

Understanding Cloud Attack Vectors

Focus on IaaS & PaaS vectors

Release Date: 06/20/2023



*Israel Chapter
Release*

Understanding Cloud Attack Vectors

The IaaS & PaaS Perspective



Description & Overview

The goal of the document is to map real-world attack vectors used during cloud-based attacks on IaaS/PaaS environments and then to map the vectors to mitigating controls identified in CSA & other resources. The motivation for this document resulted from our global cloud security research, from which we realized that while there are many risks and threats to IaaS/PaaS platforms and applications, most are associated with a specific number of attack vectors.

Key Takeaways

- 1 List of popular vectors that are frequently used in IaaS/PaaS attacks
- 2 The description, key takeaways, and examples for each vector
- 3 A list of controls that mitigate the risks and threats of the identified attack vectors
- 4 Keywords - Cloud security, cloud-native security, cloud attack vectors

Backstory

We understood that often risks and threats documents are missing the real story - how to protect from the actual vector used. The idea was to create short and technical explanations of how attackers exploit IaaS/PaaS services for hacking.

The Israeli chapter of the Cloud Security Alliance and other volunteers created this document. The full list of volunteers is available in the document.

Target Audience

1

CISO

2

CSO

3

Security professionals

4

Security practitioners

5

Cloud architects

6

DevSecOps professionals

7

Auditors

8

GRC professionals