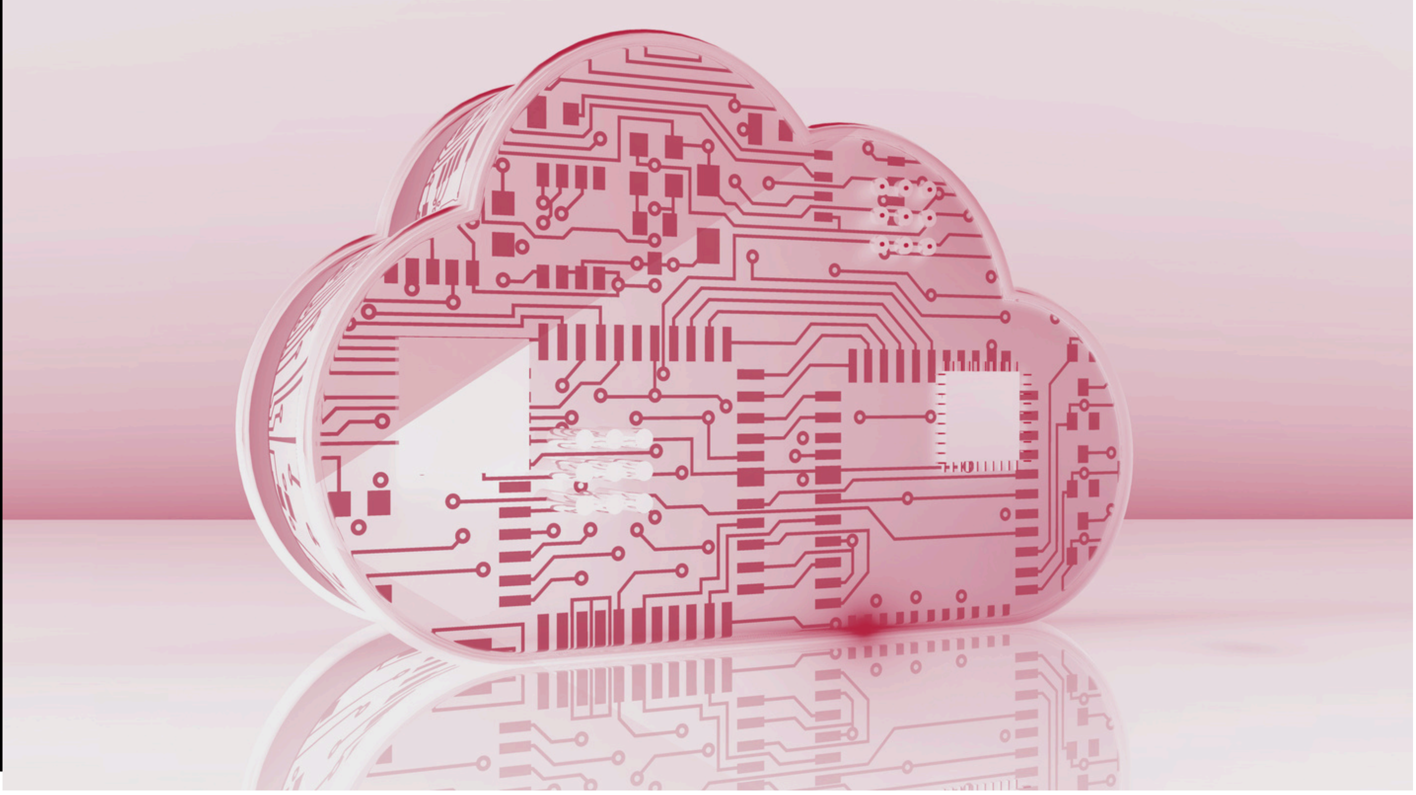
GECIĆ
LAW



Cloud Security Enters a Bold New Era: Google Acquires Wiz

In a move shaking the foundations of the tech world, Google's parent company, Alphabet, has agreed to acquire Wiz, a cloud security startup, for $32 billion in an all-cash deal. This marks Alphabet's largest acquisition to date, surpassing its previous record purchase of Motorola Mobility for $12.5 billion in 2012.

Wiz is an Israeli-founded startup headquartered in New York, specializing in cloud-native application protection. It provides agentless, real-time insights into vulnerabilities, misconfigurations, and access rights across public cloud settings.

Wiz will continue to operate as an independent platform, compatible with various cloud providers beyond just Google Cloud. This move is seen as a strategic effort by Google to expand its cloud security offerings. It also aims to help the company compete more effectively with Amazon and Microsoft in the cloud computing market.

Why is Cybersecurity Important?

Cybersecurity involves protecting systems, networks, and sensitive data from digital threats. It safeguards organizations from operational disruptions, financial losses, and privacy breaches. Strong cybersecurity practices help businesses avoid substantial financial costs, protect customer trust, maintain compliance, and ensure continuous operations. Key areas of cybersecurity protection include:

- Endpoint Security: Securing individual devices like computers, smartphones, and routers from malware and unauthorized access.
- Network Security: Protecting networks from unauthorized intrusions, ensuring secure communication and data transfer.
- Cloud Security: Safeguarding cloud-hosted data, applications, and services against unauthorized access and breaches.

The acquisition of Wiz demonstrates a growing demand for cloud computing services driven by the AI boom. Cloud computing is becoming increasingly important due to its flexibility and scalability. This also allows businesses to adapt quickly to changing needs without significant upfront investments.

EU Cybersecurity Regulation: NIS2 Directive

The NIS2 Directive (Directive EU 2022/2555) built upon NIS1 Directive, significantly enhances cybersecurity requirements within the EU. Key aspects include:

- Expanded applicability to 18 critical sectors, such as energy, finance, healthcare, digital infrastructure, transport, social platforms, and waste management.
- Obligations for medium-sized and large organizations to implement comprehensive cybersecurity measures, including incident management, risk assessments, and rapid incident reporting (within 24 hours).
- Increased management accountability, with substantial penalties for non-compliance.

The NIS2 directive requires each EU Member State to implement a national cybersecurity strategy that encompasses policies for securing supply chains, managing vulnerabilities, and promoting cybersecurity education and awareness.

Cybersecurity Regulation in Serbia

Serbia is expected to introduce a new Information Security Act by 2025, aligning with the NIS 2 Directive while incorporating some local distinctions. This move underscores Serbia's dedication to aligning its legal framework with EU standards.

Beyond the Cloud: Implications for the Future

Google's acquisition of Wiz undoubtedly marks a significant milestone in the cybersecurity landscape, underscoring the growing importance of cloud security and multi-cloud strategies. This deal further improves Google's position as a major player in cybersecurity, strengthening its capabilities to compete with its rivals.

The acquisition highlights the increasing demand for robust cloud security solutions as businesses transition to cloud environments. Furthermore, it highlights a growing trend where businesses are increasingly prioritizing cloud security over on-premises security, as the latter is more costly to maintain and less effective in the rapidly expanding digital economy.

As cybersecurity regulations evolve, such as the EU's NIS2 Directive and Serbia's efforts to align with European standards, businesses must navigate these complex frameworks while investing in advanced security technologies to stay ahead of emerging threats.

Partnering with legal experts familiar with both EU and Serbian cybersecurity regulations is essential to effectively manage risks and ensure regulatory compliance.

GECIĆ | LAW

NIKOLE SPASIĆA 2, BELGRADE
WWW.GECICLAW.COM