Stockholm, Sweden
04 November 2024 10:00:00 CET

# Network Security Survey Shows Alert Fatigue, Encryption Abuse and Cloud Visibility Are Getting Worse - But There May Be Hope

**A new report, 2024 State of Network Threat Detection, released today by Cybersecurity Insiders and sponsored by Enea, reveals that three key cybersecurity challenges—alert fatigue, the misuse of encryption to cloak cyberattacks, and limited cloud workload visibility—not only persist, but have notably worsened over the past two years. The report indicates security professionals are looking to AI and anomaly detection to help reverse these trends.**

According to a global survey among 600,000 IT security professionals recently conducted by research firm Cybersecurity Insiders, poor alert accuracy and actionability persist as the top challenge for network intrusion detection/intrusion prevention systems (NIDS/IPS). Selected by 61% of the survey respondents, the result represents an increase of 16% compared with a comparable 2022 study.

Completing the survey's top three reported challenges in network intrusion detection and prevention:

- 52% of respondents cited limited cloud workload visibility, up from 35% in 2022.
- 42% of respondents cited encrypted traffic, up from 34%. Notably encrypted traffic was also named the number one network visibility blind spot in 2024.

The fact that these and other challenges not only persist but are worsening is surprising given the significant effort and innovation that the cybersecurity industry has invested in solving them.

What might finally turn the tide on these troubles? The survey findings point to AI and automation, with the demand for automated alert triage reaching an impressive 62% in this year's survey (an increase of 20% compared to the 2022 survey). Supporting this, automatic scoring and prioritization of threats is named the #1 must-have for an effective network threat detection solution. Moreover, a striking 71% consider AI integration extremely or very important for combatting advanced cyber threats.

Another cybersecurity solution revealed by the 2024 survey as gaining in importance is the expanded use of anomaly detection, or behavioral analysis, which – particularly when powered by AI – can more effectively identify true attacks and surface the most meaningful information for remedial action. While a small proportion of security professionals report having anomaly-based network threat detection tools (17%) today, a strong majority (66%) plan to deploy them over the next 6 to 24 months.

"Over the past five years, our networks have been evolving at a pace which solution vendors have struggled to keep up with, even in the best of circumstances. And now AI is blazing an exponential growth curve; penetrating and reshaping the threat landscape in a way that makes it essential to fight fire with fire," said Laura Wilber, Sr. Analyst, Technology & Industry at Enea. "These survey findings reveal a community of security professionals who understand this evolution and are eager for white hat AI to come to their aid to automate the security tasks that are overwhelming them and catch AI threats that can evade conventional tools."

Stockholm, Sweden
04 November 2024 10:00:00 CET

On November 14, 16.00 GMT/11.00 EST, experts from Enea, Arista Networks, and Custocy will discuss the key survey findings in a webinar and explore potential solutions to the most pressing needs. To register to attend the webinar, visit **info.enea.com/network-threat-detection-webinar**

To download the report, go to **info.enea.com/2024-state-of-network-threat-detection-report**

As the most widely deployed Deep Packet Inspection (DPI) technology in cybersecurity and networking solutions, the Enea Qosmos products classify traffic in real-time and provide granular information about network activities. Enea also offers IDS-based threat detection capabilities as an SDK, enabling easy and tight integration with cybersecurity solutions while remaining highly flexible and scalable. For more information on embedded DPI visit **enea.com/dpi-tech**

**Contact**
Stephanie Huf, Chief Marketing Officer
E-mail: stephanie.huf@enea.com

**About Enea**

---

We are a world-leading specialist in advanced telecom and cybersecurity software with a vision to make the world's communications safer and more efficient. Our solutions connect, optimize and protect communications between companies, people, devices and things worldwide. We are present in over 80 markets and billions of people rely on our technology every day when they connect to mobile networks or use the Internet. Enea is headquartered in Stockholm, Sweden and is listed on NASDAQ Stockholm. Visit us at **enea.com**

**Attachments**

---

**Network Security Survey Shows Alert Fatigue, Encryption Abuse and Cloud Visibility Are Getting Worse - But There May Be Hope**