ARMIS®
from ServiceNow

CYWARE™

PARTNER BRIEF

Context over chaos: prioritizing real risk in OT/ICS environments

Security teams face a flood of vulnerabilities but lack the asset context to know which ones actually matter. Models like EPSS help by predicting near-term exploitation likelihood: they only become actionable when paired with real asset context.

OT/ICS environments raise the stakes further. Traditional scanning can disrupt sensitive systems or miss dormant assets entirely. Continuous, non-intrusive monitoring and inspection methods solve for this, maintaining operational stability while still delivering visibility.

Speed matters, but control matters more. Governance layers such as confidence scoring, tasking, and human review gates keep response fast without sacrificing reliability. Automation should trigger only when evidence is strong or a human has explicitly approved it: this is what makes rapid response safe.

How Armis and Cyware close the loop

Armis and Cyware together connect asset intelligence to automated response, enabling organizations to see, prioritize and act on the threats that matter most.

Armis provides continuous asset discovery and exposure management across IT, OT, IoT, and IoMT. It serves as the single source of truth for device profiles, vulnerability context (EPSS and KEV), and asset-level anomalies detected on the wire.

Cyware acts as the operational engine, ingesting Armis's rich asset data and adds context, correlating threat signals it against global, external threat intelligence feeds (such as ISACs and commercial threat data). From there, low-code and no-code playbooks orchestrate automated defense actions across the broader security ecosystem: firewalls, NAC, and SIEM, all driven by Armis's intelligence.

Together, the integration creates a closed-loop workflow: from asset visibility and risk context straight to intelligence-driven action, cutting time to detect and time to respond.

ARMIS from ServiceNow

Turning asset visibility into automated defense

The integration bridges the gap between passive asset visibility and active defense. By ingesting Armis's highly accurate asset, vulnerability, and exposure data, Cyware automatically triggers context-aware security playbooks. This eliminates manual analyst investigation and turns Armis's real-time visibility into immediate, cross-stack mitigation.

Armis delivers the definitive internal risk posture—knowing exactly which devices exist, their vulnerabilities, and their ransomware associations. Cyware delivers external threat contextualization and operationalization at nd scale.

Together, they create an automated, closed-loop system. An exposure identified by Armis is instantly validated against global attacker threat feeds and remediated across enterprise infrastructure, all without disrupting sensitive environments.

Use cases

Predictive Ransomware Quarantine: A vulnerable unmanaged asset is identified with a weaponized CVE.

Identify (Armis)
Armis continuously monitors the network, discovering an unmanaged OT asset and flagging it with a weaponized, ransomware-associated CVE.

Ingest & enrich (Cyware)
Cyware Intel Exchange pulls this high-severity alert from Armis and applies EPSS probability thresholds combined with external ISAC/commercial threat feeds to confirm active global exploitation of the threat.

Orchestrate & remediate (Joint)
Cyware Orchestrate triggers a targeted playbook to isolate the specific asset via the local NAC, while writing back the updated security status and investigation tags into the Armis console for continuous monitoring.

Additional joint use cases:

- **High-fidelity anomaly validation:** Cyware Intel Exchange reduces “anomaly noise” by validating Armis behavioral alerts against known malicious infrastructure.
- **OT/ICS integrity & lateral movement:** Armis identifies potential IT/OT attack paths; Cyware Intel Exchange prioritizes these based on adversary tradecraft and MITRE ATT&CK for ICS.
- **Intelligence-driven prioritization:** Merges Armis CVE context with daily EPSS updates to prioritize and auto-task remediation for the most critical exposures.
- **Third-party & supply chain governance:** As new vendor assets appear, Armis profiles them and Cyware Intel Exchange checks them against watchlists to orchestrate policy-aligned restrictions.

Key features and benefits

Security: Higher-fidelity decisions by validating Armis exposure and anomaly signals with multi-source intel. Faster containment via rules-to-playbook automation when confidence is high. Better coverage for unmanaged/agentless assets through network-based visibility and response.

Operational: Reduced analyst toil through automated ingestion, de-duplication, enrichment, and correlation. Repeatable playbooks via low-code/no-code orchestration across tooling. Clear handoffs via tasking (priority + due dates) and action tracking.

Compliance: Defensible prioritization using KEV status/due dates plus exploitation likelihood (EPSS). Trackable workflows with documented tasks and action history. Consistent enforcement patterns aligned to segmentation controls and policy.

Financial: Less wasted effort on low-likelihood work; more focus on exploitable, asset-relevant risk. Reduced incident impact by earlier, targeted containment. Lower operational friction in OT by gating automation appropriately.

Technical overview

The integration between Armis Centrix™ and Cyware's Intel Operations Suite (Intel Exchange and Orchestrate) enables a closed-loop, asset-centric threat intelligence and response workflow.

Armis provides continuous, agentless discovery and profiling of assets across IT, OT, IoT, and IoMT environments. Cyware ingests this asset and vulnerability context, enriches it with multi-source threat intelligence, and executes automated response playbooks when defined confidence thresholds are met.

Integration components

Armis Centrix™

Armis Centrix™ delivers continuous, agentless asset discovery using passive network monitoring through virtual appliance collectors deployed within the customer environment. It maintains a real-time asset inventory enriched with:

- Vulnerability assessments (CVEs with EPSS scores, CISA KEV status, ransomware association, weaponization flags)
- Behavioral baselines
- Risk scoring across all device types, including unmanaged assets

Cyware Intel Exchange

Cyware Intel Exchange is Cyware's centralized threat intelligence platform and is STIX/TAXII-native. It ingests, normalizes, de-duplicates, correlates, and scores indicators from:

- Commercial feeds (Recorded Future, Google Threat Intelligence)
- OSINT and dark web monitoring
- Cyware Sectoral Feeds from 25+ ISAC/ISAO communities
- Internal telemetry (SIEM, EDR/XDR, NDR, cloud security tools)

Cyware Intel Exchange assigns risk and confidence scores, performs adversary and malware attribution, and maps behaviors to the MITRE ATT&CK framework, providing contextual reasoning for threat determinations.

Cyware Orchestrate

Cyware Orchestrate is a low-code/no-code automation engine with 400+ pre-built integrations. It:

- Hosts Armis connector applications
- Executes multi-step playbooks
- Drives enforcement actions across security controls such as SIEM, EDR, NAC, firewalls, ITSM, and vulnerability management systems

Connector architecture

Two Cyware Orchestrate connector applications enable API-level integration with Armis:

Armis V1 Connector

- **API:** V1 and V2 REST
- **Authentication:** API key exchange for session token
- **Querying:** Armis Query Language (AQL)
- **Resilience:** Built-in retry logic (Error handling, configurable retries)

Capabilities:

- Search devices and applications using AQL
- Retrieve detailed device profiles (IP, MAC, OS, risk level, Purdue level, tags, custom properties)
- Fetch device software inventory
- Execute generic API calls for advanced use cases

Armis V3 Connector

- **API:** V3 REST (cloud-native endpoint)
- **Authentication:** OAuth 2.0 client-credentials flow
- **Authorization:** Scoped permissions aligned with least-privilege access
- **Write Support:** Full CRUD capabilities

Capabilities:

- Search assets using multiple identifiers (Asset ID, MAC, IP, serial number)
- Bulk update asset properties (tags, site assignments, custom fields)
- Discover searchable fields and filter by data source
- Retrieve collector images and data export URLs
- Manage custom properties and site configurations
- Execute generic API calls for advanced use cases

Data flow

The integration supports a multi-stage intelligence lifecycle:

01

Asset and vulnerability context ingestion (Armis → Cyware)

Playbooks retrieve:

- Asset inventory
- Vulnerability data (EPSS, ransomware flags, weaponization status)
- Device profiles and behavioral alerts

02

Threat intelligence enrichment (within Cyware)

Cyware Intel Exchange enriches data through:

- External intelligence (commercial feeds, ISAC feeds, OSINT, advisories)
- Internal correlation (SIEM, EDR/XDR, historical incidents)
- Scoring, attribution, and ATT&CK mapping

03

Response execution (Cyware → Armis and Security stack)

- Write-back to Armis: Tagging assets (e.g., quarantine, investigation flags)
- Downstream enforcement:
  - NAC isolation
  - ITSM ticket creation
  - Firewall segmentation updates
  - SIEM threat hunting and correlation
- Active monitoring:
  - Detection rule deployment
  - Look-back analysis of historical traffic

04

Verification and closure

- Armis rescans affected assets
- Validation of remediation or compliance
- Automatic closure of ITSM tasks
- Asset status updates in Armis

Representative use cases

01

Predictive ransomware quarantine

Identifies weaponized vulnerabilities and preemptively isolates high-risk unmanaged devices before exploitation:

- Combines EPSS, CVSS, and asset criticality
- Enriches with Cyware Intel Exchange intelligence
- Triggers NAC quarantine and ITSM workflows
- Writes back asset status to Armis

02

High-Fidelity anomaly validation

Validates behavioral anomalies by correlating Armis alerts with global threat intelligence.

- Differentiates benign vs. malicious activity
- Performs SIEM-based threat hunting
- Enables confidence-based escalation and response

03

OT/ICS integrity and lateral movement mapping

Maps potential attack paths across IT and OT environments.

- Uses Armis DPI insights
- Correlates with adversary TTPs
- Enables human-approved segmentation enforcement

04

Intelligence-driven vulnerability prioritization

Prioritizes remediation based on exploitability (EPSS, CISA KEV).

- Identifies vulnerable assets via SBOM
- Tracks EPSS changes and reachability
- Automates ticketing and verification workflows

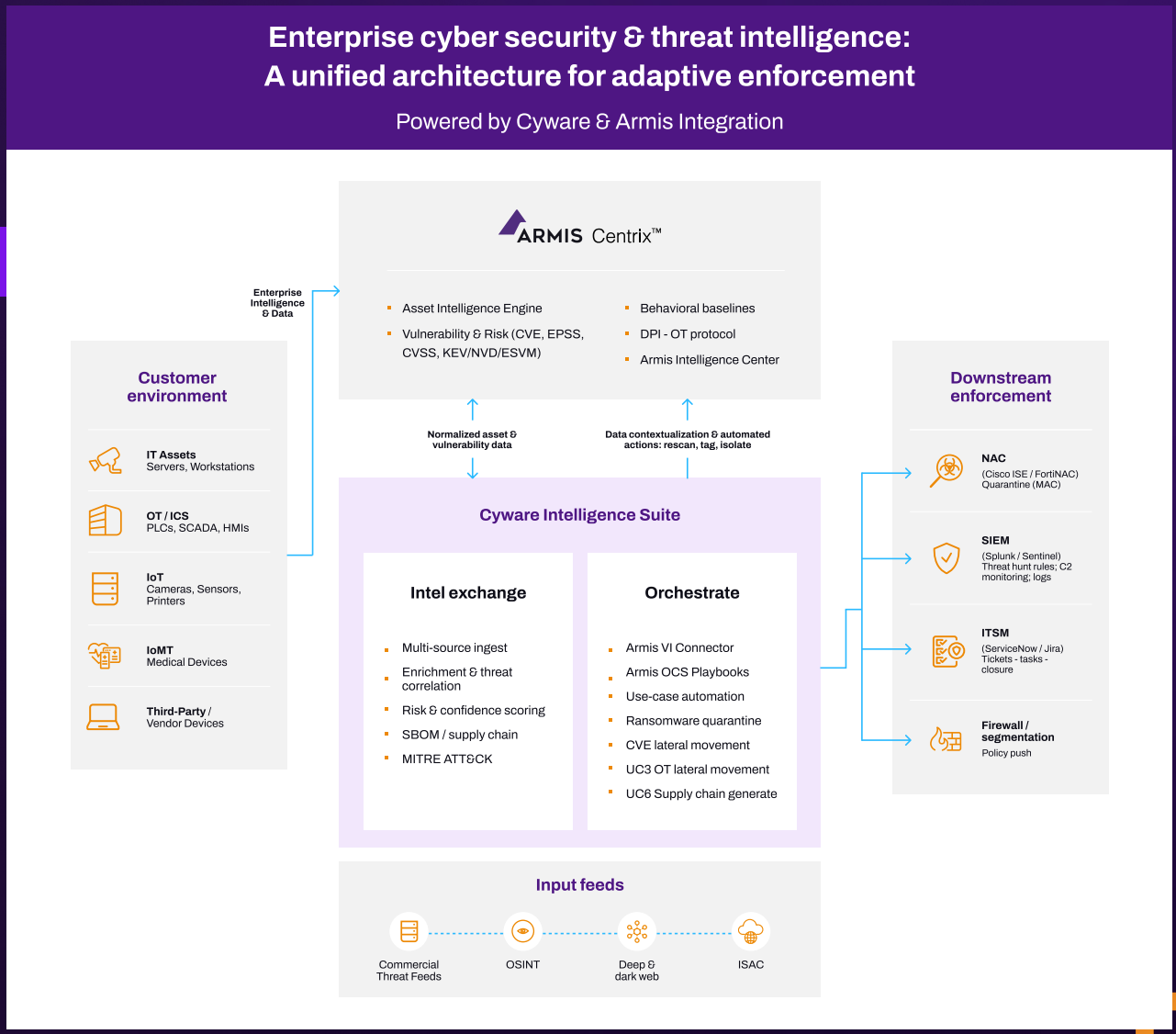
05

Third-party and supply chain governance

Implements automated “audit-on-connect” for external devices.

- Performs SBOM and lineage analysis
- Enriches with threat intelligence and vendor risk context
- Enables continuous monitoring and incident escalation

Architecture diagram:



Inside meets outside: Armis and Cyware deliver closed-loop security

The Cyware-Armis integration combines Armis's definitive real-time asset exposure visibility with Cyware's multi-source external threat intelligence management and enterprise orchestration.

This closed-loop solution lets organizations instantly validate internal asset vulnerability data against global adversary behavior, enabling rapid, automated, and safe security enforcement across IT, OT, and IoT environments.

CYWARE™

Cyware is leading the industry in Agentic AI-powered operationalized threat Intelligence and collective defense, helping security teams transform threat intelligence from fragmented data points to actionable, real-time decisions. We unify threat intelligence management, intel sharing and collaboration, as well as hyper-orchestration and automation eliminating silos and enabling organizations to outmaneuver adversaries faster and more effectively. From enterprises to government agencies and ISACs, Cyware empowers defenders to turn intelligence into action.

ARMIS®
from ServiceNow

Understand the Armis difference:

- Comprehensive visibility
- Intelligent insights
- Proven outcomes

Try Armis Centrix™ Today

Armis from ServiceNow protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

+1 888 452 4011

armis.com