SILVERLAKE MASTERSAM STAR GATE

DATA SHEET

SECURE WITH A FORMIDABLE SECURITY LAYER

Managing cybersecurity in today's fast-growing security landscape is indeed a herculean task. Insider threats have been growing tremendously and this is a trend that will continually command attention. Therefore, managing privileged access has become a priority milestone to achieve in every organization's cybersecurity blueprint.

MasterSAM Star Gate acts as a formidable security layer that manages and monitors secure privileged credential and access across the enterprise IT environment, regardless of whether it is on-premise data center, on the cloud or on hybrid infrastructure. This agent-less architecture enables organizations to meet all compliance needs in a quick deployment model.

BENEFITS

Password Protection and Management
Secured vault to store and manage privileged credentials regardless of complexity and assure flexible reset mechanism. Split password protection to hide full password during password release cycle. Password verification and reconciliation ensures passwords are always in-sync. Provides secured API for real time password retrieval by authorized script/application. Supports white list and black list tools.

Smart Mechanism to do Real-time Recording
Privileged access activities are recorded and tamper-proof and real time transfer of recorded data to central repository.

Support Multi-factor Authentication
AD, LDAP, RADIUS, username/password, SMS token, SMTP email token, built-in mobile apps token, integration with enterprise 2FA.

ONE ID to remember
Centralised access point for administrators to connect to manage systems- Broad system support protocols – SSH, RDP, Telnet, VNC, HTTP(S), software clients such as vSphere, SQL Management Studio, iSeries Navigator, X11, Toad for Oracle, HP Tandem, etc.

Seamless User experience
Allows connectivity via native clients such as PuTTY, MSTSC, WinSCP, Tectia SSH, etc. Supports Least privilege principle and emergency request to ensure operation continuity after working hours, weekend or emergency scenarios. Allows password rotation without business impact.

Guarantees Compliance to industry regulations: PCI – DSS, ISO 27001/27002, MAS-TRM, HIPAA, SOX404, APRA, COBIT, BNM -GPIS, etc

KEY FEATURES

a. **Automated Password Management**

b. **Smart Surveillance Engine**

c. **Multi-factor Authentication**

d. **Single Sign-on and Auto login**

e. **Access control and Workflow**

f. **Application to Application Control**

g. **Command Restriction**

h. **Compliance Fulfillment**

SILVERLAKE masterSAM
SYMMETRY AT WORK

SILVERLAKE MASTERSAM ANALYST

DATA SHEET

SUPERIOR SECURITY INTELLIGENCE FOR REAL-TIME ALERT AND RESOLUTION

Increasingly, we read about malicious attackers going unnoticed for months by impersonating as authorized users and wreaking havoc in the most sensitive environments of organizations. It is therefore, highly intrinsic to enforce transparency and accountability in the security platform.

MasterSAM Analyst, serving as a centralized log repository, houses indisputable evidence of user activities, which is further complemented with real-time user session replay and review capability. With such superior intelligence that promises complete visibility, one would be fully assured of security compliance for enforcement reporting and audit purposes.

BENEFITS

Real-time session monitoring and playback
Real time DVR-like playback of user activities at anywhere, anytime. Replay session from any point of a specific event.Tracks and monitors every single access, keystroke or click to system objects such as command, file/folder, database query, application, service, etc. Allows multiple reviews.

Smart Analytical Engine
Flexible and intuitive search from basic to complex scenarios that support combination of rules. Automated filtering of session logs that match with the defined rule sets. Provides scheduled or real time alert upon detection of violation against policies.

Single and centralized management console for both host and gateway based deployment model. Clear segregation of user session activities by deployment model.

Comprehensive reporting
Hundreds of out-of-the-box reports that are easily customizable. Supports ad-hoc and scheduled reporting. Allows dynamic generation of report that pin-point directly towards specific occurrence.

KEY FEATURES

a. Real-time session monitoring

b. Smart Analytical Rules Engine

c. Shared platform for Host and Gateway Based Deployment model

d. Powerful Reporting and Investigation Tool

SILVERLAKE masterSAM
SYMMETRY AT WORK

info@mastersam.com wwww.mastersam.com

SILVERLAKE MASTERSAM PRIVILEGED MANAGEMENT SYSTEM

DATA SHEET

SUPERIOR SECURITY INTELLIGENCE FOR REAL-TIME ALERT AND RESOLUTION

Increasingly, we read about malicious attackers going unnoticed for months by impersonating as authorized users and wreaking havoc in the most sensitive environments of organizations. It is therefore, highly intrinsic to enforce transparency and accountability in the security platform.

MasterSAM Analyst, serving as a centralized log repository, houses indisputable evidence of user activities, which is further complemented with real-time user session replay and review capability. With such superior intelligence that promises complete visibility, one would be fully assured of security compliance for enforcement reporting and audit purposes.

BENEFITS

Real-time session monitoring and playback
Real time DVR-like playback of user activities at anywhere, anytime. Replay session from any point of a specific event.Tracks and monitors every single access, keystroke or click to system objects such as command, file/folder, database query, application, service, etc. Allows multiple reviews.

Smart Analytical Engine
Flexible and intuitive search from basic to complex scenarios that support combination of rules. Automated filtering of session logs that match with the defined rule sets. Provides scheduled or real time alert upon detection of violation against policies.

Single and centralized management console for both host and gateway based deployment model. Clear segregation of user session activities by deployment model.

Comprehensive reporting
Hundreds of out-of-the-box reports that are easily customizable. Supports ad-hoc and scheduled reporting. Allows dynamic generation of report that pin-point directly towards specific occurrence.

KEY FEATURES

a. Centralised Management Dashboard

b. Dynamic Escalation workflow

c. Discovery of Super User Privilege

d. Active Directory User Mapping with Unix/Linux Local Users

e. Quick deployment of Unix Sudo

f. Compliance and System Integrity Check

SILVERLAKE masterSAM
SYMMETRY AT WORK

SILVERLAKE MASTERSAM FRONTLINE

DATA SHEET

ADDRESS VULNERABILITY IN END-POINT PROTECTION

Windows platforms are ubiquitous and thus, become primary targets for cyber attacks. Such targeted attacks can easily bypass endpoint security despite having multi-layered protection like antivirus, encryption, anti-phishing, IPS/IDS and more. In this context, endpoint/desktop monitoring capability must go beyond perimeter intrusion detection. Organizations need full visibility of critical activities performed on endpoints, as part of the overall strategy in endpoint protection.

MasterSAM Frontline provides the **monitoring capability** to record activities while users access the critical system or application at their desktop /end-point. With its **flexible policy**, organizations can choose to monitor specific program or application, either in full screen or active windows mode.

BENEFITS

Least privilege by default

Best industry practice for compliance - reduces the risk of attack surface for users who possess full administrator rights always. Flexible, intuitive management of privileges according to user's role. **On-demand privilege escalation** based on authorized period. No involvement of privileged password. Self service privilege escalation **frees up IT help desk for other activities.** Connected and managed centrally via MasterSAM **Privilege Management System.**

User Session Recording

Record each access to endpoint – irrespective of methods of login (remote, console, leapfrogging). Option to record the entire session, by specific program/application, active windows or by privileged activities only.

Granular Access Control

Option to automatically terminate user session upon exceeding the approved duration, or allow session continuity with **exceptional alert.** Restricts system object access to file/folder, registry, service, shared folder and event viewer, while **supporting whitelist & blacklist rules.** Non-intrusive and works on top of Windows GPO. **Immediate enforcement** without re-login and enforcement still intact despite connection failure with centralized management server.

Dectection and Tracking

Tracks modifications on sensitive file/folder, shared folder and process lifecycle. Detects non-compliant endpoints against the enterprise baseline password policy & simple password. **Detects** users that are member of Administrators group, default administrator account not being renamed, guest account not being disabled and scans and detects privileges on the system.

KEY FEATURES

a. Least Privilege Principle

b. Role based and Dynamic Privilege Escalation

c. Centralized Management and Session Control

d. 100% Surveillance Engine for User Session recording

e. In-Depth Granular Access Control

f. Compliance and System Integrity Check

g. Help desk load reduction

h. Reduce malware attack surface

SUPPORTED PLATFORMS

Windows XP
Windows Vista
Windows 7
Windows 8
Windows 8.1
Windows 10

SILVERLAKE masterSAM

SILVERLAKE MASTERSAM

SECURE@WINDOWS

DATA SHEET

SECURE, TRANSPARENT AND ACCOUNTABLE

Windows platforms are ubiquitous and thus, become primary targets for cyber attacks. Enterprises largely use Microsoft Active Directory as a main identity infrastructure solution. Moreover, common cybersecurity attacks such as Pass-the-Hash, Ransomware, etc. are much more vulnerable at Windows based platform. MasterSAM Secure @ Windows applies stringent granular access control over critical system objects, thereby, promoting greater transparency and accountability across multiple platforms.

BENEFITS

Ensures Least privilege by default - Best practice for industry and compliance regulations. Reduces the risk of attack surface for users who possess full administrator rights always.

Flexible and intuitive management of privileges according to user's role
On demand privilege escalation based on authorized period
No involvement of privileged password

Connected and managed centrally via MasterSAM Privilege Management System (PMS)
Option to automatically terminate user session upon exceeding the approved duration, or allow session continuity with exceptional alert

Records each access to server – regardless methods of login (remote, console, leapfrogging)
Compensating control to track users that bypass the authorized gateway/proxy
Option to record all users' activities – with or without privileged access

Restricts system object access on command level
Supports whitelist & blacklist rules
Restricts permission and access during file transfer
Non-intrusive and works on top of Unix permission and access control
Immediate enforcement without re-login
Enforcement still intact despite connection failure with centralized management server

Detects dormant accounts with specific inactive period and their associated services
Detects users with root equivalent rights (UID=0)
Detects non-compliant servers against simple & restricted password dictionary
Detects disabled service running
Detects syslog service status
Scans and detects privileges on the system

KEY FEATURES

a. Least Privilege Principle

b. Role based and Dynamic Privilege Escalation

c. Centralized Managment and Session Control

d. 100% Surveillance Engine for User Session recording

e. In-Depth Granular Access Control

f. Compliance and System Integrity

SUPPORTED PLATFORMS

Microsoft Windows 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2,

Active Directory

Both joint-domain and workgroup

SILVERLAKE masterSAM
SYMMETRY AT WORK

SILVERLAKE MASTERSAM

SECURE @ UNIX / LINUX

DATA SHEET

SECURE, TRANSPARENT AND ACCOUNTABLE

In Unix/Linux environment, SU and SUDO utilities are popularly being used to facilitate the privileged operation and administration. Users would need to supply the root's password during the switch of account and profile to root privilege. Thereafter, they will have full administrative rights on the operating system and they can even switch to any other privileged account without the needs to supply its password.
Once compromised, the damage is irreversible. Organizations should take proactive approach and implement control to ensure that only authorized users are given the privileged access within a specific duration, not on a permanent basis.

MasterSAM Secure @ Unix/Linux is designed for organizations to enforce Least privilege principle and apply stringent granular access control over critical system objects, including menu based access.

BENEFITS

Ensures Least privilege by default - Best practice for industry and compliance regulations. Reduces the risk of attack surface for users who possess full administrator rights always.

Flexible and intuitive management of privileges according to user's role
On demand privilege escalation based on authorized period
No involvement of privileged password

Connected and managed centrally via MasterSAM Privilege Management System (PMS) - Option to automatically terminate user session upon exceeding the approved duration, or allow session continuity with exceptional alert

Records each access to server – regardless methods of login (remote, console, leapfrogging). Compensating control to track users that bypass the authorized gateway/proxy - Option to record all users' activities – with or without privileged access

Restricts system object access on command level
Supports whitelist & blacklist rules, restricts permission and access during file transfer
Non-intrusive and works on top of Unix permission and access control
Immediate enforcement without re-login
Enforcement still intact despite connection failure with centralized management server

Detects dormant accounts with specific inactive period and their associated services, Detects users with root equivalent rights (UID=0), Detects non-compliant servers against simple & restricted password dictionary, Detects disabled service running , syslog service status and scans and detects privileges on the system

KEY FEATURES

a. Least Privilege Principle

b. Role based and Dynamic Privilege Escalation

c. Centralized Managment and Session Control

d. 100% Surveillance Engine for User Session recording

e. In-Depth Granular Access Control

f. Compliance and System Integrity

SUPPORTED PLATFORMS

AIX 5.1, HP-UX 11.11, Solaris 8, x86 or SPARC

Redhat 2.1, CentOS 6

Ubuntu

SUSE 9

Other common Linux flavors

SILVERLAKE masterSAM
SYMMETRY AT WORK