



Schibsted Case Study

How Schibsted Media expanded mobile EDR coverage from 50 to 500 devices to better protect journalists working in the field and traveling abroad.

500
devices

2 week
deployment

10x
expansion



About:

Schibsted is one of Scandinavia's leading media companies, founded in Norway in 1839 by Christian Michael Schibsted. Following a strategic split in 2024, its news media operations became a standalone company under the ownership of its largest shareholder, the Tinius Trust, allowing Schibsted Media to focus exclusively on independent journalism across the Nordics.

Today, Schibsted Media publishes some of the region's most influential news brands, including VG, Aftenbladet, Aftenposten, and Svenska Dagbladet. As of early 2025, it was reported to be Norway's largest media house, reaching more than 2.6 million people daily and achieving 86% weekly digital coverage across the country.

Challenge:

Schibsted Media needed greater visibility into the security of mobile devices used for communication, authentication, research, and access to sensitive journalistic information. The organization wanted to better understand the security state of these endpoints, identify when a device required further investigation, and give its security and SOC teams greater insight into devices that were becoming increasingly important to journalists' daily work.

“Our journalists are often working in the field, so mobile devices are a critical part of how they communicate and do their jobs.”

Solution:

When Schibsted Media began evaluating the mobile security market, the team considered several potential solutions. From the beginning, privacy was an important part of the decision.

For an organization built around independent journalism, deploying a security solution to employee mobile devices required confidence not only in its security capabilities, but also in how it operated. Schibsted Media needed to understand what information the platform could access, how it worked, and where its capabilities and limitations began and ended.

iVerify stood out during the evaluation process because of its strong focus on privacy and the transparency of the technical conversations between the two teams.

“From the start, we were able to have deep technical conversations about what the tool did and did not do. The communication was transparent, and the team were able to answer all our questions.”

From an initial deployment to 10x greater coverage

Initial Deployment

50 devices

Implementation

Deployed through existing MDM infrastructure

Expansion ahead of 2026 FIFA World Cup

~500 devices protected

Results:

With iVerify Enterprise, Schibsted Media added a dedicated layer of mobile security visibility beyond the device management capabilities already in place. The platform gives Schibsted Media's security and SOC teams greater insight into the security of mobile endpoints used throughout the organization. For journalists working in the field, those devices are often central to communication and access, making visibility into their security state an important part of the organization's broader security program. That visibility helps the security team better understand risks affecting mobile devices and determine when an issue requires further investigation. Schibsted Media also has access to iVerify's incident response team, providing additional expertise when a potential incident requires deeper analysis or response support.

Greater Mobile Endpoint Visibility

Security and SOC teams can better understand the risks affecting mobile devices that were previously difficult to assess with existing tools alone.

Support for Further Investigation

When an issue requires additional attention, Schibsted Media can investigate further and draw on iVerify's incident response expertise when needed.

A Privacy-Conscious Approach

Schibsted Media gained greater mobile security visibility through an approach that aligned with the privacy requirements and sensitivities.

Bringing Mobile Security Into the Broader Security Conversation

One unexpected outcome of the deployment has been a broader shift in how mobile devices are viewed across Schibsted Media. Mobile security has become a more visible part of the organization's security conversation, helping teams and stakeholders recognize mobile devices as security-relevant endpoints rather than viewing them solely through the lens of device management.

That shift extends to end users. Employees have become more conscious of keeping their devices up to date and considering the sensitivity of the information they store and access through them. For journalists, that can include information about sources and access to privileged journalistic material. The result is greater awareness, across both security teams and employees, of the role mobile devices play in protecting sensitive work and information.