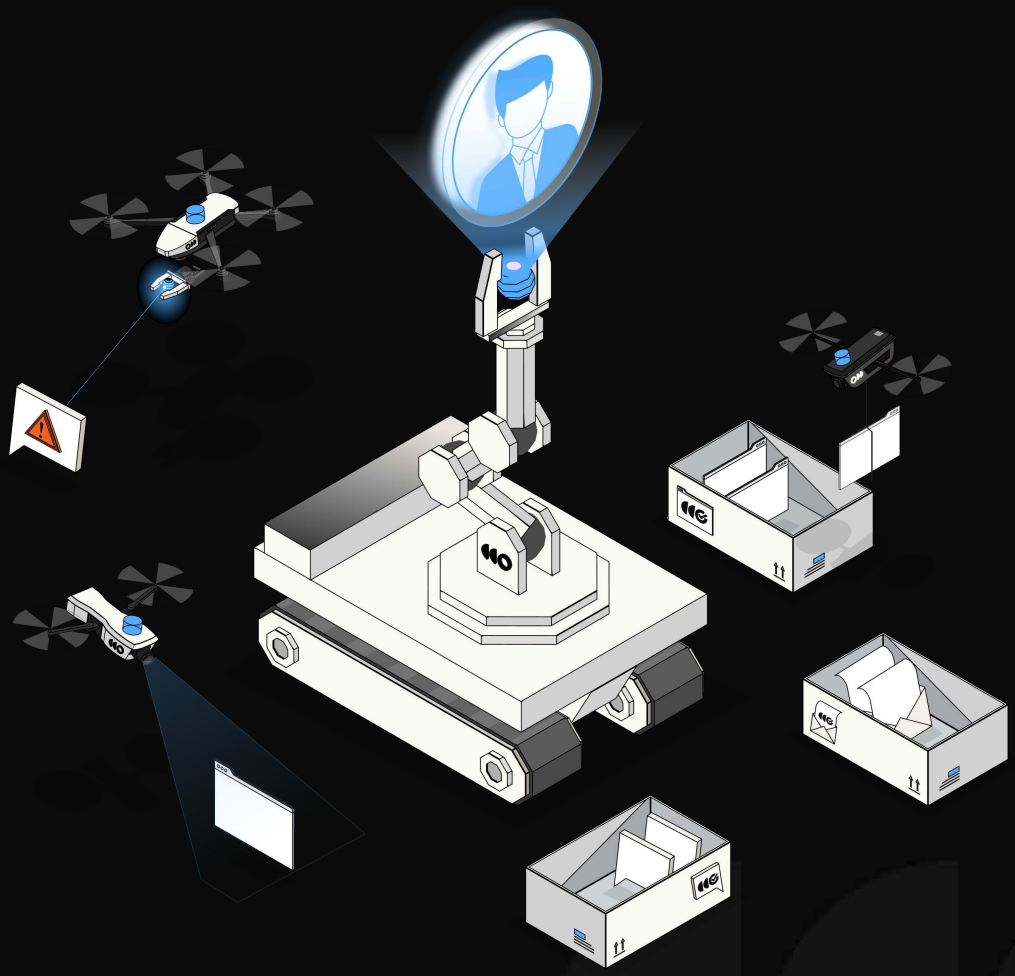
outtake labs

OUTTAKE LABS REPORT

The 2026 State of Executive Impersonation.

The industry's first report detailing where, how, and why executives are getting impersonated online.



Powered by the Outtake Digital Trust Reservoir and public industry sources. · June 2026.

EXECUTIVE SUMMARY

What the data shows

AI made it easy to impersonate the people you trust most.

01

Most attacks hit social platforms.

More than half show up on social platforms, so that's where coverage matters most.

02

No two executives are targeted alike

Attacks hit a few leaders hardest, and the pattern differs for each, so generic protection misses.

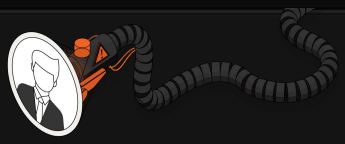
03

Manual takedown can't keep up

AI lets attackers launch impersonations in minutes, far faster than a manual team can respond.

> “I am very nervous that we have a significant impending fraud crisis.”
>
> SAM ALTMAN, OPENAI CEO. FEDERAL RESERVE BANKING CONFERENCE, JULY 22, 2025.

53%



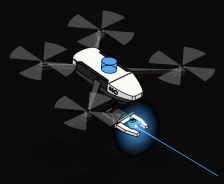
of organizations had an executive or employee impersonated.

OUTTAKE 2026 DIGITAL RISK REPORT

METHOD NOTE: 270 NAMED EXECUTIVES AT ENTERPRISE CUSTOMERS · 43,035 EXECUTIVE-IMPERSONATION ALERTS

SOURCE: OUTTAKE DIGITAL TRUST RESERVOIR; FBI IC3.

METHODOLOGY



How we counted

Three angles on the data, including our own platform, for the full picture.

01 Public industry data

FBI IC3 · FTC · SEC · DOJ

Macro shape of fraud and prosecuted cases. High credibility, low resolution.

02 Third-party research

VERIZON DBIR · ITRC · PRC

Method-level visibility on breach and broker exposure trends.

DBIR

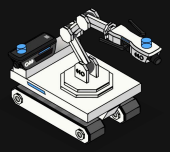
ITRC IDENTITY THEFT RESOURCE CENTER

PRC GLOBAL MARKET RESEARCH

03 Outtake Digital Trust Reservoir

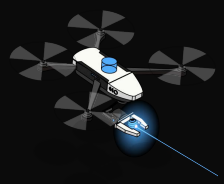
EXECUTIVE SAMPLE DATA

What our platform observed across the executives we monitor and protect.



outtake

FINDING 01 · OUTTAKE OBSERVATIONS



What we see

From the executives Outtake actively monitors and protects.

SAMPLE OF EXECUTIVES MONITORED

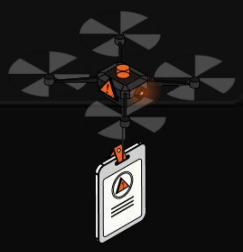
270

IMPERSONATION ALERTS IN THIS SAMPLE, 2025-2026

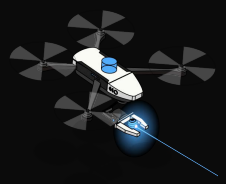
43,035

WHY IT MATTERS

Attackers use AI to skip your internal security tools completely. There's less need to break through data, network, cloud and endpoint security perimeters, when adversaries can just impersonate an executive out on the open internet, where those tools don't watch. They target your most visible leaders on purpose, because a trusted name gets them to the money faster than anything inside your network. And it lands on a handful of executives, not the whole team.



FINDING 02 · METHOD MIX



Where the threats land.

Four ways attackers come after an executive.

01

Fake profiles on social

Accounts posing as the executive on identity platforms, the most common type and highest in volume. Used for investment scams, fake giveaways, and impersonated DMs to your customers.

OUTTAKE DIGITAL TRUST RESERVOIR · FTC

02

Fake accounts on video platforms

Impersonator accounts and channels on video platforms, where one fake clip reaches a wide audience fast. Used to push crypto giveaways and fake endorsements in the executive's name.

OUTTAKE DIGITAL TRUST RESERVOIR

03

Spoofed executive domains

Domains and sites built to impersonate the executive or their office and appear completely legitimate. Used to send emails that look like they came from the executive.

OUTTAKE DIGITAL TRUST RESERVOIR · ITRC

04

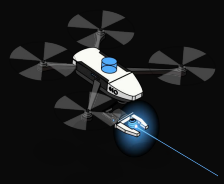
Open forum and broker exposure

Doxxing, chatter, and personal data on broker sites, the raw material attackers use to impersonate. Used as raw material for a later impersonation, fraud credential theft and blackmail.

PRC · ITRC UNITEDHEALTH 2025 PROXY

Outtake monitors and acts on all four.

SOURCES: OUTTAKE DIGITAL TRUST RESERVOIR, FBI IC3, PRIVACY RIGHTS CLEARINGHOUSE, ITRC, FTC.



FINDING 03 · SURFACE CONCENTRATION

Half the attacks hit social media.

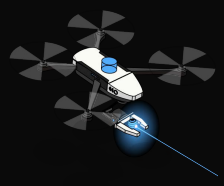
53.83% of executive impersonation alerts stem from social media.

SURFACE CATEGORY	ALERTS	SHARE
Fake profiles (social media)	23,168	53.83%
Fake accounts on video platforms	15,089	35.05%
Open community forums	2,943	6.84%
Executive lookalike domains	1,537	3.57%
News	265	0.62%

CASE STUDY: PERSHING SQUARE

Outtake scanned 11,000+ social profiles for Pershing Square and eliminated 400+ executive impersonations targeting Bill Ackman and the firm.

FINDING 04 · THE PER-EXECUTIVE SHAPE



Every executive is targeted differently

According to our data, no two executives looked the same.

CONCENTRATED

One surface, high volume.

Nearly all the volume lands on one surface, usually fake profiles on social. One problem, one place to watch.

DISTRIBUTED

Four or five surfaces at once.

The volume spreads thin across social, domains, ads, forums, and broker sites, so no single one looks urgent on its own, but together they add up.

Match protection to each executive

Targeting is uneven and it moves. You can't know in advance who gets hit, so you watch everyone and go deep where the attacks land.

IF CONCENTRATED

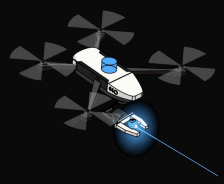
Go deep on the one surface taking the hits. Continuous monitoring and fast takedown there, since spreading effort thin elsewhere is wasted.

IF DISTRIBUTED

Go wide. Cover social, domains, ads, forums, and broker sites together, because no single one looks urgent on its own but the total does.

IMPLICATION

Look at each executive's profile first, then match their coverage to it.



FINDING 05 · SURFACE X ROLE

Each attack type hunts a different leader.

Different attacks tend to hit different people, so where an attack shows up tells you which executive is most exposed.

WHERE THE THREAT LANDS		WHO IT EXPOSES
Fake profiles on social	→	Founders, public-facing CEOs and employees
Fake accounts on video platforms	→	Public spokespeople and founders
Open community forums	→	Board chairs and execs in active matters
Executive lookalike domains	→	Spoofed exec email, financial services, IR leaders
News	→	Public-company executives

FINDING 06 · THE SPEED GAP

Closing the speed gap is extremely critical.

An impersonation goes live in minutes, but legacy DRP takes days to respond, and the damage happens in between.

THE LIVE WINDOW

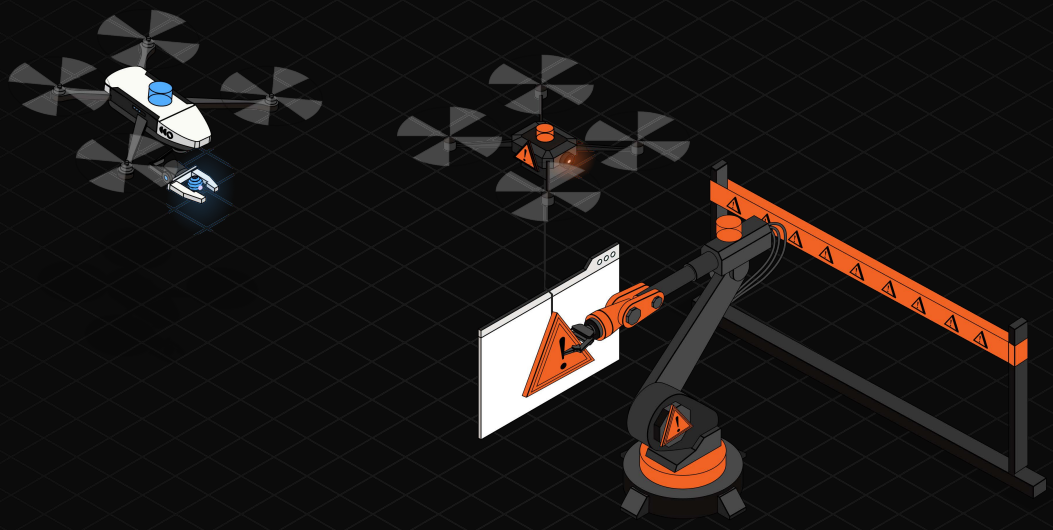
Every impersonation has a live window, the time between when it goes up and when it comes down. While it's up, it does damage: it DMs your customers, asks for wire transfers, and poses to your board. The attacker doesn't need the fake to last forever, just long enough.

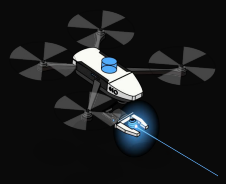
WHAT NEXT-GEN DRP DOES

Next-Gen DRP turns one alert into the whole picture. It maps the full network behind the impersonation, not just the single account, and takes it down as one automated loop, dropping the live window from days to minutes.

RECOMMENDATION

Pick the vendor that finds the whole campaign, takes it down, and proves it gone. Fast.





FINDING 07 · THE MODEL GAP

More reviewers will never close this speed gap.

Each fake costs the attacker almost nothing and costs you hours of human review.

01

The math runs against you

Each fake costs the attacker almost nothing to make, but every one still costs you time to review, so the gap widens on its own.

02

More people doesn't scale

Hiring a reviewer gives you one more set of hands, but nothing they learn makes the next fake any faster to catch.

03

A team can only watch so much

A team can only watch so many places at once, and the attacks hit all of them at the same time.

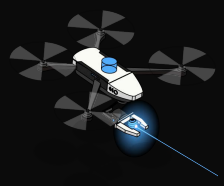
04

Ask to see it work live

Real automation shows takedowns happening live, while a queue and a delay means people are still doing it by hand.

THE GAP

This isn't about working harder. It's about how the system is built. Next-Gen DRP keeps up because automation does the work and gets sharper over time. The question isn't how big your team is. It's whether the system improves on its own.



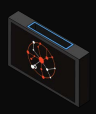
Critical steps to better protect Executives against impersonation

Stop being reactive to impersonation attacks. Get ahead of them.

01 

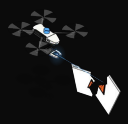
Know what you're protecting

Map every brand, person, location, and product you expose, and give each one a clear owner.

02 

Put coverage where the attacks are

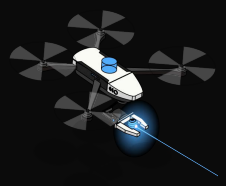
Most impersonation lands on social first, then video, then lookalike domains, so weight your coverage the same way.

03 

Make takedown a standing capability

Treat takedown as an ongoing process, not a one-time scramble. Track how fast you remove threats, and use each one to make the next removal faster.

SEE OUTTAKE IN ACTION



Protect the executive impersonation surface.

Next-Generation Digital Risk Protection. Continuous, role-aware defense that compounds, across every platform and every entity, in real time.

> APPLOVIN
>
> “Outtake delivered 120 imposter takedowns at 10x the speed of legacy DRP and accelerated threat reviews 3x.”
>
> JEREMIAH KUNG, GLOBAL HEAD OF INFORMATION SECURITY & COMPLIANCE, APPLOVIN

Book a Demo →

SOURCES & CITATIONS

01 FBI Internet Crime Complaint Center (IC3), 2024 Internet Crime Report

02 Federal Trade Commission Consumer Sentinel Network, 2024 Data Book

03 Verizon 2026 Data Breach Investigations Report

04 Privacy Rights Clearinghouse, 2025

05 Identity Theft Resource Center (ITRC), 2025 Annual Data Breach Report

06 UnitedHealth Group 2025 Proxy Statement

07 Wall Street Journal (Pershing Square Facebook impersonation, March 2024)

08 Outtake Digital Trust Reservoir, executive-impersonation alert dataset (n=43,035 / 270 executives)