ASSERTION®
a voice security company

Smart Logging

Get real-time observability across all your voice assets on a single dashboard by proactively monitoring logs for issues. Go from issues to logs in 1-click. Detect errors, call & recording failures to improve service levels for managed services & cloud customers.

It integrates with 53+ voice products through Syslog for Linux and a custom log collector script for Windows.

October 2025

Voice teams are blind to issues until they impact service quality

1. **Delayed Issue Detection** - Voice systems lack real-time monitoring, leading to unexpected failures.

2. **Fragmented or Unavailable Logs** - Data is scattered across systems, making incident analysis slow and inefficient.

3. **Reactive Troubleshooting** - Engineers scramble to diagnose and resolve issues, increasing downtime.

4. **SLA Violations & Escalations** - Long resolution times result in business impact and lost revenue.

"Without proactive monitoring, every voice failure is a costly surprise!"

Bring visibility & efficiency to voice operations with **Smart Logging**

1. **One-Click Access to Logs -** Access event-specific logs without manual searching or waiting for NOC

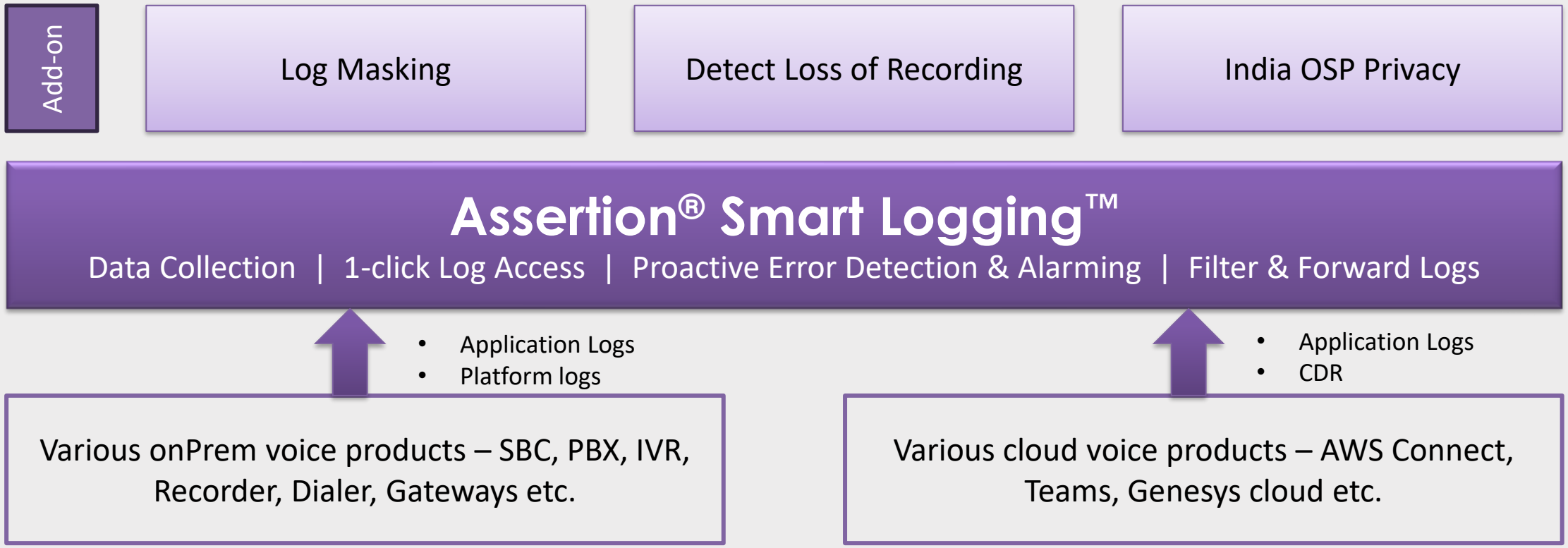
2. **Real-Time Error Detection -** AI-powered monitoring scans all voice logs, identifying issues in real time

3. **Better SLA Compliance -** Reduced troubleshooting & down time prevents SLA violations

4. **Automated Alerts & Insights -** Alerts are triggered instantly, with root-cause analysis

"See the problems before they happen, fix them before they hurt!"

AI based Observability and Proactive fault monitoring



Features

Collect logs from 53+ voice systems without a log collection agent

Vendor agnostic. Supports all major Voice vendors.

Collect any log file – platform (OS) or application. Can add more files to pipe.

Clone filters and forward logs for selective archival. Output in CEF, JSON and CSV to support all SIEMs.

Single dashboard to monitor errors and system health

1-click access to logs from the web portal.

Configure and manage simple log patterns on portal

Detect complex patterns / correlate logs using workflows

Custom dashboard widget for better observability

Store local copy of logs for 30 days for immediate access

Integrate with AD for authentication

Get a report of alarms raised in last 30 and 365 days.

Ability to transpose each log line into custom format

servicenow

Integration with ServiceNow for tickets.

Rest API for downstream automation.

Why Assertion Smart Logging is Better than SNMP, CDR Analytics, Voice Monitoring Tools & SIEM?

Log Monitoring for Voice Apps

- Collect Platform, Application or Custom logs in near real-time.
- Understand log formats of 100s of log files from 53+ products out of the box.

Proactive Fault Monitoring

- Auto detect critical and major errors
- Self-service portal to detect known log patterns
- Suppress unwanted events to avoid alert fatigue

1-Click Log Access

- Instant log access via the central portal
- No more missing or overwritten logs
- No need to raise ticket, share privileged ID with vendors or wait for experts

Clone, Filter and Forward logs

- Create copies of logs to run multiple filters
- Selectively archive only important logs to save on archival (SIEM) costs
- Support forwarding to all major SIEMs

AI Powered PII Masking

- Mask structured and unstructured PII using a combination of Regex and AI
- Mask before Store, View or Export
- Self-service configuration on portal

Detect Loss of Recording

- Monitors logs in near real-time to detect loss of recording
- Correlate logs across systems to detect failures
- Highlight top 10 Agents with recording failures

AI Powered Log Insights*

- Get daily highlights of Security, Compliance and Operational events
- Chat with the logs to get insights on health of each component and incidents.

Prescriptive Root Cause Analysis*

- Detect RCA by correlating logs across various connected systems and inferring the causal relationships
- Remediation suggestions using OEM KB

* Upcoming

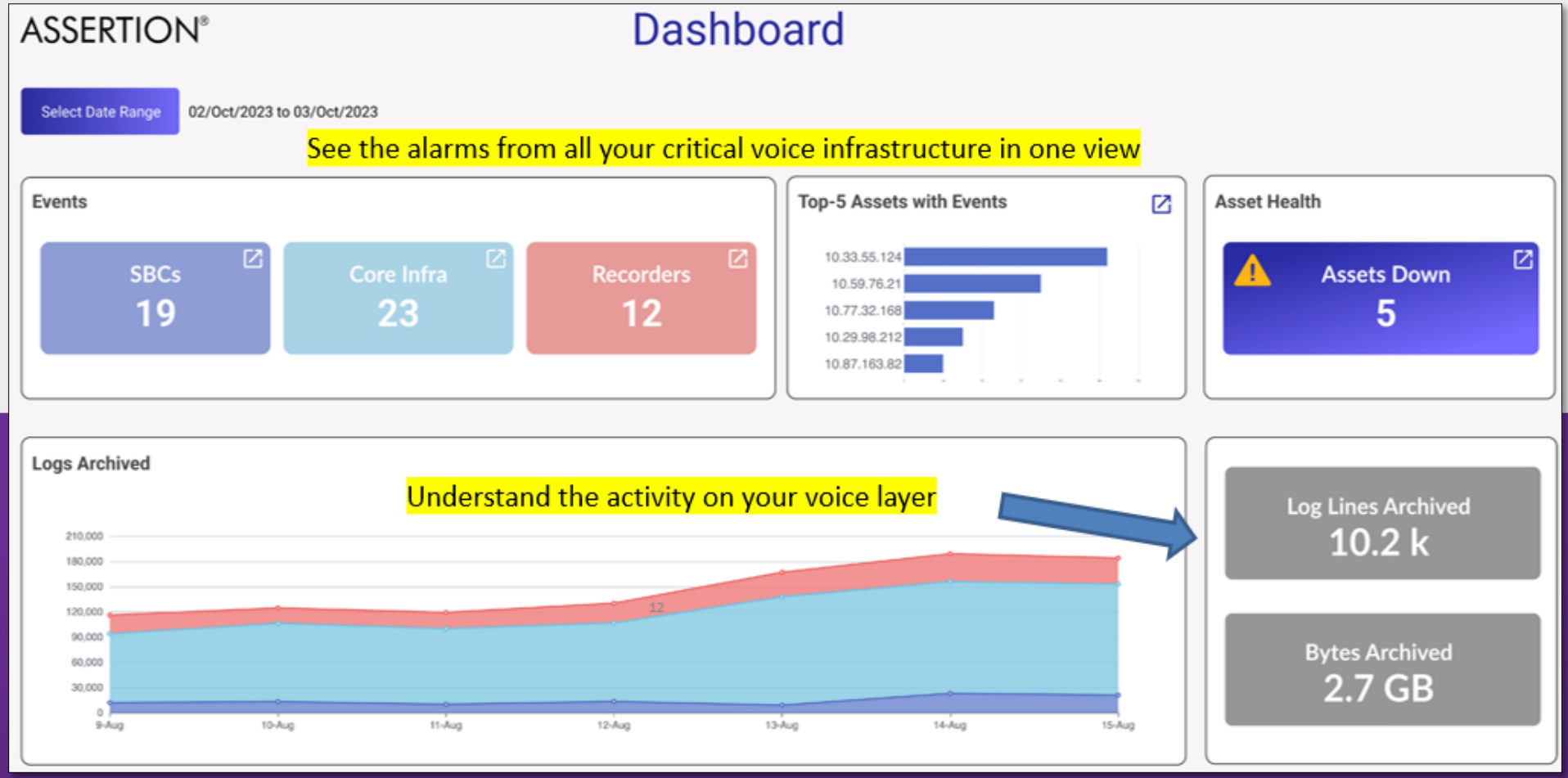
Log Monitoring for Voice Apps

- Amazon Connect (AMCON)
- Atos Unify Openscape Voice (AUOSV)
- AudioCodes One Voice Operations Center (ACOVOC)
- AudioCodes Session Border Controller (ACSBC)
- Avaya Analytics Cluster Control Manager (AACCM)
- Avaya Aura Appliance Virtualization Platform (AVP)
- Avaya Aura Application Enablement Services (AES)
- Avaya Aura Communication Manager (ACM)
- Avaya Aura Device Services (AADS)
- Avaya Aura Media Server (AMS)
- Avaya Aura Messaging (AAM)
- Avaya Aura Session Manager (ASM)
- Avaya Aura System Manager (ASMGR)
- Avaya Aura Utility Services (AUS)
- Avaya Breeze (ABRZ)
- Avaya Call Management System (ACMS)
- Avaya Contact Recorder (ACR)
- Avaya Contact Recorder Advanced (ACRA)
- Avaya Control Center Control Manager (ACCCM)
- Avaya Experience Portal EPM (AEP-EPM)
- Avaya Experience Portal MPP (AEP-MPP)
- Avaya Media Gateway (AMG)
- Avaya Oceana Cluster Server (AOCS)
- Avaya Session Border Controller (ASBC)
- Avaya Social Media Hub (ASMH)
- Genesys Administrator (GEADM)
- Genesys Engage SIP Server (GESIP)
- Genesys ICON Server (GEICON)
- Genesys Infomart (GEINFO)
- Genesys Media Control Platform (GEMCP)
- Genesys Orchestration Server (GEORS)
- Genesys Pulse Server (GEPULSE)
- Genesys Resource Manager (GERM)
- Genesys Stat Server (GESTAT)
- Genesys Universal Routing Server (GEURS)
- Microsoft Dynamics 365 Omnichannel (MSD365O)
- Microsoft Skype for Business (SFB)
- Nice Engage Recorder (NICEREC)
- Oracle Enterprise Session Border Controller (OSBC)
- Verint Impact 360 Recorder (VI360)
- Verint Verba (VFC)
- Verint WFO Forecasting and Scheduling (VWFS)
- Verint WFO Knowledge Management Back End (VWKMBE)
- Verint WFO Knowledge Management Front End (VWKMFE)
- Verint WFO Knowledge Management Jenkins (VWKMJ)
- Verint WFO Knowledge Management Reporting (VWKMR)
- Verint WFO MobileGateway (VWMG)
- Verint WFO Portal (VWP)
- Verint WFO Speech Analytics (VWSA)
- Verint WFO Speech Analytics Transcription (VWSAT)
- Verint WFO Text Analytics (VWTA)
- Verint WFO Text Analytics Data Store (VWTADS)
- Verint WFO Text Analytics Management (VWTAM)

Out-of-the-box support for 53+ OEM voice systems

Collect and Understand all the important log files from every one of these products

Proactive Fault Monitoring



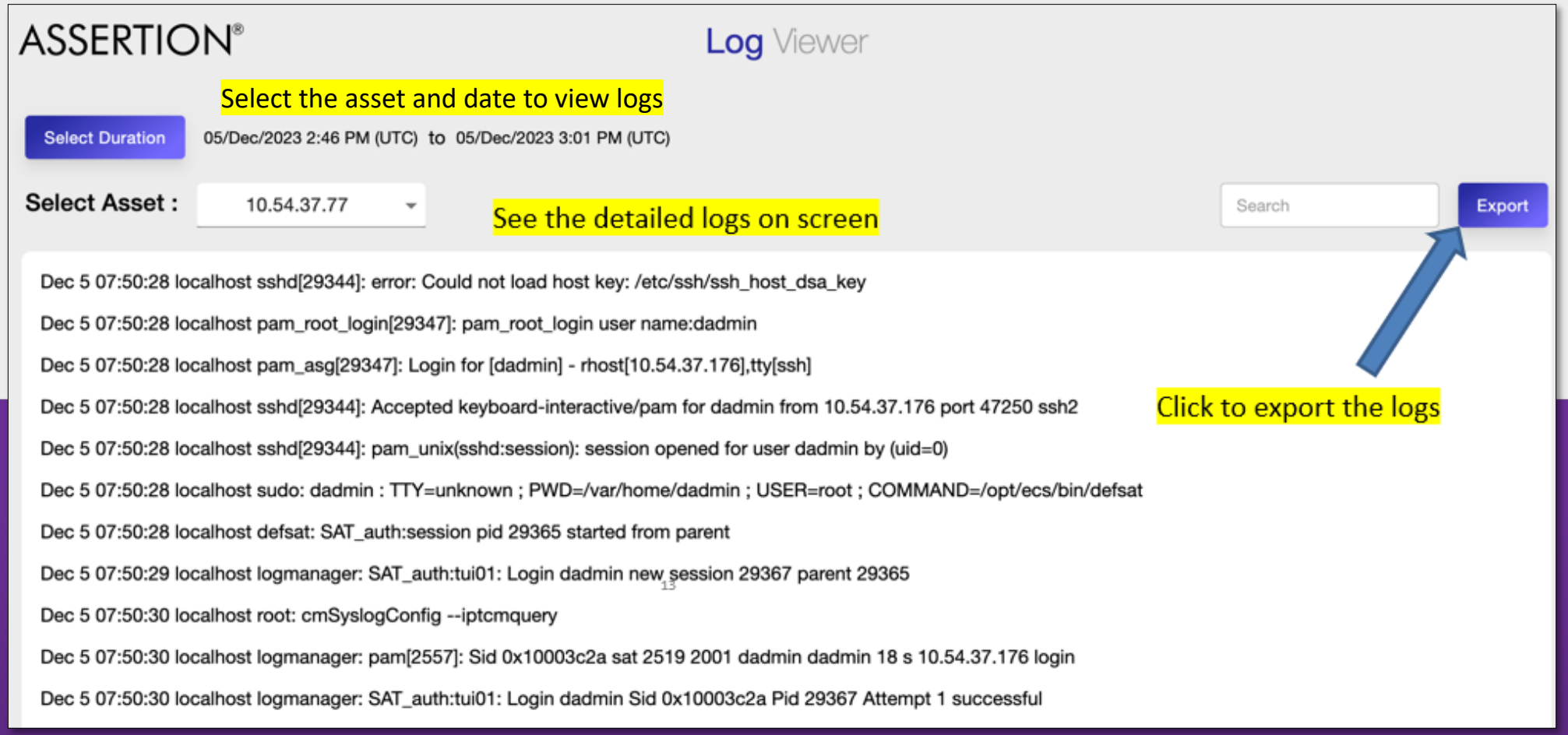
Detect Critical and Major alarms out of the box

Self service portal to configure custom patterns

Suppress unwanted events to avoid alert overload

Alert using email, Ticket (REST API) or Dashboard

1-Click Log Access

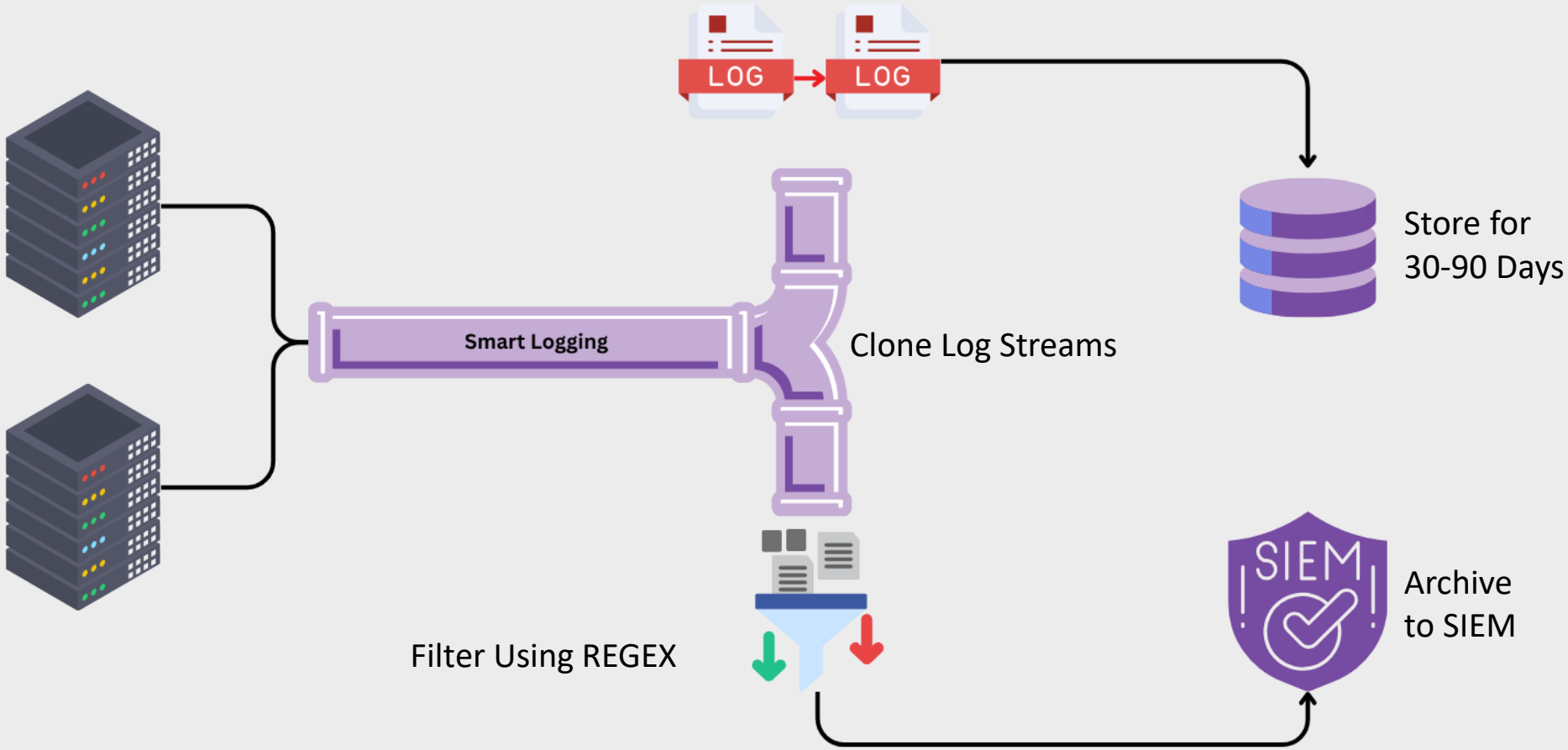


View logs of all assets in an instant

No wasting time on getting Login credentials and access, waiting on technicians to connect and pull data.

Select the Asset, Time duration and View logs

Clone, Filter and Forward Logs

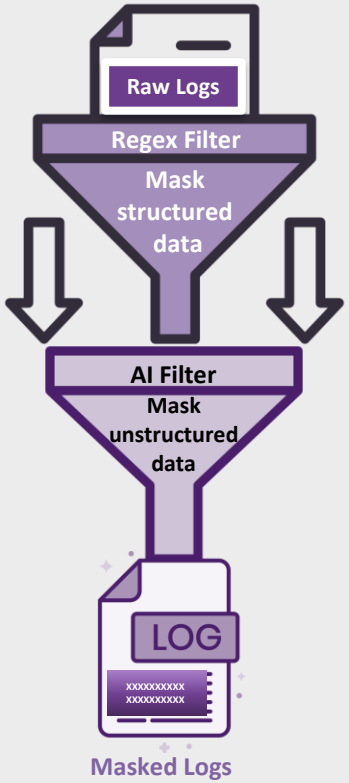


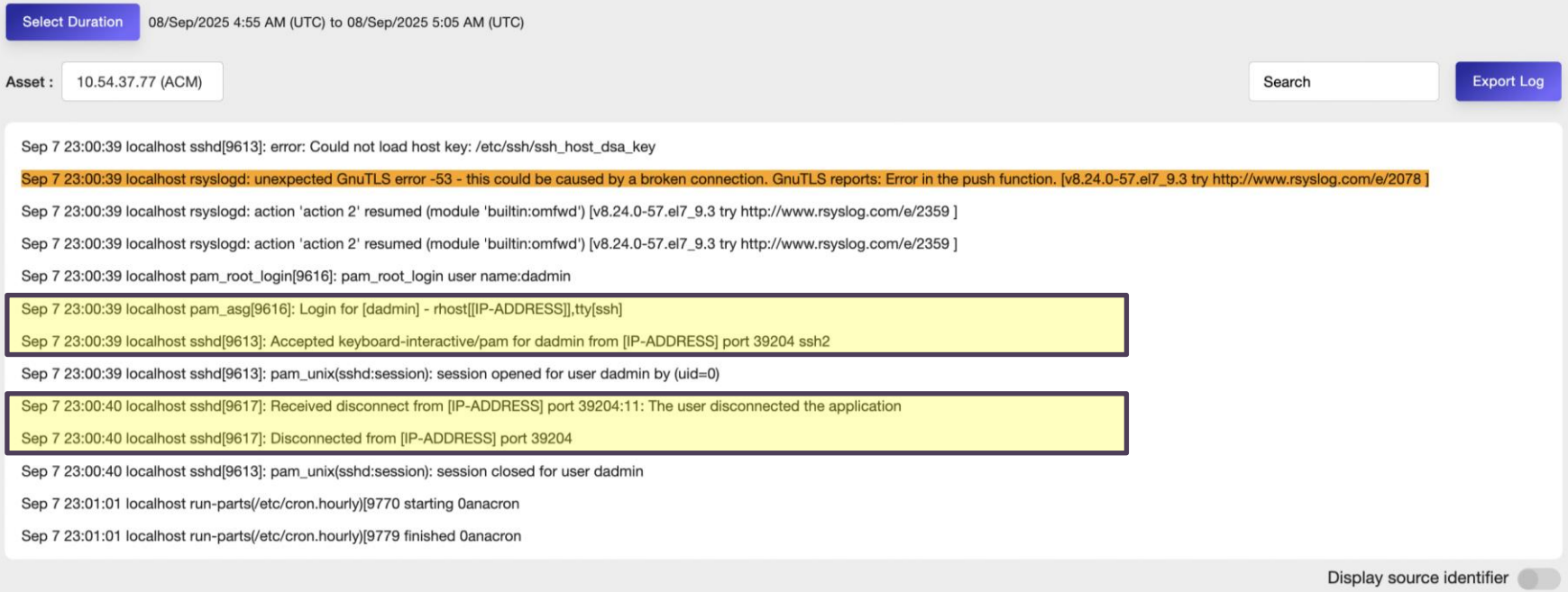
Filter what is important and only Archive that.

Save up to 80% on the costs of archival by not archiving transaction and chatty logs.

Store locally for 90 days for instant log access on the portal.

AI Powered PII Masking



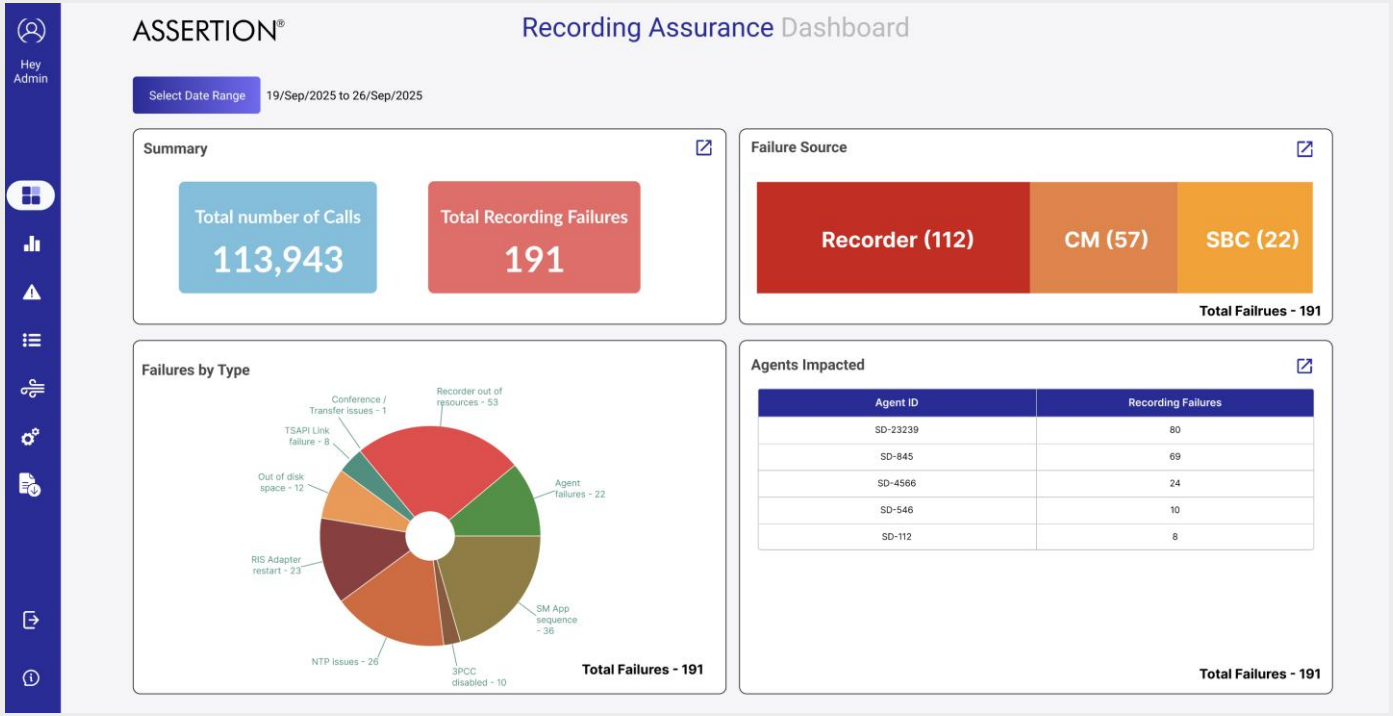


Mask structured & unstructured PII using a combination of Regex and AI

Mask before Store, View or Export

Self-service configuration on portal

Detect Loss of Recording



Additional scenarios, if observed on your site, can be coded in within days.

ID	Scenario	Platform
1	Recorder out of disk space leading to failed recordings	Any CC - Verint
2	Recorder out of XML records leading to failed recordings	Any CC - Verint
3	RIS adapter restart causing loss of recording	Any CC - Verint
4	3PCC parameter in CM is disabled and no call recording happened	Avaya - Verint
5	CM App Sequence was not enabled on Session Manager, and no calls are recorded	Avaya - Verint
6	Manual call made by the Agent who is already nailed, call was not recorded occasionally	Avaya - Verint
7	AES NTP issue leading to recording outage	Avaya - Verint
8	AES TSAPI adapter link to Recorder down causing loss of recording	Avaya - Verint

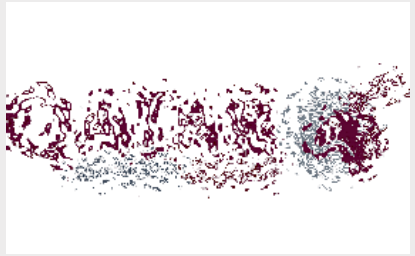
Monitors logs in near real-time to detect loss of recording

Correlate logs across systems to detect failures

Highlight top 10 Agents with recording failures

Success Stories

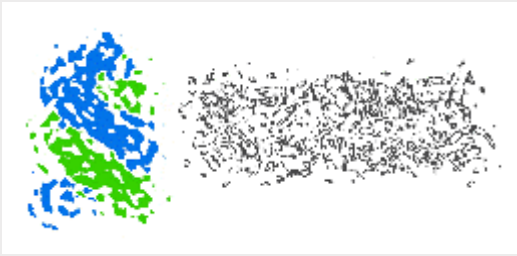
Airline



A top airline in Asia that operated an Avaya, Cisco, Oracle and Verint contact center products wanted to proactively monitor the systems for errors, warnings and custom events and be notified of the same in practically real-time. Since sensitive customers could be in the logs, they wanted to mask any such PII, if found.

They implemented Assertion Smart Logging for 200+ voice servers, with near real-time log processing and alerts for errors, warnings, and custom events. The comprehensive dashboard improved network health visibility, while automated email alerts and ServiceNow tickets. The Voice Ops team gained quick access to 30 days of raw logs, significantly improving SLA adherence. PII masking ensured compliance with data privacy rules, and secured access via the bank's AD enhanced security.

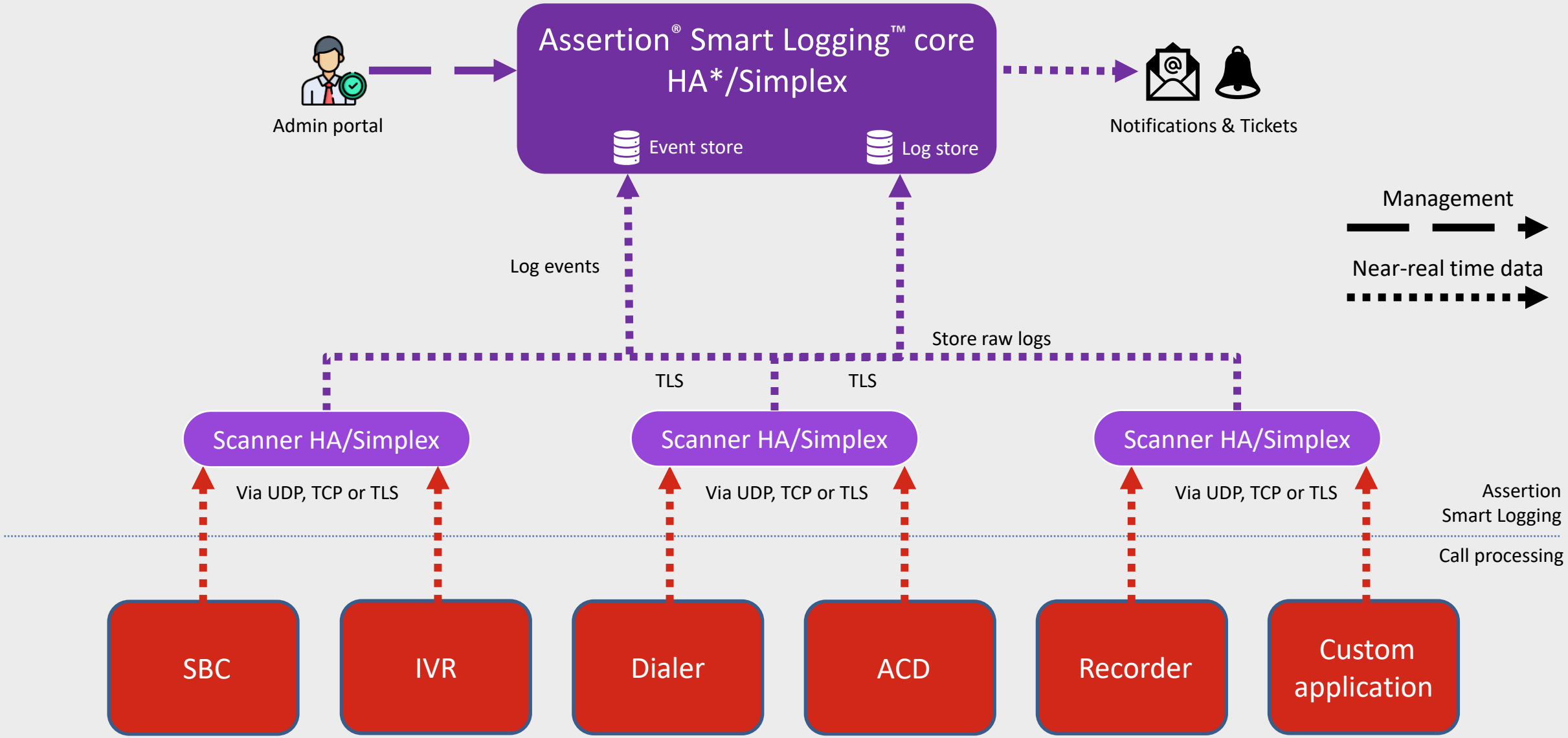
Bank



A top 30 global bank operating in 60+ countries with a diverse voice network (Avaya, Cisco, AudioCodes, Oracle, Verint, and Microsoft Skype for Business) needed to collect logs from 800+ systems, filter IAM logs, and archive them separately for audit purposes. Not all products supported the Splunk HIDS agent, so collecting logs from every voice asset was not possible. Some systems could send logs to only one destination, so a method was needed to "clone" logs, archiving one copy in raw format and filtering another for IAM logs.

Assertion Smart Logging collated and collected logs from about 800+ voice servers from the bank. This agent-less system gathered logs from every voice system via various protocols and methods, cloning them into two copies. Raw logs were stored on a NAS, while filtered IAM logs were organized by product, asset, and date for easy retrieval. This streamlined log management and ensured compliance with audit requirements.

Architecture Design - Proactive Log Monitoring with 1-Click Log Access



HA* – Virtual IP, Same subnet (no GR)

Hardware, Software and Network requirements

- **Assertion® Smart Logging Core**
  - Hardware requirements – VM with 16GB RAM, 4 vCPU * 2.2GHz, free disk space of 5 TB (inclusive of Log store)
  - Software requirements – OVA provided with RHEL 9.x. Customer to provide license.
  - ESXi – 7+
  - Network – 1 NIC cards, 1Gbps

Only core is sufficient for pilot

- **Assertion® Scanner**
  - Hardware requirements – VM with 8GB RAM, 4 vCPU * 2.2GHz, free disk space of 150 GB.
  - Software requirements – OVA provided with RHEL 9.x. Customer to provide license.
  - Network – 1 NIC cards, 1Gbps
  - ESXi – 7+

ASSERTION®
a voice security company

Thank you

Contact us today to discover how Assertion's innovative solutions can elevate your technology infrastructure and meet your evolving needs.