# Dispel Announces Partnership with Armis from ServiceNow to Bring Asset Visibility into Every OT Remote Access Decision

*New integration, announced at Black Hat USA 2026, combines Armis Centrix™ with the Dispel Zero Trust Engine, closing the gap between security and operations.*


LAS VEGAS, NV, UNITED STATES, August 4, 2026 /EINPresswire.com/ -- Dispel, recognized as a Gartner® Cool Vendor in Cyber-Physical Systems (CPS) Security, today announced at Black Hat USA 2026 an integration with Armis from ServiceNow, a global leader in cyber exposure management & security. The joint offering combines Armis Centrix™, the Armis Cyber Exposure Management Platform, with the Dispel Zero Trust Engine, extending Armis' AI-powered risk mitigation across the attack surface directly into every Dispel remote access decision.

Historically, industrial organizations have relied on siloed teams and air-gapped networks to manage risk: security-owned visibility into the attack surface, operations-owned access decisions, and the two rarely intersected. That separation is no longer sufficient. As OT environments grow more connected and third-party access becomes routine, organizations must close the gap between what security sees and what operations decides, in real time. According to SANS (2025), roughly half of industrial cybersecurity incidents begin with unauthorized external access, exactly the gap this integration is built to close.

"Dispel Intelligence was built for exactly this moment," said Ben Burke, President and COO of Dispel. "AI-driven threats demand continuous defense, not just at login but across every minute of every session. With Armis' asset intelligence enriching every risk score, OT operators can detect and respond before threats reach the assets that matter most."

ELIMINATING THE FRICTION BETWEEN OT ASSET INTELLIGENCE AND SECURE REMOTE ACCESS

Industrial operations depend on fast, reliable access to critical systems. Legacy VPNs, jump

hosts, and fragmented tools introduce delays and manual vendor workflows that slow down the OEMs, contractors, and operators who need to reach mission-critical assets, compounding operational drag across all sites and incidents.

As industrial organizations scale remote access across plants, distributed sites, and third-party vendors, maintaining a current, accurate picture of every OT asset, managed and unmanaged alike, is the foundation of efficient access decisions. This integration solves that at the source: Armis' real-time asset intelligence, spanning each asset's characteristics, configuration, behavior, and vulnerability profile, synchronizes automatically into the Dispel Zero Trust Engine, so remote access policies always reflect the real-world state of the environment, with no manual reconciliation required. This results in faster vendor onboarding, quicker access approvals, and one less manual step standing between a vendor and the asset they need to reach.

The integration also closes the loop end to end: when Armis Centrix™ identifies a vulnerability, a vendor's subsequent just-in-time access request through the Dispel platform is recorded and audited automatically. Once the fix is applied, Armis' continuous monitoring re-checks the asset and automatically reflects the vulnerability as resolved. The result is a complete evidence chain, from vulnerability discovery through controlled access to confirmed remediation, that compliance teams can produce without manual assembly, supporting the operational resilience both companies are built to protect.

SESSION FORENSICS WITH DYNAMIC RISK SCORING, ENRICHED BY ARMIS FROM SERVICENOW

The integration extends Dispel Intelligence's Session Forensics with Dynamic Risk Scoring, which continuously scores every OT remote access session in real time across identity, device, and connection from login through disconnect. OT, IoT, and ICS asset data from Armis Centrix™ is correlated with the Dispel platform's session-level behavioral analysis, so administrators understand not only how a user's behavior compares to the baseline but also the criticality and vulnerability profile of the assets involved.

At the moment of access approval, administrators see a composite risk view merging session behavioral risk with asset criticality and vulnerability data enriched by Armis Centrix™, putting the full context of OT asset intelligence directly into the access decision. As AI-enabled threats demonstrate the ability to autonomously exploit vulnerabilities at machine speed, AI-powered risk mitigation matters more than ever. Unplanned OT downtime already averages $169,889 per hour (ABB, 2025), and every hour an exposure goes unaddressed compounds that cost. Enriched, real-time risk scoring gives OT operators the visibility to close that window of exposure before it becomes an incident.

"Mapping the entire attack surface needs to be a strategic priority for maintaining operational resilience, but visibility alone isn't enough. Risk mitigation must occur the moment an access decision is made," said Nadir Izrael, Group Vice President at Armis from ServiceNow. "By integrating our comprehensive AI-powered platform with the Dispel remote access workflow, our

joint customers can execute access decisions and prioritize remediation from one unified view, without adding a single new tool to their environment.”

AVAILABILITY

The integration is available now within the Dispel Zero Trust Engine for all joint customers across cloud and on-premises deployments. Dispel will be demonstrating the joint offering at Black Hat USA 2026. Organizations can learn more and request a demo at dispel.com/book.

ABOUT DISPEL

Dispel delivers security that makes industrial operations run faster. The Dispel Zero Trust Engine securely connects people and operational data across complex OT environments, unifying secure remote access, industrial data streaming, Dispel Intelligence, Dispel Identity, Dispel Compliance, and OTFusion into one platform built for industrial scale. Founded in 2015, Dispel pioneered network-level Moving Target Defense (MTD) and holds 60 patents, protecting over $500 billion in manufactured goods annually and securing remote access for more than 60 million utility users worldwide. Built for Efficiency. Secure by Design. Audit Ready. Learn more at dispel.com.



Mark Lennon
Dispel
email us here
Visit us on social media:
LinkedIn
YouTube