

# Ströer uncovers the most relevant external risk exposures - at scale

Maximum visibility across all portfolio companies, proactive intelligence for fast remediation and unified cybersecurity.

Source: blowUP.media GmbH

## The Challenge: eliminating external threats across all portfolio companies

Ströer is a leading German out-of-home advertiser and offers advertising customers individualized and fully integrated, end-to-end solutions along the entire marketing and sales value chain. Ströer is focusing on the strength of the OOH business with its "OOH+" strategy, supported by the 'Digital & Dialog Media' and 'DaaS & E-Commerce' segments. The Company has approximately 10,000 employees at over 100 locations. In fiscal year 2021, Ströer generated revenue of EUR 1.63b. Ströer SE & Co. KGaA is listed in Deutsche Börse's MDAX.

Tasked with creating a unified, healthy, and shared security culture across the entire group, Benjamin Bachmann, Head of Group Information Security Office, was initially seeking to gain total visibility into exposed external-facing assets across all portfolio companies - no easy feat due to the sheer size of each company in terms of known and unknown assets.

Benjamin and his team were evaluating different solutions, one for External Attack Surface Management (EASM), and one for mitigation. This changed during Cyberint's POV with Ströer, where the team realized the degree of visibility and actionable insights the solution delivered.



*"In the POV we realized that Cyberint was much more than an EASM solution, it delivered much value with highly relevant intelligence from the deep and dark web."*

*Benjamin Bachmann*

## STRÖER

### Challenges

Obtaining extensive integrated visibility into external risk exposure across all portfolio companies

### Solution

Deployed Cyberint Argos Edge™

### Impact

- Continuously uncover and mitigated the most relevant known and unknown external risks
- Achieved dramatic reduction in false-positives kept teams laser-focused on the right actions to minimize digital risk exposure
- Continuously sanitizes data and optimize results with ongoing support from Cyberint's analyst team

## Harnessing the power of autonomous discovery was a game changer

The team immediately started acting on the insights that Argos Edge™ delivered, dramatically improving cyber-posture across all of the group's companies.

Leveraging threat intelligence tailored specifically for each company's external-facing assets, the team was able to communicate at the company level what needed to be done, monitor progress, and continuously improve cyber-posture of 100+ portfolio companies, elevating the organization's overall posture.

## On the path to zero false-positives

Upon completion of Cyberint's EASM autonomous discovery, the relevant threat intelligence - sourced from the open and deep and dark web was mapped to Ströer's specific exposed assets.

With the help of Cyberint's team of analysts, the findings were sanitized, teaching the algorithm, gradually reducing false-positives down to minimum - laying the grounds for proper performance benchmarking and measurement.

*"The Cyberint team was really responsive and helpful in every step of the way."*

## A whole new level of knowledge

In addition to gaining visibility at the group-level, Cyberint's deep and dark web threat intelligence reports helped Ben and his team gain a clear understanding of the bigger picture: Trends, hacker groups, threat actors' interests and more. This allows them to increase cybersecurity knowledge and awareness across all portfolio companies and keep up with the ever-evolving threat landscape.

"It's no wonder we stopped our vendor evaluation after the POV with Cyberint," says Ben, "It simply checks all our boxes. Visibility, actionable insights, support and knowledge - all in one platform that's easy to use. The focus it delivers is phenomenal."

## About Cyberint

Cyberint is a cybersecurity solution provider that pioneered attack surface reconnaissance. The solution fuses threat intelligence with attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, it allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities and more, ensuring continuous external protection from cyber threats.

To learn more how cyberint helps organizations uncover and mitigate their most relevant external risks visit [www.cyberint.com](http://www.cyberint.com)

Cyberint