ARMIS®
from ServiceNow

PENTERA.

PARTNER BRIEF

Evidence over assumption: proving which exposures attackers can actually reach

Security teams already have broad visibility across IT, IoT, OT, cloud, and external attack surfaces. What they lack is proof. Without knowing which exposures an attacker can genuinely reach, prioritization stays theoretical and remediation queues keep growing.

Traditional validation compounds the problem. Manual penetration testing delivers a static, point-in-time view that ages the moment the environment changes, and it runs in isolation from live asset data. Teams end up remediating against assumed exposure rather than validated risk.

Dynamic environments raise the stakes further. New assets appear, configurations drift, and risk scores move daily. Validation has to follow those changes as they happen instead of waiting for the next scheduled assessment.

How Armis and Pentera close the loop

Armis and Pentera together connect asset intelligence to attack-path evidence, so teams act on the exposures an adversary can actually use.

Armis Centrix™ discovers, classifies, and continuously monitors every asset across IT, OT, IoT, cloud, and external attack surfaces. It detects exposures, scores risk against asset criticality and threat context, and flags the changes that matter. Pentera acts as the validation engine. Pentera Validation OS™ receives Armis risk and change events, selects the right validation engine for the asset and environment, and safely tests what an attacker could achieve.

Validated findings flow back into the Armis exposure management workflow, adding proven exploitability and attack-path context to prioritization and remediation. The result is a closed loop: discover, prioritize, validate, remediate, then re-validate to confirm the risk is closed.

Turning asset intelligence into validated risk

The integration bridges the gap between knowing what is exposed and knowing what is exploitable. Armis risk events trigger Pentera validation automatically, so evidence arrives while the finding is still current.

Armis delivers the internal picture: which assets exist, how they are configured, what they are exposed to, and how much they matter to the business. Pentera delivers adversary proof at scale across on-prem, cloud, and external attack surfaces.

Together they replace theoretical severity with demonstrated impact. Teams stop triaging by score alone and start closing the exposures that carry a viable attack path.

Use cases

Risk-triggered validation: Armis detects a new critical asset or a material risk change that needs proof before remediation.

- **Identify (Armis):** Armis Centrix™ discovers a new critical asset, vulnerability, or exposure, or detects a risk score increase or configuration change on an existing asset.
- **Validate (Pentera):** The Armis risk event triggers Pentera Validation OS™, which selects the relevant validation engine for that asset and attack surface and safely tests whether the risk creates a viable attack path.
- **Prioritize and remediate (Joint):** Pentera returns exploitability, attack path, and reachability evidence into the Armis exposure management workflow, driving prioritization, ServiceNow remediation tasks, and automatic re-validation once the fix lands.

Additional joint use cases:

- **Cross-surface validation:** Apply Pentera validation across the on-prem, cloud, and external attack surfaces Armis identifies and monitors.
- **Remediation noise reduction:** Give security and IT teams shared evidence to separate theoretical exposure from actionable risk.
- **Re-validation on new asset, risk change, or close:** Automatically re-test to confirm current risk status.
- **CTEM operationalization:** Connect Armis discovery and prioritization to continuous validation and measurable remediation.

Key features and benefits

- **Security:** Remediation focuses on the vulnerabilities and assets proven to create exploitable risk, backed by attack-path evidence rather than theoretical severity. Safe, non-disruptive validation extends that proof across on-prem, cloud, and external attack surfaces.
- **Operational:** Event-driven validation replaces scheduled assessments, so proof arrives when risk changes. Automatic engine selection removes manual test scoping, and validated findings land directly in the existing Armis and ServiceNow remediation workflow.
- **Compliance:** Defensible prioritization based on demonstrated exploitability. Continuous validation and automatic re-validation create an auditable record that a gap was found, fixed, and confirmed closed.
- **Financial:** Less effort spent on exposures that cannot be reached, faster closure of the ones that can, and lower incident impact from removing viable attack paths earlier.

Technical overview

The integration between Armis Centrix™ and Pentera Validation OS™ enables an event-driven, asset-centric validation workflow. Armis asset and risk events trigger validation over a secure API and SDK channel, and validated findings return to enrich Armis-driven prioritization and remediation.

Armis provides continuous, agentless discovery and risk assessment across IT, OT, IoT, cloud, and external assets. Pentera receives Armis risk events, orchestrates the appropriate validation engine based on asset type, environment, and risk, and returns validated exploitability and attack-path evidence.

Integration components

Armis Centrix™
Armis Centrix™ delivers continuous, agentless asset discovery and exposure management across IT, OT, IoT, cloud, and external attack surfaces. It maintains a real-time asset inventory enriched with:

- Deep asset context and relationships across managed, unmanaged, IoT, OT, IoMT, IT, cloud, and external assets.
- Vulnerability and exposure detection across all assets and environments.
- Risk scoring and prioritization based on asset criticality, exposure, and threat context.
- Change detection and continuous monitoring, backed by the Asset Intelligence Engine (device knowledgebase, threat intelligence, behavioral analytics, and risk engine).

Pentera Validation OS™
Pentera Validation OS™ is Pentera's AI-powered security validation platform, operating in validation-on-demand mode when triggered by Armis. It:

- Selects the right validation engine automatically, based on asset type, environment, and risk.
- Executes safe validation, authenticated or unauthenticated, scoped to the selected engine.
- Returns exploitability, attack path and evidence, impact and reachability, and remediation guidance.
- Re-validates automatically after remediation to confirm the risk is resolved.

Pentera validation engines
Three engines cover the surfaces Armis monitors:

- On-prem validation engine, delivered through the Pentera Validation Agent embedded in the Armis Collector.
- Cloud validation engine, delivered as SaaS via API and SDK.
- External attack surface engine, delivered as SaaS via API and SDK.

Integration architecture

Armis and Pentera exchange risk events and validated findings over a secure API and SDK channel, in two directions:

Armis to Pentera: risk and change events

- Trigger: Armis risk and change events.
- Transport: Secure API and SDK call to Pentera Validation OS™.
- Event types: New critical asset discovered, new vulnerability or exposure identified, risk score increased, asset configuration change, new external exposure detected.
- Engine selection: Automatic, based on asset type, environment, and risk.

Pentera to Armis: validated findings

- Transport: Secure API and SDK response into the Armis exposure management workflow.
- Findings returned: Exploitability (yes or no), attack path and evidence, impact and reachability, remediation guidance.
- Enrichment: Validation results enrich Armis risk context for prioritization and remediation planning.
- Closure: Automatic re-validation after remediation confirms whether the risk is resolved.

Data flow

The integration supports a four-stage validation lifecycle:

1. Asset and risk event detection (Armis)
Armis generates the events that drive validation:

- Continuous discovery and classification across IT, OT, IoT, cloud, and external assets.
- Exposure detection and risk scoring against asset criticality and threat context.
- Change detection that generates the risk events used as validation triggers.

2. Validation trigger and engine selection (Armis → Pentera)
The event routes to the right engine:

- Armis risk event calls Pentera Validation OS™ via API or SDK.
- Validation OS selects the on-prem, cloud, or external engine for the asset and surface.
- Scope and validation mode are set for safe, non-disruptive execution.

3. Safe validation execution (Pentera)
Pentera executes the test without disrupting the environment:

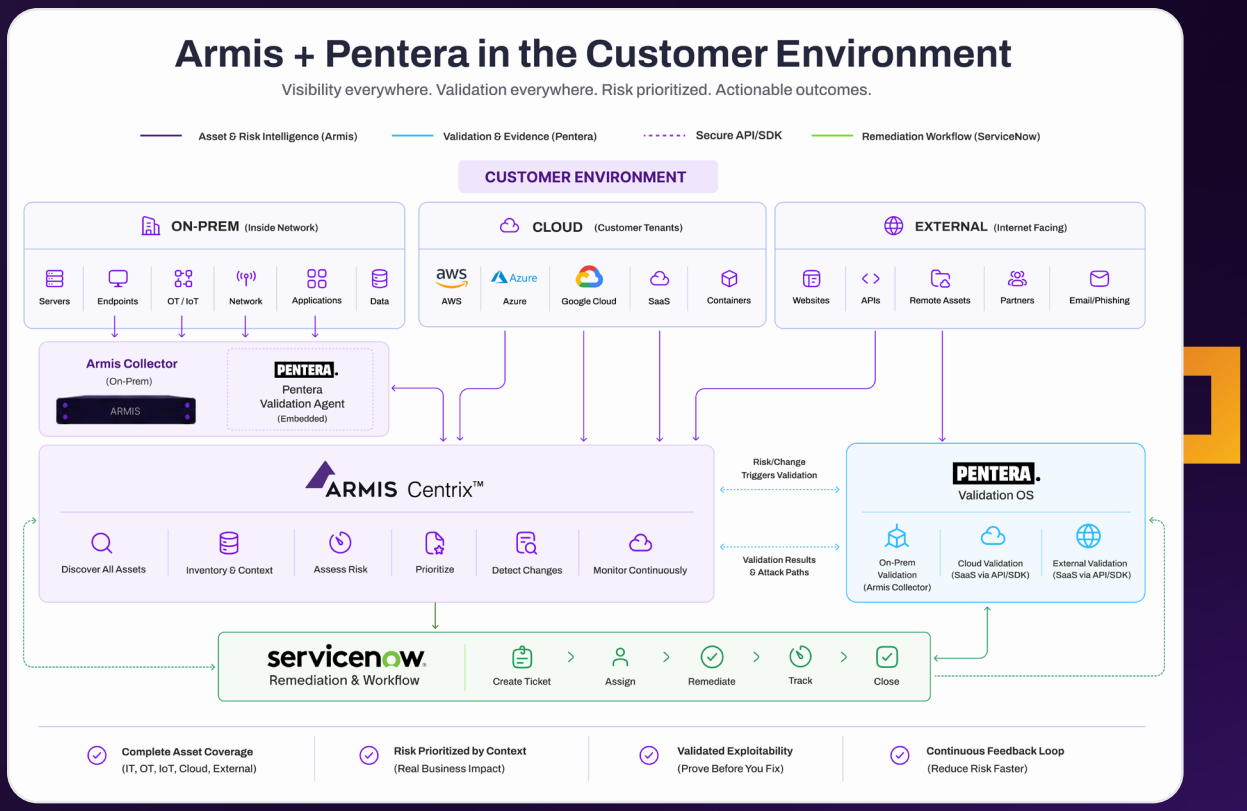
- Authenticated or unauthenticated validation, based on engine and scope.
- On-prem validation through the Pentera Validation Agent embedded in the Armis Collector.
- Cloud and external validation through the SaaS engines.

4. Findings write-back and remediation (Pentera → Armis and ServiceNow)
Evidence returns and remediation runs:

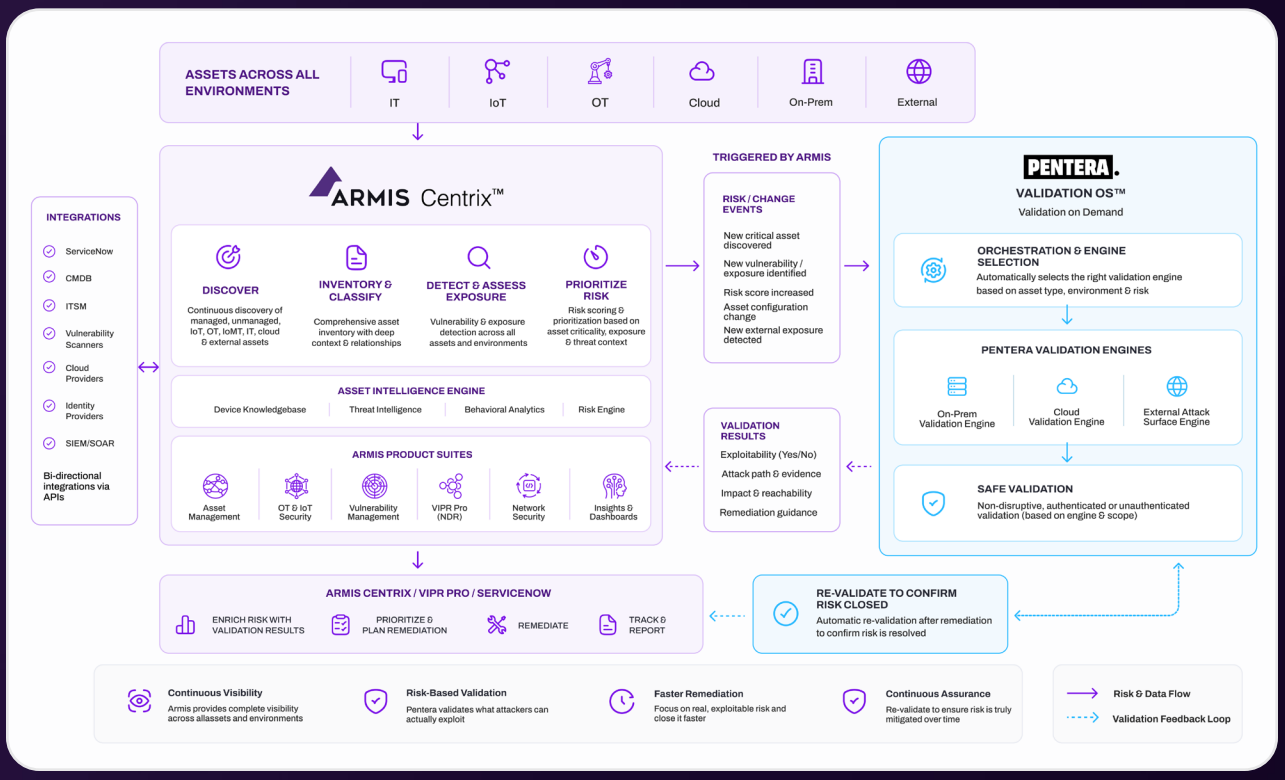
- Validated exploitability, attack path, impact, and remediation guidance return to Armis.
- Armis Centrix™ and VIPR Pro enrich risk and plan remediation. VIPR Pro is Armis' unified risk management solution that ingests, prioritizes, and deduplicates enterprise-wide security findings to automatically assign and track remediation across IT, OT, and IoT environments.
- ServiceNow creates, assigns, tracks, and closes the remediation task.
- Pentera re-validates the asset to confirm the risk is closed.

Architecture diagrams

Architecture in the customer environment:



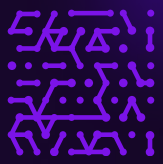
High-level architecture:



Visibility meets validation: Armis and Pentera prove what matters

The Pentera and Armis integration combines Armis's comprehensive, real-time visibility across assets, exposures, and changes with Pentera's automated security validation.

Once Armis identifies a change or an exposure, Pentera triggers a validation test to prove what an attacker can actually exploit. Together they enable evidence-based prioritization and faster remediation, closing real, exploitable risk across on-prem, cloud, and external attack surfaces.



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