Submission to the European Commission on the Proposed Acquisition of Wiz, Inc. by Google LLC (Case M.11964)

Third-Party Observations under the European Union Merger Regulation

I. Executive Summary and Phase II Request

We are a coalition of civil society organisations deeply concerned about the growing concentration of power in cloud and digital ecosystems. We strongly urge the Commission to open a Phase II investigation under Article 6(1)(c) EUMR of the proposed acquisition of Wiz, Inc. ("Wiz") by Google LLC ("Google") which sits in a wider context of serial acquisitions and partnerships that reinforce Google's excessive market power.[1] The transaction raises serious doubts as to its compatibility with the internal market under the "significant impediment to effective competition" ("SIEC") test. The concentration enables Google, a hyperscale cloud provider, to acquire and control a leading multi-cloud security control layer, creating powerful incentives and mechanisms to foreclose rivals in both cloud and cloud security. In addition to threatening the resilience of the core functions of our economies, the transaction creates credible and interlocking risks of conglomerate leveraging and ecosystem entrenchment and increased lock-in, particularly through non-price and technical parameters that are difficult to assess and remedy in Phase I.

We submit that this is not a case that should be resolved in Phase I either through unconditional clearance or through straightforward commitments. The likely remedies would be behavioural, difficult to define, and vulnerable to circumvention through subtle product and engineering choices, and difficult to monitor effectively in a fast-moving technical environment.

II. The merger risks significantly impeding effective competition

The proposed concentration raises serious doubts under the SIEC test due to credible vertical, conglomerate and innovation harms that operate through non-price, technical parameters requiring Phase II scrutiny.

A. Vertical/ non-horizontal foreclosure: soft degradation of multi-cloud neutrality

A defining feature of Wiz's role is that it operates as a multi-cloud security platform across major hyperscalers. Google has publicly stated that Wiz's products will continue to work and be available across all major clouds, including AWS, Microsoft Azure and Oracle Cloud platforms.[2] Wiz has similarly stated that it "needs to remain a multicloud platform" and will continue working closely with AWS, Azure and Oracle.[3] These statements underscore that multi-cloud neutrality is central to Wiz's competitive function and that this neutrality becomes vulnerable when a hyperscaler cloud provider acquires control.

[1] This acquisition revives the important debate regarding the necessary reversal of the Commission's burden of proof when companies are particularly powerful (see the Commission's ongoing review of the merger guidelines).
[2] https://cloud.google.com/blog/products/identity-security/google-announces-agreement-acquire-wiz?
[3] https://www.wiz.io/blog/wiz-joining-google?

Post-merger, Google would have both the ability and the incentive to steer outcomes in cloud competition by influencing Wiz's product development, integration and performance in ways that favour Google Cloud Platform ("GCP"). In this sector, foreclosure is most likely to occur through subtle, cumulative forms of discrimination (soft degradation) rather than an overt refusal to supply, for example through slower feature parity for non-GCP environments, reduced priority for AWS/Azure connectors and integrations, differences in reliability or responsiveness in non-GCP deployments, or support and escalation practices that systematically favour GCP-native deployments. Because cloud procurement and governance decisions are highly sensitive to perceived security risk and operational burden, even incremental and non-transparent differences can distort competition over time.

B. Conglomerate effects: bundling and ecosystem leveraging through procurement power

The transaction also raises serious doubts because it strengthens Google's ability and incentive to use portfolio power and enterprise procurement dynamics to entrench its position in cloud and cloud security. Post-merger, Google would be able to integrate Wiz more deeply into Google Cloud Platform and to structure commercial strategies that make Wiz adoption more attractive (or operationally simpler) when paired with GCP and Google's wider security stack, weakening contestability for independent security vendors and rival clouds. Such strategies can be effective in cloud procurement because customers often seek integrated workflows, simplified contracting and a reduced compliance burden, which can magnify the foreclosure effects of bundling and defaulting.

This concern is reinforced by Google's demonstrated strategy of expanding its cloud security capabilities through acquisition and integration, including the acquisition of Mandiant and its integration into Google Cloud's security offering. This type of serial acquisition would enable the creation and facilitation of a walled garden around GCP, thereby locking in consumers, reducing choice and raising barriers to entry especially for smaller cloud providers.

It also raises a related ecosystem risk in AI-enabled cloud security workflows, since Google is deploying Gemini-branded assistants within Google Cloud products. Integrating Wiz into these experiences could further steer customers toward bundled "cloud + security + assistant" solutions and disadvantage competing tools through defaults and reduced interoperability in practice.

C. Data and information effects: leveraging Wiz cross-cloud telemetry and insights

As a multi-cloud security layer, Wiz is positioned to have broad visibility into customers' cloud environments and security posture signals across heterogeneous deployments, including configuration patterns, exposure paths, and vulnerability trends. Post-merger, Google would have increased incentives to leverage this cross-cloud telemetry and associated insights to reinforce its competitive position in cloud and cloud security, including by shaping product strategy and roadmap prioritisation, targeting customers with tailored migration and bundling narratives, and optimising commercial and technical offerings in ways that competing cloud

providers cannot replicate. Even absent any allegation of unlawful data use, the structural concern is that a cloud competitor would obtain a privileged vantage point across rival clouds, reinforcing information asymmetries, raising barriers to effective competition, especially for smaller cloud providers, and entry over time. This concern might also extend to other areas of Google ecosystem where it is dominant, for instance in advertising, internet search and operating systems.

D. Lock-in and switching costs: security driven dependence and reduced customer mobility

Once a cloud security layer is adopted and integrated, switching costs can be substantial. Cloud security tooling is typically embedded into day-to-day governance and operational processes, including compliance reporting, vulnerability management, security monitoring, incident response workflows, and remediation automation. This creates switching costs that are not merely financial, but operational and organisational, because replacing a security layer can require re-architecting workflows, re-validating compliance evidence, re-training teams, and managing transitional risk.

By integrating Wiz into GCP and Google's wider security ecosystem, the merged entity could increase customer dependence on a single vertically integrated stack. Over time, this may reduce customers' practical ability to change either cloud provider or security vendor without significant disruption, particularly where security considerations influence cloud procurement decisions. The result can be reduced contestability in both cloud and cloud security, as customers become less able to credibly threaten switching, and rivals face higher barriers to winning tenders even where they offer competitive pricing or innovation. These effects are likely to be reinforced by information asymmetries and by the risk aversion inherent in security procurement, where customers may prioritise perceived stability over switching even in the presence of better alternatives.

E. Loss of an independent competitive constraint: reduced innovation and multi-cloud neutrality

As an independent provider, Wiz' incentives are aligned with multi-cloud neutrality and broad interoperability. Its commercial proposition depends on providing consistent security visibility and usability across heterogeneous environments. Its rapid growth has also strengthened competitive pressure on incumbent providers to improve product performance, integration depth, and customer experience. In this sense, Wiz functions as a meaningful competitive constraint not only through pricing, but through innovation and quality competition in cloud security tools.

The acquisition risks removing that independent constraint and shifting innovation priorities toward deeper integration with Google's ecosystem. Post-merger, the commercial logic of maintaining a neutral multi-cloud roadmap may be diluted as engineering prioritisation and go-to-market strategy align more closely with Google's incentives, including strengthening GCP's attractiveness in enterprise procurement. This may reduce innovation diversity in the

market, particularly on the dimensions most valuable for customers operating across multiple clouds, such as interoperability, portability, and consistent parity of functionality. The effect may therefore be felt not only in the near-term product choices, but in the longer-run direction of market development, where independent multi-cloud security providers may face weaker prospects and hyperscaler-centric security stacks become more entrenched.

III. Cloud as essential infrastructure and significance of the transaction for European resilience

In addition to the competition concerns set out above, the transaction should be understood in the wider context of cloud's role as essential infrastructure and the implications for European resilience.

Cloud computing and cloud security services have become essential digital infrastructure for a wide range of sectors in the EU economy. Recent outages and cybersecurity incidents affecting hyperscalers propagate rapidly and at scale, with significant operational consequences for business, public services and society.[4] Our collective dependence on a few powerful cloud providers magnifies the dangers posed by the failure or disruption of this infrastructure. This makes market structure, and who controls critical layers of cloud and cloud security, directly relevant to resilience, switching options and systemic dependency. [5]

In our view, past regulatory under enforcement in the digital sector, including in merger control, has contributed to the concentration of power in a small number of global technology firms. This transaction risks further entrenching Google's already powerful position in the broader digital ecosystem and extending that power into adjacent layers of cloud and cloud security.[6]

The proposed concentration would further integrate important cloud security capability into GCP. Wiz's current value proposition is closely linked to in its independence and multi-cloud neutrality, allowing customers to maintain visibility across heterogeneous environments and reduce single-vendor blind spots.[7] Post-acquisition, Wiz would sit within Google's ecosystem, and the Commission should examine how this change in ownership may affect key non-price parametres of competition in cloud and cloud security, including interoperability, integration parity, reliability, business continuity and support responsiveness.

---

[4] In 2025, an outage hit Google Cloud Platform and paralyzed critical Google services including Gemini, Youtube and Google maps. 1.4 million users were presumably affected by this incident (https://www.ookla.com/articles/google-cloud-outage-june-2025). In 2024, the Crowdstrike outage paralyzed 8.5 million Microsoft devices and seriously affected major businesses, airports, airlines, courts, government and public healthcare systems (https://www.washingtonpost.com/technology/2024/07/20/microsoft-outage-crowdstrike-regulatory-scrutiny/).

[5] For more information on the risks posed by cloud dependency on a few powerful providers: https://www.openmarketsinstitute.org/publications/report-rethink-regulatory-approach-to-essential-cloud

[6] More on how antitrust has failed to prevent Google from gaining market power, here: https://arxiv.org/abs/2511.02931 .

[7] https://www.wiz.io/academy/cloud-security/cloud-service-providers.

This is therefore not a routine case. The Commission has itself recognised that cloud markets can raise structural concerns[8], including lock-in dynamics, reinforcing the need for careful merger scrutiny where a transaction may further entrench dependency and reduce effective customer choice. These issues warrant in-depth scrutiny because the relevant competitive parameters are technical and dynamic and require evidence from customers, partners and competitors to assess them credibly. Over time, increased dependency on a small number of vertically integrated providers can also increase systemic risk and undermine Europe's strategic objective of digital sovereignty and infrastructure robustness.

This context reinforces why the competitive effects identified in Section II warrant in-depth scrutiny.

IV. Why the merger warrants an in-depth Phase II investigation

We submit that this transaction should not be resolved in Phase I because the principal risks arise through non-price and technical parameters that cannot be assessed reliably within the Phase I timeframe. Competition in cloud and cloud security often turns on interoperability, integration parity, product quality and reliability, roadmap timing, service continuity and support responsiveness, and these parameters are shaped by product design and engineering prioritisation decisions that are not readily visible to outsiders.

The transaction also raises interdependent concerns that are unlikely to be captured by a narrow, static assessment. In particular, questions of customer switching and dependency, neutral access and interoperability in multi-cloud environments, the practical significance of cross-cloud visibility and governance arrangements, barriers to entry and expansion, and the likely impact on innovation and competitive constraints are closely connected and may only be understood through a fuller evidential assessment.

For these reasons, this is not a case that can be safely resolved through unconditional Phase I clearance, nor is it suitable for resolution within Phase I through straightforward commitments. It is our position that the Commission requires a more complete evidential basis and market validation to reach a robust conclusion under the SIEC test.

An in-depth Phase II investigation is therefore necessary to assemble an adequate factual basis and to enable effective market testing with affected customers, partners and competitors, alongside scrutiny of internal evidence relevant to incentives, product strategy and competitive effects. This is particularly important given the fundamental role of cloud services in the core functions of the European economy and society, and the potential for incremental changes in technical performance and commercial strategy to have significant competitive consequences over time.

---

8 https://digital-markets-act.ec.europa.eu/commission-launches-market-investigations-cloud-computing-services-under-digital-markets-act-2025-11-18_en

Only a Phase II investigation provides a sufficiently robust framework for the Commission to reach a well-supported conclusion under the SIEC test in this case, including in relation to the risk of increased dependency on vertically integrated providers and the implications for resilience, digital sovereignty and infrastructure robustness.

V. Conclusion

For the reasons set out above, we submit that the proposed concentration raises serious doubts as to its compatibility with the internal market under the SIEC test. We therefore respectfully request that the Commission open an in-depth Phase II investigation pursuant to Article 6(1)(c) EUMR. We remain available to provide any additional information that may assist with the Commission's assessment.

* * *

Balanced Economy Project

Open Markets Institute

Rebalance Now

SOMO

ARTICLE 19