Dispel Identity Unveiled at Black Hat 2026, the First Identity Assurance Capability Built for OT Remote Access

AI makes it easier to impersonate the person behind a credential. Dispel Identity brings NIST IAL2 verification to every OT remote access decision.

LAS VEGAS, NV, UNITED STATES, August 3, 2026 /EINPresswire.com/ -- Dispel, recognized as a Gartner® Cool Vendor in Cyber-Physical Systems (CPS) Security, today announced at Black Hat USA 2026 the launch of Dispel Identity, bringing identity proofing to OT remote access — verified through government ID checks and biometric matching, to the NIST IAL2 standard. Where existing platforms verify a credential, Dispel Identity verifies the person, protecting the crown jewel assets where OT remote access carries the greatest risk.

Every OT remote access platform on the market trusts the credential, never independently verifying the person holding it. Credentials get shared. Sessions stay open. Logins get handed to whoever is on shift. For work reaching control systems, where a single action carries physical and safety consequences, that safety and audit gap is no longer acceptable.

"The question in OT remote access isn't whether the right password was used, it's whether the real person behind that account is the one actually connecting," said Ethan Schmertzler, Co-CEO of Dispel. "Credentials can be phished or handed off, allowing attackers to use the front door to gain access to your organization's most important assets. Dispel Identity is the standard that OT remote access has always needed, giving you the confidence and control to know exactly who is in your system."

PROVING THE PERSON, NOT JUST THE PASSWORD

Dispel Identity brings an industry-first identity capability to operational technology, joining Dispel's Intelligence and Compliance capabilities to confirm who actually holds the account. Authentication confirms the right credential was used; identity proofing confirms the person is who they claim, and is the one connecting now. Dispel Identity delivers Identity Assurance Level 2 (IAL2) under NIST SP 800-63A, extended to OT remote access through an accredited provider that confirms, in three stages, that a person is who they claim:

• Resolution: Confirms the applicant is a distinct, real person.

• Validation: Confirms their government-issued ID is genuine.

• Verification: A liveness check and facial match confirms they are the person that ID describes.

The result is permanent. Once verified, that person is tied to a single Identity record, with every account connecting back to it. Verification runs independently of the login path, so a slow provider never locks anyone out.

That assurance runs on a compliance and privacy stack:

• Central platform for IAL2 identity verification (IDV) and fraud indicators.

• Global document support across all 195 countries, with FRVT-benchmarked face-matching for 1:1 verification and 1:N identification.

• Native integrations with your IdPs: Microsoft Entra, Okta, PingIdentity, and any SAML or OIDC provider, with support for hybrid environments mixing social sign-on and local accounts.

• Privacy-first architecture: U.S.- or EU-located processing; GDPR data-minimization; BIPA-compliant consent, storage, and deletion controls; independent eIDAS audit; and certification under the EU-U.S. and Swiss-U.S. Data Privacy Frameworks, with UK extension. Biometric data is encoded in a non-reversible, non-reconstructable format.

EXTENDING VERIFIED IDENTITY TO THIRD-PARTY ACCESS IN REGULATED INDUSTRIES

At 2 AM, when a third-party vendor connects to a critical asset, the question is simple: is this a real, verified person tied to the account? Dispel Identity answers it, confirming a real human against a government ID and tying that person to the account, giving operators confidence at any hour.

Contractor credentials are especially prone to this gap, moving within a firm or to whoever is on shift. Dispel Identity scopes verification to third parties, requires a live check before high-risk access, and maps verified identities to vendor-imposed shared accounts. The operator always knows who came in; the evidence is auditable.

In utilities, energy, and manufacturing, in-person identity verification is standard on-site. NERC CIP, for example, requires it at the gate, but not for remote sessions. Dispel Identity extends that standard to every remote connection, satisfying IEC 62443-3-3 SR 1.1 RE1 (unique user identification), SR 1.3 (account management), and SR 2.12 (non-repudiation).

MANAGING ACCESS BY PERSON, NOT JUST ACCOUNT

Dispel Identity gives operators a single, easy-to-use view for vendor identity and account management. Blocking an Identity denies sign-in across every account that person holds, including shared ones: one action, not a hunt across every login. Unlinking corrects the record if tied to the wrong person, without deleting history. This matters most at offboarding, where blocking the person once covers every account they held.

POLICY-DRIVEN VERIFICATION, APPLIED ONLY WHERE IT MATTERS

Through Dispel's Policy Builder, operators define exactly when identity proofing triggers:

• By user type: All users, internal operators, or third-party contractors only.

• By asset risk score: Devices flagged above a risk threshold by integrations like Nozomi Networks, Dragos, or Armis require live verification.

• By Session Forensics score: A behavioral risk threshold crossed mid-session requires verification before the connection continues.

• By geography: Block access attempts from specific countries or regions.

The policy enforces automatically: not optional, not dependent on anyone remembering to ask. At 2 AM, when every second counts, evidence generates automatically, removing the decision from the person under stress and making compliance structural.

DISPEL IDENTITY JOINS A UNIFIED PLATFORM

Dispel Identity now joins a unified platform built around OT Secure Remote Access. Dispel Intelligence scores every session through Session Forensics and Dynamic Risk Scoring. Dispel Compliance generates audit-ready evidence across NERC CIP, NIST, IEC 62443, and EU NIS2. Industrial Data Streaming moves data across environments, and the platform deploys cloud-managed, on-premises through Site Console, or hybrid, with Browser Connect, Virtual Desktop, and Application connection types.

AVAILABILITY

Dispel Identity is available now within the Dispel Zero Trust Engine. Dispel will be demonstrating Dispel Identity live 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

unifies secure remote access, industrial data streaming, Dispel Intelligence, Dispel Identity, Dispel Compliance, and OTFusion into one platform. 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 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
