

**VERSATILITY**

# Observability & Insights for Network Operations

**Roopa Bayar**

VP Engineering

# Agenda

- Challenges with Observability solutions
- Versa's Observability solution
- Observability driven insights
- Observability components
- Conclusion
- Demo
- Q&A

# Observability Challenges: **Scale**

*Massive telemetry + distributed systems = complexity, cost, and noise*

## Data Explosion & Cost

---

- Logs, metrics, traces at massive scale
- High storage and compute cost
- Retention vs cost trade-offs

## Signal vs Noise

---

- Too many alerts, low signal
- Alert fatigue
- Hard to extract insights

## Distributed Complexity

---

- Logs from disparate sources
- Difficult end-to-end tracing
- Complex dependencies

## High Cardinality

---

- User/device/IP explosion
- Query performance impact
- Indexing overhead

# Observability Challenges: **Fragmented Landscape**

*Multiple tools and vendors lead to siloed data, higher cost, and poor visibility*

## **Multi-Vendor Monitoring**

---

- Different tools for network, app, security
- Lack of standardization
- Integration complexity

## **Multiple Panes of Glass**

---

- Separate dashboards
- No unified view
- Slower troubleshooting

## **Visibility Gaps**

---

- Siloed data
- Hard correlation
- Missed insights

## **Cost & Complexity**

---

- Multiple licenses
- Duplicate storage
- Operational overhead

# Versa's Observability Solution

Unified platform, policy, data lake & console for centralized visibility



End-to-end optimization across data collection, processing, and analysis



Rich, context-aware telemetry generated at the source



Enhanced correlation & faster detection through augmented telemetry



Minimizes deep log analysis and manual investigation effort



High-level actionable insights & alerts instead of raw data noise



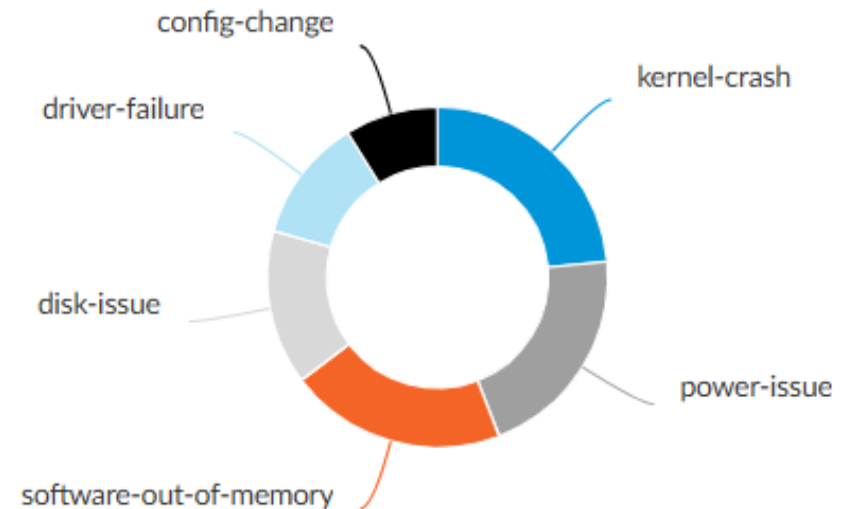
# Observability driven insights

# Observability driven insights: *Branch Issues*

- Why was the branch unreachable?
  - Is it due to local or network or other issues?
  - Did my branch restart due to s/w core dump, upgrades or power issues?
  - Did my branch restart due to recent config changes?
  - Did my branch lose connectivity to controllers due to network issues?

## Local Issues: Top causes

Top 10 



# Observability driven insights: *Branch Issues*

SITES WITH ISSUES    LOCAL ISSUES    NETWORK ISSUES    UNKNOWN ISSUES

34    32    1    3

Insights for sites with network issues

Set filters here...    Apply | Clear | Copy Filter    Show 10 Entries

Generation Time	Appliance	Description	Sub Category
Apr 27th 2026, 8:30:47 PM PDT	SDWAN-Branch-15	Network connectivity issues towards controller/analytics	network-issue

Insights for sites with local issues

Set filters here...    Apply | Clear | Copy Filter    Show 10 Entries

Generation Time	Appliance	Description	Sub Category
Apr 28th 2026, 9:18:21 PM PDT	SDWAN-Branch-20	Service disruption due to configuration change, push, or rollback	config-change
Apr 28th 2026, 9:18:19 PM PDT	SDWAN-Branch-19	System crash due to kernel panic causing complete service outage	kernel-crash
Apr 28th 2026, 9:18:16 PM PDT	SDWAN-Branch-18	System impacted due to disk failure, disk full, or I/O errors	disk-issue
Apr 28th 2026, 9:18:14 PM PDT	SDWAN-Branch-17	System impacted due to disk failure, disk full, or I/O errors	disk-issue

# Observability driven insights: *Link Issues*

## Prolonged LTE Link Usage

- Costly, constrained, and unreliable for sustained traffic, requiring operator intervention

## Poor LTE Signal Strength

- Degrades throughput, increases latency, and causes packet loss — directly impacting branch application performance

SITES WITH LINK ISSUES: 14

**SITES WITH LTE ISSUES: 3**

SITES WITH HIGH WAN UTILIZATION: 11

SITES WITH HIGH WAN INTERFACE FLAPS: 0

SITES WITH ONE OPERATIONAL WAN LINK: 5

SITES WITH WAN LINK LATENCY SPIKES: 1

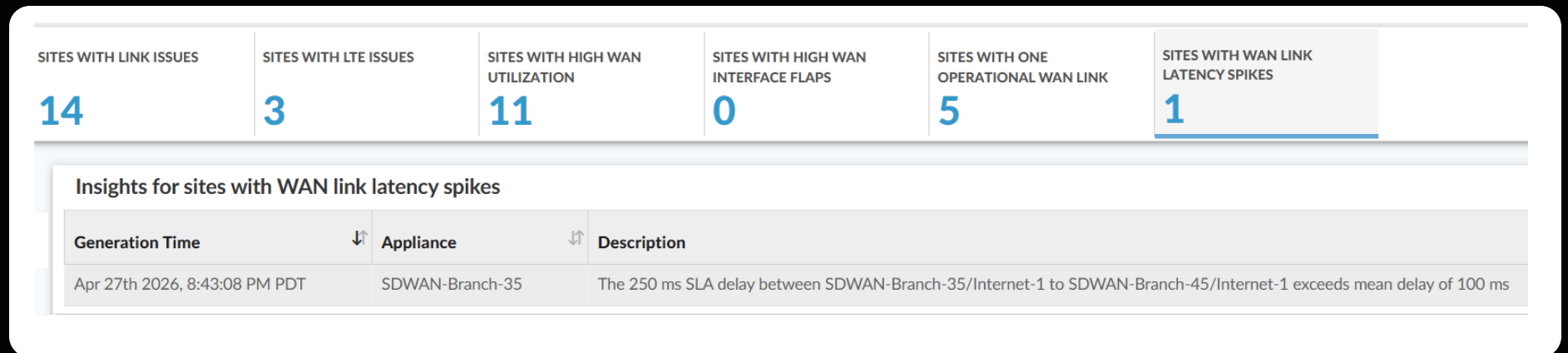
**Insights for sites with LTE issues**

Set filters here... Apply | Clear | Copy Filter

Generation Time	Appliance	Description
Apr 24th 2026, 6:50:00 PM PDT	SDWAN-Branch-61	LTE signal for SDWAN-Branch-61 on access circuit vni-0/100.0 fell to 25 dBm, below 40 dBm, indicating weak connectivity
Apr 24th 2026, 6:50:00 PM PDT	SDWAN-Branch-7	LTE signal for SDWAN-Branch-7 on access circuit vni-0/100.0 fell to 25 dBm, below 40 dBm, indicating weak connectivity
Apr 24th 2026, 6:50:00 PM PDT	SDWAN-Branch-91	LTE signal for SDWAN-Branch-91 on access circuit vni-0/100.0 fell to 25 dBm, below 40 dBm, indicating weak connectivity

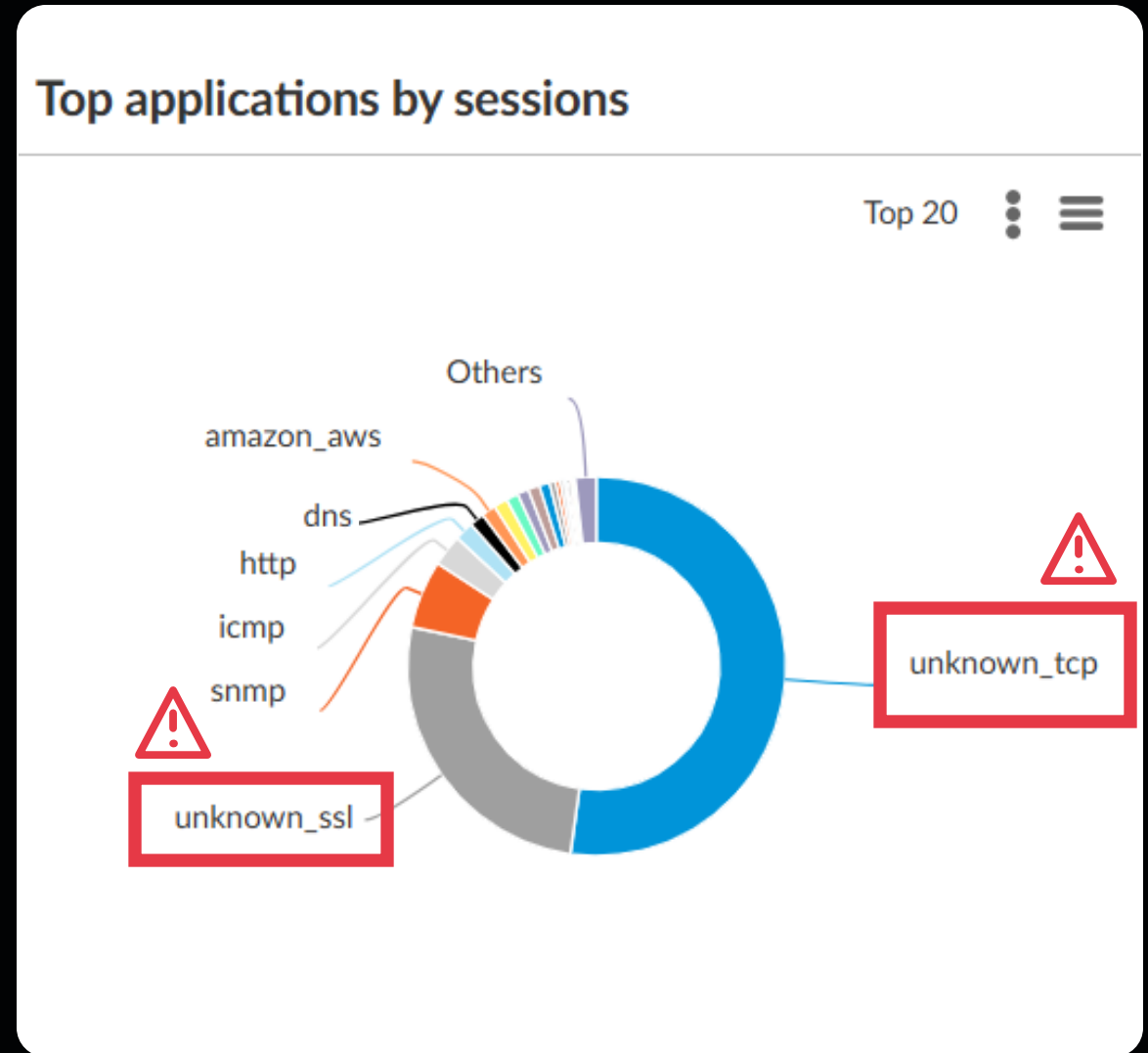
# Observability driven insights: *Link Issues*

- Single WAN Link Branches
  - Indicates a single point of failure requiring immediate operator action to prevent mission critical service disruption
- Latency Spikes on SD-WAN Path
  - Indicates traffic flowing on non-optimal paths, degrading application performance
- Excessive WAN Link Flaps
  - Points to potential misconfiguration or ISP instability requiring investigation
- WAN Utilization Spikes
  - Signals the need to upgrade bandwidth to avoid congestion and maintain application performance



# Observability driven insights: *Unknown Traffic Anomalies*

- Why is there a high number of application sessions unidentified?
  - Eg: Unknown TCP, UDP, SSL traffic
  - Is it because of:
    - Unidirectional flows
    - Short flows
    - Missing signatures
- Identifying and categorizing unknown application traffic helps admins apply informed traffic management and security policies



# Observability driven insights: *Unknown Traffic Anomalies*

- Provides top destination IP and port of unknown traffic for admins to add signatures for custom apps.

UNIDIRECTION TCP FLOWS: 30.57 M

SHORT TCP FLOWS: 26.23 M

PRIVATE DESTINATION TCP FLOWS: 23.09 M

PUBLIC DESTINATION TCP FLOWS: 19.54 M

### Unknown TCP unidirection traffic destination ports

Show 10 Entries

Destination Port	Description	Count
2022	TCP: down, UDP: xinuexpansion2	128191
443	http protocol over TLS/SSL	5059
8443	PCsync HTTPS	2700
389	Lightweight Directory Access Protocol	2548
9092	Xml-lpc Server Reg	2471
22	The Secure Shell (SSH) Protocol	1221
9183	Unknown Port	916
80	World Wide Web HTTP	744
135	DCE endpoint resolution	437
9182	Unknown Port	361

Showing 1 to 10 of 27,827 entries

### Unknown TCP unidirection traffic destination IP

Show 10 Entries

Destination Address	Hostname	Count
2.59.151.134	2.59.151.134	19372
156.234.156.74	156.234.156.74	8261
10.192.63.17	10.192.63.17	3307
10.0.0.13	10.0.0.13	2509
192.168.95.2	192.168.95.2	2473
34.96.126.106	106.126.96.34.bc.googleusercontent.com	2275
10.70.211.68	10.70.211.68	1644
10.10.10.10	fortigate.versa-networks.com	1629
10.40.19.250	10.40.19.250	1602
10.1.1.6	10.1.1.6	1484

Showing 1 to 10 of 3,263 entries

# Observability driven insights: *Logging Traffic Anomalies*

Did logging rates increase significantly - and why?

- **Logging rate baseline** — Establish per-device logging volume baselines to accurately size analytics and monitoring infrastructure.
- **Logging rate threshold alerts** — Trigger alarms when device logging exceeds defined thresholds to prevent system overload and ensure operational continuity.
- **Logging rate root cause analysis** — Determine whether logging spikes are driven by a traffic surge, configuration change, or topology change to enable targeted remediation

Heavy logging activity alarms			☰
Generation Time	Appliance	Description	↕
May 4th 2026, 10:15:57 PM PDT	Corp-Inline-Controller-1	Appliance log volume on 2026-05-04 (17,936 logs) is 101.8 % above the baseline for this day of the week (mean: 8,890, typical range: 6,991 - 10,789).	
May 3rd 2026, 10:15:50 PM PDT	Corp-Inline-Controller-1	Appliance log volume on 2026-05-03 (17,857 logs) is 109.3 % above the baseline for this day of the week (mean: 8,530, typical range: 6,727 - 10,333).	
Apr 27th 2026, 10:15:51 PM PDT	HE-DC-Standby-Device	Appliance log volume on 2026-04-27 (15,022 logs) is 58.0 % above the baseline for this day of the week (mean: 35,748, typical range: 29,247 - 42,249).	
Apr 27th 2026, 10:15:51 PM PDT	Chennai-Office-Preferred-Active	Appliance log volume on 2026-04-27 (948,869 logs) is 99.2 % above the baseline for this day of the week (mean: 476,301, typical range: 327,433 - 625,170).	
Apr 26th 2026, 10:15:20 PM PDT	HE-DC-Standby-Device	Appliance log volume on 2026-04-26 (14,995 logs) is 57.6 % above the baseline for this day of the week (mean: 35,394, typical range: 29,388 - 41,401).	

# Observability driven insights: *Other Traffic Anomalies*

- Fat flow: Traffic sessions utilizing high bandwidth
- Large uploads: Traffic sessions with large #of bytes transferred
- Risky countries: Traffic sessions originating from risky countries

**LARGE UPLOADS**  
13

**FAT FLOWS**  
1

**RISKY COUNTRIES**  
2

### Anomalies

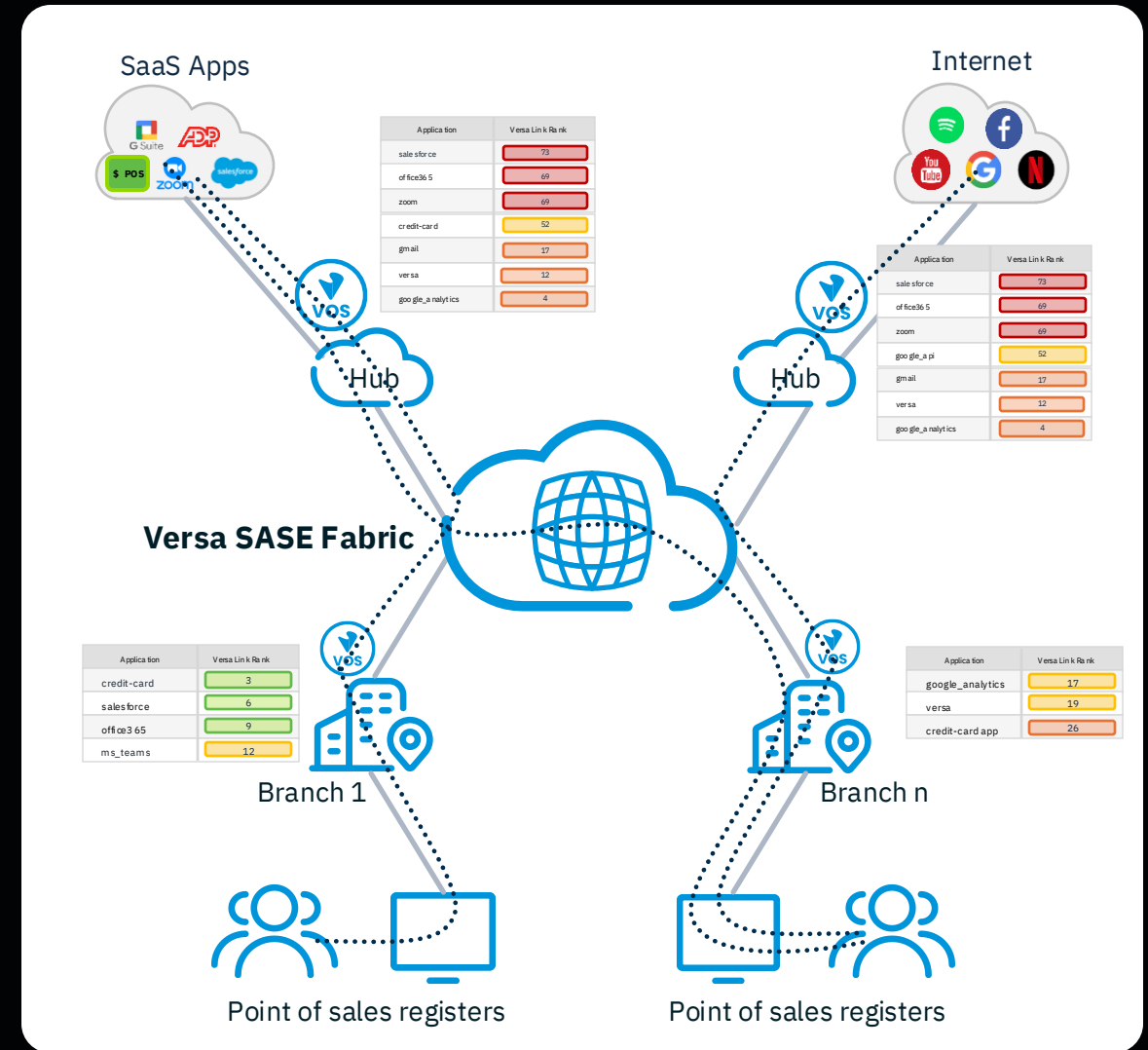
Show Domain Names

Set filters here... [Apply](#) | [Clear](#) | [Copy Filter](#) Show 10 Entries

↕ User	↕ Source Address	↕ Destination Address	↕ Destination Port	↕ RX Bytes	↕ TX Bytes	↕ Session Duration	↕ Event Type	↕ Session Close
jyoona@versa-networks.com	172.30.60.159	10.0.252.51	22	27.14 M	1.47 G	12m 49s	end	Normal
Keerthi Kumar Nalla	172.30.61.254	10.0.36.232	22	21.68 M	1.32 G	37m 47s	end	Normal
Prashant B	172.30.61.105	10.42.144.216	22	19.43 M	1.45 G	1m 44s	end	Normal

# Observability driven insights: *User Application Experience Troubleshooting*

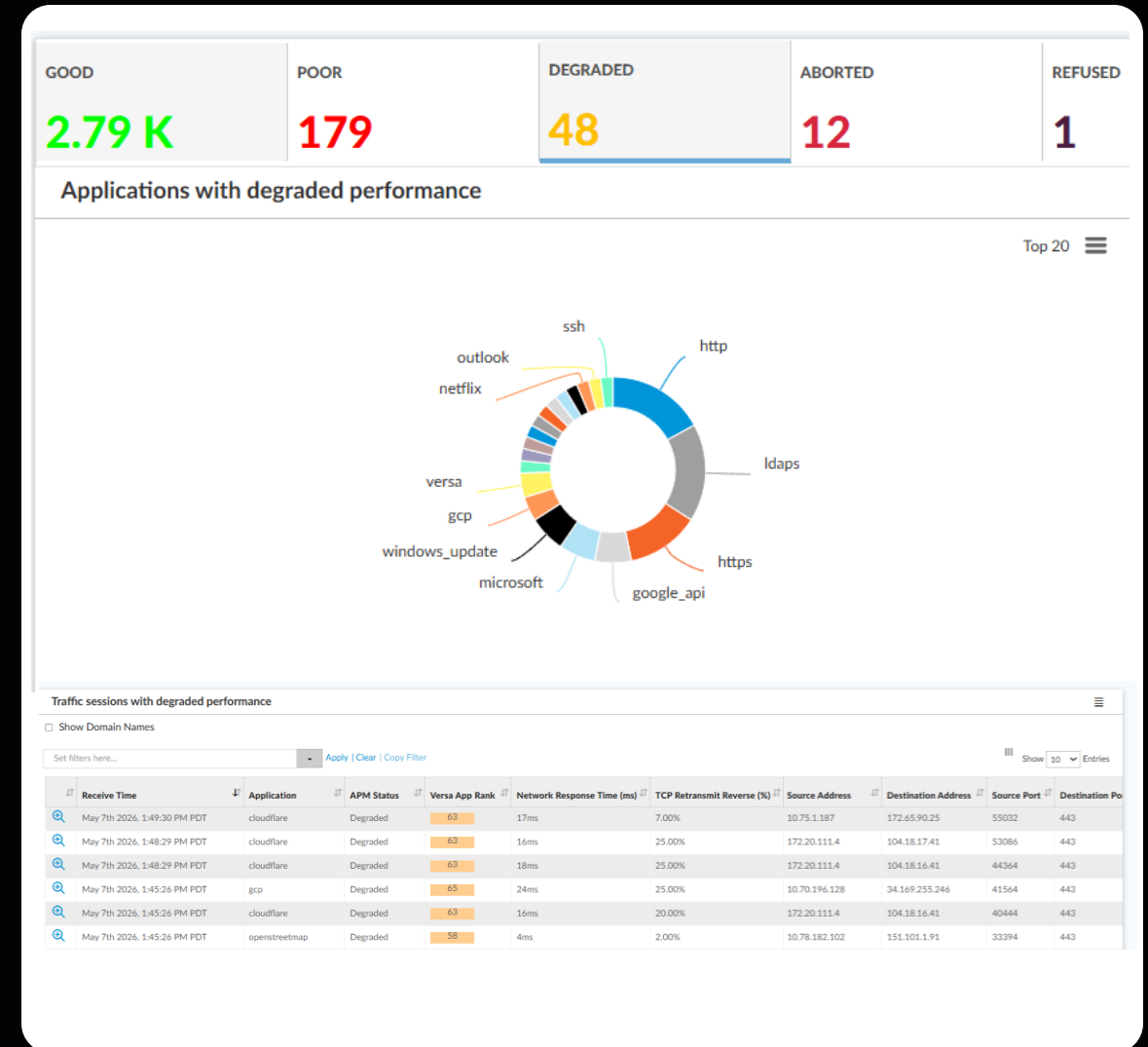
- What is root cause of poor application experience?
  - Is issue local to the user or branch or it is network wide issue?
  - Is issue seen across various branches of a specific region or ISP?
  - Is the issue due to a specific application server?
  - Is traffic taking optimal path to the application server?



Case study of a large retail store with application performance issues

# Observability driven insights: *User Application Experience Troubleshooting*

- Active and passive monitoring techniques such as end-to-end DEM and TCP APM aggregated metrics provides probable root cause.
- A new enhancement to include APM metrics inside traffic monitoring flow log helps drilldown to actual flows with issues.
  - Helps derive insights at various levels:
    - Tenant, user, network, server
  - Application flows having bad/degraded performance
  - Application flows having abnormal termination of connections.
  - Voice / Video application flows having poor Mean Opinion Score



# Observability Components

# Versa components to support observability at scale

## Real-Time Streaming



- Streaming of all events & logs with full context
- Secure & reliable data transfer

## Telemetry Cache



- Contextualizes and correlates raw data
- Delivers actionable insights on demand

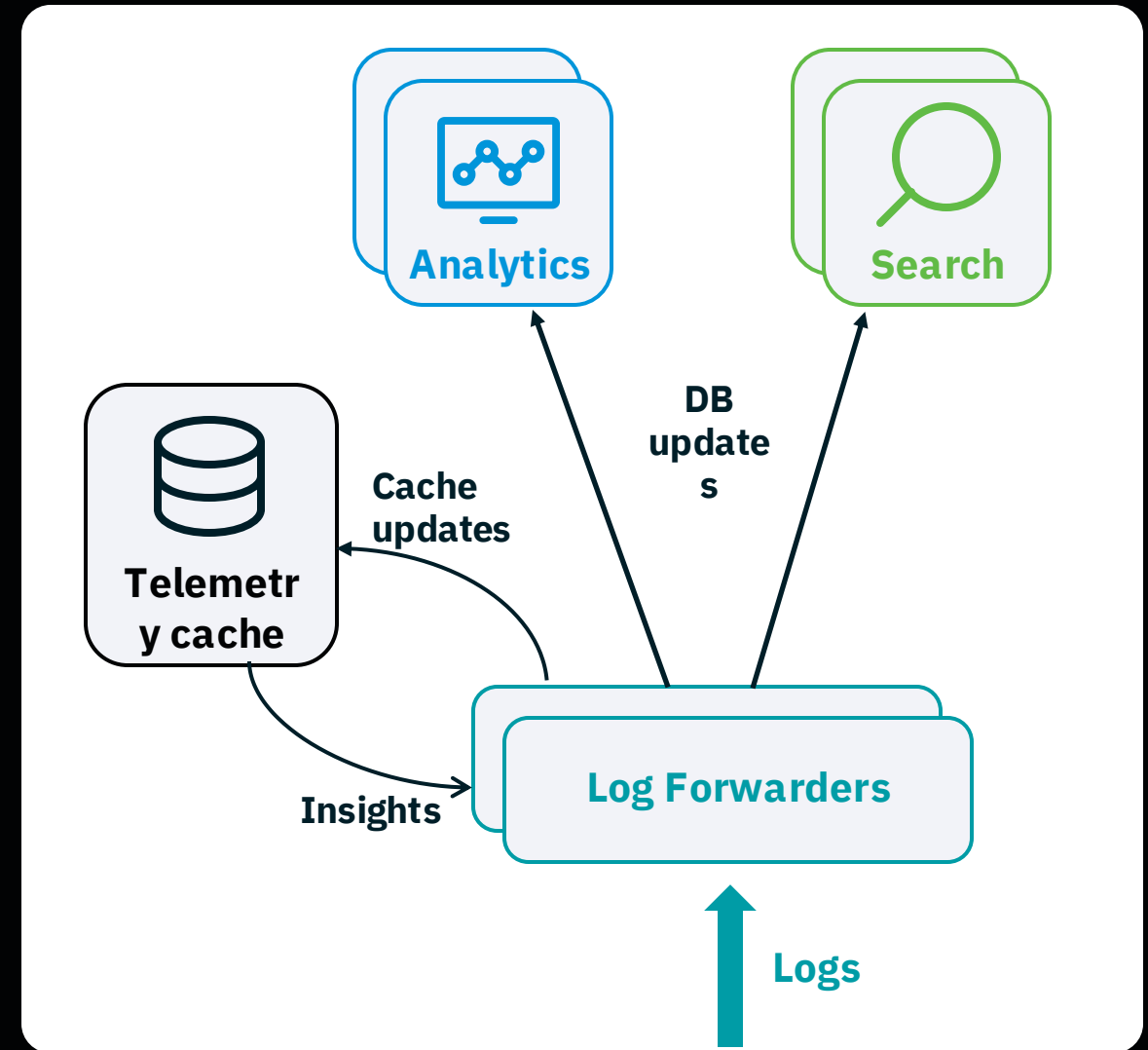
## Advanced Logging Service



- Unified data platform for centralized access
- Real-time & historical insights
- Long term analytics reporting using data lakehouse integration

# Versa Telemetry Cache (VTC)

- Contextualizing and correlating the raw data to get actionable insights.
- Implemented using distributed Redis Cache on one or more of the analytics nodes.
- Related data to derive insights for branch, link, paths etc. are maintained in the cache and evaluated periodically.
- Welford algorithm used for baseline computation optimally.



# Versa Telemetry Cache (VTC)

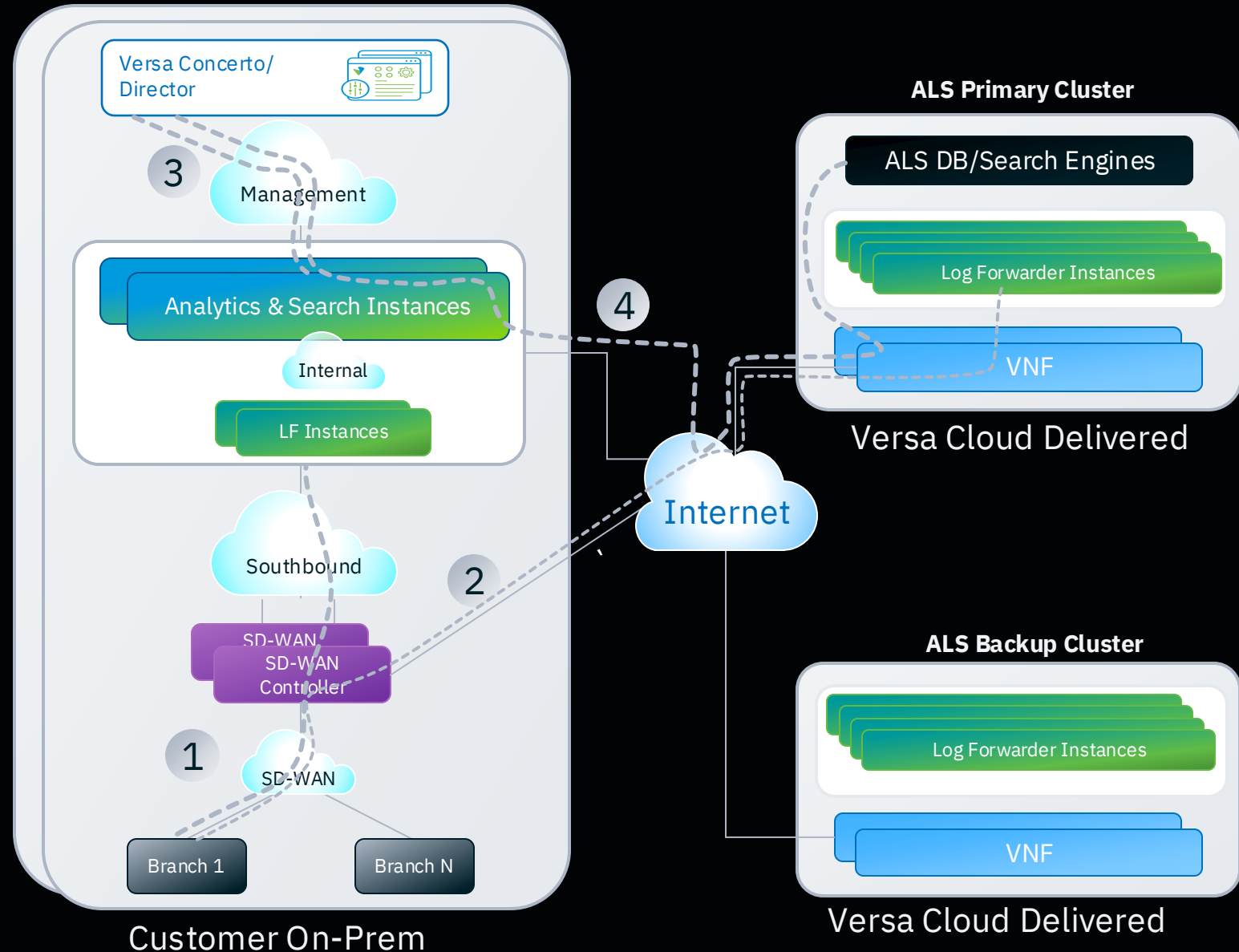
- Insights and alarms generated can be seen in analytics portal.
- Alarms can also be streamed to other monitoring and ticketing systems.

The screenshot displays the 'Alarms' section of the Versa Telemetry Cache (VTC) analytics portal. The breadcrumb navigation shows 'Alarm > Insights >'. The current view is 'Insights', with other tabs for 'Logs', 'Charts', and 'Summary'. The filters are set to 'Corp-Inline-Customer-1', 'all', and 'Last day'. The table shows several major alarms related to log volume and SLA delays.

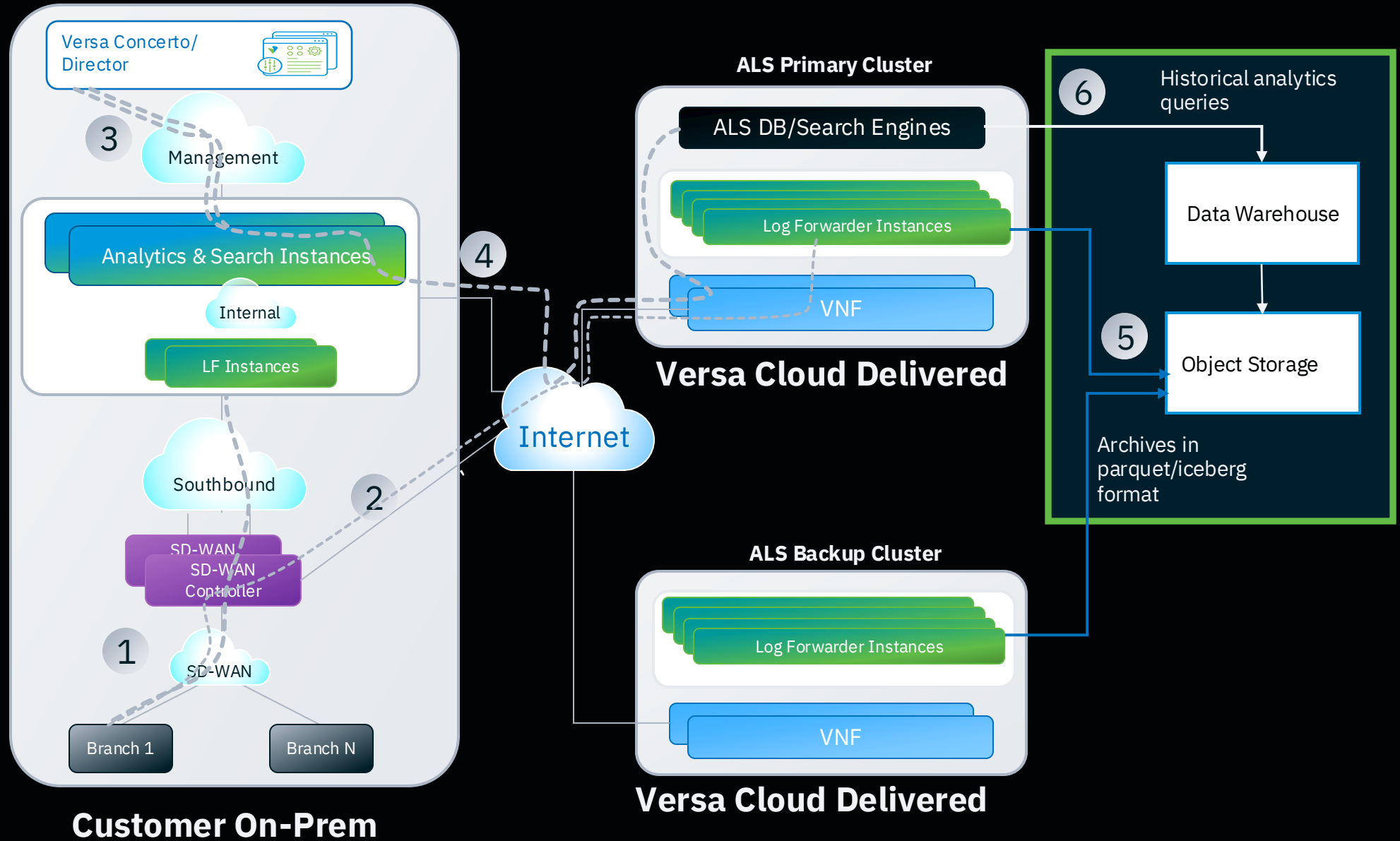
Receive Time	Severity	Appliance	Type	Description	Class	Key
Apr 26th 2026, 10:15:20 PM PDT	major	Chennai-Office-Preferred-Active	appliance-logs-insights	Appliance log volume on 2026-04-26 (677,854 logs) is 155.4 % above the baseline for this day of the week (mean: 265,430, typical range: 133,938 - 396,922).	new	search1
Apr 26th 2026, 10:15:20 PM PDT	major	HE-DC-Standby-Device	appliance-logs-insights	Appliance log volume on 2026-04-26 (14,995 logs) is 57.6 % above the baseline for this day of the week (mean: 35,394, typical range: 29,388 - 41,401).	new	search1
Apr 26th 2026, 10:10:19 PM PDT	major	Colovore-DC-Branch-1	link-insights	VOS had only one operational link for majority of the time.	new	search1
Apr 26th 2026, 10:10:19 PM PDT	major	HE-DC-Branch-1	link-insights	VOS had only one operational link for majority of the time.	new	search1
Apr 27th 2026, 7:54:24 AM PDT	major	Colovore-DC-Branch-1	sdwan-b2b-slam-delay-insights	The 8 ms SLA delay between Colovore-DC-Branch-1/Internet-1 to HE-DC-Branch-1/Internet-1 exceeds mean delay of 4.14 ms	new	Colovore-DC-Branch-1 Internet-1 HE-DC
Apr 27th 2026, 12:01:52 AM PDT	major	Bangalore-ECT-DC-Standby	sdwan-b2b-slam-delay-insights	The 231 ms SLA delay between Bangalore-ECT-DC-Standby/Internet-1 to Corp-Inline-Controller-1/Internet-1 exceeds mean delay of 224.93 ms	new	Bangalore-ECT-DC-Standby Internet-1 Co
Apr 27th 2026, 7:04:15 AM PDT	major	Chennai-Office-Preferred-Active	sdwan-b2b-slam-delay-insights	The 55 ms SLA delay between Chennai-Office-Preferred-Active/Internet-2 to Bengaluru-Office-Standby/Internet-2 exceeds mean delay of 17.54 ms	new	Chennai-Office-Preferred-Active Internet

# Versa ALS

- Versa managed, cloud hosted **Advanced Logging Service (ALS)** provides scalable solution for Observability
  - Unified data lake provides ability to scale on demand
  - Single pane of view using customer's on-prem or cloud portal
  - Reduces TCO and operational complexity by maintaining data in a unified environment



# Versa ALS Integration with Data Lakehouse Solutions



# ALS Integration with Data Lakehouse

- Cost-Efficient Archival Storage
  - Long-term retention of observability data in low-cost, scalable storage
- Columnar Data Pipeline
  - Transforms archived data into columnar format for efficient storage and faster SQL-based analytics
- On-Demand Historical Analytics
  - Query historical observability data to surface trends and insights on demand
- Native Data Lake Streaming
  - Stream archived columnar data seamlessly to third-party data lakes and platforms

# Conclusion

- Many issues facing observability solutions
  - Data explosion
  - Lack of connected insights
  - No single pane of view
- Versa's observability platform is designed to handle data at scale
  - Unified view for all services
  - Context aware insights and alerts using the telemetry cache
  - Data lakehouse to generate insights using historical data

# Why Does Observability Matter?

Generates actionable insights  
by enriching data

Reduces the mean time  
to detect and the mean time  
to recovery

Delivers business outcomes  
by improving productivity &  
reducing cost

# Demo

VERSATILITY

Thank you!