Characteristics	Qradar	Splunk	Azure Sentinel	LogRhythm	ExaBeam	Arcsight	FortiSIEM	CDC ON	Description and CDC-On Approach
Features									
All inclusive License in one package	NA	NA	NA	NA	NA	NA	NA	Yes	
Lowest per EPS price	NA	NA	NA	NA	NA	NA	NA	Yes	
Make in India Compliance	NA	NA	NA	NA	NA	NA	NA	Yes	
Low footprint and on-demand scaling with containerization support	NA	NA	NA	NA	NA	NA	NA	Yes	
Bespoke customization as per client requirements	NA	NA	NA	NA	NA	NA	NA	Yes	
Code level inspection and validation of product suite	NA	NA	NA	NA	NA	NA	NA	Yes	
Scalable Architecture and Deployment Flexibility	Complex	Complex	Complex	Complex	Complex	Complex	Complex	Simple	CDC-ON features a streamlined deployment model suited for both multi-location enterprises and small to mid-sized businesses. Unlike other players in the list containerized architecture enables seamless horizontal and vertical scaling to match your evolving needs.
Real-Time Event Data Collection	Advanced	Advanced	Limited	Advanced	Advanced	Advanced	Advanced	Advanced	CDC-ON includes native agents for Windows, Linux, and Mac, along with high-performance collectors built to efficiently manage and process large volumes of data streams. All the low price tier providers(made in India), and most of top tier solution uses third party data collection mechanism causing security risks.
Event Normalization and Taxonomy	Advanced	Advanced	Advanced	Limited	Advanced	Advanced	Limited	Advanced	CDC-ON provides built-in data modelling(UDM) capabilities to extract, parse, and categorize various log types, ensuring structured and efficient data handling.
Log Management and Reporting	Basic	Advanced	Limited	Advanced	Limited	Limited	Limited	Advanced	CDC-ON includes built-in data management mechanisms optimized for both clustered and single-server deployments. Its real-time alerting system ensures rapid detection(Zero time-to-detect) and remediation of threats with minimal SLAs. Unlike other vendors CDC-On support on-the-fly log enrichment and threat intelligence correlation for zero day threat detection.
User Monitoring	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced	Basic	Advanced	CDC-ON's analysis engine is unified engine(analytic, correlation, historic analysis, user entity behaviour analytics) unlike other vendors. The engine continuously monitors and scores user, application, and entity behaviour to detect anomalies and
Data and Application Monitoring	Advanced	Advanced	Advanced	Advanced	Limited	Limited	Limited	Advanced	

Advanced Analytics	Limited	Advanced	Limited	Advanced	Advanced	Basic	Basic	Advanced	potential threats in real time.
Deployment and Support Simplicity	Moderate	Complex	Moderate	Complex	Simple	Complex	Moderate	Simple	CDC-ON enables hassle-free deployment with minimal setup and versatile integration options for a quick start. Continuous support, comprehensive documentation, and expert guidance ensure smooth and efficient SOC operations.
Customizable Reports	Basic	Advanced	Advanced	Advanced	Basic	Basic	Basic	Advanced	CDC-ON provides a wide range of real-time visualizations and charts, enabling users to build dynamic reports and dashboards directly from active data streams. Other vendors provide pre-defined reports and dashboard with minimal customisation option for users.
Customizable Dashboards	Basic	Advanced	Limited	Basic	Limited	Basic	Basic	Advanced	
Correlation Rules	Limited	Advanced	Limited	Advanced	Advanced	Limited	Advanced	Advanced	CDC-ON comes preloaded with a comprehensive set of correlation rules for multi-source data, while also allowing users to define custom rules tailored to their specific needs. Other vendors may not ship the correlation rule with the platform license, or require separate subscription(Limited)
Real Time Application of correlation rules	Advanced	Limited	Advanced	Advanced	Basic	Advanced	Advanced	Advanced	
Backup system configuration	Limited	Limited	Advanced	Advanced	Basic	Advanced	Advanced	Advanced	Automated backups ensure your CDC-ON system configuration is always protected and recoverable. Restore settings effortlessly to minimize downtime and maintain continuity. Due to containerised deployment unlike other vendors on failure of hardware as well the service restoration time will be minimal
Event aggregration by type	Basic	Advanced	Advanced	Advanced	Advanced	Advanced	Basic	Advanced	CDC-ON intelligently aggregates events by type, reducing noise and enhancing clarity. This enables faster analysis and more efficient threat detection across your environment. CDC-On unlike other vendor do support event aggregations post indexing, which helps in historical analysis and zero day detection
Machine learning	Limited	Limited	Limited	Limited	Advanced	Advanced	Basic	Moderate	CDC-ON leverages machine learning to detect anomalies, adapt to evolving threats, and reduce false positives. It continuously learns from your environment to enhance threat detection accuracy over time. CDC-On AI capabilities are increasing with new detection models, technique getting added on the go
Detailed Investigations	Limited	Advanced	Basic	Limited	Limited	Basic	Basic	Advanced	CDC-ON provides comprehensive investigation tools with full event context, timelines, and correlation. Analysts can trace incidents end-to-end for faster, more informed response.

Incident Management and Remediation	Advanced	Advanced	Average	Advanced	Advanced	Basic	Average	Advanced	CDC-ON streamlines incident management with automated workflows and real-time collaboration tools. Built-in remediation actions help contain and resolve threats swiftly and effectively. Other vendors have separate toolset requirement for response actions
Support for Cloud services	Advanced	Advanced	Advanced	Average	Advanced	Advanced	Advanced	Advanced	CDC-ON offers native support for major cloud platforms, ensuring visibility and protection across hybrid and multi-cloud environments. Easily monitor, detect, and respond to threats in your cloud infrastructure.
Behaviour based anomaly detection	Advanced	Advanced	Advanced	Advanced	Average	Advanced	Basic	Moderate	CDC-ON uses behaviour-based anomaly detection to identify deviations from normal activity, uncovering hidden threats and zero-day attacks. It adapts to your environment for smarter, context-aware security.
Automated Response	Advanced	Advanced	Average	Advanced	Advanced	Basic	Basic	Advanced	CDC-ON enables automated response actions to contain threats in real time, reducing response time and limiting impact. Customizable playbooks ensure swift, consistent handling of security events.
Real time alerts and notifications	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced	Basic	Advanced	CDC-ON delivers real-time alerts and notifications, keeping your team informed of critical threats as they occur. Stay ahead with instant visibility and actionable insights.
Advanced threat detection	Limited	Advanced	Limited	Limited	Limited	Basic	Basic	Advanced	CDC-ON combines signature-based, behavioural, and AI-driven analytics for advanced threat detection. It uncovers sophisticated attacks across your network, endpoints, and cloud environments.
Insider threat identification	Limited	Limited	Limited	Limited	Limited	Limited	Limited	Advanced	CDC-ON identifies insider threats by analysing user behaviour, access patterns, and anomalies. It detects risky activities early to prevent data breaches from within your organization.
Infrastructure									
Basic Approach	Moderate	Moderate	Moderate	Moderate	Simple	Complex	Moderate	Simple	CDC-ON follows a modular, scalable architecture designed for high availability and performance. Its flexible deployment options support diverse infrastructures, from on-prem to cloud-native environments.
Full Active - Active System	Advanced	Advanced	Limited	Advanced	Limited	Basic	Limited	Advanced	CDC-ON supports a full active-active architecture, ensuring continuous availability and load balancing across all components. This design eliminates single points of failure and maximizes system resilience.
Active Collector Backup	Advanced	Advanced	Limited	Advanced	Basic	Limited	Limited	Advanced	CDC-ON ensures data continuity with active collector backups that automatically take over in case of failure. This guarantees uninterrupted log collection and event flow across your infrastructure.

Distributed Service Backup	Limited	Advanced	Limited	Advanced	Basic	Average	Basic	Advanced	CDC-ON features distributed service backups that maintain high availability across all critical components. In the event of a service failure, backup instances seamlessly take over to ensure continuous operation.
Distributed Services Load Balancing	Limited	Advanced	Limited	Advanced	Limited	Average	Basic	Advanced	CDC-ON leverages distributed services with built-in load balancing to optimize performance and scalability. Traffic is intelligently routed to ensure efficient resource utilization and zero downtime.
Search Speed (Multi user SOC Deployment and screens)	Average	Advanced	Basic	Average	Advanced	Basic	Basic	Advanced	CDC-ON delivers lightning-fast search performance, even in multi-user SOC environments with multiple active screens. Its optimized query engine ensures real-time access to critical data without lag or delays.
Log Retention and Storage	Limited	Advanced	Advanced	Limited	Advanced	Limited	Limited	Advanced	CDC-ON offers flexible log retention and storage options, supporting compliance and long-term analysis needs. Scalable storage architecture ensures efficient handling of high-volume data without performance compromise.
Offline Backup	Advanced	Advanced	Limited	Advanced	Advanced	Limited	Limited	Advanced	CDC-ON supports secure offline storage for logs to safeguard critical data against network failures or cyber incidents. Easily restore configurations and logs to maintain operational integrity anytime.
Real-Time Event Data Collection									
Indexing Capacity for Real Time Range	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced	CDC-ON features high-performance indexing optimized for real-time event ranges, enabling instant access to fresh data. It ensures low-latency search and analysis across massive event volumes.
Indexing Capacity for Near Time Range	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced	CDC-ON efficiently indexes near-time data, balancing speed and storage optimization. It enables fast retrieval and correlation for events occurring minutes to hours prior, supporting deep, responsive analysis.
Any Type Data Collection	Advanced	Advanced	Limited	Limited	Limited	Advanced	Limited	Advanced	CDC-ON supports collection of any type of data—structured, unstructured, logs, packets, and telemetry—from diverse sources. Its flexible connectors ensure seamless ingestion across all environments.
Data Logging for Cloud Infrasructure	Advanced	Advanced	Limited	Limited	Advanced	Advanced	Limited	Advanced	CDC-ON provides robust data logging for cloud infrastructure, capturing events from platforms like AWS, Azure, and GCP. It ensures complete visibility and compliance across your cloud environments.

Correlation, Data, Log, Flow views / Same Screen	Limited	Advanced	Limited	Limited	Advanced	Limited	Limited	Advanced	CDC-ON unifies correlation, raw data, logs, and flow views on a single screen for streamlined analysis. Analysts gain full context at a glance, accelerating threat detection and response. Other vendors require multiple modules to be added or multiple product to be setup as standalone systems.
Drill Down Search (Powered with Analytics)	Limited	Advanced	Limited	Limited	Limited	Limited	Limited	Advanced	CDC-ON offers drill-down search powered by advanced analytics, enabling users to pivot through data layers effortlessly. Investigate events in depth with contextual insights and intelligent filtering.
Search Result Analysis	Advanced	Limited	Advanced	Advanced	Average	Basic	Limited	Advanced	CDC-ON enhances search result analysis with interactive visuals, pattern recognition, and contextual enrichment. Quickly identify anomalies, trends, and root causes directly from your query results.
Normalized Data Collection	Advanced	Advanced	Limited	Limited	Advanced	Limited	Limited	Advanced	CDC-ON performs normalized data collection across diverse sources, ensuring consistency and compatibility for analytics. It simplifies correlation, search, and reporting across your entire security stack.
Unnormalized Data Collection	Limited	Advanced	Basic	Advanced	Advanced	Limited	Limited	Advanced	CDC-ON also supports unnormalized data collection, preserving raw logs for full fidelity and compliance needs. This ensures complete visibility and flexibility in forensic investigations and audits. Eg: Network Packets, File Contents
Monitoring/Analytics									
Extensible Analytics	Limited	Advanced	Limited	Limited	Advanced	Limited	Limited	Advanced	CDC-ON features extensible analytics capabilities, allowing users to build custom queries, dashboards, and detection rules. Adapt and scale analytics to match evolving threats and organizational needs. Unlike other vendors CDC-On built as analytic and response tool than an alerting solution.
Use of Threat Intelligence	Advanced	Advanced	Advanced	Limited	Advanced	Advanced	Basic	Advanced	CDC-ON integrates threat intelligence feeds to enrich event data with real-world context. It enhances detection accuracy and speeds up response by correlating threats with known indicators. CDC-On include inbuilt Threat Intelligence Module/Platform (TIP) to collect and correlate intelligence from various sources.
Threat Intelligence Sources	Advanced	Advanced	Average	Limited	Limited	Advanced	Limited	Advanced	CDC-ON supports multiple threat intelligence sources, including commercial, open-source, and custom feeds. This multi-source approach ensures comprehensive coverage of emerging threats and indicators of compromise. CDC-IN CTI system unlike other vendors do support non-standardised feeds as well(like GitHub, web sites, email messages) this specifically help to process intelligence provided by public and source like governmental agencies.

Monirtoring/Auditing	Advanced	Advanced	Advanced	Limited	Limited	Basic	Advanced	Advanced	CDC-ON provides continuous monitoring and auditing capabilities, ensuring visibility into system activities, user actions, and policy changes. It supports compliance and strengthens security posture with detailed audit trails.
Automation	Advanced	Advanced	Limited	Limited	Advanced	Limited	Basic	Advanced	CDC-ON delivers powerful automation across detection, investigation, and response workflows. Predefined and custom playbooks streamline operations, reduce manual effort, and accelerate threat mitigation.
User Interaction (Visibility and Context)									
Detection and Logging	Limited	Advanced	Limited	Limited	Advanced	Limited	Limited	Advanced	CDC-ON provides real-time detection and comprehensive logging with rich context for every event. Users gain immediate visibility into threats with detailed, actionable insights for faster response.
Response Logging	Limited	Advanced	Limited	Limited	Advanced	Limited	Basic	Advanced	CDC-ON captures detailed response logs for every action taken, whether manual or automated. This ensures full traceability, audit readiness, and accountability throughout the incident lifecycle.
Visualization	Limited	Advanced	Basic	Limited	Basic	Basic	Limited	Advanced	CDC-ON offers dynamic visualizations that transform complex data into intuitive dashboards, charts, and timelines. Users can quickly grasp patterns, anomalies, and trends for smarter decision-making.
Integration of Visibility and Context Functionlaity	Limited	Advanced	Limited	Limited	Limited	Limited	Limited	Advanced	CDC-ON seamlessly integrates visibility and context functionality, correlating data across sources to present a unified view. Users gain deep, actionable insights with minimal effort, enhancing investigation and response efficiency.