

# Microsoft Azure confronts security challenges

Article

**The news:** Microsoft cloud services, including Azure, are attracting sharp criticism for lax security protocols, slow response to threats, and lack of transparency.

**Sounding the alarm:** The CEO of security firm Tenable, Amit Yoran, said that Microsoft is "grossly irresponsible" with its security practices on Azure and that the company has a "culture

of toxic obfuscation.”

- The criticism was in response to a critical Azure vulnerability that has remained unpatched for months.
- The “cross-tenant” security issue can enable unauthorized access to data and applications belonging to other customers.
- The flaw was reported March 30 but won’t be fixed until September 28, per [Bank Info Security](#).
- In response, Microsoft provided an explanation of the “extensive process” the company follows when a vulnerability is disclosed, stating that it wants to ensure protection without significant customer disruption.

**Zooming out:** Security experts aren't the only ones chiding Microsoft for cloud exploits and vulnerabilities.

- [US Sen. Ron Wyden wrote a letter](#) to **CISA** director **Jen Easterly**, attorney general **Merrick Garland** and **FTC** chair **Lina Khan** urging them to hold Microsoft responsible for “negligent cybersecurity practices.”
- This is in relation to a hacking campaign against Microsoft in July that targeted organizations and US government agencies. “At least hundreds of thousands of individual US government emails” were stolen.
- Microsoft revealed July 14 that hackers had stolen an encryption key that gave them widespread access to cloud services. The company mitigated the issue and said it would improve security.

**The bigger the cloud, the bigger the risk:** As [a key vendor to the US government and Department of Defense](#), Microsoft’s cloud security practices will continue to be under scrutiny.

**Our take:** The benefit of the Pentagon’s **\$9 billion Joint Warfighting Cloud Capability (JWCC)** is that it divides the contract among **Amazon Web Services (AWS)**, **Google Cloud**, Microsoft Azure, and **Oracle**.

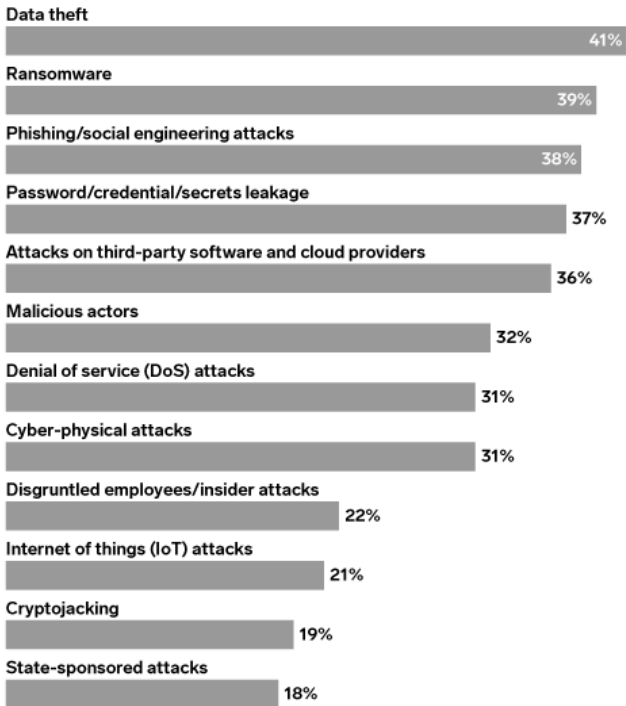
- The contract ensures that technology and solutions are not tied to one vendor and can be adjusted should the need arise.

- The downside: Microsoft will have an uphill battle in restoring customer and government confidence in its services or risk losing brand capital and cloud customers to competitors.

---

### Biggest Threats Their Company Faces in Cloud Security According to Cloud Tech Professionals Worldwide, June 2022

% of respondents



Note: n=1,039 whose company has a roadmap for implementing a multicloud strategy  
Source: Forrester Consulting, "Unlocking Multicloud's Operational Potential" commissioned by HashiCorp, Aug 4, 2022

277349

[InsiderIntelligence.com](https://InsiderIntelligence.com)