2024 HYBRID CLOUD SECURITY SURVEY

Closing the Preparedness Gap

Our annual survey of over 1,000 Security and IT leaders revealed that organizations are not prepared for today's cyber attacks. While AI technology brings promise, cyber criminals are also adopting AI at a rapid rate, and organizations' current security tool strategies are creating blind spots for hackers to exploit. As evolving legislation elevates cyber risk within the boardroom, gaining deep observability across hybrid cloud infrastructure will be critical to success.

ORGANIZATIONS UNDERSTAND THE RISKS

83%
of responding organizations agree that visibility into all data in motion is critical for cloud security

73%
agree that lateral, East-West visibility is a greater priority for cloud security than North-South

87%
of respondents believe that gaining visibility into encrypted traffic is critical to cloud security

...BUT THEY ARE FALLING SHORT

1 IN 3
organizations failed to detect a recent breach with existing security tools

60%
of organizations lack visibility into lateral, East-West traffic

62%
admit that encrypted traffic is less likely to be inspected by security teams

Modern Challenges Call for New Solutions

The increased complexity of organizations' hybrid cloud infrastructure and the sophistication of cyber threats resulted in a **20% increase** in undetected breaches between 2023 and 2024.

83%
of respondents believe that cloud complexity is increasing their cyber risk, a challenge that continues to escalate each year

41%
of respondents report seeing a surge in AI-powered attacks, bringing new risks

Only 45%
feel strongly prepared to identify threats lurking in lateral, East-West traffic

Despite growing security spend, **65%** of Security and IT leaders believe existing security tools are not as effective as they could be when it comes to detecting breaches.

The Consequences of Blind Spots are Stark

EXTORTION THREAT

31%
of organizations only detected a breach once they received an extortion threat

DARK WEB

31%
of organizations failed to detect a breach until proprietary information leaked on the dark web

REAL-TIME RESPONSE

25%
of organizations were able to detect and respond to the threat in real-time

ROOT CAUSE

25%
of organizations failed to identify the root cause of a detected breach, impairing their ability to prevent future attacks

DEEP OBSERVABILITY IS THE ANSWER

Deep observability defined: The ability to efficiently deliver network-derived intelligence to cloud, security, and observability tools to eliminate blind spots, reduce tool costs, and enable organizations to better secure and manage hybrid cloud infrastructure.

84%
agree that deep observability into hybrid cloud infrastructure is key to strengthening security posture

61%
believe that greater visibility into all data in motion will empower more secure AI deployments

82%
agree that deep observability is strongly linked to Zero Trust success

No matter what strategy security leaders choose...

...network-derived intelligence is key to their success.

Respondents universally agreed that deep observability can optimize tooling, offer unmatched threat insights, and form a robust foundation for Zero Trust network architecture.

It's no surprise that **80%** of respondents report that deep observability is discussed at the board level as a priority for hybrid cloud security.

Discover insights from your region in the full report.

DOWNLOAD NOW

Data collection: March 22-April 6, 2024
Respondents: 1,013 CIOs/CISOs/CTOs, and other Network and Cloud leaders
Regions: Australia, France, Germany, Singapore, UK, and USA

Gigamon®