# Article information:

The Cloud Is Under Attack: The State of Cloud Security in 2023 | CSO Online
<https://www.csoonline.com/article/3684768/the-cloud-is-under-attack-the-state-of-cloud-security-in-2023.html>

# Article summary:

1. A survey of 4,984 IT professionals in SMBs across 31 countries found that 56% experienced an increased volume of attacks on their organization, with resource misconfigurations and unpatched vulnerabilities being top conduits for ransomware actors and other adversaries to gain access to an organization’s environment.

2. Only 37% of survey respondents said their organization tracks and detects resource misconfigurations in their IaaS infrastructure, while just 34% of beginner and intermediate IaaS users have visibility into all resources and their configurations.

3. Advanced IaaS users are twice as likely to report a decrease in attack volume, complexity, and impact over the last year compared to beginners, highlighting the benefits gained by implementing strong cloud practices such as ensuring visibility into cloud environments and investing in tools to shore up cloud defenses.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article titled "The Cloud Is Under Attack: The State of Cloud Security in 2023" by CSO Online discusses the results of a survey conducted by Sophos on the state of cloud security for small-to-medium-sized businesses (SMBs) that use Infrastructure as a Service (IaaS). The article highlights the increased volume, complexity, and impact of cyberattacks on SMBs using IaaS, with 56%, 59%, and 53% respectively reporting an increase in these areas. Additionally, 67% reported being hit by ransomware.

The article points to resource misconfigurations and unpatched vulnerabilities as top conduits for ransomware actors and other adversaries to gain access to an organization's environment. However, only 37% of survey respondents said their organization tracks and detects resource misconfigurations in their IaaS infrastructure, and fewer than half (47%) said they routinely scan IaaS resources for software vulnerabilities. Visibility into configurations and resources across all levels of maturity is another challenge for SMBs.

While the article does provide some positive news regarding advanced IaaS users reporting a decrease in attack volume, complexity, and impact over the last year compared to beginners, it also emphasizes the need for strong cloud practices to reduce threat risk. The article recommends approaching principles of cloud security as one would for traditional on-premises security, ensuring visibility into cloud environments, evaluating gaps in cloud security, investing in tools to shore up cloud defenses such as firewalls and managed detection and response services.

Overall, the article provides valuable insights into the state of cloud security for SMBs using IaaS. However, it could benefit from exploring counterarguments or potential biases towards certain solutions or providers. Additionally, while it notes possible risks associated with adopting cloud technology, it does not present both sides equally or explore potential benefits that may outweigh these risks.

# Topics for further research:

* Benefits of using IaaS for SMBs
* Best practices for cloud security in SMBs
* Comparison of cloud security solutions/providers
* Risks and benefits of cloud adoption for SMBs
* Impact of cloud security breaches on SMBs
* Future trends in cloud security for SMBs

# Report location:

<https://www.fullpicture.app/item/7c9fbe6d994c6aab9c6ca207a991493d>