Gartner®

Cybersecurity Threat: Deepfake Identity Impersonation

Insights

- The use of generative-AI-created deepfakes has dramatically expanded the attack surface for identity impersonation and disinformation, threatening organizations with significant financial harm, reputational harm and many other types of harm. Cybersecurity leaders must think beyond just isolated deepfake detection tools to implement defense-in-depth strategies and cross-functional governance to maintain trust and operational integrity.
- By next year, attacks using AI-generated deepfakes on face biometrics will mean that 40% of enterprises will no longer consider such identity verification and authentication solutions to be sufficient in isolation.
- The primary way that deepfakes can be used against organizations is as part of identity impersonation attacks against biometric systems or in social engineering attacks on employees such as recruiters or finance teams (see Figure 1).

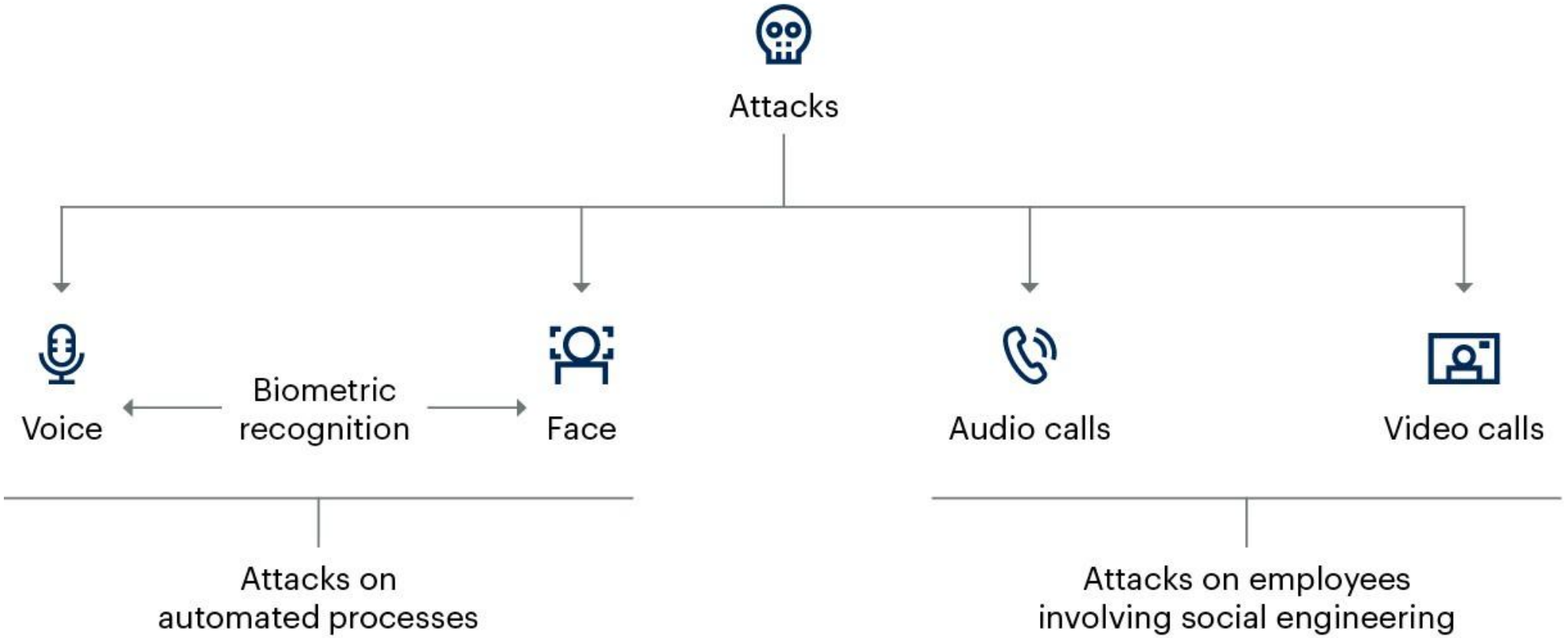
Key Insights and Data Points

- 41% of organizations have experienced an attack involving a deepfake and social engineering on an audio call.
- There has been a surge in reports of operatives from sanctioned countries such as North Korea applying for remote roles at organizations, which in many instances has included using deepfakes while on interview calls.
- The deepfake detection vendor landscape is rapidly expanding, but there is a lack of standards or benchmarks for assessing their accuracy.

Recommendations

- Recognize the limitation of relying on deepfake detection technology alone as a control due to the pace of innovation in deepfake creation and limitations in how to assess detection accuracy.
- Use layers of controls across the different use cases where deepfakes present a risk, augmenting deepfake detection with contextual signals, additional authentication factors and checks on content provenance.
- Form cross-functional trust councils involving cybersecurity, IT, communications, marketing, legal, and risk leaders to manage deepfake-driven identity impersonation, disinformation security strategy, and, if necessary, crisis response.

Figure 1: Attack Vectors for Deepfake Identity Impersonation



Actionable, objective insights

Position your organization for success. Explore these additional complimentary resources and tools for digital workplace leaders:

Conferences

Gartner Cybersecurity & Risk Management Summit

Secure your organization in the face of increasingly complex and evolving cyberthreats.

View Calendar

How We Help

Gartner for Chief Information Security Officers

Accelerate outcomes with AI-powered tools, on-demand insights and interactive experiences.

Explore Now

Tool

AI Controls Assessment

Assess your AI governance against leading frameworks and benchmark maturity against peers.

Learn More

Insights

Quarterly Insights for Cybersecurity Leaders

View the most utilized resources among cybersecurity leaders in 3Q26.

Learn More

Already a client? Get access to even more resources in your client portal. Log In ↗

Gartner®

Connect with us

Get actionable, objective business and technology insights that drive smarter decisions and stronger performance on your mission-critical priorities.

U.S.: 1 855 322 5484
International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for Digital Workplace Leaders
gartner.com/en/cybersecurity

Stay connected to the latest insights

Attend a Gartner conference
View Conference

Gartner