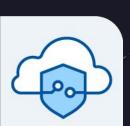


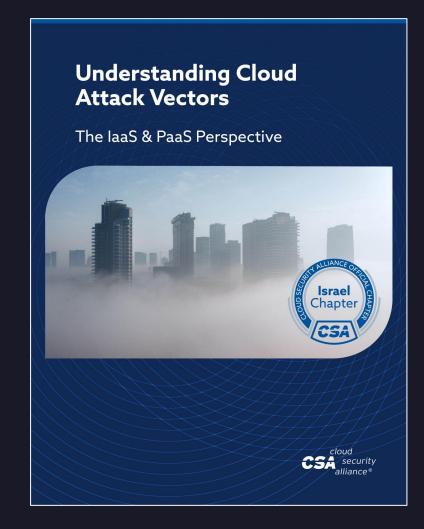
Understanding Cloud Attack Vectors

Focus on laaS & PaaS vectors

Release Date: 06/20/2023



Israel Chapter Release



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

List of popular vectors that are frequently used in laaS/PaaS attacks

- The description, key takeaways, and examples for each vector
- A list of controls that mitigate the risks and threats of the identified attack vectors
- 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 laaS/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

5 Cloud architects

2 CSO

6 DevSecOps professionals

3 Security professionals

7 Auditors

4 Security practitioners

8 GRC professionals