

# Dispel Launches OT Remote Access Compliance at Gartner® Security & Risk Summit 2026, Eliminating Six-Figure Audit Costs

*Continuous NERC CIP, NIST, and NIS2 audit evidence built into OT and CPS remote access — Dispel Compliance eliminates manual prep and six-figure readiness costs*



NATIONAL HARBOR, MD, UNITED

STATES, May 28, 2026 /EINPresswire.com/ -- Dispel, recognized as a Cool Vendor in the 2025 Gartner® Cool Vendors™ in Cyber-Physical Systems Security 2025. Today, the company announced the general availability of Dispel Compliance — a new Governance, Risk, and Compliance (GRC) capability within the [Dispel Zero Trust Engine](#) that delivers continuous, automated audit readiness for Operational Technology (OT) and ICS organizations.

Audit readiness is one of the largest hidden cost centers in industrial cybersecurity. For utilities, manufacturers, and energy operators, maintaining compliance under frameworks like NERC CIP, NIST SP 800-53, IEC 62443, and EU NIS2 requires dedicated teams, manual evidence collection, and repeated screenshot-gathering every audit cycle. Average large cap industrial companies spend \$700,000 to \$1.2 million annually on these programs — cost that represents staff time, not tooling. That burden compounds with every new remote access tool added to the environment.

Compliance friction also stalls adoption. When an OT team wants to deploy a new zero trust remote access platform, their GRC organization requires proof the tool meets audit requirements before it goes into the factory. That evaluation has historically taken months. Dispel Compliance eliminates that burden entirely: the evidence is already built, structured, and ready to hand to an auditor on day one.

“OT organizations are spending millions of dollars proving something that should be automatic — that the tools they deploy are configured correctly and meet their audit requirements,” said Ethan Schmertzler, Co-CEO, Dispel. “Dispel Compliance makes that proof continuous and immediate. The months-long GRC evaluation period disappears. What remains is a real-time

view of compliance posture across your entire OT remote access program, always ready for your auditor.”

## The Industry’s First Inherited Controls Engine for OT Remote Access

Dispel Compliance is built on OSCAL 1.1.2 — the NIST Open Security Controls Assessment Language specification used by FedRAMP and federal audit platforms. The platform continuously evaluates its own implementation of each in-scope control against the customer’s live tenant configuration. The result is a current, timestamped inheritance claim that is ready for any audit — not assembled manually in the weeks before one.

Dispel Compliance addresses three friction points across the OT and ICS compliance lifecycle:

- Pre-deployment GRC approval: GRC teams receive an immediate, exportable assessment of the Dispel platform’s configuration against applicable frameworks, replacing months of manual evaluation with a same-day answer.
- Ongoing compliance maintenance: Real-time framework scoring surfaces misconfigured controls the moment they drift from baseline. A configuration impact simulator lets administrators preview how any setting change shifts inherited control coverage before making it.
- Audit evidence delivery: Timestamped evidence packages export as an OSCAL Component Definition — the standard artifact accepted by leading GRC platforms — alongside CSV and PDF executive summary formats for auditors still on spreadsheet-based workflows.

One evidence pipeline covers every active framework simultaneously. Organizations reporting under both NERC CIP and NIST SP 800-53 — or NIS2 and NIST CSF — draw from the same underlying evidence without maintaining separate workflows. For the EU NIS2 Directive, where no official ENISA OSCAL catalog yet exists, Dispel publishes its own first-party catalog derived directly from Implementing Regulation 2024/2690 and cross-walked to NIST 800-53 — a gap no other OT remote access vendor has addressed.

Supported frameworks at launch: NERC CIP, NIST SP 800-53 Rev 5, NIST CSF 2.0, EU NIS2, IEC 62443, and SANS ICS Critical Controls.

## Replacing Screenshots with Structured, Audit-Ready Evidence

No [OT or CPS secure remote access](#) vendor has offered native compliance automation at this depth. The prevailing approach remains manual: operators screenshot individual settings, populate auditor-provided Excel spreadsheets, and upload documentation to third-party audit platforms. A single NERC CIP audit cycle can require thousands of screenshots, with no automated mechanism to prove configurations were continuously maintained throughout the

audit period.

Because Dispel Compliance is embedded in the platform itself, every configuration state is captured automatically, every change is timestamped with full provenance, and the complete audit trail exports in a single structured package. Auditors receive verifiable OSCAL evidence, not unlinked screenshots. The capability is available across cloud and on-premises Dispel Zero Trust Engine deployments — including environments requiring on-premises OT secure remote access infrastructure under NERC CIP.

## Availability

Dispel Compliance is available now within the Dispel Zero Trust Engine. Dispel will be demonstrating Dispel Compliance live at the Gartner Security & Risk Management Summit 2026. Organizations can learn more, schedule a meeting at the event, or request a demo at [dispel.com/book](https://dispel.com/book).

## About the Gartner Security & Risk Management Summit

Gartner analysts will present the latest insights for security and risk management leaders at the Gartner Security & Risk Management Summits, taking place March 9-10 in Mumbai, March 16-17 in Sydney, June 1-3 in National Harbor, MD, July 22-24 in Tokyo, August 4-5 in Sao Paulo and September 22-24 in London. Follow news and updates from the conferences on X and LinkedIn using #GartnerSEC.

Gartner, Cool Vendors in Cyber-Physical Systems Security 2025, Katell Thielemann, 18 September 2025

GARTNER and COOL VENDORS are trademarks of Gartner, Inc. and/or its affiliates. Gartner does not endorse any company, vendor, product or service depicted in its publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner publications consist of the opinions of Gartner's business and technology insights organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this publication, including any warranties of merchantability or fitness for a particular purpose.

## 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, and OTFusion into a single platform built for industrial scale. Founded in 2015, Dispel protects over \$500 billion in manufactured goods annually and

secures access for 54 million utility users worldwide. Built for efficiency. Secure by design. Audit ready. Learn more at [dispel.com](https://dispel.com).

Mark Lennon

Dispel

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/915208272>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.