iapp + feroot

The Global State of Privacy Compliance Across the Digital Experience Layer

Tuesday, June 30, 2026
08:00–09:00 PDT
11:00–12:00 EDT
17:00–18:00 CEST
19:00–20:00 CET

Welcomes and Introductions

MODERATOR

KPMG

Oskar Trpisovsky

Ontario & Atlantic Privacy & Data Protection Lead

MSc ETH · AIGP · CIPM · CIPP/C · CIPP/US · CIPP/E

Oskar leads KPMG's Privacy & Data Protection Practice across the Ontario and Atlantic regions, is part of KPMG's Global Trusted AI Privacy Leadership Team.

His expertise covers international program and project leadership, strategic advice as well as design and operationalization of target operating models. Oskar served over 50 different clients around the world and led multiple international programs in close collaboration with senior executives.

PANELIST

Reddit

Ian Wardell, J.D.

Senior Privacy and Risk Engineer — Security

J.D. · Privacy & Security Engineering

Ian works at the intersection of privacy law and security engineering at Reddit, one of the world's largest platforms, home to over 100,000 communities. He translates regulatory obligations across GDPR, CCPA, and state privacy laws into scalable technical controls, integrating privacy-by-design into the software development lifecycle. He bridges a legal background with hands-on engineering to close compliance gaps at scale.

PANELIST

Feroot Security

Ivan Tsarynny

CEO & Co-Founder

Ivan co-founded Feroot Security to address the compliance gaps that emerge at the digital experience layer. His research on TikTok data collection and DeepSeek's connection to China Mobile has been cited by the U.S. Congress and covered by major outlets. He testified before Congress on cybersecurity risks from foreign-linked applications. Ivan was recently featured on ABC News for research on Chinese humanoid robots and their threats to privacy and personal data protection. He has also been featured on Bloomberg, the Wall Street Journal, the Associated Press and Forbes.

About the Research

Censuswide conducted this study independently on behalf of Feroot Security in May 2026, surveying 800 privacy, legal, marketing, and IT professionals across four countries and five industries.

800+	4	5	Mid–Large
Respondents	**Countries**	**Industries**	**Enterprise Focus**
Privacy, Legal, Marketing & IT	US · UK · Canada · Australia	Financial Services, Healthcare, Retail, Technology, Media	Mid-size to large organizations

WHAT WE'LL COVER

1 Third-Party Script Landscape

2 CMP Confidence & Failures

3 Vendor Governance & Accountability

4 Regulatory Enforcement Reality

5 Resources, Maturity & Investment Outlook

SECTION 1

Third-Party Script Landscape

How many scripts are running — and who is in control?

Third-party tracking scripts are code snippets embedded into a website by an outside company to monitor, collect, and analyze visitor behavior across the internet.

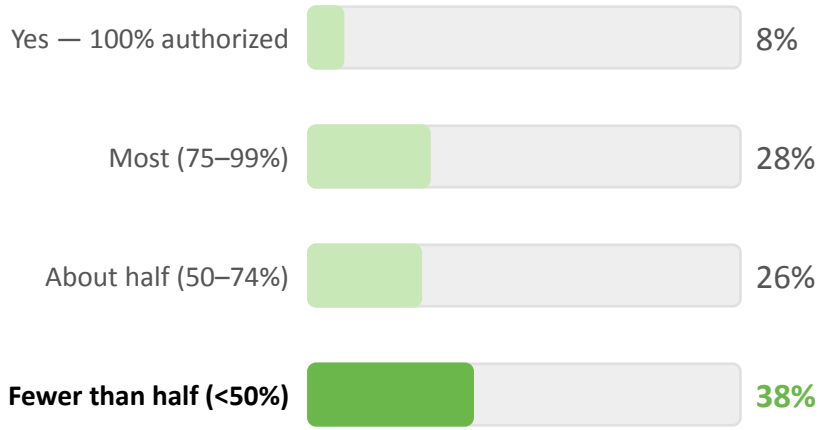
How Many Vendor Scripts Are Running on Your Websites?

Nearly every organization surveyed — 99.4% — runs at least one third-party script. The median operating environment is 11 to 50 scripts running simultaneously.

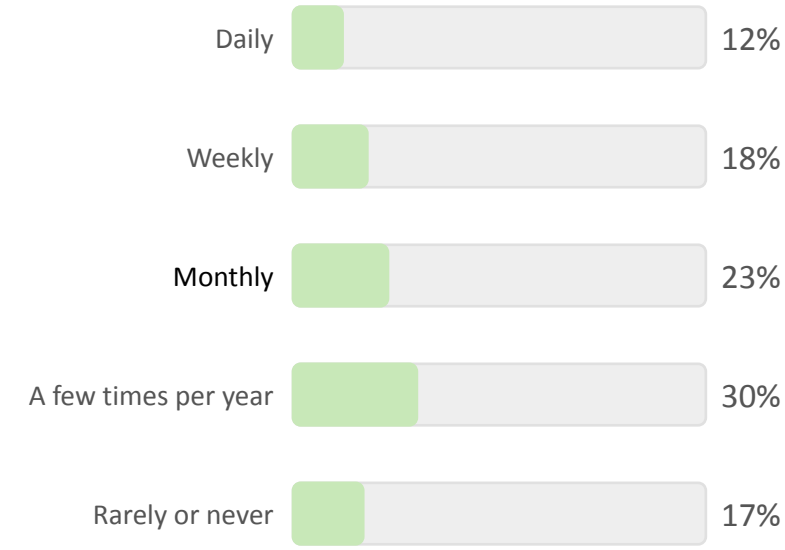
Source: Censuswide / Feroot Security — Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

Script Authorization & Unauthorized Discovery

Are all scripts on your website fully authorized?



How often are unauthorized scripts discovered?

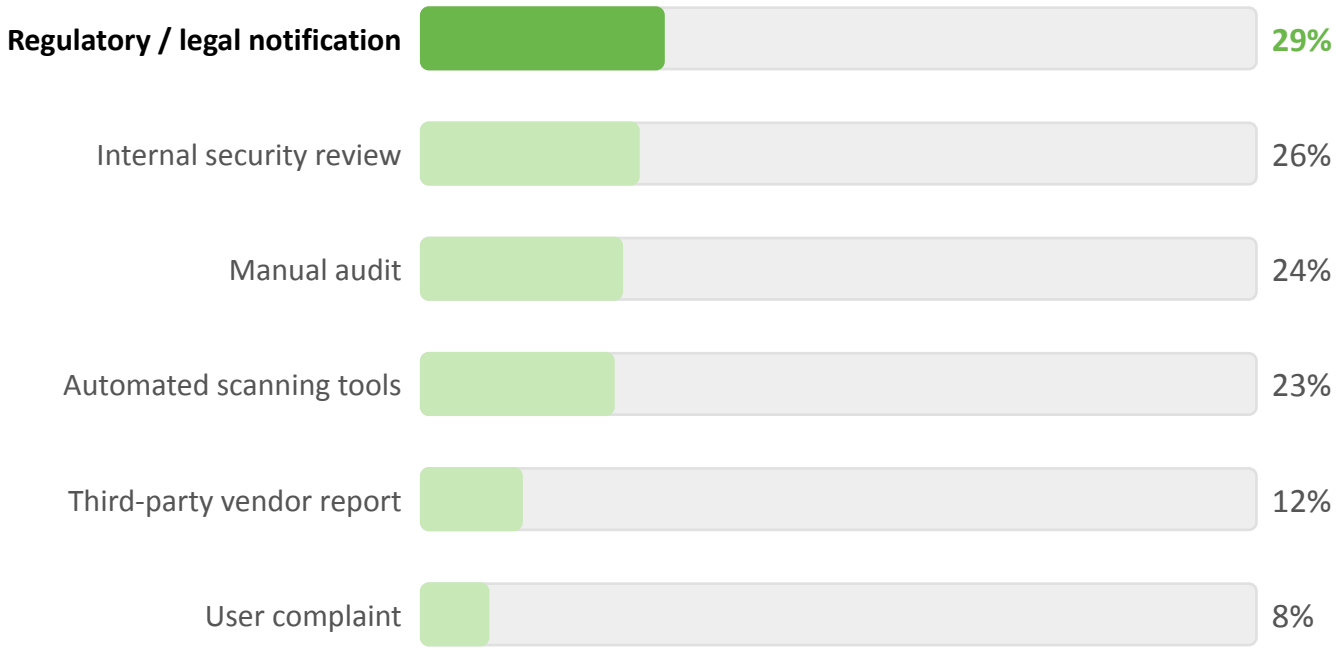


Only 8% believe all their scripts are fully authorized — 92% cannot account for all data collection activity on their properties. More than half (53%) discover unauthorized scripts monthly or more.

Source: Censuswide / Feroot Security — Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

How Are Unauthorized Scripts Typically Discovered?

The most common discovery method is regulatory or legal notification — meaning organizations learn of compliance failures through enforcement, not internal monitoring.



Fewer than 1 in 4

organizations use automated scanning for proactive detection

Source: Censuswide / Feroot Security — Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

AUDIENCE POLL

How many third-party vendor scripts are actively running on your website(s)?

A None or 1–10 scripts

B 11–50 scripts

C 51–100 scripts

D More than 100 scripts

Survey finding: 65.5% of organizations run 11–50 scripts · ~19% run more than 50

SECTION 2

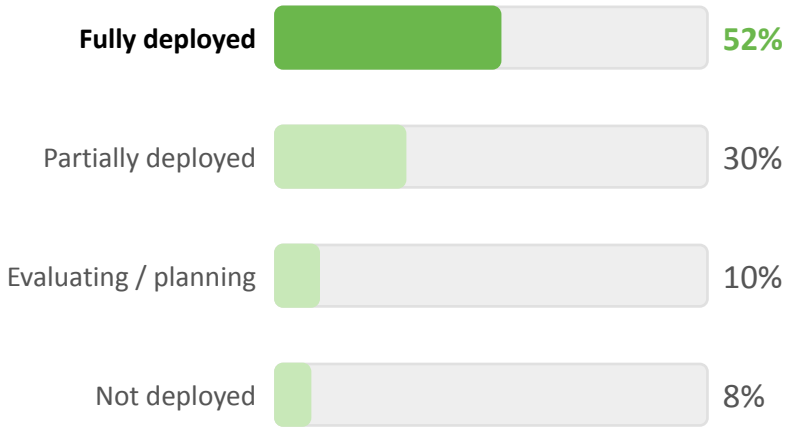
Consent Management Platform (CMP) Confidence & Failures

What happens after users make a consent choice?

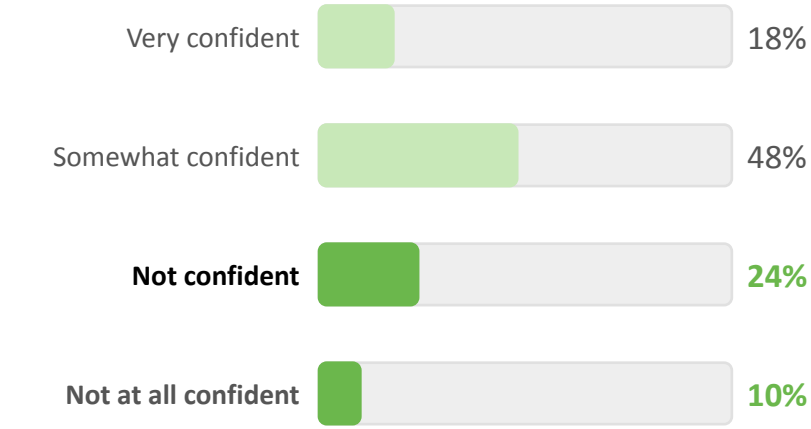
A Consent Management Platform (CMP) is more than just a technology solution; it is a combination of technology, governance, legal requirements, business processes, and user experience controls designed to collect, manage, enforce, and demonstrate user consent preferences across digital channels.

CMP Deployment vs. Confidence in Blocking

CMP deployment status



Confidence that CMP blocks all pre-consent scripts (among CMP users)



82% of organizations have a CMP deployed. Yet among those users, only 18% are very confident it is blocking all non-consented scripts. One in three CMP users actively lacks confidence their consent infrastructure is functioning correctly.

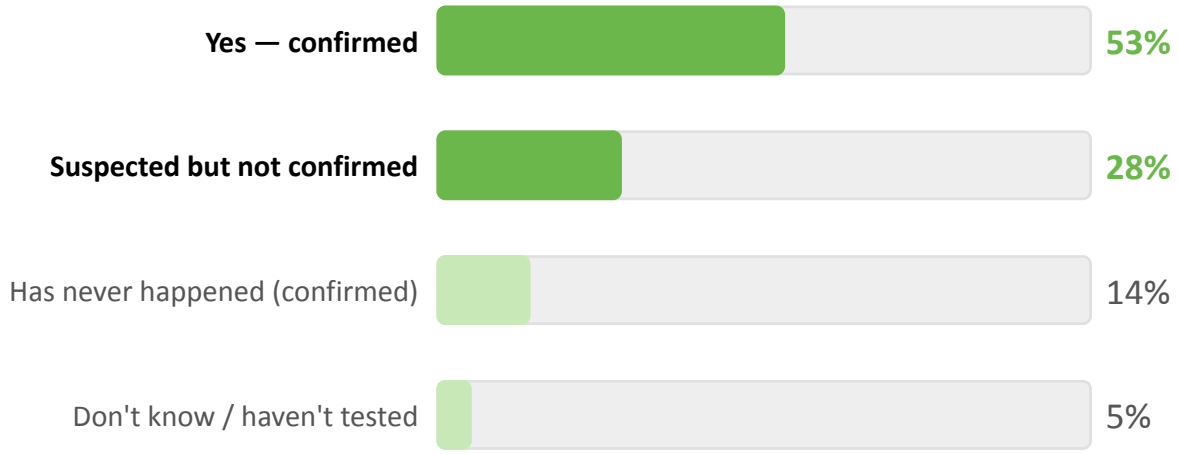
Source: Censuswide / Feroot Security — Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

Pre-Consent Script Firing — The Defining Statistic

81%

of CMP-deployed organizations have confirmed or suspected scripts firing before user consent was given

Among organizations with a CMP deployed:



These organizations did the right thing — they deployed a CMP. And their consent infrastructure still failed them. Only 14% can confirm pre-consent firing has never occurred. Deploying a CMP configures consent rules. It does not verify they work at runtime.

Source: Censuswide / Feroot Security — Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

AUDIENCE POLL

Has your organization experienced scripts firing before a user gives consent?

A Yes — we have confirmed this happened

B We suspect it but haven't confirmed

C No — we've tested and confirmed it hasn't

D We don't know / haven't tested for this

Survey finding: 53% confirmed · 28% suspected — 81% total have experienced or suspect pre-consent firing

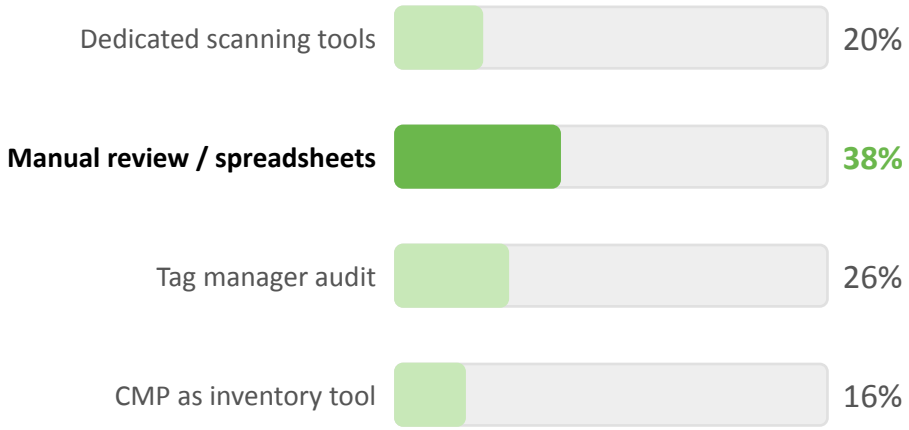
SECTION 3

Vendor Governance & Accountability

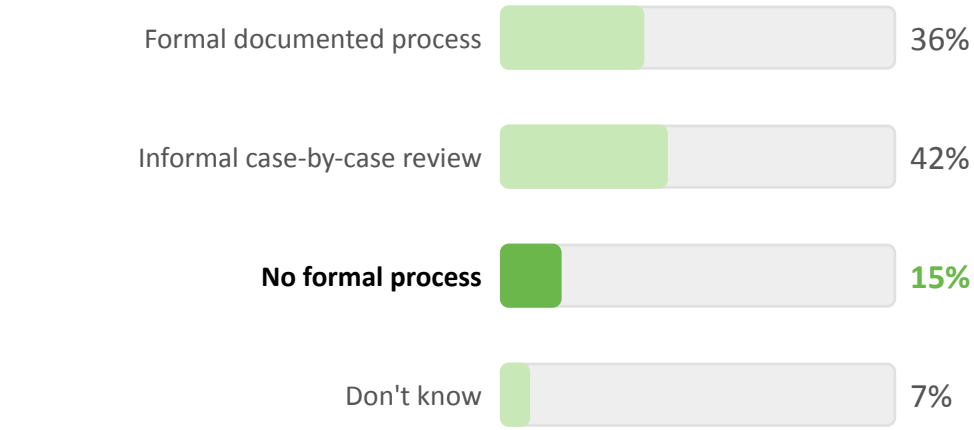
Who is adding scripts — and who is responsible when they change?

How Organizations Track and Vet Third-Party Scripts

Primary method for tracking active scripts



Vetting process for new third-party scripts

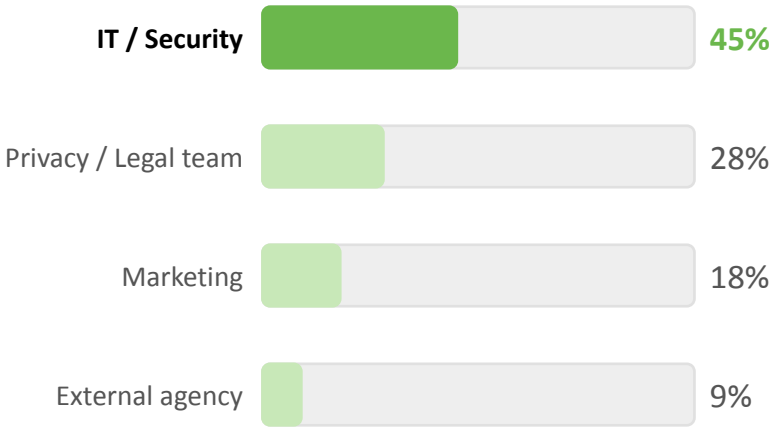


Only 1 in 5 organizations uses a dedicated scanning tool — most rely on manual reviews and spreadsheets. Only 36% have a formal documented vetting process. Informal methods cannot keep pace with the velocity of change in live digital environments.

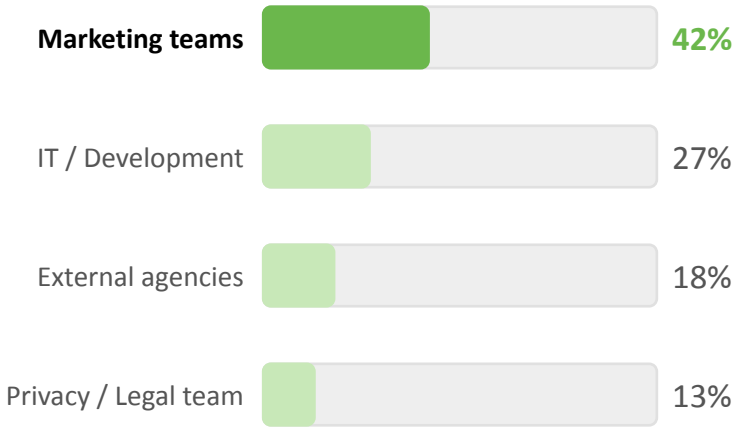
Source: Censuswide / Feroot Security — Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

The Governance Gap: Authority vs. Who Actually Adds Scripts

Who holds formal approval authority for new scripts?



Who most frequently adds new scripts in practice?



On paper, IT and Security hold script approval authority (~45%). In practice, Marketing is adding scripts — and external agencies add another layer. This misalignment between governance authority and operational reality is a primary driver of unauthorized script proliferation.

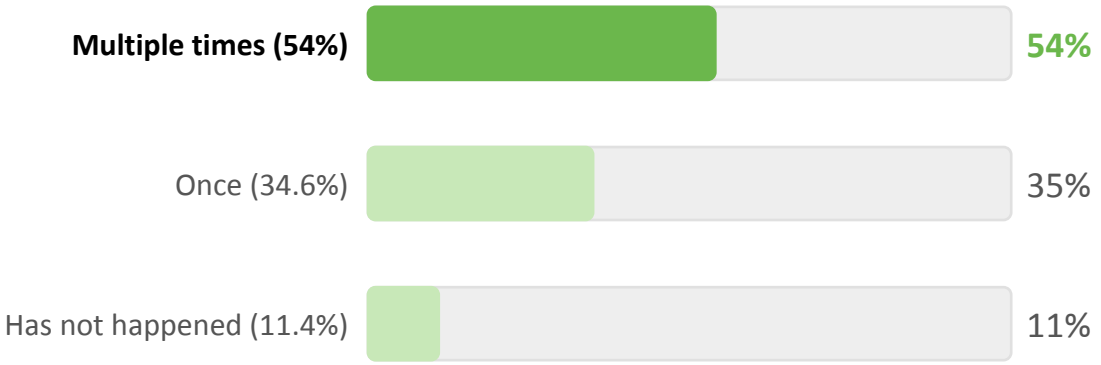
Source: Censuswide / Feroot Security — Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

Vendors Changing Data Collection Practices Without Notice

88.6%

of organizations have had a marketing vendor silently change their data collection practices without notifying the privacy team

How often did silent vendor changes occur?



If your compliance posture depends on vendor self-reporting, this data suggests you are operating on faith.

When a vendor updates their SDK or tag, data collection behavior can change silently — with no notification and no audit trail unless you are actively monitoring.

Source: Censuswide / Feroot Security — Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

AUDIENCE POLL

Has a marketing vendor ever changed their data collection practices without notifying your privacy team?

A Yes — it happened multiple times

B Yes — it happened once

C No — vendors always notify us

D We don't monitor for this

Survey finding: 88.6% experienced silent vendor changes · 54% say it happened multiple times

SECTION 4

Regulatory Enforcement Reality

What are the actual consequences, and how ready are organizations?

Regulatory Inquiries, Penalties & Audit Readiness

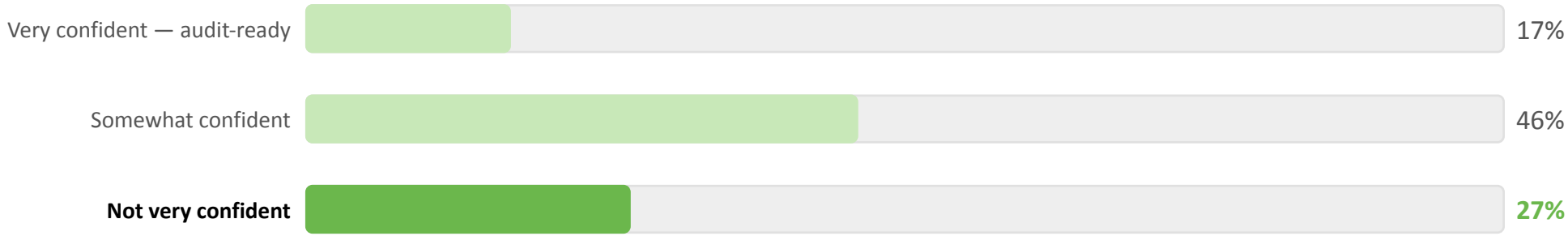
~50%

Received a regulatory inquiry related to website privacy compliance

~31%

Of all respondents have experienced a regulatory penalty or enforcement action

Audit Readiness: If a regulator came today, could you demonstrate compliance?



Approximately half of organizations surveyed have already received a regulatory inquiry related to website privacy compliance. Among those organizations, nearly two-thirds experienced a regulatory penalty or enforcement action, highlighting the growing enforcement focus on the Digital Experience Layer.

Source: Censuswide / Feroot Security — Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

AUDIENCE POLL

If regulators asked for evidence of consent compliance today, how confident would you be?

A Very confident — we are audit-ready

B Somewhat confident — we have most of what's needed

C Not very confident — we have significant gaps

D Not at all confident — we are not audit-ready

Survey finding: Only 17% are very confident · 37% are not confident or not at all confident

SECTION 5

Resources, Maturity & Investment Outlook

Where are teams today — and where are they heading?

Operational Burden and Compliance Maturity

57%

spend 11+ hours/week

on digital experience privacy — up year-over-year

75%

say time has increased

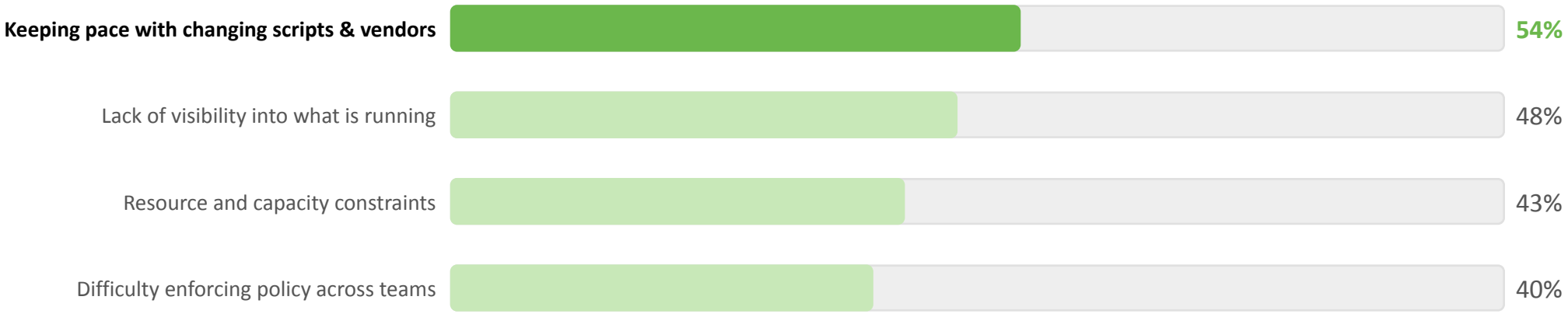
over the past 12 months

72%

describe their posture as primarily reactive

vs. only 6% fully proactive with real-time monitoring

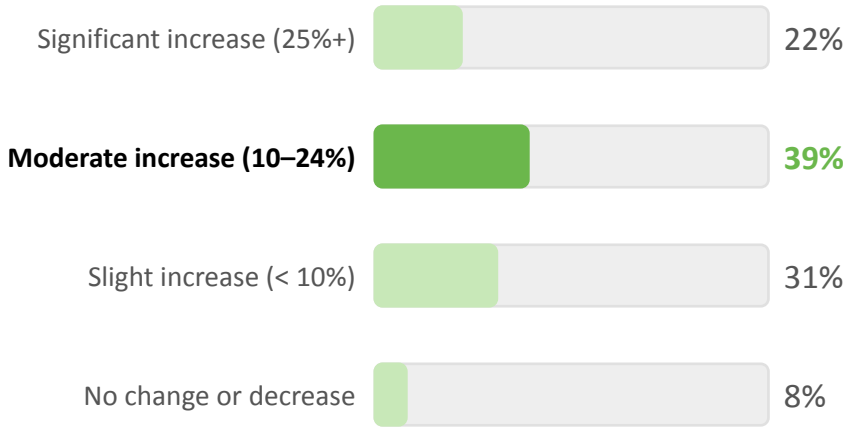
TOP CHALLENGES REPORTED



Source: Censuswide / Feroot Security — Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

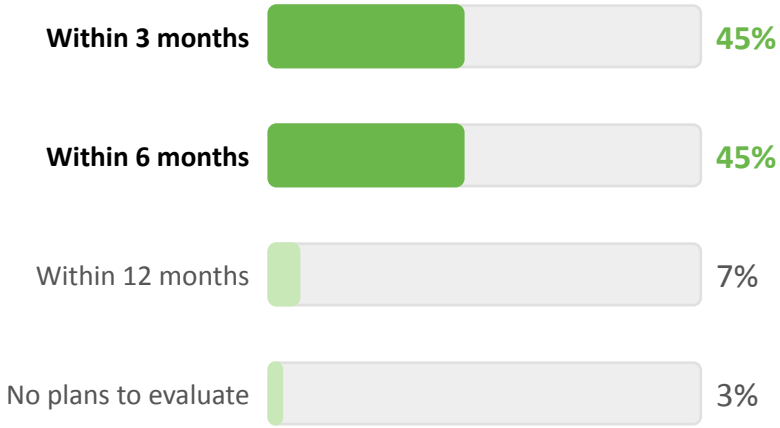
Investment Intentions and Automation Demand

Privacy investment plans over the next 12 months



92% plan to increase privacy investment over the next 12 months

Plans to evaluate digital experience privacy automation tools



97% plan to evaluate automation tools — 90% within 6 months

Source: Censuswide / Feroot Security — Survey of 800 Privacy, Legal, Marketing & IT Professionals, May 2026

Key Findings at a Glance

99.4% run at least one third-party script — median range is 11–50 simultaneously

88.6% have had a vendor silently change data collection practices without notice

92% cannot confirm all scripts on their digital properties are fully authorized

~31% of all respondents have experienced a regulatory penalty or enforcement action

81% of CMP users have experienced or suspected scripts firing before user consent

97% plan to evaluate digital experience privacy automation tools within 12 months

Questions and Answers

Oskar Trpisovsky

Moderator · KPMG

Ian Wardell, J.D.

Panelist · Reddit

Ivan Tsarynny

Panelist · Feroot Security

Submit your questions using the Q&A panel in the webinar platform.

DISCUSSION TOPICS

- Marketing teams as the primary source of unauthorized scripts — and their role in compliance
- Practical steps to improve script visibility without adding headcount
- How to validate that a CMP is actually working at runtime
- What audit-ready evidence looks like for digital experience privacy
- Evaluating automation tools — must-have capability criteria

Next Steps

Oskar Trpisovsky

Moderator · KPMG

Ian Wardell, J.D.

Panelist · Reddit

Ivan Tsarynny

Panelist · Feroot Security

Submit your questions using the Q&A panel in the webinar platform.

DISCUSSION TOPICS

- Marketing teams as the primary source of unauthorized scripts — and their role in compliance
- Practical steps to improve script visibility without adding headcount
- How to validate that a CMP is actually working at runtime
- What audit-ready evidence looks like for digital experience privacy
- Evaluating automation tools — must-have capability criteria

Free Digital Experience Privacy Consent Assessment

- ✓ Verify what's actually happening across your digital experience layer
- ✓ Understand your privacy risk posture relative to key global regulations
- ✓ Prioritize remediation with confidence
- ✓ Get results in less than 2 business days

feroot

feroot.com/dx-privacy-assessment

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ87I5

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form at iapp.org.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings, please contact:

livewebconteam@iapp.org

For more information: www.iapp.org

This webinar was brought to you by Feroot Security · feroot.com