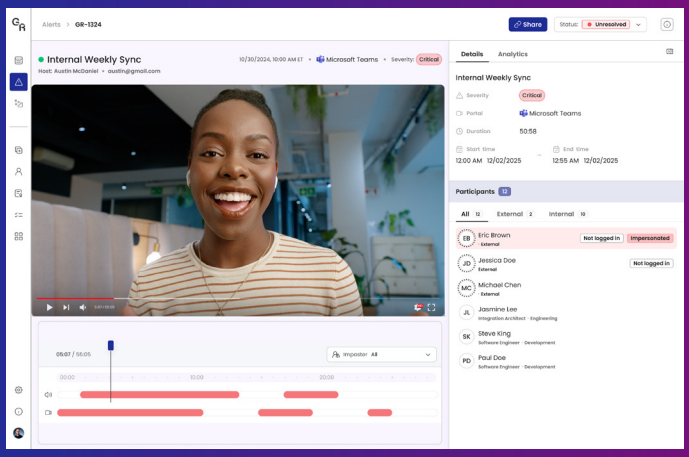
Solution Sheet

GetReal Protect

Real-Time Deepfake Protection

GetReal Protect



Stop real-time deepfake attacks with videoconferencing detection and response

Threat actors increasingly use real-time videoconferencing deepfakes to impersonate executives, vendors, job candidates, and employees, enabling financial fraud, insider access, and account takeover. As generative AI (GenAI) tools become more accessible and produce increasingly high quality, real-time deepfakes, the risk is growing.

IBM reports 16% of data breaches involved AI last year, and a third of those included deepfakes. Nearly half (41%) of U.S. organizations reported deepfake attacks targeting executives over a similar period, a 7% increase according to Ponemon Institute. Research also shows most people can't reliably distinguish real from fake faces any better than random chance.

Humans can no longer rely on their eyes and ears to know what's trustworthy. Protecting against deceptive and synthetic identities powered by malicious AI now requires technological controls.

Fast, accurate detection, however, is only a starting point. Effective real-time deepfake protection must:

- ➜ Enable investigation, response, and containment through integrations with your security and IT teams' existing workflows.
- ➜ Meet enterprise requirements for compliance, privacy, and security.
- ➜ Remove end-user friction with easy-to-add monitoring and configurable policy.

Highlights

- ➜ **Rapid Detection —** Flags manipulated videoconferencing streams in seconds
- ➜ **Evidence-Based Accuracy —** Trustworthy detection backed by proven digital forensics expertise
- ➜ **Frictionless Protection —** Automated monitoring without disrupting users
- ➜ **Enterprise-Ready:** Integrates with existing IT and Security workflows for investigation and response
- ➜ **"Blast Radius" Mapping —** Identity Threat Graph maps deceptive identities to reveal impact over time
- ➜ **Videoconferencing Attack Surface at a Glance —** View meeting coverage, internal vs. external participants, alerts, and trends

Easy-to-Use, Accurate Detection in Seconds

GetReal Protect's real-time detection goes beyond generic classifiers, extracting and alerting on forensic artifacts of AI manipulation within seconds. The technology is built by a world-renowned team of experts in digital forensics, image and signal processing, machine learning, OSINT, and threat research, led by digital forensics pioneer Dr. Hany Farid. Ongoing validation ensures detections you can trust that are accurate, explainable, and grounded in scientific rigor.

Enriched with Threat Intelligence

In addition to identifying forensic evidence of deceptive videoconference streams, GetReal Protect applies curated threat intelligence from the GetReal Security threat research team. This includes fraudulent remote worker identities, "default faces" packaged with deepfake creation tools, and other adversary tactics. This combination delivers more holistic protection against deepfakes and adversary methods employed in the wild.

Operationalize Deepfake Protection with a Policy Builder

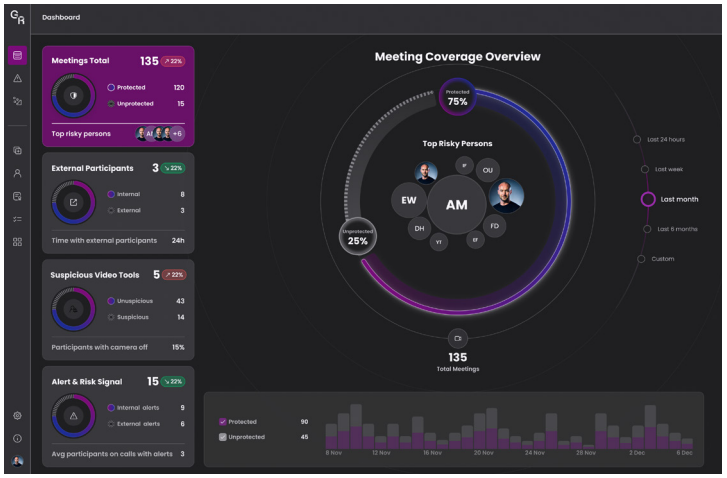
GetReal Protect makes response decisions simple and consistent with an intuitive policy builder. Enterprises can protect every videoconference or only those involving specific teams or users. Security can configure whether flagged participants require host action within the videoconferencing interface, are automatically ejected, or trigger meeting termination. The policy builder ensures enforcement follows corporate policy and is automated where appropriate, without leaving decisions to end users in the heat of the moment.

Map a Deepfake's "Blast Radius" with the Identity Threat Graph

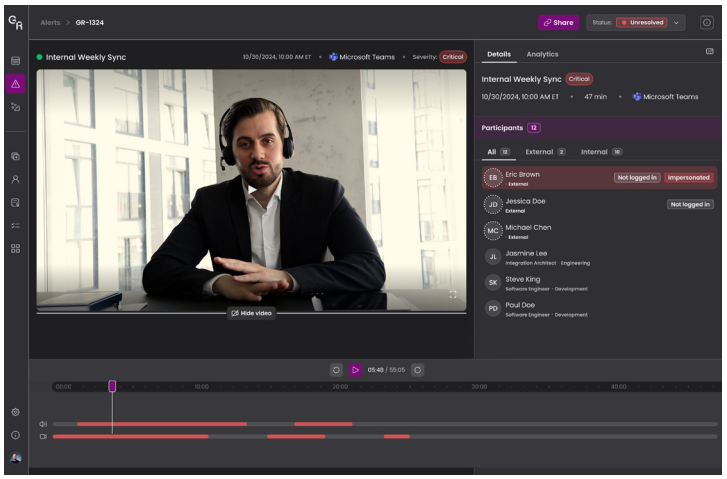
Deepfake detection alone isn't enough – your teams need context. The Identity Threat Graph maps flagged identities across virtual meetings and users, showing the full "blast radius" of any incidents and flagged identities. Analysts can see which employees interacted with a suspicious participant, impacted meetings, and drill into details by incident severity, timeframe, or affected users to accelerate investigation, response, and containment.

Visit the "Scene of the Crime"

Investigators can jump straight to the moment a deepfake was detected in a meeting, replay the exact segment, and zoom in on the flagged participant. Alert details include the evidence that triggered the detection, participants exposed, and a clear explanation of how and why the identity was determined to be deceptive.



See videoconferencing attack surface and risk exposure at a glance



As needed, dive deeper into alerts to review explainable evidence of a deepfake detection