SESSION FORENSICS · DEVICE RISK INTELLIGENCE

Eliminate the Friction Between Security, Operations & Compliance

Every OT security program answers to three teams with competing goals: security wants tight controls, operations wants production moving, and GRC needs to prove it all works. As remote access scales across plants, sites, and vendors, every safe access decision rests on one foundation — a current, accurate picture of every asset and who accesses what. The Dispel + Tenable integration solves that at the source: **Tenable One OT Exposure**'s real-time OT/IoT asset visibility — characteristics, configuration, behavior, and vulnerability profile — syncs automatically into the **Dispel Zero Trust Engine**, so access policies always reflect the real state of the environment, with no manual reconciliation. The result is faster onboarding and quicker approvals.

From there, the integration puts that intelligence into the moment of access. It extends Dispel Intelligence's **Session Forensics** with **Dynamic Risk Scoring**, continuously scoring every session across identity, device, and connection — login to disconnect. **Tenable One OT Exposure** asset data is correlated with Dispel's behavioral analysis, so at approval administrators see one composite view: how a user compares to baseline, merged with the criticality and vulnerability of the assets involved. It matters more as AI-enabled threats exploit vulnerabilities at machine speed — enriched, real-time scoring closes the window of exposure before it becomes an incident, so all three teams move faster, together.

SECURITY TEAM

Security Friction

30% reduction

Up to 30% of OT cyber risk is directly addressable through secure remote access and defensible architecture.

— Dragos, 2025 OT Cybersecurity Financial Risk Report

DISPEL WITH TENABLE ONE OT EXPOSURE

Device risk scores, VPRs, and criticality ratings flow into every access decision — so security prioritizes patching by how often a vulnerable device is actually accessed, not just its VPR score.

OPERATIONS TEAM

Efficiency Friction

$169,889/hr

Average cost of unplanned downtime. A vendor who can't connect for 30 minutes represents $60K in exposure — before anything goes wrong.

— ABB, Modernization for Resilience, 2025

DISPEL WITH TENABLE ONE OT EXPOSURE

Color-coded risk scores blend device risk with session risk, so operators get the vendor to the fix at the speed production demands — not the speed of a manual security review.

GRC TEAM

GRC Friction

$700K–1.2M/yr

Spent annually on audit readiness — staff time, not tooling. Evaluations that should take days take months.

— Dispel Compliance research, 2026

DISPEL WITH TENABLE ONE OT EXPOSURE

Every access tied to a Tenable One OT Exposure-flagged vulnerability builds its own evidence trail automatically — discovery to remediation, audit-ready without the manual hunt.

> "The security team has their PhD in cybersecurity. The operator in the field does not — and we shouldn't force that on them. Green user, green device? Easy yes. Red + red? That's a conversation before I approve anything.

THE COMMON LANGUAGE

One Score, Three Teams Can Act On

Session risk and device risk combine into a single, color-coded verdict at the moment of access, enabling security and operations to build a playbook — so the field operator makes the same call the security team would.

SESSION	DEVICE	
🟢	🟢	Standard approval
🟢	🔴	Proceed with caution
🔴	🟢	Verify identity
🔴	🔴	Enhanced security

AUDIT-READY, NOT BOLTED ON

Audit Readiness, Built In

Imagine telling your GRC team this story — one continuous evidence chain, from discovery to closure:

JAN 1	JAN 1	JAN 3	JAN 3	JAN 3	JAN 3
Tenable flags a critical vulnerability in a PLC.	Security and operations agree on a remediation plan.	Vendor technician requests access to patch it.	Admin approves a just-in-time window with session justification.	Technician connects through a recorded, disposable session — scoped ACLs only.	Tenable confirms the vulnerability closed. Evidence chain complete.
TENABLE	BOTH	DISPEL	DISPEL	DISPEL	TENABLE

THE OUTCOMES

The Value This Integration Delivers

Flexible Co-Deployment

Connect the two platforms in a ramp-up or staggered approach, wherever you are in your OT journey.

Unified Risk View

Tenable's device risk combined with Dispel's connection risk — one clear picture of exposure, every connection.

Common Language

Security and operations work from the same score, so the two teams pull together instead of against each other.

Audit-Ready, Out of the Box

An automatic audit trail that makes GRC teams audit-ready without extra process.

Together, Dispel and Tenable address the operational friction that security, operations, and GRC teams each face — with one integration. When friction disappears, the sanctioned path becomes the fastest path.