data centre security for our customers.

Today with our SIA USAM X Series, we have shifted the focus towards enabling technology to meet various challenges. With Intel's software and hardware technologies, Silverlake's MasterSAM technology stack designed for USAM, will form an all-new and powerful cyber security USAM product line that will be the foundation for our customers to reduce their company's cyber security risks.

The primary SKUs of X Series: X3 Series, X5 Series and X7 Series, which aim to be the right solution fit for a small, mid-sized and large-sized enterprise, operating in multiple industry verticals.

1.1 SILVERLAKE INTEL APPLIANCE (SIA) UNIVERSAL SECURE ACCESS MANAGEMENT (USAM) X SERIES

The key products on which our proposals are based are as follows:

X3 Series

X310
Agentless
100 Resources

X5 Series

X510, X580
Agentless, PMS Add-On
500 Resources

X7 Series

X710, X780
Agentless, PMS Add-On
1500 Resources

SIA USAM X310

This entry level purpose-built standalone model is designed for small-sized deployments to offer basic USAM functionality and it can support up to 100 resources.

SIA USAM X3 series supports Agentless deployment method for secure access management, which allows for ease of setup with minimal maintenance. This type of deployment does not require any the installation of additional services or program in the associated resource in order to provide USAM services. As what a small enterprise may seek, this model provides basic surveillance and access control together with password management.

Maintaining High Level of Security for a small business is now made easy and Cost-Efficient with SIA USAM X3 Series

SIA USAM X510 and SIA USAM X580

This enterprise level Mid-range X5 Series model is carefully designed for medium-sized deployments of up to 500 resources. This model can be deployed using Agentless deployment. Additionally, this model offers power redundancy and RAID 1.

As an add-on feature, this X5 Series can be integrated with Privilege Management System, that offers features such as Granular Access Control and Advanced Surveillance to support de-centralized / distributed topology.

Eliminating all possible security gaps and meeting the budget in a growing mid-sized enterprise is now effortless with SIA USAM X5 Series

SIA USAM X710 and SIA USAM X780

This high-end X7 Series model supports high-end deployments with up to 1500 resources. It provides power redundancy and RAID 1. Similar to the X5 Series, this model also offers add-on feature of Privilege Management System, thus enabling a hybrid style of deployment method.

Deployed as an adaptive intelligent solution set for larger enterprises, protecting all key data assets, while meeting international compliance mandates becomes manageable with all-encompassing SIA USAM X7 Series

With these key appliance products, the process of individual solutions can be implemented with minimum technical effort. Identified individual solutions can be categorized into two, namely:

- **Universal Secure Access Management (USAM) Platform**
- **Enterprise Common Shared Services**

1.1.1 Universal Secure Access Management (USAM) Platform

USAM facilities are those of necessity for today's environment. Silverlake MasterSAM approaches USAM as part of its overall Secured (S) Access (A) Management (M) [hence the name MasterSAM] strategy since its inception in 2002. Its fundamental design is based on the core belief that Secure Access Management is not to be done in isolation; It requires to be tightly integrated with Access control and Complete Surveillance.

With this core design philosophy, Silverlake MasterSAM is able to offer:

Innovative USAM Solution

Our USAM solution offers flexibility in deployment methods: proxy or host-based deployment methods to suit client needs. Both methodologies secure privileged management access without exposure or manipulation of vulnerable passwords in the process.

360° Surveillance Technology

All-round tight surveillance monitoring on user's activities in Operating System (not dependent on video, nor key-logger). This way, no user activity on the production system can go without detection and record.

Granular Access Control

Flexible granular access control implementation further enhances degree of system security

Enterprise wide compliance audit

Monitors access or policy violation to classified system files, DB and directories – provides session report and alert

Privileged Password Management and custodian

Provides password vaulting, managed reset, policy-based password, password deposit, password retrieval and more.

1.1.2 Enterprise Common Shared Services

Common shared services are those which have always been addressed by our customer vertical business lines / core or channel applications and is historical; Although it may be time to share them at the customer's enterprise level (to reduce cost, remove redundancy and provide common view to internal and external users), depending on whether the customer would still consider them of competitive value to justify their individual cost.

The following SIA products can be deployed standalone or as add-on to SIA USAM X Series to deliver wider enterprise shared services.

- **The VariA Solution Suite** - A purpose built generic standalone Multi-Factor Authentication that provides an additional layer of authentication, in addition to your current authentication – can be positioned as an enterprise shared service i.e. this service can be extended beyond the standard proposed enterprise USAM implementation.
- **The Aurora Solution Suite** - A purpose built generic standalone Identity Access Management solution that offers Authentication using passwords, tokens, certificates, and multi-factors, Authorization management, Single sign-on and more. This includes

a. **Aurora IDM - Identity Manager**
b. **Aurora AM - Access Manager**
c. **Aurora DS - Directory Services**

Fundamentally, a deployment would usually involve delivery channels and core, complete with mid and back office systems / applications. It is estimated to involve multiple software suppliers, complete with the events that will occur in these external party's program. In an effort to standardize USAM delivery platform across the enterprise's infrastructure services in this context is complex and risky due the number of parties involved who have to work together across multiple initiatives. Integration (people working together and trying to remain consistent and synchronized) then becomes the key success factor for such deployment initiatives.

In our paper, we would address this key success factor with our Silverlake Intel Appliance (SIA) Universal Secure Access Management (USAM) X Series, a system not only to serve as the foundation for a USAM implementation, but also to ensure the resultant is managed across its life cycle to protect the investment.

With SIA serving as the foundation for success in the complex situation, we address the USAM functionality for the system with our SIA USAM X3, X5, and X7 and all new Multi-Factor-

Authentication Service Platform (VariA) - a full function Enterprise USAM system which crystallizes Silverlake's 20+ years of practicing USAM cyber security expertise on the fringes of its core banking and channels business into a holistic system suitable for today's Digital Economy.

As with all Silverlake products, emphasis on ASEAN compliances and practices is first and foremost. Hence rest assured this product is localized and will fit all geographies in and beyond ASEAN complete with compatibility with Silverlake core systems, business applications etc.

Add to the SIA product suite our presence and project support levels in Singapore, Malaysia and the region; we are confident we have the most cost effective, least time to market, minimum risk and highest protection of investment solution for this project.

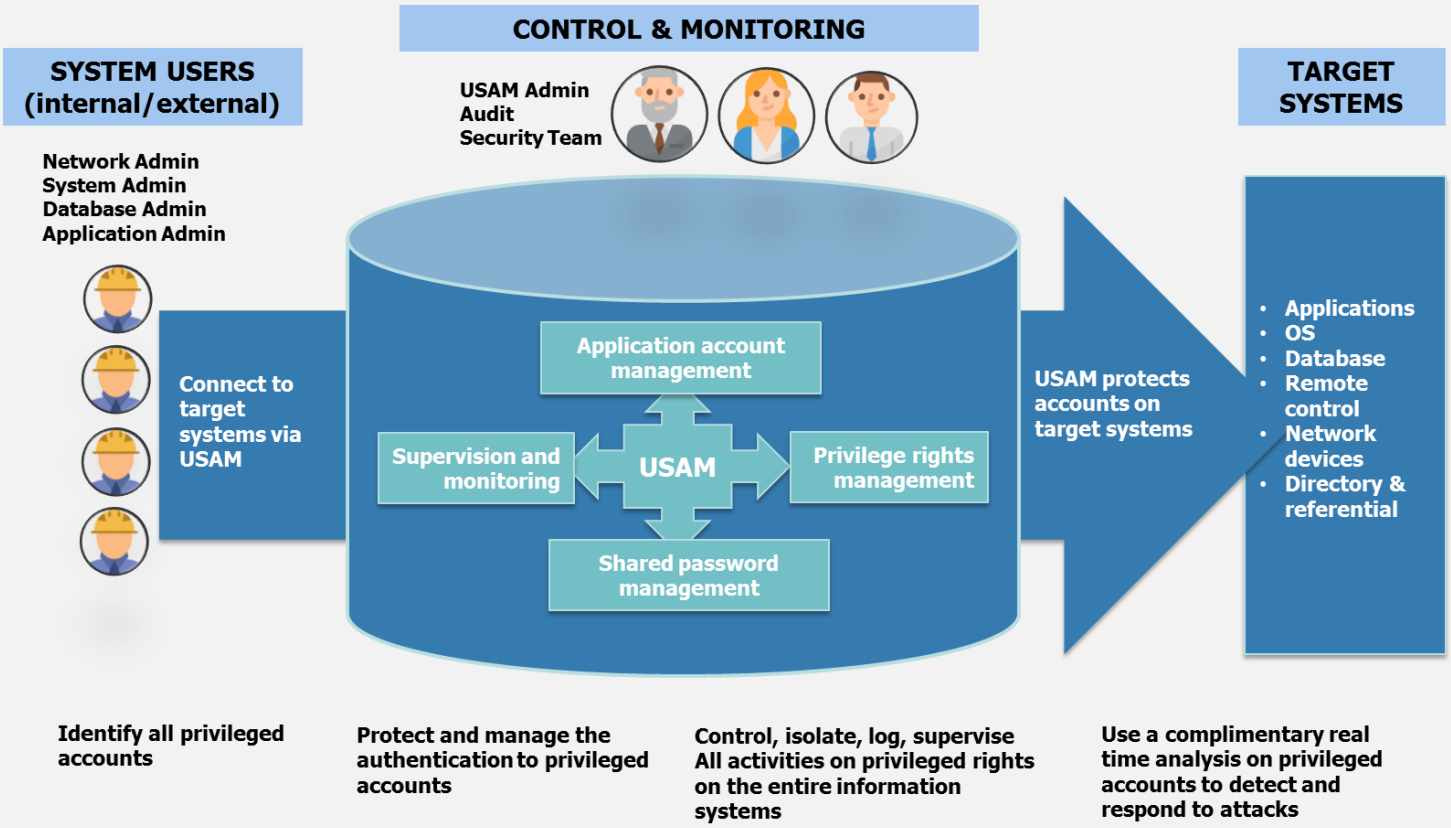
Our proposal to deploy SIA is to mitigate unprecedented security risks of today.

As we become more digitally connected, the more vulnerable we become. Anything that is connected is a target. In the past, the focus was on building a strong defence against an attack from the outside. However, along with the multitude of changes in the present-day Internet of things and connected technologies, traditional line of defence is increasingly becoming obsolete. More and more breaches involve data integrity loss which comes from insiders intentionally or unintentionally. Companies are now shifting their attention to tightening internal security.

Modern-day cyber security requires new set of techniques to protect the integrity of networks, programs, and data from attack, damage or unauthorized access. Implementing effective cyber security measures is particularly challenging today because there are more systems and devices, and attackers are becoming more sophisticated in their approaches.

Specifically, Privileged accounts are vulnerable to the double whammy of external cyber-attacks and potential perpetrators within the enterprise. These accounts are popular targets for malicious hackers because they hold the key to most important and confidential databases, servers and systems which are dubbed "crown jewels" of every organization. Once access is gained inside the system, perpetrators will seek the heart of the enterprise with the intent to cause harm to the organization. Dire consequences ensue which include strained business reputations, financial losses, and stolen intellectual property.

A USAM solution, the core of cybersecurity, tackles this very challenge by managing and securing access to every layer, protecting the organization's digital assets.



1.2 SIA USAM APPLIANCE OVERVIEW

The SIA USAM X Series Appliance resides at your facility or data center, within your security measures. This deployment model offers more control over security, giving you a safe way to integrate privileged access and making it easy to export reporting data and videos for a complete audit trail.

The SIA USAM X Series Appliance is a robust USAM solution that is powered by advanced Intel Xeon Scalable platform that can fully automate provisioning and de-provisioning process, giving IT full power over the access rights of employees, partners, contractors, vendors, and guests. This not only speeds up the enforcement process but helps eliminate human error. The scalable and modular architecture of SIA will ensure businesses can mitigate cyber threats with more deterministic performance and efficient cost containment. It also reduces the trusted computing base (TCB) to the smallest possible footprint, prevents memory bus snooping, memory tampering, and "cold boot" attacks against memory images in RAM; provides hardware-based attestation capabilities to measure and verify valid code, data signatures, and the TCB.

The appliance creates a hardware protected container for apps to protect secrets at run time and at rest. This means secrets remain protected even when attackers have full control of the platform. So even if an attack happens, our customers' data remains safe. It can be tailored to the customers' needs and features flexible simplified configuration and maintenance.

With this collaboration with Intel, we now have a highly secured system that has the best of technologies from Silverlake and Intel - all in one platform – delivering the best value for our customer.

The SIA USAM X Series appliance uses Intel vPro technology that enhances Remote Desktop Support for SIA Appliance. Customer's IT Operations support may use Intel vPro Technology to power a remote PC on/off, reboot to BIOS, re-image a remote computer and access remote desktops regardless of operating system state. Silverlake also offers remote support (on a managed services model) to multiple operating systems with SIA USAM X Series, including troubleshoot beneath the operating system on systems powered by Intel vPro Technology with following steps:

- Access an Intel vPro-enabled device right from your SIA Console.
- Start a secure SIA remote session (unattended and attended options).
- View the device at the BIOS level, below the operating system.
- Take action to resolve the issue, including power on or off, reboot to BIOS, re-image, and more.

SIA USAM is delivered pre-configured after extensive testing and optimized to work with other SIA USAM X Series appliances or a custom MasterSAM USAM solution stack to maximize performance and reliability. Scaling with an appliance becomes easier as scaling options now only require additional appliances to be plugged in or upgrading to a higher-end model. Self-managed systems require users to manage hardening of hardware and operating systems. This can be complicated

and incurs additional cost to maintain. The appliance comes pre-hardened, closing any unnecessary access points into the appliance.

SIA USAM X Series appliances are fully backward compatible with all supported MasterSAM implementations.

1.3 SERVICES

Our proposals may include the full Silverlake engagement method for such projects with the same senior officers in the project providing oversight responsibilities. The project team includes specialists in all areas of the system, and incumbent personnel and a full project teams deployed.

The SIA USAM X Series product together with our service ability; we are confident of producing success through our committed effort.

Depending on the customer preference, project implementation and support services can be also be delivered by our certified eco-system partners.

1.4 WHY SILVERLAKE?

We would emphasize that we represent a low risk, cost effective and forward- looking solution, complete with the almost mandatory requirement of Business Agility that is necessary for today's Digital Economy.

- Support in the region by Silverlake is extensive and very long term in nature for our prospective customers which forms the foundation for sustained incremental capacity increase to include the engagement of this regional directive for payment processing.
- Stress on an enterprise's resources during heightened activities (e.g. security audits, compliance etc.) brings with it the requirement to increase capacity for support and administration of the supplier for the USAM system initiative across years. We bring along economies of scale as such capacity issues at the customer are only incremental on today's USAM cyber security program.
- Proven product, service ability and commitment are the corner stone of all Silverlake offering and we are pleased that our proposal represents one of the strongest solutions we have ever deployed. It incorporates 3 decades of specialist know how in integration technology packaged in an appliance product which is localized/evolved/matured Secure Access Management functionality, proven for our customers.

2 CHALLENGES FACED WITHOUT USAM

- NO automation of password rotation - Passwords are exposed to developers and vendors with greater risks of compromising the organization.
- NO centralized integration and management of privileged accounts with existing enterprise solutions of the organization.
- NO visibility of privileged account usages - Who, when and what was done using the account is unknown.
- NO central passwords management, which usually ensues in storing passwords in Excel spreadsheets which become highly vulnerable and susceptible to exposure to users, turning validity of passwords void.
- NO passwords complexity as passwords are manually created by developers or IT personnel and may need to be used in emergencies and such passwords generally tend to be easy to remember.
- DIFFICULTIES to achieve compliance as there is no process of regulating the privileged accounts. This may cause organizations to violate security standards and regulations, and lead to failure of internal and external audits.

3 KEY BUSINESS OBJECTIVES AND PRODUCT KEY STRENGTHS

SIA USAM X Series features include:

Business Facilitation

- Mergers and Acquisitions impact organizational technology strategies
- Technology and regulatory challenges due to globalization initiatives

Risk Management

- No single view exists of the organization's control, security and privacy requirements and operating framework
- Challenges in responding and addressing audit and regulatory issues

Cost Containment

- Cost cutting measures cause difficulty in maintaining current performance levels and SLAs
- Increased management skepticism associated with IT spending

Compliance

- Changes in existing regulations and increase in new regulations are creating compliance challenges
- Cross-boundary regulatory needs are causing the organizations to rethink compliance strategies

Operational Efficiency

- There is a need to manage use accounts and passwords centrally to reduce operational overheads
- Organizations have issues with respect provisioning access to users in a timely fashion to increase productivity

The primary business objectives of most organizations may be summed up as follows:

- To establish automated central repository password safekeeping on Privilege ID/Super ID for Microsoft Windows platform (Windows 2003 and above), Open system platform (Linux and Unix), ESX hypervisor, Microsoft SQL databases and various network devices (Firewall, Intrusion Detection Systems, switches, router, etc.);
- To maintain confidentiality of privilege IDs password without interrupting routine / ad-hoc jobs that require privilege IDs;
- To change the password of privilege IDs on scheduled basis without manual intervention from Server/ System Administrators.
- To have an audit trail on the activity being carried out while using privilege IDs as an evidence that the job being carry out as intended;
- To strengthen the security posture and adhere to Circular for Cyber Security.

Listed below are the highlights of product key differentiators and strength compared to other products in the market. Being a leading USAM solution provider, we truly understand the market requirements and are constantly developing new innovative technology and improving the product to deliver the best solution to our customers.

No	Feature	Description
1	Automated and comprehensive password management	Provides secure vault to store and manage privileged credentials according to complex policy and flexible reset mechanism – automatically after use, manual or scheduled Split password protection to ensure none can get to know the entire password during the password release cycle, satisfying the 4-eyes principle rule Password verification and reconciliation to ensure managed passwords are always in-sync Broad system support to enterprise systems including server, database, application, security and network devices, and more.
2	Smart surveillance engine and complete audit trail of privileged activities	Real-time recording with screen capture technology (not Video) for each privileged access activities in proprietary format Smart mechanism to record based on user interactive activities, color / grayscale recording Offers tamper proof and real-time transfer of recorded data to centralized log repository to allow real time session playback Provides complete audit trails for privileged activities Advanced 360º surveillance technology implemented on MasterSAM host-based agent is crucial for safeguarding high valued assets. More significantly this is important in a typical gateway implementation approach where there is always a risk that users bypass the gateway to directly access the high value asset. For example, direct console access or leapfrog (multiple server hops). In that scenario, one would lose the visibility and in worst case, there will be no alert when the rule is breached. Silverlake MasterSAM offers alert capability based on configured rule set.
3	2-Factor Authentication	Extra layer of security authentication for each privileged access Supports Multi-Factor authentication (MFA) such as AD, LDAP, RADIUS, SMS, email, and mobile apps, and integration with enterprise MFA
4	Full compliance to best practices for managing cyber risk	PCI DSS SOX 404 ISO 27002-2013

5	Alternative access during emergency break-glass event	Provides secure offline password retrieval with dual security control Supports emergency request (with auto approval) to ensure operation continuity after working hours, weekend or emergency situation, with the limit of up to max 3 hours for each session, and configurable alert notification
6	Flexible and scalable deployment – host based and gateway based to provide in-depth and wide coverage	Allows quick deployment (gateway-based) to promptly monitor all privileged user activities Flexible (user's choice) to apply host-based deployment to critical servers to achieve in-depth security control (granular access control and console monitoring) as part of future expansion planning Supports host based, gateway based or even combination of each Software-based solution – thus easily compatible with most hardware provider and simplify future scalability, vertically or horizontally Centralized access via web console
7	Minimized password exposure with Silverlake MasterSAM auto-login capability	Provides Single-Sign-On (SSO) capability Supports native standard protocol – SSH, RDP, VNC, Telnet Allows native login with 3rd party tools (web/client) – MSSQL Management Studio, Oracle Developer, Putty, Apache Tomcat, Toad for Oracle, Info Express, IBM Tivoli Endpoint Manager, IBM iSeries Navigator, IBM iSeries SST login, vSphere/vCenter, Microsoft Hyper-V manager, Cisco, Check Point, Alcatel, Juniper, FortiGate, Bluecoat, and more
8	Advanced Keyword Analyzer technology (AKA)	Breakthrough technology to capture and analyze keywords that display on the screenshot/image – not achievable via typical key-logging or meta title logging Integrated into powerful search engine to allow definable security policy for auto filtering and real-time alert

4 SAMPLE PROPOSED SOLUTION FOR AN UPGRADE

4.1 USAM SCOPE OF WORK FOR SAMPLE PROPOSED SOLUTION UPGRADE TO SIA USAM X SERIES

The project will cover the following:

- Migration of PMS to appliance
- Migration of existing agents to new PMS IP
- Installation and upgrade of agents
- Installation of new agents
- Migration of Analyst to appliance
- Install & Configuration of VARIA

Upon migration to the appliance PMS will need to handle a total load of 300 users to 2000 agents*.

* Numbers are based on initial information gathered. Actual figures might be different after a complete study of customer environment during project implementation. However, grand total of users and also servers' coverage should not exceed total scope.

4.2 SIA SOLUTION FUNCTIONAL OVERVIEW

4.2.1 SIA USAM X710

SIA USAM X Series technology stack includes MasterSAM Privileged Management System (PMS), which is a purpose built generic centralized policy management server for host-based deployment architecture to ease operational, deployment and policy maintenance. The appliance is seamlessly compatible with other SIA USAM X Series appliances, delivers MasterSAM Privileged Management System (PMS) function.

MasterSAM Privileged Management System (PMS) is centralized policy management server for host-based deployment architecture to ease operational, deployment and policy maintenance. It provides the centralized management solution to bridge the communication with MasterSAM host-based solution and improve the turnaround time to manage each server locally. It also serves as centralized management console that controls and configures for MasterSAM secure agents.

PMS synchronizes users from Active Directory and leverages on an organization's existing Active Directory infrastructure for user authentication. It provides complete host-based server surveillance management to protect backdoor access to enhance security. It also manages Granular Access Control (GAC) policies for Unix/Linux and Windows, whereby one-click button to publish mass policies with immediate enforcement control to target secure agent host.

With GAC configuration, no one can escape the access control imposed and this includes users who bypass or circumvent proxy gateway and firewall, and any user login directly via local console mode (e.g., root & admin with local console login). With easy and intuitive configuration by grouping of user or system, supporting standard and customizable role-based access control, more effective access control management can be achieved. Supported types includes blacklist and whitelist of service, file/folder, registry, shared folder and command. This feature is also non-intrusive to OS or kernel and will take immediate effect upon publish of policy without requiring the user to logoff from existing session.

SIA USAM X Series technology stack also includes MasterSAM Analyst (ANL), which is a purpose built generic centralized log repository server that consists of analytical tools for enterprise IT audit and compliance which has the ability to provide views and reports which summarize and comprises details of consolidated user access behaviors and actions for all the targeted systems. The appliance is seamlessly compatible with other SIA USAM X Series USAM appliances, delivers MasterSAM Analyst USAM functionality.

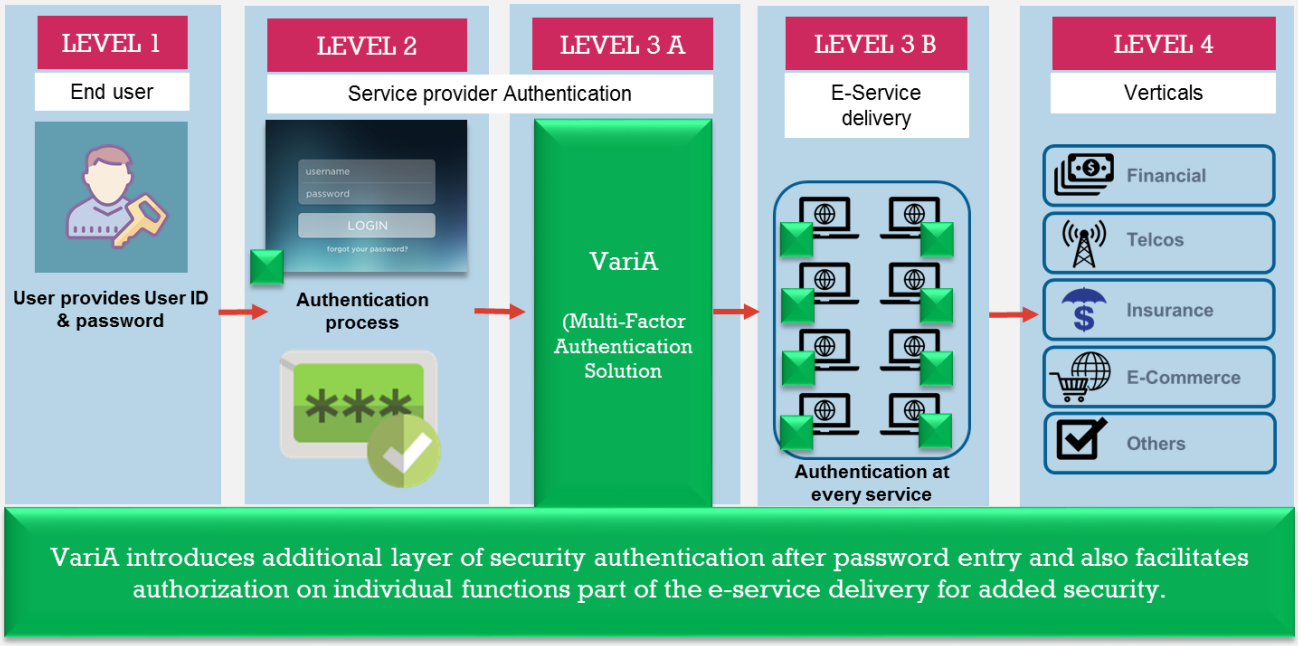
MasterSAM Analyst server is a centralized log repository server that consists of analytical tools for enterprise IT audit and compliance which has the ability to provide views and reports which summarize and comprises details of consolidated user access behaviors and actions for all the targeted systems. These reports, which can be dynamically generated, can filter or group results according to various reporting options such as users, servers, keywords, date/time, file names etc. It also provides real-time dashboard view for user to get the relevant information at one glance.

MasterSAM Analyst logs and records every user's activity in its proprietary text cum video format, to ensure security, compactness and robustness. It does not hog resources like video recording. It does not hook your key strokes like key logger. Coupled with the most powerful MasterSAM Analyst which provides policy-based auto search and filter capability, MasterSAM offers the most efficient surveillance audit tool within USAM arena.

With its powerful agent installed onto Windows & Unix/Linux target system, MasterSAM is able to offer all round surveillance audit on any login user (whether such user is privilege assigned or not). This will certainly include console-based super privileged ID login and some examples are: root in Unix and Administrator in Windows. With the gateway implementation, surveillance audit is possible on the user(s) tunnel through the gateway to access the target server or device, this surveillance approach covers more platforms (Unix, Windows, terminal based or web-based devices). Therefore, MasterSAM offers the best combinational approach in Windows and Unix/Linux – if anyone wants to have 100% coverage, go with agent-based implementation, if not go with gateway approach. It also offers basic surveillance on other platforms through its simpler gateway implementation.

4.2.4 SIA USAM X Series for Multi-factor Authentication (VariA product suite)

VariA is a Multi-Factor Authentication Service Platform - A purpose built generic standalone multi-factor authentication that provides an additional layer of authentication, in addition to your current 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 - Multi-Factor Authentication solution is a standalone multi-factor authentication that provides an additional layer of authentication, in addition to your current authentication. Only one instance of VariA is required to serve multiple channels in your organization. Once registered, your 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.

Integration of existing channels to VariA is made easy through secure RESTful web service calls. A single platform removes the complexity of various implementations for the same functionality.

Future upgrades would be available to all channels, without the need to engage various vendors and stakeholders to perform system enhancements.

VariA works on a centralized management model, making it easy for channels and end users to be on-boarded, or subsequently off-boarded. With a single action, an end user's access to multiple channels can be revoked. Management and monitoring can be performed by one dedicated group, with the help of informative dashboards and audit logs.

4.2.5 SIA USAM Enterprise System Architecture

System architecture of Silverlake MasterSAM solution suite offers various implementation and deployment methodologies, on both physical and virtualized environment, to suit various security needs of our customers. With comprehensive and complete suite of solutions and features, Silverlake MasterSAM is able to help customers enforce segregation of roles effectively for various responsibilities and tasks. It provides separate management console for privileged access, password and access control management and a separate central log repository management for compliance and surveillance review audit. Grouping of users and servers for access control matrix can be done effortlessly through intuitive web management portal.

Silverlake MasterSAM allows in depth surveillance onto each user's activity on the system to ensure all events performed are logged and recorded. We believe that enhancements are possible only if there are proper checks and visibility. As such, our USAM solutions ensure complete host-based surveillance on all its implementation on both Wintel and Unix (Linux) instances. With this as a basis, an effective USAM solution can be implemented.

As a universal approach for access control, there are 3 main types of Privileged Access methods named:

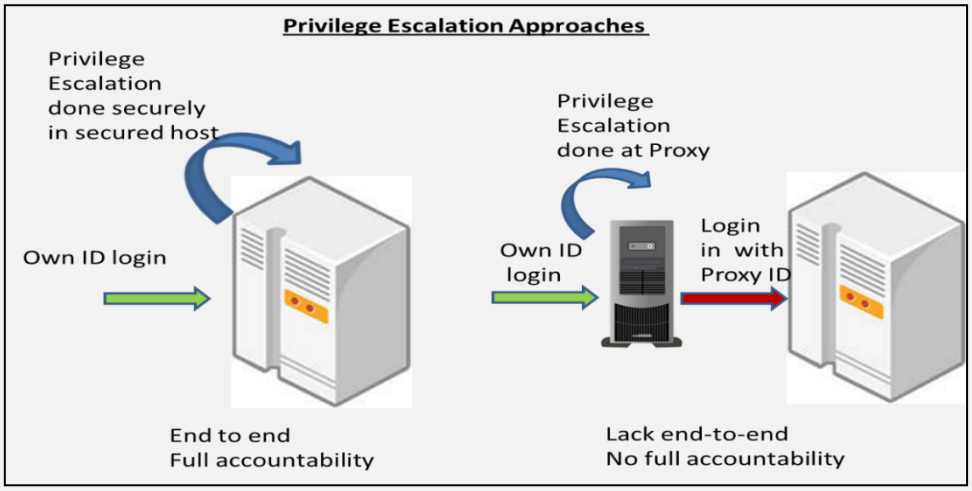
- Host-based
- Gateway proxy-based
- Hybrid based

Silverlake MasterSAM offers solution that not only cover host-based and gateway proxy-based, but also provisions for a better method that combines the best of two worlds and presents a new hybrid model to fulfil the complex security needs of today.

4.2.5.1 Host-Based Deployment

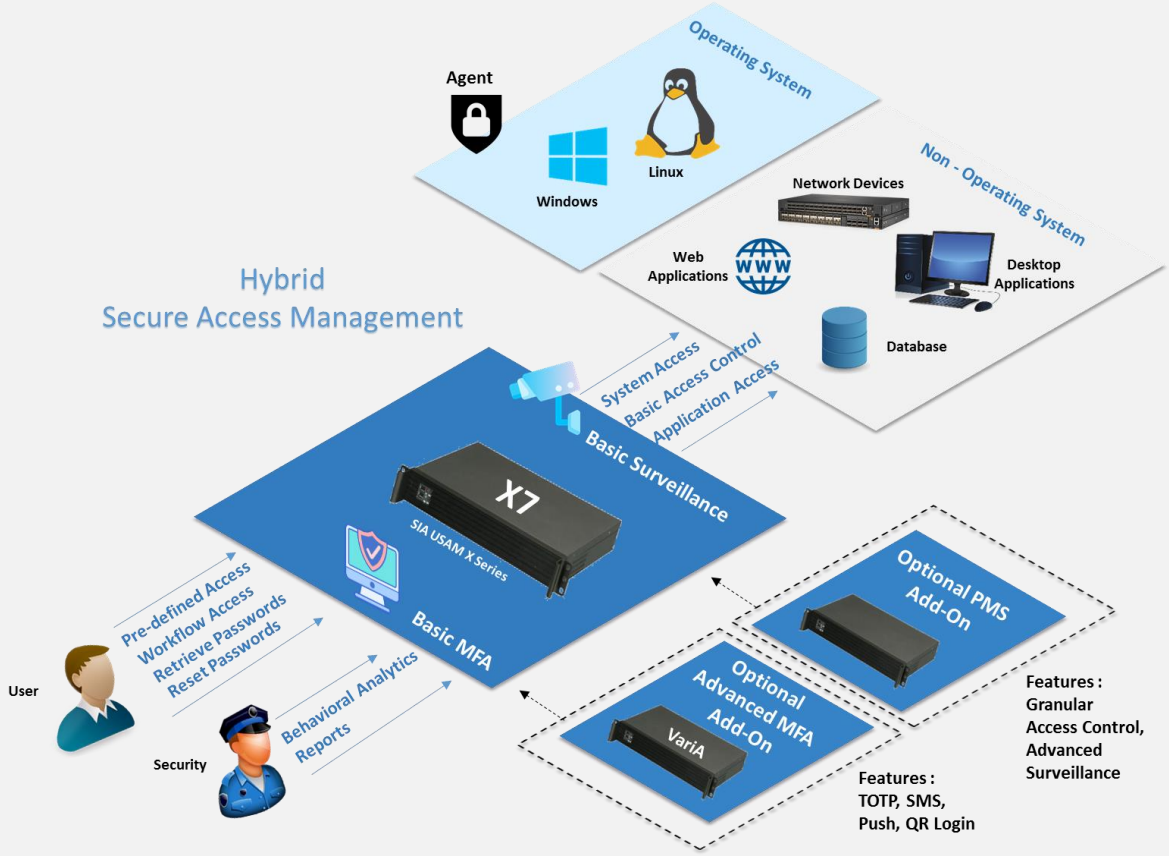
Host-based USAM in Silverlake MasterSAM is done within the secure boundary of system host. This is to ensure that there is no password leakage and full end-to-end accountability is always enforced. No one is to log in hiding behind a proxy common privileged ID. User has to log in using his/her own least privilege ID at all points of entry to the system. No exception is given to anyone, regardless of admin or root privilege.

Such architecture offers secure operation as privileged escalation on user is determined within the secured system host. It is not done outside as in the case of proxy approach or password assisted login, which is considered less secure and thus cannot enforce true end-to-end accountability.



4.3 PROPOSED SIA USAM X SERIES USAM DESIGN

The primary purpose is to migrate existing servers that have operating systems that are approaching EOL (End of Life). It is hereby proposed to keep existing architecture as similar as possible to the original and migrate existing servers to an appliance on a one to one mapping.



The logical architecture diagram above introduces the addition of the VariA MFA add-on appliance.

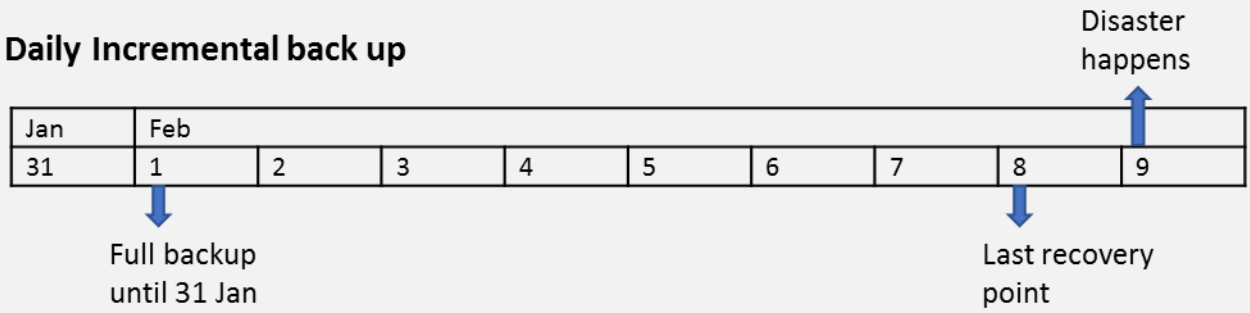
4.3.3 Business Continuity Plan

(i) Backup and Restore Plan

There will be a backup script that is bundled together with each release. It will automate the backup of all the necessary files i.e. database, configuration file, application data, etc. The script is usually deployed in scheduled basis. We recommend the backup to be performed in incremental daily mode, weekly and monthly full. Backup files can be stored at customer's existing centralized storage point.

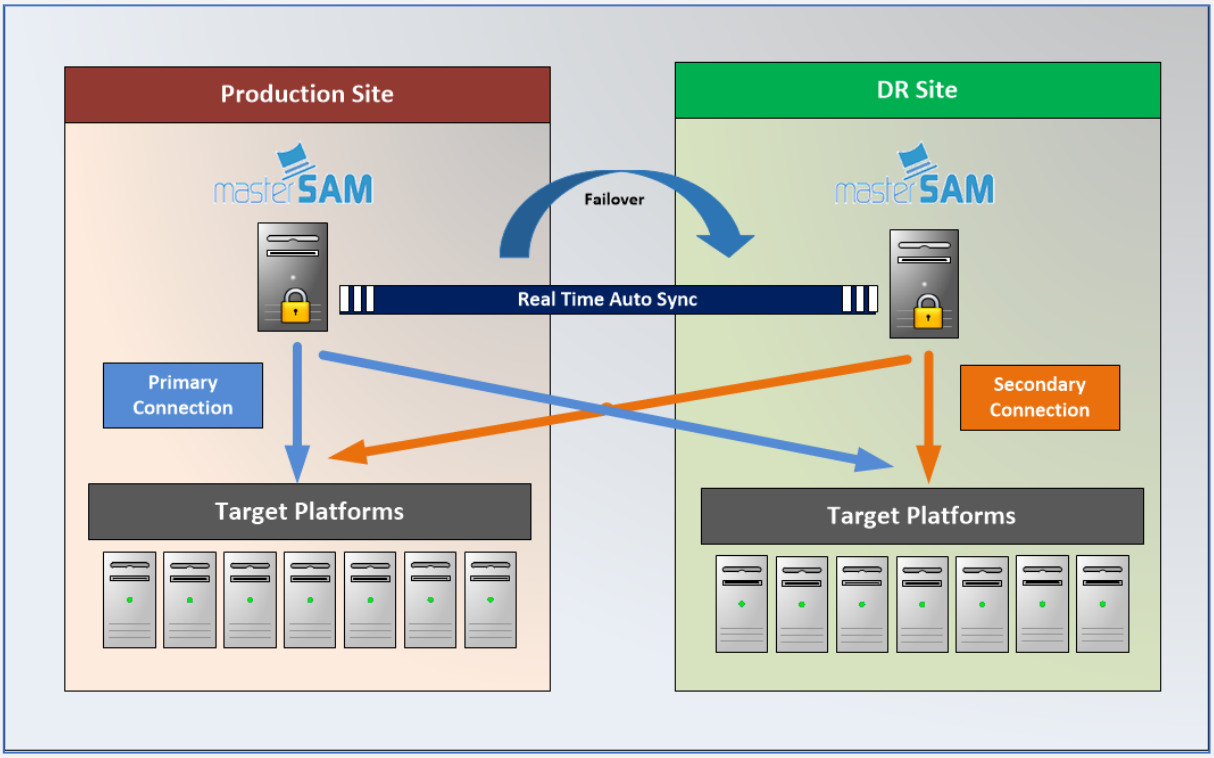
The proposed system is bundled with maintenance script which is schedulable to perform data backup, archival and restoration based on the defined retention period. The system provides automation script that can be scheduled to perform data maintenance with defined parameters such as data range, days to keep, full or incremental. Customer can restore the archived data at any time via the same maintenance script but with different parameters according to the archival data.

In the event of restoration, it is required to perform a fresh installation of OS, database and application; including setting up the similar firewall. Thereafter, the backup needs to be restored to resume the service. Please refer to below example of scenario.



Full back up is performed monthly on 1st February for all data up to 31st January. Incremental backup is scheduled daily. When a disaster happens on 9th February, the full backup has to be restored first, followed by each individual daily backup until 8th February – the last recovery point.

(ii) Disaster Recovery



- Silverlake MasterSAM solutions will be implemented in both production and DRC mode.
- There will be setup of auto-sync from production to DRC for Silverlake MasterSAM via Microsoft File Replication and MSSQL DB Replication technology.
- Target servers at both production and DRC will be configured to connect to production MasterSAM (Primary Connection) and to DRC Silverlake MasterSAM (Secondary Connection).
- In the event of disaster occurring for Silverlake MasterSAM at production site, there will be a failover to Silverlake MasterSAM at DRC.
- User would need to login to Silverlake MasterSAM DRC to perform normal operation.
- All the access, connection and data will flow into Silverlake MasterSAM at DRC while recovery process is taken in place at production site.
- Upon Silverlake MasterSAM recovery at production site, there would be a manual replication activity of data transfer from Silverlake MasterSAM at DRC to production site.

---------- **END OF DOCUMENT** ----------

About Silverlake
Silverlake is a leading Technology Innovations, Banking, Financial and Cyber Security solutions provider in the ASIA Pacific region. Silverlake's business transformation itself is fueled by its relentless desire to delight its customers. Executing parallel efforts in pursuing technology innovations as well as keeping its more than three-decade legacy of deploying core banking at 100% success rate is paramount to the company's strategy. It's subsidiary business, Silverlake MasterSAM, is one of the global market players in Privilege Access Management and cyber security domain. Recognized as Top 25 APAC Compliance solutions providers, Silverlake MasterSAM, headquartered in Singapore, has offices in the Malaysia, Thailand, Philippines, Vietnam and India. For more information, please visit www.mastersam.com or email to info@mastersam.com

Silverlake MasterSAM is an Affiliate member of the Intel® Internet of Things Solutions Alliance. From modular components to market-ready systems, Intel and the 400+ global member companies of the Intel® Internet of Things Solutions Alliance provide scalable, interoperable solutions that accelerate deployment of intelligent devices and end-to-end analytics. Learn more at: intel.com/iotsolutionsalliance