Dispel Launches Session Forensics, Bringing Real-Time Dynamic Risk Scoring to OT Remote Access as AI Threats Escalate

New capability scores every OT remote access session in real time across identity, activity, and behavior— mitigating modern AI threats and minimizing friction.

AUSTIN, TX, UNITED STATES, May 14, 2026 /EINPresswire.com/ -- Dispel, the leader in Secure Remote Access (SRA) for Operational Technology (OT), today announced the general availability of Session Forensics with Dynamic Risk Scoring — the first capability within Dispel Intelligence. Dispel Intelligence gives operators context when they need it most and helps defend against the latest emerging AI attack vectors. Session Forensics ships as part of the Dispel Zero Trust Engine platform, continuously evaluating every remote access session from login through disconnect with real-time, dynamic risk scoring.

Most OT remote access programs stop at the front door. A vendor authenticates, multi-factor authentication (MFA) is confirmed, and the session opens. What happens inside that session — how behavior compares to baseline, whether the risk profile shifted between login and minute forty-five, and what a compromised account looks like — remains invisible. That gap is where incidents develop. Session Forensics with Risk Scoring closes it.

"The OT industry is moving beyond login access," said Ethan Schmertzler, Co-CEO of Dispel. "Our Session Forensics capability gives industrial teams continuous visibility into what is happening during every remote access session — not just when someone logged in, but what risk they carried and whether that risk was acceptable. That context decreases operator mistakes and improves security and performance outcomes. Session Forensics is the intelligence OT programs have been missing."

Session-Level Risk Intelligence, Built for OT

Session Forensics with Risk Scoring introduces a session-centric security model that evaluates risk across three critical dimensions: identity, device, and connection. Every session is automatically assigned a dynamic risk score based on behavioral signals including MFA

assurance level, impossible travel, concurrent sessions, time zone anomalies, new IP addresses, and deviation from established user baselines. Risk scores are presented through a green / yellow / red stoplight model, designed for plant administrators and OT staff — not just security specialists.

Behavioral baselines are built at three levels — organization, group, and individual user — maturing to deliver increasingly precise, personalized risk detection. Critically, Dispel's baseline model learns only from trusted logins, preventing attackers from poisoning behavioral profiles.

At the moment of access approval, administrators see a composite risk view that merges session risk with asset criticality and vulnerability data enriched by integrations with Nozomi Networks, Dragos, Armis, Forescout, and TXOne Networks — putting existing OT security investments directly into the access decision workflow.

Session Provenance and Compliance Evidence

Session Forensics also delivers full session provenance — a complete, timestamped record of how every session token was issued, including password attempts, MFA success and failure events, and authentication assurance level evidence aligned to NIST SP 800-63B AAL2 and AAL3 requirements. Failed access attempts are logged even when no session is granted, exposing brute force activity and credential testing that would otherwise go undetected.

Every session produces a complete evidentiary package — detection through remediation — ready for NERC CIP, IEC 62443, NIST SP 800-82, and TSA SD02 audits without additional tooling or manual compilation.

Availability

Session Forensics with Dynamic Risk Scoring is available now as part of Dispel Intelligence within the Dispel Zero Trust Engine, our OT secure remote access platform. 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, intelligence, and OTFusion into a single platform built for industrial scale. Founded in 2015, Dispel pioneered network-level Moving Target Defense (MTD) and holds more than 43 patents. Dispel protects over $500 billion in manufactured goods annually and secures remote access for 54 million utility users worldwide. Built for Efficiency. Secure by Design. Learn more at dispel.com.

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