# CyberQuest Data Source Intelligence - Native Capabilities & Strategic Integration

## Introduction

CyberQuest is a Data Security Analytics platform delivered as an integrated physical or virtual appliance running on the Linux Debian operating system.

It is designed for broad compatibility in data collection, capable of ingesting audit events from **virtually any source or format** - including Syslog, Windows event logs, structured files (.csv, .txt, .log), database tables, and network flow metadata such as NetFlow and sFlow. The platform includes built-in connectors for widely used systems like Microsoft Windows, Unix-like operating systems, network devices, databases, and allows the **creation** of dedicated connectors for specialised **or proprietary data sources**.

Data streams - whether all incoming events or selected subsets - can be directed into the integrated correlation engine for advanced analysis. Users can build tailored dashboards and reports to visualize and monitor security posture.

Access control supports Active Directory integration, with the option to add **two-factor authentication** for enhanced security. The proprietary **Data Transformation Services** (DTS) module enables further parsing, enrichment, and transformation of collected event data. Real-time alerts can be defined and customized to match organizational requirements, ensuring timely detection and response to critical incidents.

## Tag Based Parsing

CyberQuest's internal architecture follows a modular, queue-based data flow designed for flexibility and performance. Data can be ingested through the CyberQuest Collecting Agent - supporting WMI, ODBC, and file-level collection - or via direct streams such as Syslog and NetFlow. Collection can also be performed by dedicated Data Server instances or Windows Agents, all communicating through RabbitMQ for resilient, ordered message delivery.

The **Data Server** acts as a pre-processing layer, **tagging events before forwarding** them to the **Data Acquisition Service (DAS)**. DAS applies acquisition rules and API parsers to process events, then routes them to the online ElasticSearch database for fast querying, the Data Storage service for long-term retention, and the **Data Correlation Service (DCS)** for real-time detection.

The **Data Storage Service (DSS)** encrypts and compresses all archived events, supporting very large repositories with immediate retrieval capabilities - a critical feature for compliance and forensic readiness.

**Automatic parsing** is triggered when events arrive with valid tags assigned by the Data Server. Untagged or unknown events require adding the corresponding data source in the web application. The **Tag Alias** function enables remapping an initial tag to a predefined final tag, allowing reuse of existing parsers without rewriting parsing logic. Final Tag is selected from a predefined parser list in the CQ interface.

**Enhanced Parsing** adds contextual forensic enrichment to events, particularly Windows logs, by populating dedicated fields:

- **Who**: Identifies the user or account responsible.
- **What**: Classifies the event type.
- **Where**: Specifies the originating system.
- **Why**: Explains the trigger for the event.

The **Data Correlation** service continuously analyses incoming events, applying correlation logic to generate meaningful alerts. Integration with **OpenVAS** further expands detection capabilities with vulnerability scanning.

# High Level CyberQuest Internal Data Flow

**[Data Sources]**
↓
Any IT/OT source → Syslog, WinEvents, CSV/TXT/LOG, DB tables, NetFlow, sFlow
**[Collection Layer]**
↓
Data Server → Pre-process & tag events → RabbitMQ
Windows Agent → Windows events → RabbitMQ
CQ Collecting Agent → WMI/ODBC/File/Syslog/NetFlow → RabbitMQ
**[Message Queue]**
↓
RabbitMQ → Reliable, ordered event transport
**[Processing Layer]**
↓
Data Acquisition Service (DAS) → Acquisition rules + API parsers
→ ElasticSearch (fast search/dashboards)
→ Data Storage (encrypted, compressed archives)
→ Data Correlation (real-time alerts)
**[Tag Management]**
↓
Tag Alias → Remap unknown tags → existing parsers
**[Enrichment Layer]**
↓
Enhanced Parsing (Windows Enricher) → Who / What / Where / Why
**[Storage Layer]**
↓
Data Storage Service (DSS) → Long-term, instant-access archives
**[Correlation Layer]**
↓
Data Correlation Service → multi-source event linking + alerting
**[Security Modules]**
↓
OpenVAS → Vulnerability scan integration
**[Output & Interaction Layer]**
↓
ElasticSearch → Queries, analytics, dashboards
Web App → Reports, alerts, browser viewer
Automatic Actions → Triggered by correlation rules

## Supported Data Sources

CyberQuest is an advanced **Big Data Security Analytics platform** engineered to deliver complete auditing and security visibility across enterprise environments. It consolidates and correlates data from **all layers of the infrastructure** - including existing SIEM solutions, business-critical applications, and complementary security tools such as vulnerability scanners, IDS/IPS systems, DLP platforms, and firewalls.

Supported data sources span a wide range of categories:

- **Operating Systems** - Comprehensive coverage for Windows, Unix-based, and Linux environments.
- **Networking Equipment** - Managed switches, routers, firewalls, and wireless network infrastructure.
- **Security Devices** - Intrusion detection and prevention systems, data loss prevention tools, and specialized security appliances.
- **Network Data Formats** - Native support for NetFlow and related telemetry standards.
- **Applications** - Collection from enterprise software and custom-developed business applications.
- **Cloud Platforms** - Integration with major cloud providers such as AWS, Microsoft Azure, and Google Cloud, as well as other SaaS/IaaS services.
- **On-Prem Infrastructure** - Servers, storage, and core on-premises networking assets.
- **Print Services** - Logging and monitoring of print infrastructure.
- **Databases** - Ingestion from multiple database types, both SQL and NoSQL.
- **Threat Intelligence Feeds** - Direct integration with external intelligence providers for proactive detection and correlation.

This broad native support ensures that CyberQuest can deliver a unified, real-time security picture without the need for extensive custom parsing or third-party middleware.

**Operating Systems - Data Sources**

CyberQuest offers broad and detailed operating system log collection across Windows, Unix-based, and Linux environments. Each supported source has a predefined **TagName**, enabling precise parsing, correlation, and enrichment without manual tag setup.

### Windows-based Systems

- **Core logs** - Application `(WindowsApplication)`, Security `(WindowsSecurity)`, System `(WindowsSystem)`, Setup `(WindowsSetup)`
- **Service-specific logs** - DNS Server `(WindowsDNSServer)`, Print Service Operational `(WindowsPrintService)`, Backup Service Operational `(WindowsBackupService)`
- **Virtualization (Hyper-V)** - Full coverage including Compute, Hypervisor, VMMS, VmSwitch, and Worker logs in both operational and admin contexts:
  - `HyperVComputeOperational, HyperVComputeAdmin`
  - `HyperVHypervisorOperational, HyperVHypervisorAdmin`
  - `HyperVVMMSAdmin, HyperVVMMSNetworking, HyperVVMMSOperational, HyperVVMMSStorage`
  - `HyperVVmSwitchOperational`
  - `HyperVWorkerAdmin, HyperVWorkerOperational`
- **Additional channels** - Print Service via Syslog `(WindowsPrint)`, File Audit via Syslog `(CQWindowsFileAudit)`

**Advantage:** Hyper-V event channel coverage, file audit integration, and specific print service logs are available without building custom parsers.

### Unix-based Systems

- Huawei EulerOS `(HuaweiEulerOS)`
- VMware vCenter Server Appliance `(VmWareVCSAParser)`
- Firmware update manager logs `(CQfwupdmgr)`

**Advantage:** Direct coverage for Huawei EulerOS and firmware update logs, often requiring specialized collectors elsewhere.

### Linux Systems

- **Transport protocols** - Syslog over TCP `(SyslogTCP)` and UDP `(SyslogUDP)`
- **Generic distributions** - Debian `(GenericDebian)`, CentOS `(GenericCentOS)`, generic Linux `(GenericLinux)`
- **Audit & access control logs** - `CQaudispd, CQsudo, CQsu, CQchfn, CQgroupadd, CQuseradd, CQuserdel, CQusermod, CQpasswd`
- **Scheduling & job management** - CRON `(CQCRON)`, crontab `(CQcrontab)`
- **Database audit** - MariaDB `(CQmariadb)`
- **System services** - systemd `(CQsystemd)`, systemd-timesyncd `(CQsystemd-timesyncd)`
- **Networking & containers** - dhclient `(CQdhclient)`, Docker daemon `(CQdockerd)`
- **Storage & device management** - multipathd `(CQmultipathd)`, RNG tools `(CQrngd)`
- **Maintenance & management logs** - logrotate `(CQlogrotate)`, system login manager `(CQsyswrapper)`, filesystem trim `(CQfstrim)`

**Advantage:** Predefined tags for MariaDB audit, container daemon logs, multipathd, RNG tools, and Linux service logs are included out-of-the-box.

# Aggregated OS & Networking Data Source Advantages

| Category | Source / Device | Tag Name | Technology | Native / Unique Advantage* | Market-Common Capability |
|---|---|---|---|---|---|
| ***Windows OS*** | Application | WindowsApplication | Windows OS | Core log coverage without custom parser | Standard Windows event log ingestion |
| | Security | WindowsSecurity | Windows OS | - | Common in most SIEMs |
| | System | WindowsSystem | Windows OS | - | Common in most SIEMs |
| | DNS Server | WindowsDNSServer | Windows OS | - | Common DNS Server log support |
| | Setup | WindowsSetup | Windows OS | - | Common setup log ingestion |
| | Print Service Operational | WindowsPrintService | Windows OS | Specific print event channel support | Often requires manual mapping in other SIEMs |
| | Backup Service Operational | WindowsBackupService | Windows OS | - | Common backup event ingestion |
| | Hyper-V Compute Operational/Admin | HyperVComputeOperational / HyperVComputeAdmin | Windows OS | Hyper-V full lifecycle monitoring | Basic Hyper-V logging supported by some SIEMs |
| | Hyper-V Hypervisor Operational/Admin | HyperVHypervisorOperational / HyperVHypervisorAdmin | Windows OS | - | Common in SIEMs with virtualization modules |
| | Hyper-V VMMS (Admin, Networking, Operational, Storage) | HyperVVMMSAdmin / Networking / Operational / Storage | Windows OS | - | Common VM management logging |
| | Hyper-V VmSwitch Operational | HyperVVmSwitchOperational | Windows OS | - | Common VM networking log ingestion |
| | Hyper-V Worker Operational/Admin | HyperVWorkerOperational / HyperVWorkerAdmin | Windows OS | - | Common worker process logs |
| | Windows Print Service (Syslog) | WindowsPrint | Syslog | Print logging via Syslog without translation | Rarely native in other SIEMs |
| | Microsoft Windows Security File Audit (Syslog) | CQWindowsFileAudit | Syslog | File-level auditing without extra parser | Many SIEMs require extra agent or mapping |

| | | | | | |
|---|---|---|---|---|---|
| ***Unix-based OS*** | Huawei EulerOS | HuaweiEulerOS | Syslog | Direct ingestion for niche OS distributions | Not universally supported in competitors |
| | VMware VCSA | VmWareVCSAParser | Syslog | - | Common VMware VCSA support |
| | Firmware update manager | CQfwupdmgr | Syslog | Firmware log coverage without manual mapping | Rarely included by default |
| ***Linux OS*** | Syslog TCP/UDP | SyslogTCP / SyslogUDP | Syslog | Flexible transport method support | Standard |
| | Generic Debian | GenericDebian | Syslog | - | Standard |
| | Generic CentOS | GenericCentOS | Syslog | - | Standard |
| | Generic Linux | GenericLinux | Syslog | - | Standard |
| | Audit dispatcher, sudo, su, chfn, group/user add/del/mod, passwd | CQaudispd, CQsudo, CQsu, CQchfn, CQgroupadd, CQuseradd, CQuserdel, CQusermod, CQpasswd | Syslog | Comprehensive native Linux auditing coverage | Often partial in competitors |
| | Scheduling (CRON, crontab) | CQCRON, CQcrontab | Syslog | - | Standard |
| | MariaDB audit | CQmariadb | Syslog | Native DB audit ingestion | Often requires DB-specific parser |
| | System services (systemd, timesyncd) | CQsystemd, CQsystemd-timesyncd | Syslog | - | Standard |
| | Network/container services (dhclient, Docker) | CQdhclient, CQdockerd | Syslog | Container and DHCP log support without plugin | Requires additional config in other SIEMs |
| | Storage & device management (multipathd, RNG tools) | CQmultipathd, CQrngd | Syslog | - | Common with extensions |
| | Maintenance & management (logrotate, syswrapper, fstrim) | CQlogrotate, CQsyswrapper, CQfstrim | Syslog | Lifecycle and FS optimization logs supported | Rarely default |
| ***Managed Switches*** | HP Switch | HPSwitch | Syslog | Native parser for HP enterprise switches | Vendor-specific in other SIEMs |
| | Cisco Switch | CiscoSwitch | Syslog | - | Common |
| | Unify Switch | CQswitch | Syslog | - | Common |
| ***Routers*** | Cisco Meraki | CQCiscoMeraki | Syslog | Direct cloud-managed router integration | Partial support in some SIEMs |

| | | | | | |
|---|---|---|---|---|---|
| | Keepalived VRRP Daemon | CQKeepalived_vrrp | Syslog | VRRP HA logging without custom setup | Often manual config required |
| ***Firewalls*** | Cisco ASA | CiscoASA | Syslog | Extensive vendor-native firewall coverage | Common in SIEMs with FW parsers |
| | Check Point | CheckPointFirewall | Syslog | - | Common |
| | Fortinet FortiGate | FortinetFortiGate | Syslog | - | Common |
| | Fortinet FortiWeb / WAF / FortyWeb | FortinetFortiWeb, FortiWaf, FortinetFortyWeb | Syslog | Multiple WAF product line support | Rarely native |
| | Imperva WAF | ImpervaWAF | Syslog | - | Common |
| | Juniper | Juniper | Syslog | - | Common |
| | StormShield Firewall | StormShieldFirewall | Syslog | - | Common |
| | SonicWall CEF | SonicWallCEF | Syslog | CEF-formatted support for SonicWall | Common |
| | SonicWall Firewall | SonicWallFirewall | Syslog | - | Common |
| | ForcePoint CEF / CQForcePointCEF | ForcePointCEF, CQForcePointCEF | Syslog | - | Common |
| | pfSense Firewall | PFSenseFirewall | Syslog | - | Common |
| | Palo Alto Firewall | PaloAltoFW | Syslog | - | Common |
| | Endian Firewall | EndianFirewall | Syslog | - | Common |
| ***Wi-Fi*** | NetGear Access Point | NetGearAP | Syslog | AP log ingestion without SNMP or manual parsing | Rare in other SIEMs |
| ***NetFlow*** | NetFlow (Syslog or native) | NetFLow, NetFlow | Syslog / NetFlow | Flexible NetFlow export format compatibility | Common |
| | CQ NetFlow from network devices | CQnetflow | Syslog | Pre-optimized for CQ ingestion from multiple device types | Rare in other SIEMs |

***Note:** CQ in tag means a native parser is implemented.

# CyberQuest Supported Data Sources - Applications & Databases

| Category | Source / Application | TagName | Technology | Native / Unique Advantage | Market-Common Capability |
|---|---|---|---|---|---|
| ***Cloud Apps.*** | AWS CloudTrail | AWSCloudTrail | Syslog | Built-in AWS CloudTrail parsing with CQ schema mapping. | Common in SIEMs but often requires parser tuning. |
| | Office 365 (Exchange, SharePoint, Azure AD) | Office365 | CQApi | Unified ingestion of all O365 services via a single API. | O365 supported, but typically requires separate connectors. |
| | Change Auditor for Azure AD | ChangeAuditorAzureActiveDirectory | Applications | Native Azure AD change audit parsing. | Supported via vendor apps. |
| | Cloudera (HDFS, HBASE, HIVE, HUE, NAVMS, SENTRY, SOLR, IMPALA) | cloudera_*_AUDIT | Applications | Prebuilt big data audit parsing. | Often requires manual mapping elsewhere. |
| | Cloud GravityZone | CloudGravityZone | Syslog | Native Bitdefender cloud endpoint logs. | Syslog-based ingestion common. |
| ***On-Prem Anti-malware*** | Bitdefender GravityZone | BDGravityZone | Syslog | Predefined AV log parser. | Syslog ingestion common. |
| | McAfee | McAfeeSplit | Syslog | Native McAfee parsing. | Vendor parser available. |
| | Symantec Endpoint Server | CQSymantecServer | Syslog | Built-in Symantec endpoint parsing. | Supported via vendor apps. |
| | ESET Antivirus / PROTECT Center | EsetAntivirus / EsetProtectCenter | Syslog | Ready ESET log ingestion. | Common in Syslog-based SIEMs. |
| ***On-Prem App. Servers*** | Veeam Agent | WindowsVeeamAgent | Windows OS | Native backup agent log coverage. | Supported via Windows log connectors. |
| | Microsoft IIS | WindowsIISEventLog | Windows OS | Built-in IIS event parsing. | Common via IIS parser. |
| | WSO2 | CQwso2is | Syslog | Native identity platform support. | Syslog mapping possible. |
| | IBM SAN | IBM-SAN | Syslog | SAN logs parsed natively. | Supported via generic SAN parsers. |
| | Synology FTP/NAS | SynologyFTP-NAS | Syslog | NAS integration built-in. | Common Syslog ingestion. |
| | Dovecot, Postfix, Sendmail, Amavis | CQdovecot, MailPostfix, CQsm-msp-queue, CQpostfix/* | Syslog | Full MTA coverage with granular subcomponent mapping. | Mail server logs supported but often less granular. |
| | Apache / nginx (combined, error) | ApacheDatasource, CQapache_combined, | Syslog | Native web server log parsing. | Common parser support. |

| | | | | |
|---|---|---|---|---|
| | CQnginx_combined, CQnginx-error | | | |
| Qnap | Qnap | Syslog | NAS logs parsed. | Syslog ingestion standard. |
| ElasticSearch / LogStash | GenericElasticSearch, LogStash | CQApi | ELK integration native. | Supported elsewhere via APIs. |
| CQHttpServer / Generic CQ API | CQHttpServer, GenericCQApi | CQApi | Generic API ingestion without middleware. | Supported via API modules. |
| Dekeneas | DekeneasOrangeRo | CQApi | Threat feed parsing native. | Possible with API integration. |
| Generic Files / CSV Files | GenericFile, GenericCSVFile | Applications | Structured/unstructured ingestion built-in. | Common CSV ingestion. |
| Exchange Message Tracking | ExchangeMessageTracking, MSExchnangeParser | Applications / Syslog | Native mail flow tracking. | Supported with custom parsers. |
| Subversion Mail, GitLab (Rails/Shell) | CQsvn, GitLabRails, GitLabShell | Syslog | SCM platform coverage built-in. | Syslog mapping possible. |
| Insoft Audit | InsoftAuditLog | Syslog | Native parser. | Generic ingestion possible. |
| nginx error, sftp-server | CQnginx-error, CQsftp-server | Syslog | SFTP and error logs parsed. | Common Syslog support. |
| Documenta | DocumentaA$AUDIT, DocumentaLog | Syslog | ECM logs native. | Supported with mapping. |
| DHCP server | Dhcpd | Syslog | DHCP event parsing. | Common in most SIEMs. |
| LXD container/VM logs | CQlxd.activate | Syslog | Container logs parsed natively. | Supported via Syslog. |
| VMware ESXi (full suite) | Multiple CQ tags | Syslog | Complete ESXi component coverage with predefined parsers. | Supported but often partial. |
| F5 Big-IP | F5BigIPAudit | Syslog | ADC/security logs parsed natively. | Vendor parser common. |
| Cisco Firepower | CQSFIMS, CQHMNOTIFY, CiscoFirePower | Syslog | Multiple Firepower log formats supported. | Vendor app or parser needed. |
| Unify (various processes) | Multiple CQ tags | Syslog | Edge/wireless OS logs parsed at process level. | Process-level mapping less common. |
| LDAP Daemon | CQslapd | Syslog | Directory service logs parsed. | Common Syslog mapping. |
| Canonical Livepatch | CQcanonical-livepatch | Syslog | Kernel patch logs native. | Syslog ingestion possible. |
| Python3 logs | CQpython3 | Syslog | Runtime log parsing built-in. | Supported with custom parser. |

***On-Prem Virtualisation***

| | | | | | |
|---|---|---|---|---|---|
| | VMware Alias Manager & Ticket Service | CQVGAuthService | Syslog | Native parser. | Rare but possible elsewhere. |
| ***On-Prem Security Apps.*** | FortiMail | FortiMail | Syslog | Email gateway logs native. | Supported via vendor parser. |
| | Safetica DLP | SafeticaDLP | Syslog | DLP logs parsed. | Supported via integration. |
| | Cisco ISE | CiscoISE | Syslog | NAC/AAA logs parsed natively. | Vendor parser common. |
| | DarkTrace | DarkTrace | Syslog | AI threat detection logs native. | Vendor app needed. |
| | FireEye IPS | FireEyeIPS | Syslog | IPS log ingestion built-in. | Common in enterprise SIEMs. |
| | HAProxy | HAProxy | Syslog | LB/WAF logs parsed natively. | Vendor parser common. |
| | Cisco Duo Security | CiscoDuoSecurity | Syslog | MFA logs native. | Supported elsewhere. |
| ***Data-bases*** | Oracle 11 / 12 Audit Logs | Oracle11AuditLog, Oracle12AuditLog | Databases | Native Oracle audit log parsing. | Supported but sometimes paid. |
| | MISP DB Threat Intelligence | MispDatabase | Databases | TI DB logs native. | Possible via DB integration. |
| | PostgreSQL Audit / General Logs | SimTAX, PostgreSQL, CQpostgres | Databases / Syslog | Native Postgres audit & operational log parsing. | Common with manual config. |
| | DocumentaClient DB Logs | PostgreSQL | Databases | Application DB integration native. | Common via DB connectors. |
| | Generic Oracle Database | GenericOracleDatabase | Databases | Generic Oracle DB parsing. | Widely supported. |
| | DMS Client (Flux, Audit, FluxPas, Log) | DMSClientFlux, DMSClientAudit, DMSClientFluxPas, DMSClientLog | Syslog | Document management DB logs parsed. | Supported in Syslog-based SIEMs. |
| | FogLight Audit | FogLightAudit | Applications | DB monitoring logs parsed. | Vendor parser common. |
| | MSSQL | Generic_MSSQL_Tag | Databases | Native MSSQL parsing. | Supported widely. |
| | Sas Viya Cas Audit | SasViyaCas | Databases | Analytics platform logs parsed. | Rare but possible with mapping. |

***Note:** CQ in tag means a native parser is implemented.

# CyberQuest Supported Data Sources - Threat Intelligence, Metadata & Vulnerability Scanners

| *Category* | Source | TagName | Technology | Native / Unique Advantage | Market-Common Capability |
|---|---|---|---|---|---|
| ***Threat Intelligence*** | CQTI | CQThreatIntelligence | CQApi | CQ's proprietary TI feed integrated directly into DAS/DTS correlation. | Other SIEMs can ingest TI but often via paid add-ons or marketplace apps. |
| | Nucleon TI | NucleonThreatIntelligence | CQApi | Direct API pull from Nucleon without third-party connectors. | API ingestion possible, but typically via custom connectors. |
| | Nucleon Active Threats | NucleonActiveThreats | Syslog | Real-time Syslog ingestion with no format conversion. | Syslog TI feed support is common. |
| | MISP (Malware Information Sharing Platform) | - | - | MISP integration aligns with CQ correlation engine. | MISP widely supported but often external to core SIEM flow. |
| | Dekeneas | - | CQApi | API-based Dekeneas ingestion parsed natively. | Other SIEMs can integrate via scripting. |
| ***Metadata*** | Active Directory Information | ActiveDirectoryInformation | Applications | Direct AD metadata collection without ETL tools. | AD integration common but may require licensed connectors. |
| ***Vuln. Scanners*** | Nexpose | Nexpose | Syslog | Predefined parser for Rapid7 Nexpose Syslog events. | Nexpose Syslog support is widespread but mapping may be manual. |
| | OpenVAS - Reports | openvas-reports | Syslog | Feeds vulnerability reports directly into CQ correlation. | OpenVAS parsing common but often requires config. |
| | OpenVAS - Assets | openvas-assets | Syslog | Asset inventory integrated with CQ correlation rules. | Asset log support common but outside real-time correlation in many SIEMs. |
| | Nessus - Reports | nessus-reports | CSV | CSV import mapped directly to CQ's event schema. | Nessus imports possible but often require format conversion. |

## Conclusion & Executive Summary

This document has outlined CyberQuest's extensive native capabilities in collecting, parsing, and correlating data from a wide spectrum of operating systems, network devices, applications, databases, cloud platforms, and threat intelligence feeds. The structured approach - supported by predefined tags and built-in parsers - ensures rapid onboarding of diverse log sources without extensive engineering effort or reliance on third-party connectors.

**CQ Native Capability Matrix - Executive Roll-Up**

| Category | Source / Capability | Native / Unique Advantage |
|---|---|---|
| **Windows OS** | Hyper-V full lifecycle coverage (Compute, Hypervisor, VMMS, VmSwitch, Worker) | Complete virtualization event visibility without custom parsers |
| | Microsoft Windows Security File Audit via Syslog | File-level auditing without additional agents or mapping |
| **Unix & Linux OS** | Huawei EulerOS | Direct ingestion for niche OS distributions |
| | Native MariaDB audit parsing | DB audit ingestion without DB-specific connector |
| | Container & DHCP logs (Docker, dhclient) | Ingested without plugins or manual mapping |
| **Networking** | HP Enterprise Switches | Vendor-native parser for HP enterprise switches |
| | Cisco Meraki | Direct cloud-managed router integration |
| | Keepalived VRRP | HA failover logging without custom setup |
| **Firewalls & Security** | Fortinet FortiWeb/WAF suite | Multi-product WAF coverage native to CQ |
| | SonicWall CEF | Native CEF parsing for SonicWall |
| **Cloud & SaaS** | Office 365 (Exchange, SharePoint, Azure AD) | Unified ingestion of all O365 services via single API |
| | AWS CloudTrail | Built-in parsing with CQ schema mapping |
| **Threat Intelligence** | CQ Threat Intelligence Feed | Proprietary TI directly integrated into correlation engine |
| | Nucleon TI & Active Threats | API/Syslog ingestion without third-party connectors |
| **Applications & Databases** | Cloudera Big Data Suite | Prebuilt parsing for multiple Cloudera components |
| | Full MTA coverage (Postfix, Dovecot, Sendmail, Amavis) | Granular mail server subcomponent mapping |
| | VMware ESXi full suite | Component-level parsing for all ESXi services |

Across all categories, CyberQuest demonstrates **native advantages** that directly impact operational efficiency:

- **Broad Native Coverage** - Predefined parsers for common and niche data sources, including Huawei EulerOS, Hyper-V event channels, and Fortinet's full WAF product line.
- **Unified API Ingestion** - Consolidated cloud and SaaS connectors (e.g., Office 365, AWS CloudTrail, Cloudera) without requiring separate marketplace add-ons.
- **Granular Forensic Enrichment** - Automatic population of contextual fields (Who, What, Where, Why) for faster investigation.
- **Direct Threat Intelligence Integration** - Built-in correlation with CQ's proprietary feed, Nucleon TI, and MISP without additional scripting.
- **Optimized for Scale** - A modular, queue-based architecture that can handle high-volume, multi-source event streams in real time.

With its deep native integration capabilities, flexible architecture, and real-time correlation engine, CyberQuest delivers an immediate uplift in visibility and detection while reducing integration overhead. This positions it as a long-term, adaptable platform capable of evolving alongside emerging technologies, compliance mandates, and threat landscapes - ensuring sustained value for security operations teams and business stakeholders alike.