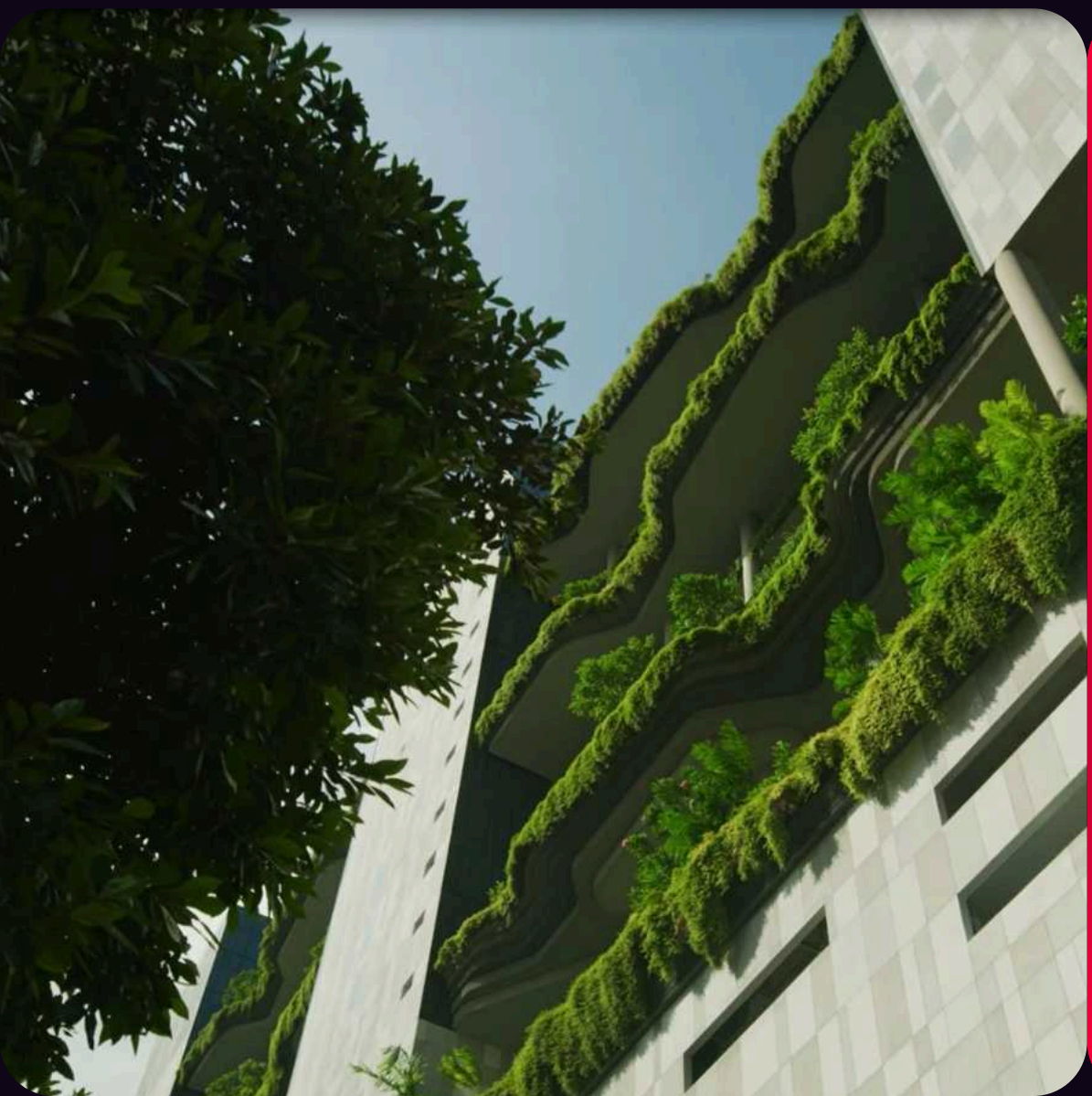
HADRIAN

Budenheim

CASE STUDY

How Budenheim strengthened continuous external security visibility

CHEMICAL MANUFACTURING, GERMANY



About Budenheim

Budenheim is a global specialty chemicals company delivering high-quality ingredients and solutions across food, health, and industrial applications. With approximately 1,300 employees and production sites across Europe, North America, and Asia, the company operates in a highly regulated environment shaped by chemical and pharmaceutical industry standards.

Headquartered in Germany, Budenheim maintains a mature security and governance framework built on strong internal controls, regular audits, and established operational processes. To further strengthen its external security posture, the company focused on improving visibility into externally exposed assets and enabling more continuous validation of potential exposures.

CUSTOMERS	OPERATING COUNTRIES	REVENUE
2,100	103	500M EUR

Challenges

01 **Expanding visibility beyond periodic testing**

Budenheim's security program already included established governance processes such as audits and regular penetration testing. However, these activities were primarily point-in-time assessments and provided limited visibility between testing cycles.

02 **Keeping pace with a growing external attack surface**

Budenheim's attack surface was growing more complex. As the number of externally exposed systems and services expanded, the need for a consolidated, continuously updated external view became impossible to ignore.

03 **Complementing internal controls with an attacker's perspective**

Budenheim's security operations centered largely on internal processes, administrative controls, and audit requirements. The organization wanted to complement this perspective with continuous external visibility, giving it a clearer understanding of how exposures might appear from an attacker's point of view.

✓ **Continuous exposure visibility as an added security layer**

To strengthen continuous exposure visibility, Budenheim implemented Hadrian as an additional layer within its existing security operations and governance framework.

✓ **Attacker-oriented techniques for smarter prioritization**

Hadrian provides continuous visibility into externally exposed assets while supporting ongoing validation of potential exposures. By incorporating attacker-oriented techniques and automated validation capabilities, the solution helps contextualise findings and improve prioritisation of remediation activities.

✓ **Seamlessly integrated into existing security operations**

Hadrian was integrated into Budenheim's existing security workflows and supports more informed decision-making by providing continuously updated external visibility alongside existing security controls and processes.

Outcome

From periodic assessments to continuous visibility

Budenheim's security operations were historically built around structured validation processes such as audits and scheduled penetration tests. While effective from a governance perspective, these approaches naturally reflected snapshots in time rather than continuous visibility.

By introducing continuous external exposure monitoring, the organisation strengthened its ability to identify and reassess changes across its external attack surface on an ongoing basis. This improved transparency between traditional assessment cycles and supported a more dynamic understanding of externally visible risks.

> **"We now have a continuously updated external perspective on our environment, which significantly improves transparency and complements our existing security controls and processes."**
>
> Markus Garber - Vice President IT at Budenheim

Improving risk prioritization through continuous validation

Prior to implementing continuous external validation, prioritisation activities were often based on isolated findings, severity ratings, or manual analysis efforts. This sometimes made it difficult to assess which exposures represented the most relevant operational risk.

With continuous external visibility and validation capabilities in place, Budenheim can now evaluate exposures with additional context regarding reachability and potential exploitability. This helps the security team focus remediation efforts more effectively and supports a more risk-oriented prioritisation approach.

The result is a more transparent and continuously updated understanding of the organisation's external exposure landscape.

Outcome

Supporting faster and more informed security decisions

The introduction of continuous external visibility also improved operational decision-making processes within the security organisation.

Rather than relying solely on point-in-time assessments, the team now operates with continuously updated visibility into externally exposed assets and validated findings. This supports faster prioritisation, clearer remediation ownership, and improved tracking of exposure reduction over time.

As a result, Budenheim further strengthened its ability to proactively manage external exposure in alignment with its existing governance, security, and compliance framework.