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

Feature List

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.

Feature	X5 Series
Platform, Deployment & Architecture	
Type	**Mid-Enterprise Level USAM functionality**
Options / Configurations Available	**X510, X580**
Type of processor	**2nd-Gen Intel Xeon Scalable processors**
Type of Disk Type	**SATA, SCSI, SSD**
Type of Network Adapter	**10/25/40 Gigabit Intel® Ethernet Network Adapters for OCP**
Supports Agent deployment (distributed USAM)	✓ **(In-house, fully integrated with surveillance, access control and privilege escalation for Windows & Unix/Linux and compliance audit)**
Agentless deployment (centralised USAM)	✓
Hybrid deployment	✓
Supports Adopted enterprise hardening policy	✓
Integration with SIEM	●
Native Integration with Silverlake Aurora[1] solution suite for IDM, AM & DS	✓
Integration with 3rd party IDM	●
Integration with 3rd party ticketing/change management system	●
Native Integration with Silverlake VariA[2] solution suite (Multi-factor Authentication Service Platform)	✓
Support third party Multi-Factor Authentication	✓
Secured credential Vault with multiple security layers	✓
Unified policy engine (Master Policy concept)	✓
Auto discovery	✓
Easily Scalable, to allow larger deployments or new devices or platform technologies	✓

Low-Impact Architecture, minimal changes required to existing architecture	✓
Tamper proof audit logs, session recordings and retention policy to comply to SOX	✓
High Availability and Seamless Disaster Recovery Architecture	✓
Built-in 2FA	✓
Privileged Password, User Access, Session, Credential Protection and Management	
Request approval workflow	✓
Emergency workflow	✓ **(Auto approval for specific users under certain condition)**
Access policy	✓
Support split password dual control	✓
Password verification	✓
Automated password management	✓
Support complex password policy	✓
Eliminate hard-coded password	✓
Supported password reset protocol	**Unix, Windows, Telnet, Web API, Database Connector, IBM-i Connector, Proprietary MasterSAM agent protocol, and others**
Whitelist - allow specific privilege	✓
Blacklist - deny specific privilege	✓
Command restriction via proxy/gateway	✓
Privilege escalation - automated privileged rights assignment and demotion to user own ID, without password involvement	✓
Prevent leap frogging	✓
Auto login session establishment	✓
Supported auto login protocol	**SSH, Telnet, RDP, VNC, Web based, Client based, and others**

Access policy	✓
Centralised web access proxy - Single Sign On portal	✓
No changes of user access existing method	• **Proxy/Gateway** ✓ **Host based approach, maintain user existing access method**
File transfer	✓
Terminate user active session	✓
IBM-i autologin compatibility (native client login, SST dual login)	✓
Manage privilege user access onto the system	✓
Restrict privilege user access onto the system based on allowed IPs, time.	✓
Manage privilege user access + monitor/record such access	✓
Fully Agentless password management for a variety of platforms, including SSH Keys	✓
Verifies credentials on an on-going basis and automatically recovers and resets passwords when out of sync	✓
Least privilege default to every user	✓
Lock down system access from any privilege user's ID login	✓
Centralized web-based Request-Approval workflow Management	✓
Multiple approval level(s) with various delegated approval group(s)	✓
Works with multiple authentication services like RADIUS, RSA, PKI, Oracle SSO, SAML, LDAP	✓
Integration with Ticketing System	✓
Surveillance & Compliance Audit	
Recording for access via proxy/gateway	✓
Recording for access via local/console	✓ **(With host-based approach)**

Recording for access via multiple leap-frogging	✓ **(With host-based approach)**
Recording format	**Text & Image** **(Proprietary format)**
Real time surveillance record transfer & playback	✓
Smart recording based on user interactive activities	✓
Analyse keyword output on recorded sessions	✓
Support grayscale recording	✓ **(Save up to 50% storage)**
Support granular search including keywords	✓
Support session review function	✓
Pinpoint specific violation event	✓
Audit trails and reports	✓
File integrity check	✓
Shared/Mapped drive integrity check	✓
Process life cycle check	✓
Compliance check	●
Dormant account detection	●
Isolated and hardened environment to access privileged accounts	✓
No credentials will be known to users or copied to their endpoints' memories	✓
Fully Agentless session management for a variety of platforms, including SSH Keys	✓
Track & Monitor Every User	✓
Record & Log User Activity	✓
Replay User Activity	✓
System process life cycle audit	✓

File & folder integrity check	✓
Combined Video & Text based Logs in user session	✓
Interactive text & keyword search ability	✓
100% full surveillance recording – on every user	✓
Export to SIEM tools	✓
Small foot print recording	✓
Granular search & filter criteria	✓
Comprehensive report(s)	✓
Customizable connectors to connect to various platforms / software / web using privileged credentials. E.g., launching Microsoft SQL Server Management to access an MSSQL account without having the software installed on the user's workstation	✓
Provide universal keystroke audit which is typed during privileged session	✓
Offers command line control and native SSH access while still providing secure access to privileged users using either passwords or SSH keys	✓
Provide Blacklist (Deny) action to be carried out by user within system	✓
Provide Whitelist (Allow) action to be carried out by user within system	✓
Provides AD Bridge capabilities that enable organizations to centrally manage Unix users and accounts that are linked to AD.	✓
Securely Connect into devices that are not managed by the management tool	✓
Live Monitoring and Termination of Ongoing Sessions	✓
Application Control for Endpoints & Servers	
Support for updating password on Windows Services	●
Support for updating password on Windows Scheduled Tasks	●
Support for updating password on Windows IIS Pools	●
Support for updating password on Windows COM+ Applications	●

Support for updating password on Windows IIS Directory Security (Anonymous Access)	●
Support for updating password on text-based config files	●
API and SDK for applications to call for passwords instead of relying on embedded or hard coded credentials with minimal code change	●
Integrate with application middleware such as WebLogic, WebSphere, Jboss, and Tomcat to eliminate hardcoded password without the need of code changes	●
Integration and Automation	
Enterprise Class Integration. Ready to leverage on existing security investment with out of the box support	✓
SIEM Tools	✓
Cloud Services like AWS, Azure and Corporate Social Media Accounts	✓
Vulnerability Managers like Rapid7, Tenable Nessus, Qualys	✓
Identity Managers like RADIUS, RSA, SAML etc	✓
Ticketing Systems like ServiceNow or BMC Remedy	✓
Integration with analytical tools or solution. Analytics and alerting on malicious privileged account activity.	✓
Detects and alerts in real-time	✓
Enables automatic response to detected incidents	✓
Establishes profiles of typical privileged user behaviour	✓
Identifies anomalies including malicious privileged account activities and suspicious Kerberos traffic	✓
Adapts threat detection to a changing risk environment with self-learning algorithms	●
Correlates incidents and assigns threat levels	●
Enhances the value of existing SIEM solutions with out-of-the-box integrations	✓

Improves auditing processes with informative data on user patterns and activities	✓
Command Line Interface Tool available for scripting various automation needs e.g., automatically onboarding and removing new accounts	●
Hardware	
Intel Software Guard Extensions (Intel SGX) Technology	✓
Intel Active Management Technology (AMT)	✓
Redundant power supply	✓
RAID 1	✓

[1]Aurora is an Identity Access Management solution offered by Silverlake Sheaf, a Silverlake Group Company
[2]VariA is Multi-Factor Authentication Solution offered by Silverlake Sheaf, a Silverlake Group Company

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. Silverlake Sheaf, acts as authorized reseller for all solutions of Silverlake MasterSAM. For more information, please visit www.silverlakegroup.com and www.mastersam.com.

For direct purchase enquiries on the above solution, please visit www.silverlakesheaf.com/rimba/ or write to sheaf_sales@silverglobe.com

Rimba is the Official Online store by Silverlake Sheaf, a Silverlake Group Company. Offering a spectrum of Certified Intel Market Ready Appliance Based Solutions including cyber security products, Rimba makes acquiring enhanced security seamless. Our products have been specially curated to address modern-day cyber security concerns, while adhering to latest technological developments. Browse through our products and experience an effortless shopping experience, all at the convenience of your time and space.