Pindrop

REPORT

The Deepfake Readiness Index

How enterprise security leaders think about their own deepfake defenses

74%

of security leaders report deepfake attacks, but **only 10%** have tools built to catch them.

Deepfakes are not just a nuisance or an isolated issue for hiring or PR teams. Deepfakes are squarely a security issue, one that can **lead directly to data theft and intrusion.**

Most companies have already adopted tools that model Zero Trust, embedding verification across their network and systems. Yet deepfakes evade those controls; they can pose a risk to every virtual business interaction: phone calls into your helpdesk, remote job interviews, and sensitive video meetings with executives. Until companies treat deepfakes like the serious enterprise threat they are, most will remain vulnerable.

Pindrop surveyed 250 U.S. security leaders at enterprise companies to find out exactly how unprepared companies are.

1 in 4

affected organizations lost $1 million or more to a single deepfake incident.

74%

believe deepfake defenses will improve faster than attack quality.

3 in 4

leaders say it will take a company leader being fooled or impersonated to make this a boardroom priority.

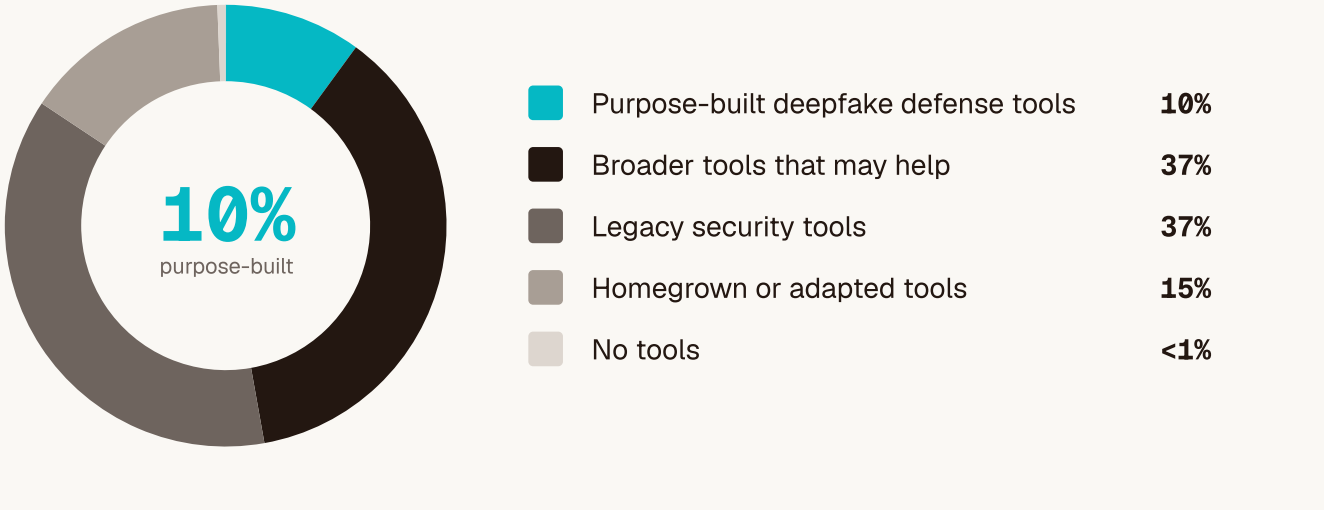
37%

believe one successful attack could put a company like theirs out of business.

FINDING 1

More than 1 in 3 enterprises are fighting deepfakes with obsolete, legacy defenses

Most security leaders (93%) report that they're at least somewhat concerned about deepfake attacks, yet their organizations aren't rolling out tools that directly address this concern.



Legacy security tools are no match for the scale and sophistication of today's deepfake attacks, largely because attacks are happening in channels that these tools weren't designed to defend.

Real-time communication channels have become a prime target for deepfake and AI-backed impersonation attacks. Without a way to evaluate whether the person on a video meeting or phone call is real, organizations are flying into a danger zone with zero visibility—and attackers know it.

In February 2026, Pindrop reported on this spike in AI attacks. At that time, among the Pindrop customer base, from Q4 2024 to Q4 2025, AI attacks had jumped by **1210%**. Just three months later, that number was **1390%**. And by the end of June 2026, the growth had reached **1680%**. Compared to traditional attack types, AI attacks are **growing 8x faster**.[1]

Deepfake detection point-solutions may seem like a promising answer to the crisis. But a point solution is not a long-term solve. AI has created a **foundational identity and trust question** that requires an equally foundational change in the security strategy for real-time channels. Those channels have now become identity checkpoints—checkpoints where we can't trust our eyes and ears. That's exactly why a new layer of defense is needed, one that extends continuous, real-time verification to these vulnerable channels.

The survey also revealed a startling tension. **While only a fraction of leaders have invested in purpose-built tools, 74% believe that defenses will improve faster than attack quality.** That's a contradiction; most respondents are at least somewhat concerned, only 10% have invested in a solution, yet three-quarters are optimistic.

PINDROP POV

It's possible this is a prioritization problem. While there's real exposure, and respondents know sophisticated tools exist, this attack surface just isn't prioritized in the boardroom yet.

But for those who prioritized, understood the exposure, and advocated for purpose-built defenses, **52% report a strong return on investment.**

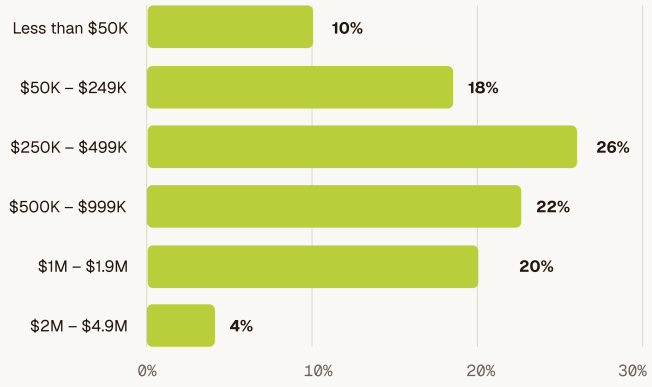
> "For thousands of years, trust was based on perception, recognizing someone's voice or seeing someone face-to-face. We're now in an age where **trust can be synthesized**. AI has changed what we think of as proof."
>
> **Ajit Gaddam**
> Head of Fraud, Financial Crimes, and Trust Systems, *HealthEquity*

FINDING 2

A single deepfake can be a million-dollar security failure

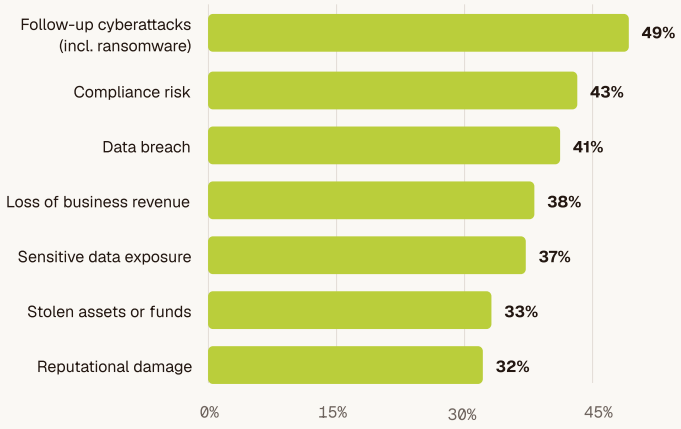
When a deepfake attack lands, the financial exposure is significant. Among organizations that experienced or suspected a deepfake attack, **almost half reported total costs of $500,000 or more**. Approximately 25% crossed the $1 million threshold.

Total cost of attack



Includes direct losses, remediation, and staff time.

Consequences that followed



% of affected organizations reporting each consequence

What came next only added to the damage. **49% of affected organizations faced follow-on cyberattacks,** like ransomware, a particularly troubling trend given the potential impact.

In May 2026, the FBI published an alert on The Silent Ransom Group (SRG), which targets companies, particularly law firms, using social engineering. In some cases, SRG impersonates an IT professional and manipulates an employee into granting remote desktop access. From there, the group exfiltrates data and extorts the organization.

The consequences can be severe: data exfiltration, network intrusion, ransom payouts, and operational disruption. After hackers impersonated an employee on a call with MGM's IT helpdesk, they launched a ransomware attack that disrupted operations for days. MGM projected a $100 million hit to quarterly earnings.

When costly attacks are hitting channels once considered protected, it becomes difficult to know where to focus.

> "No one wants to buy insurance to use it, but you want to have it at your disposal when the time comes."
>
> **Doug Innocenti**
> CISO, MoonPay

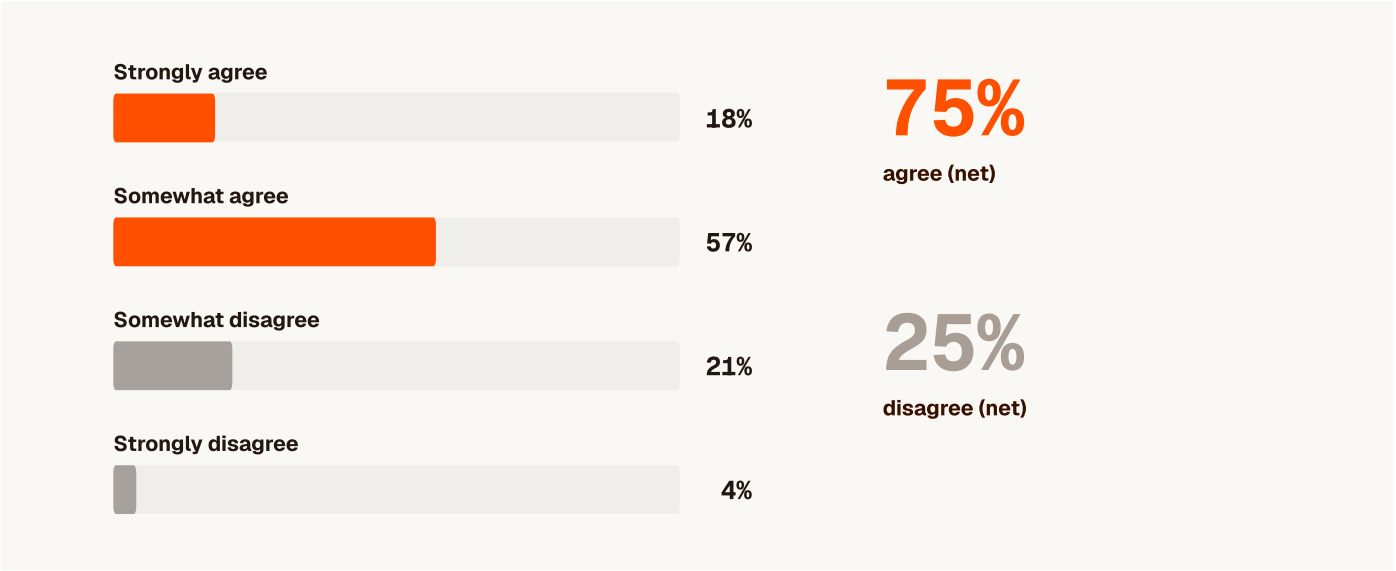
In May 2026, Pindrop published a report based on findings from the CISO Deepfake Defense Council, a group of security executives from seven Fortune 500 enterprises and other leading organizations. The Council is focused on delivering strategic guidance to help enterprises understand, prepare for, and defend against deepfakes—one of the fastest-emerging threats to trust and identity.

Of the six AI attacks impacting real-time channels, council members mapped six based on reputational and financial risk. Three of those attacks (fake job candidates, IT helpdesk attacks, and executive impersonation) landed as catastrophic or critical threats, reflecting high risk to both finances and reputation.[2]

That's why the missing detection layer matters. The financial and reputational exposure from a deepfake attack can compound if it goes undetected. If security leaders understand the problem and know that the implications can be severe, why is the adoption of purpose-built tools so low?

FINDING 3

Deepfakes won't become a boardroom priority until it hits an executive



75% of security leaders agree it will take a leader at their organization being personally fooled or impersonated before deepfakes become a genuine boardroom priority. That's **3 out of 4 security professionals,** people who understand the threat most clearly, who don't believe their leadership teams will act until the threat hits home.

It's possible boardrooms still view deepfakes as a public figure or celebrity issue, one defined by manipulated videos on social media that spread like wildfire and make headlines. That framing made it easy for leadership teams to file deepfakes under "reputational risk for high-profile individuals" rather than "persistent enterprise security threat requiring infrastructure investment." It's true that incidents that make the news are dramatic and visible. It's also true that companies face impacts far beyond just reputation—they can face data theft and system intrusion.

PINDROP POV

Deepfakes are simply today's identity attacks, and need to be treated as such. This means recognizing that the live communication channel is a gap in an otherwise Zero Trust stack, and closing that gap requires the same commitment organizations brought to endpoint protection, cloud security, and identity management.

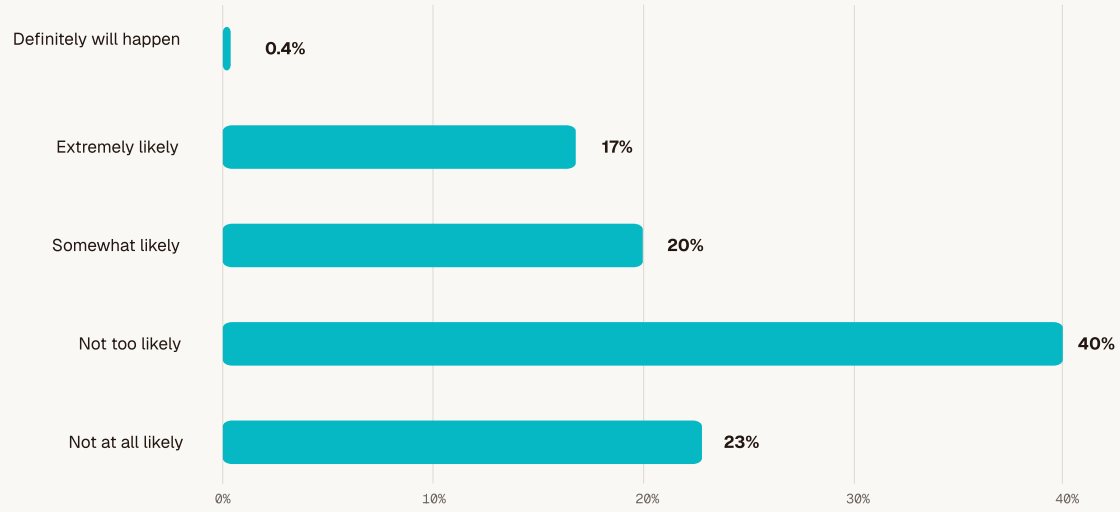
The next step is getting the board and higher-level leadership to understand the risk in terms they already use: a threat that is active, financially significant, and getting more sophisticated faster than the defenses already in place.

> "The security leaders prioritizing deepfake detection today are the only ones who'll have a real answer when their board starts to ask questions."
>
> **Jim Routh**
> Chairman of The CISO Deepfake Defense Council and former 6X CSO/CISO in financial services and healthcare

FINDING 4

More than a third of leaders think deepfakes are a threat to a company's survival

"How likely do you think it is that the damage caused by a single deepfake attack could cause a company like yours to go out of business?"



37% of security leaders consider it at least somewhat likely that a single deepfake attack could put a company like theirs out of business, including 17% who consider it extremely likely or certain.

PINDROP POV

These are the people inside organizations who have seen the attack surface up close, who understand what a successful synthetic identity attack means, and who are responsible for the defenses meant to stop it. When they describe a threat as potentially company-ending, it's time to act urgently.

Deepfakes are an identity attack that exploits how your organization verifies trust in human communication. This attack can touch **every function in your business**: finance authorizing a wire transfer, IT resetting credentials, an executive making a decision based on a voice they recognized. And the impact of a single successful attack isn't contained to one system or one team.

With 90% of security leaders without real-time detection tools and **AI attacks growing 8x faster than traditional tactics**, attempts are inevitable. But exposure is not.

Security leaders have solved complex security challenges before. Now organizations must enable risk detection at the exact moment their enterprise needs it.

CONCLUSION

Pindrop: your deepfake detection partner

AI has introduced doubt into every real-time communication, which has left many security leaders at a crossroads: do you patch your current tech stack or do you rethink your identity strategy entirely?

Since 2010, Pindrop technology has defended Fortune 500 companies and their customers against voice fraud, identity attacks, and social engineering, including 14 of the top 20 banks and 5 of the top 7 insurers. Across more than 8 billion analyzed interactions, we became experts in fraud and attack tactics.

That experience put us in front of the next wave before it even had a name.

In 2025, our own hiring pipeline came under coordinated attack. Across open roles, 1 in 6 applicants showed signs of fraud. One in 343 was linked to activity affiliated with the Democratic People's Republic of Korea (DPRK). Of those, 1 in 4 used a deepfake during a live interview.

It confirmed what the data from our enterprise customers already indicated: bad actors had moved beyond calls. The same tactics, impersonation, synthetic identity, social engineering, were now running across video meetings, job interviews, and IT helpdesk requests.

Pindrop technology is built on three trust engines: synthetic detection, risk analysis, and authentication. Pindrop Pulse® for Meetings brings together all three in real time, verifying voice and video in virtual meetings.

So your organization has the trust it needs, the moment it needs it.

Assess where you stack up against your peers

TAKE THE ASSESSMENT → TALK TO A REAL HUMAN →

Methodology

The Pindrop Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 250 US Security Leaders at organizations with a minimum of 1,000 employees), between June 11th and June 22nd, 2026, using an email invitation and an online survey. Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 6.2 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

Sources

[1] Based on Pindrop customer data analysis from Q2 2026 in comparison to the previous six quarters.

[2] Compiled based on five anonymous mapping exercises with security leaders from the CISO Deepfake Defense Council.