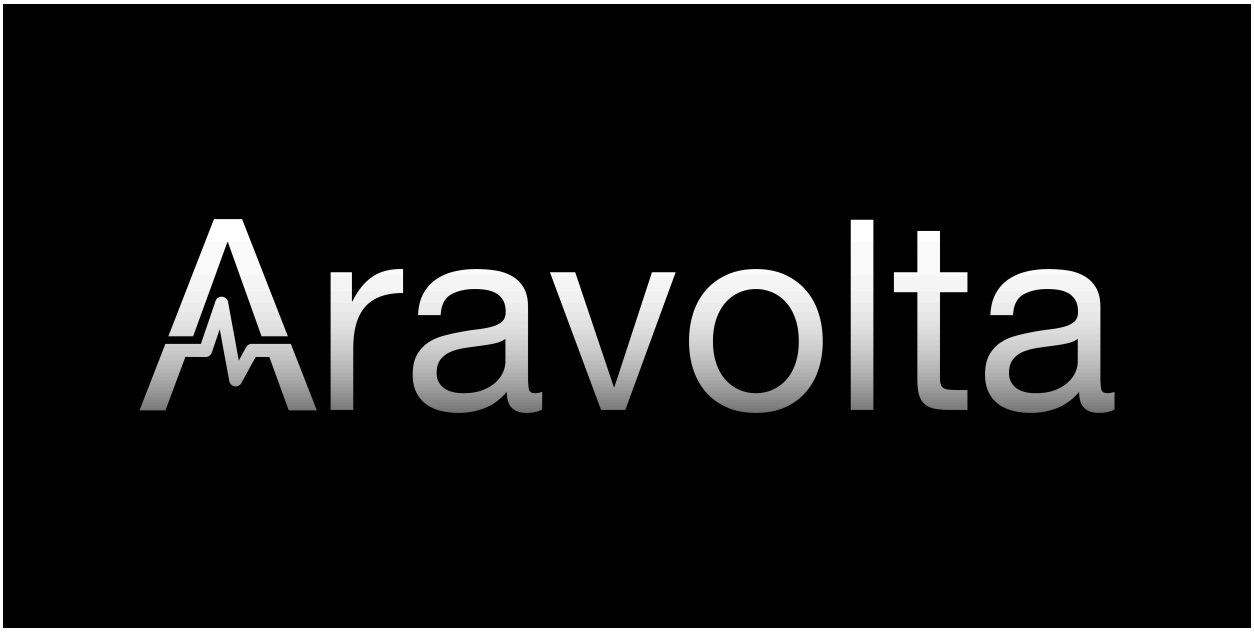
Aravolta Security White Paper



Aravolta Platform Overview

Aravolta is an asset-level telemetry collection and normalization platform designed to operate alongside existing infrastructure systems or serve as a primary system of record. The platform collects telemetry from infrastructure assets in both whitespace and greyspace, including power, cooling, and server hardware. This data is exposed through a centralized asset API. Aravolta also includes an optional Data Center Infrastructure Management (DCIM) visualization layer.

The platform consists of two primary components:

- A **collector agent** deployed within the customer environment
- A **cloud-based normalization, storage, API, and visualization layer**

All active data collection occurs within the customer environment. Aggregation, normalization, analytics, alerting, and integrations are handled in the cloud.

Deployment Model

The Aravolta collector is deployed within the customer's environment and may run as a physical node or, where preferred, a customer-managed virtual machine. In both cases, the same collector software is used and the runtime behavior is identical.

The collector is intentionally designed as a single-purpose service with no inbound management surface. Customers retain full control over where the collector runs and may disable or remove it at any time, at which point telemetry collection from that environment will cease.

The collector software is versioned and updated through a controlled release process. Updates may be applied by the customer or automatically, depending on deployment preferences. Update behavior is designed to be non-disruptive and does not require inbound access or manual intervention.

Key deployment characteristics:

- Single-purpose collector process

- No inbound network services
- No SSH or remote shell access
- Customer-controlled lifecycle (deploy, pause, remove)

Network Architecture and Data Flow

Inbound/Ingress Connectivity

The Aravolta collector does not accept inbound connections. This design results in a minimal inbound network exposure profile and simplifies firewall configuration.

Inbound traffic policy:

- No inbound connections supported
- No exposed management interfaces
- No externally initiated access paths

Outbound/Egress Connectivity

All communication from the collector to the Aravolta cloud platform is outbound-only and strictly limited. The collector initiates connections as needed to transmit telemetry and receive configuration updates.

Outbound traffic is limited to:

- **TCP 443 (HTTPS):** control plane, configuration, and authenticated API communication
- **TCP 8086:** outbound telemetry data transmission
- **TCP/UDP 53**: DNS and DNS fallback

Additional characteristics:

- All traffic encrypted in transit
- Connections initiated exclusively by the collector
- Customer may restrict egress via IP whitelisting

Internal Network Access

Within the customer environment, the collector communicates only with infrastructure devices that are explicitly configured. It does not perform network discovery or scanning beyond its defined scope.

Internal access characteristics:

- Read-only communication with configured devices
- Customer-provided credentials
- Least-privilege access model
- No access to tenant workloads or customer applications

Device Communication and Protocol Support

Aravolta is designed to integrate with a wide range of infrastructure devices and management systems commonly found in data center and facilities environments. The platform supports both standardized industry protocols and system-level integrations, allowing it to operate across heterogeneous infrastructure without introducing vendor lock-in.

The platform can communicate directly with infrastructure devices, intermediary management systems, or centralized control platforms, depending on deployment architecture and access patterns.

Supported communication methods and integration surfaces include:

- Standard infrastructure protocols such as SNMP, Modbus, Redfish, IPMI, iDRAC, BACnet, etc
- Direct integrations with data center and facilities management systems, including DCIM, EPMS, DCS, and BMS platforms
- Custom protocol adapters and vendor-specific interfaces for specialized or proprietary hardware

Telemetry is collected using a poll-based model initiated by the Aravolta collector. Polling frequency is configurable and determined based on device capabilities, protocol constraints, and operational considerations. In environments with existing

polling systems, Aravolta is designed to align with established limits to avoid contention or performance impact on upstream devices.

Security characteristics

- Poll-based, outbound-initiated data collection
- Read-only access to devices and systems
- No configuration changes, control operations, or actuation
- No firmware updates or write operations performed by the platform

---

Resilience, Redundancy, and Buffering

Collector Redundancy

For production environments using physical collectors, Aravolta supports a three-collector per network deployment model. This model provides operational continuity in the event of hardware failure and simplifies replacement without requiring changes to network configuration.

For virtual deployments, Aravolta recommends running multiple collector instances to avoid single-instance outages.

Recommended deployment models:

Physical deployments

- 1 primary collector
- 1 failover collector
- 1 spare collector (cold standby)

Virtual deployments

- At least 2 concurrently running collector instances

Failover occurs without inbound connectivity and does not require changes to firewall rules or network policy.

Local Buffering and Fault Tolerance

The collector includes local buffering to handle transient network interruptions. Telemetry data is queued locally when connectivity to the cloud is unavailable and is forwarded once connectivity is restored. Buffering behavior is bounded and designed to operate within available system resources.

Fault-tolerance characteristics:

- Local buffering of telemetry data
- Automatic retry and forward on reconnection
- No device interaction during connectivity outages
- No impact to infrastructure device operation

Authentication and Access Control

Each collector deployment authenticates to the Aravolta cloud platform using a unique, customer-scoped token. Tokens can be rotated or revoked at any time and are scoped to specific environments or sites. If a token is revoked, the associated collector is unable to authenticate and telemetry ingestion from that deployment ceases.

Authentication and access controls include:

- Unique per-deployment authentication tokens
- No hard-coded credentials

Data Handling and Privacy

Aravolta collects telemetry and asset metadata related to infrastructure monitoring and analytics. The platform does not collect customer application data or tenant workloads.

Data scope:

- Infrastructure telemetry and asset metadata
- No collection of end-user personal data
- No application-layer or tenant workload data

Data handling characteristics:

- Encryption of data in transit and at rest
- Logical isolation of customer data
- Configurable data retention based on agreement

Customers retain ownership of all collected data.

Cloud Infrastructure Security

The Aravolta cloud platform is hosted on Amazon Web Services (AWS) and designed for availability and resilience. The platform is deployed across multiple Availability Zones within each region and operates in multiple geographic regions, not all confined to the United States.

Cloud security characteristics:

- Multi-AZ deployments
- Regional isolation
- Segmented virtual networks
- Least-privilege access controls
- Continuous monitoring and logging
- Standard patching and update processes

Integrations and External Systems

Aravolta supports integrations with external systems for alerting, ticketing, analytics, and data export. Integrations are implemented through platform APIs and webhook-based events and operate entirely from the Aravolta cloud platform. No connectivity from external systems into customer data center networks is required.

Integration security characteristics:

- Use of official APIs and webhook mechanisms provided by third-party systems
- Token-based authentication scoped to individual integrations

- Customer-controlled enablement, configuration, and disablement
- No direct access to infrastructure devices or collector instances

---

Security Testing, Monitoring, and Assurance

Aravolta maintains an ongoing security assurance program designed to identify, assess, and remediate security risks across the platform.

Security assurance activities include:

- Periodic external penetration testing conducted by independent third parties
- Ongoing automated vulnerability scanning of infrastructure and applications
- Formal tracking, prioritization, and remediation of identified high- and critical-severity findings
- Centralized logging, monitoring, and alerting across cloud and platform components
- Documented incident response and risk management processes

Aravolta maintains a **SOC 2 Type I & II report**, which provides independent assurance over the design and operating effectiveness of its security controls. The report is available at:

https://trust.delve.co/centralaxis
