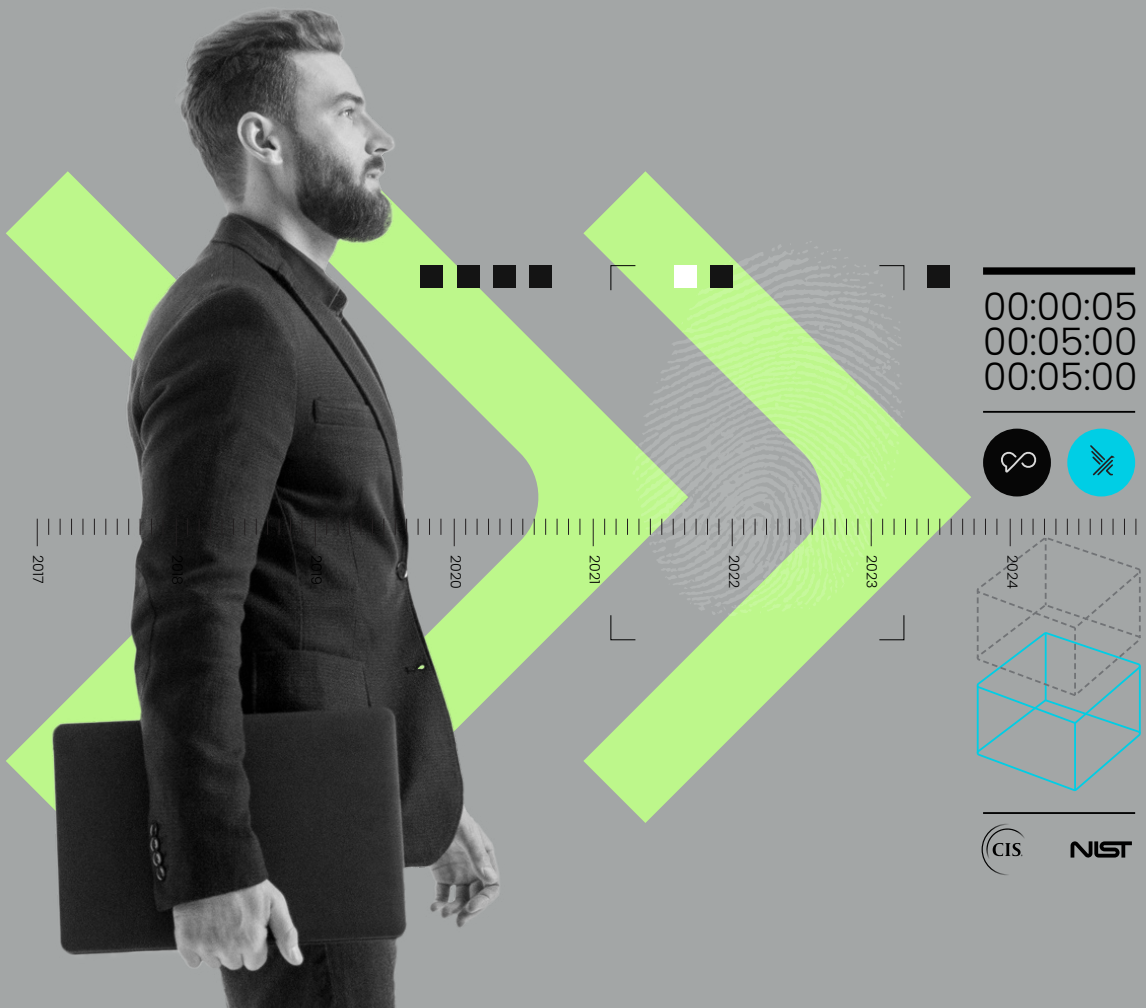
sysdig TrueFullstaq

2025 Cloud-Native Security and Usage Report

BeNeLux Regional Highlights



Key trends

Machine identities are 7.5x more risky than human identities and there are up to 40,000x more of them to manage

Workloads using AI/ML packages grew by 500% and public exposure decreased by 38% over the last year, showing that secure AI implementation has become a clear organizational priority

Real-time detection and response in under 10 minutes — when tools alert within seconds — is possible, and companies are initiating response actions in under 4 minutes

60% of containers live for 1 minute or less

In-use vulnerabilities have decreased to less than 6%, but image bloat quintupled year over year

Organizations across the globe in all business sectors are **leveraging open source software**, like Falco, regardless of their size

Cybersecurity regulations are essential, and EU-based organizations are leading the charge by prioritizing compliance more than their global counterparts.

This is a special edition of Sysdig's 2025 Cloud-Native Security and Usage Report, providing cloud security trends for the BeNeLux region.

Executive summary

The "Sysdig 2025 Cloud-Native Security and Usage Report" is back for its eighth year, analyzing real-world data and the current state of cloud security and container usage. The findings detailed here indicate that security teams have made significant advancements across key areas, not only year over year, but also looking back on previous reports. With this in mind, our 2025 report provides benchmarks for maturity and efficiency, helping security teams, developers, and organizational leaders measure progress in the coming year.

In October 2023, the Sysdig Threat Research Team (TRT) concluded that cloud attacks can take place in 10 minutes or less. In this report, we have detailed how organizations today are detecting, investigating, and responding to real-world threats within this time frame using innovative tools and techniques. We've also found that open source software is not just a trend, but has become a dependency for today's cloud security. The open source threat detection tool Falco has been downloaded over 140 million times and is used across large enterprises and small businesses (SMBs) alike, signaling that organizations of all sizes have found value in the power of open source security.

The security community has also made advancements in vulnerability management and AI workload security. For the second year in a row, we've identified a significant reduction in runtime vulnerabilities. We also saw significant growth in the number of workloads that use AI and machine learning (ML) packages and — despite this growth — the percentage of workloads publicly exposed to the internet has decreased significantly, an indication that organizations are prioritizing AI security.

In assessing identity management from a different perspective than years past, we found that organizations are managing exponentially more service accounts than user accounts, and that these service accounts present higher risk profiles. No wonder supply-chain attacks have become increasingly common!

Finally, in a few surprising turns of events, it turns out that organizations are prioritizing nuanced technical security benchmarks for compliance policies over the federally prescribed regulations we often read about in the news. And last but certainly not least, our beloved container lifespan statistic of many years has taken a new form. Short-lived workloads are purpose-built for speed and only live long enough to complete their task — all the more reason for real-time detection and continuous monitoring.

Read the full report for all of this year's findings.

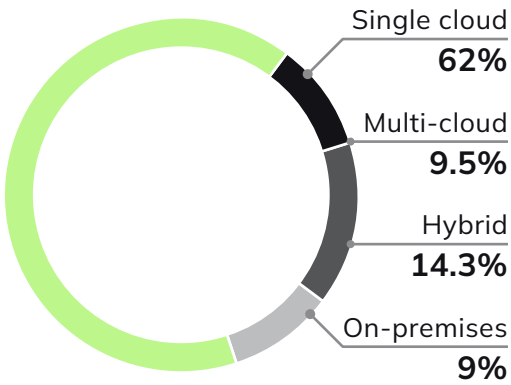
BeNeLux Trends

In 2025, cloud-native security patterns in the BeNeLux region are positively distinct from global trends. Based on data analyzed for this report, Belgium, the Netherlands, and Luxembourg have clear strategic security priorities. Their path forward is guided by compliance and strengthened by the implementation of innovative technologies and processes that prevent modern threats.

BeNeLux goes all-in on cloud

Organizations in BeNeLux are fully embracing the flexibility provided by the cloud. While **global cloud adoption** is at **approximately 80%**, nearly **86% of businesses in the region** are using cloud infrastructure. Strong regional industries like fintech and logistics, especially in the Netherlands and Luxembourg, rely on cloud scalability to grow their business operations. Belgian organizations are likely influenced to adopt secure cloud infrastructure, as Brussels is home to the EU institutions where Europe's regulatory and compliance frameworks are developed.

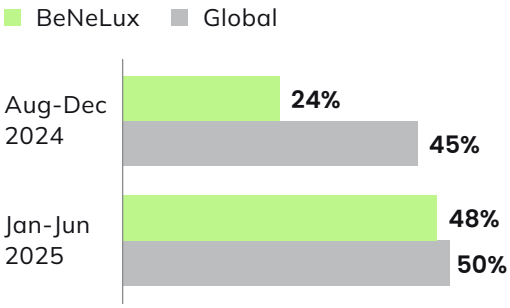
Regional infrastructure adoption



Cautiously adopting AI for security

There appeared to be a reluctance to integrate AI into security processes at the end of 2024 in the BeNeLux region, where only 24% of organizations implemented a GenAI security solution by December. Globally, the adoption rate was a more eager 45%. While the global implementation rate continued to slowly increase to 50% by the end of June 2025, BeNeLux experienced a boom, increasing adoption to 48%. The shift is likely driven by a growing trust in tooling, an increasing demand for secure GenAI use cases, and policy clarity. The EU AI Act may have had an impact, as it entered into force in August 2024, and provisions began to phase into effect in February 2025.

AI adoption over time



Ahead of the curve in automating incident response

BeNeLux is discreetly pulling ahead of global peers in automating incident response actions. In this region, **14% of organizations** are automating some of their response actions for specified alerts or attack types, while the **global average is only 11%**. The use of automation suggests proactive security strategies are being encouraged across the region to enhance efficiency and reduce response times. This practice is helping build a scalable foundation for incident workflows — without overcommitting resources — to combat the speed of the modern cloud-native threat landscape.

Prioritizing identity security

Teams in the BeNeLux region are showing strong identity governance practices. While **60% of global organizations maintain risky service accounts**, only **44% of the region** faces the same issue, signaling a more disciplined approach to identity and access management. Additionally, there were **no risky users within BeNeLux organizations**, whereas **eight percent of global organizations maintain risky users**. These statistics suggest that the region prioritizes security best practices like least-privilege and zero-trust policies, which align with the demands of EU-wide compliance frameworks like GDPR and NIS2.

Advanced centralized identity control

Some organizations have **no user accounts connected to their cloud service provider** likely due to the use of a third-party verification service. With that said, BeNeLux security teams have advanced their identity and access management practices, with **61% of organizations** not providing users with direct access to their cloud service providers. By comparison, only **15% of global organizations** are believed to have an SSO verification process in place. This practice centralizes identity control, reduces the attack surface, and the temporary session tokens make privilege escalation harder for attackers.

Netherlands put the region on the map for OSS usage

Falco, an open source tool used by 60% of the Fortune 500 companies, detects anomalous activity within containers, hosts, Kubernetes environments, and more. In the first half of 2025, there were nearly 10 million global downloads of the tool. Since Falco's CNCF graduation in February 2024, adoption in the Nordics has been distributed across the region fairly consistently with the countries' population shares. The **Netherlands**, with a strong open source culture promoted by the government, has emerged as a regional leader in open source adoption, accounting for **62% of the region's Falco downloads**. Falco usage across the region indicates that real-time runtime threat detection and cloud-native strategies are a regional priority as organizations seek to enhance visibility into containerized environments, improving their overall security posture while maintaining data sovereignty.

What's next for BeNeLux

The BeNeLux region is firmly rooted in the cloud. With exponential growth in GenAI implementation this year and a strong foundation in identity governance, the region will likely continue to gain momentum in automated incident response and build a more secure and resilient digital future. As home to the capital of Europe, BeNeLux is likely to set an example for compliance-driven cloud security.

sysdig

Sysdig helps security and development teams prevent, detect, and respond to threats instantly. Founded by the creators of Falco and Wireshark, and built on agentic AI, Sysdig delivers real-time defense grounded in the uncompromising truth of runtime. No guesswork. No black boxes. Just cloud security, the right way.

LEARN MORE →

TrueFullstaq

TrueFullstaq is a cloud-native pioneer and leading expert in Kubernetes services, delivering customized solutions for cloud infrastructure, container orchestration, and managed Kubernetes environments. With certified expertise and a focus on innovation, TrueFullstaq helps you run applications seamlessly in the cloud while keeping costs under control.

LEARN MORE →

RP-016 REV. A 10/25