Cloud Access Security Brokers (CASBs)

Characterization of the CASB market and its alignment with corporate expectations

SNE/OS3.nl - Research Presentation - Commissioned by KPMG (Ruud Couwenberg)

Marius Brouwer
University of Amsterdam
mbrouwer@os3.nl

Anand Groenewegen
University of Amsterdam
agroenewegen@os3.nl

29 June - 2021

Introduction and Problem Statement

- The importance of Cloud Access Security Brokers has grown due to the COVID pandemic and led to a rise of employees becoming caretakers of their IT resources.

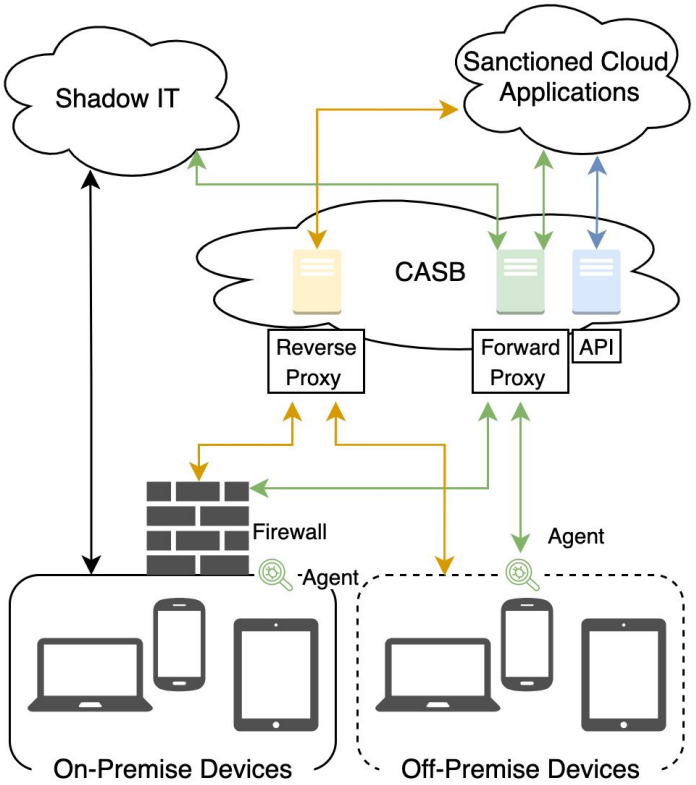
- Research shows that one in five organizations experienced a cyber event due to Shadow IT.

- Research Questions
  - **RQ: How do market-leading CASBs align with corporate expectations?**
  - SQ1: How do market guides and corporations define a CASB?
  - SQ2: How does Shadow IT, including risk and mitigation, relate to CASB?
  - SQ3: How do the Leaders of the Gartner Magic Quadrant (2020) address Shadow IT?
  - SQ4: How can a CASB be implemented in such a way that the responsible party is capable of managing the administrative overhead generated by CASBs?

- Providing an analysis of the current capabilities of the CASB market; leaders versus the capabilities expected by corporations.

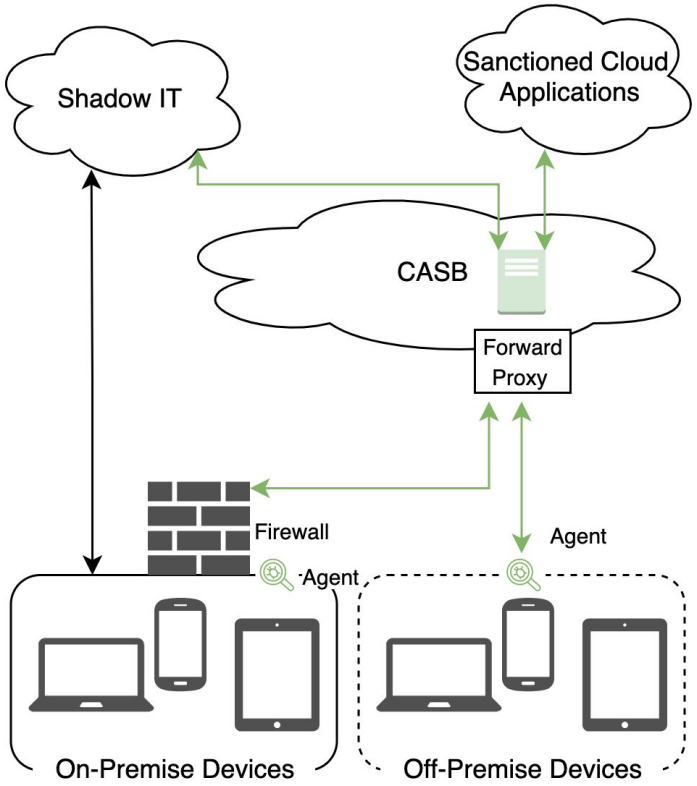
Background

- Shadow IT also known as unsanctioned IT
- Inline versus Out-of-Band



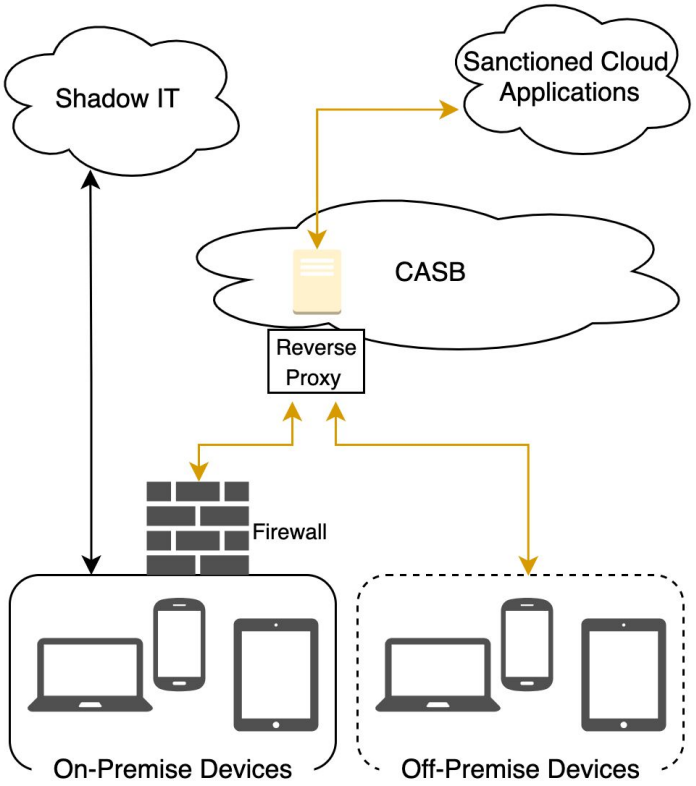
Background (Forward Proxy)

- Proxies (Inline protection)
  - **Forward** / Reverse
- Agents
  - Transparent / Explicit
- API (Out-of-band protection)



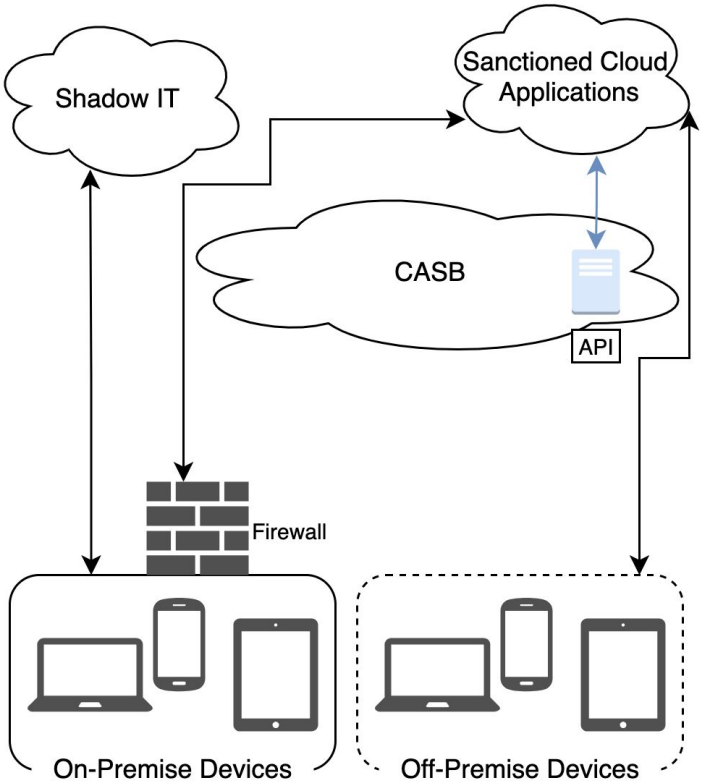
Background (Reverse Proxy)

- Proxies (Inline protection)
  - Forward / **Reverse**
- Agents
  - Transparent / Explicit
- API (Out-of-band protection)



Background (API)

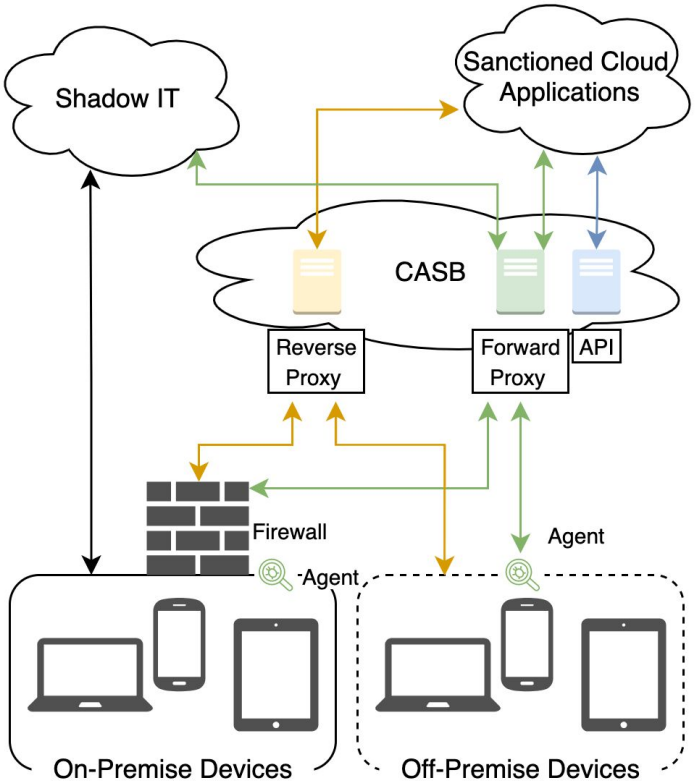
- Proxies (Inline protection)
  - Forward / Reverse
- Agents
  - Transparent / Explicit
- **API** (Out-of-Band protection)



Background (Cont'd)

- Four pillars of CASB
  - Visibility
  - Data security
  - Threat protection
  - Compliance

- Proxies (Inline protection)
  - Forward / Reverse
- Agents
  - Transparent / Explicit
- API (Out-of-band protection)



Related Work

- Gartner reporting on the subject…
  - Gartner (seminal, 2012): The Growing Importance of Cloud Access Security Brokers
  - Gartner (2020): Magic Quadrant for Cloud Access Security Brokers

- Academic work on the subject…
  - Wadhwa et al: Making Sense of Academia-Industry Gap in the Evolving Cloud Service Brokerage
  - Kaur et al: Enhancing Features Of Cloud Computing Using Cloud Access Security Brokers -To Avoid Data Breaches
  - Silic et al: Understanding Shadow IT risks, benefits and opportunities
  - Hulsebosch, UT: An analysis of cloud-based shadow IT and a framework for managing its risks and opportunities

Methodology

- Interviewing
  - Nine candidates originating from...
    - Cloud Service Provider
    - Professional Services Firm
    - Telecommunications
    - Managed Security Service Provider
    - Academia
  - Four CASB vendors...
    - Bitglass
    - McAfee
    - Microsoft
    - Netskope
- Literature Study
- Hands-on Review / Use Cases
  1. Assessing risk and compliance of cloud applications
  2. Enforcing fine-grained Shadow IT policies on cloud applications
  3. Ease of onboarding and implementation
  4. Aligning CASB policies with organizational structure

Results: The definition of CASB

- Market Guides
  - Text Analysis
- Interviews
  - Focus on Visibility over remaining pillars
- Providers
  - Introduce CASB to…
    - ...replace software and hardware (e.g. gateways)
    - ...discover Shadow IT
    - ...increase compliance

Software that addresses security gaps in an organization’s cloud usage by extending security policies leveraged from on-premise to the cloud

Results: Shadow IT and CASBs

- Identify the relationship between Shadow IT and CASBs
  - Analyzed one academic project and one master's thesis

- Approach Shadow IT in phases
  - Phase 1: Determine the Shadow IT being used - Discovery
  - Phase 2: Define policies to match organization risk appetite
  - Phase 3: Mitigate the unsanctioned apps to protect against threats

The relationship between Shadow IT and CASB is found within the extra contextual information that can be leveraged for an organizational perimeter

Results: Addressing Shadow IT with CASBs

- Validate risk assessment of cloud applications
  - Cloud Index
  - HTTP security headers

- Enforcing fine-grained Shadow IT policies on cloud applications
  - Relate to personally identifiable information
  - GDPR compliant
  - Data center housing in EU/preferably Netherlands
  - Set alerts if the risk level is medium risk
  - If more than X amount of data is transferred in X time

Header	Findings	McAfee	Microsoft	Netskope
Strict-Transport-Security	5/5	4/5	2/5	2/5
X-Content-Type-Options	5/5	3/5	3/5	2/5
X-XSS-Protection	5/5	3/5	3/5	3/5
Content-Security-Policy	5/5	3/5	2/5	1/5
X-FRAME-OPTIONS	5/5	4/5	2/5	4/5
Total rate	100% (25/25)	68% (17/25)	48% (12/25)	48% (12/25)

Table 1: Cloud Index Validation

Results: Mitigating overhead from CASBs

- Ease of onboarding and implementation
  - Scoping
  - Assisting Frameworks
  - Native Integrations
  - Managed Security Service Provider
- Aligning CASB policies with organizational structure
  - Scoping
  - Multi-tenancy
  - Fine-grained level
- Approach to mitigate overhead
  1. Onboarding Trajectory
  2. Integration with existing tooling
  3. Implementing organizational structure
  4. Piloting

Discussion

- Limited to the Dutch demographic
  - In the field of professional services, service providers, telecommunications and academia

- Validity of Cloud Index
  - Lack of transparency: unclear on the exact properties the Cloud Index attributes are based on

- Limited to the trial environments obtained

Conclusion

How do market-leading CASBs align with corporate expectations?

- Misalignment in…
  - ...level of requirements of the Dutch marketplace relative to the feature set of CASB vendors
- Try to address Shadow IT via…
  - ...their built-in Cloud Index are inaccurate and differ from one another
- Not mature enough on…
  - ...the ability to enforce *fine-grained* policies
- Alignment in…
  - ...ability to extend to native integrations of an organization

Leading CASBs are ahead of corporate expectations in regards to the featureset. While vendors are extending their capabilities, organizations are hesitant to implement a CASB while acknowledging the need of one.

Future Work

- Analyze the trend of vendors moving from standalone CASB to integrated within SASE platforms
- Analyzing the cloud indexing scores of CASBs more in-depth
- Case study implementation
- Evaluation of native integration with SIEM and/or SOAR

Summary

- We've researched...
  - ...the cloud access security broker (CASB) definition of organizations and vendors
  - ...where the relationship between Shadow IT and cloud access security brokers is found
  - ...how market leading vendors address Shadow IT with their CASB
  - ...how to mitigate administrative overhead generated with a CASB
- We've concluded...
  - ...the definition is 'Software that addresses security gaps in an organization's cloud usage by extending security policies leveraged from on-premise to the cloud'
  - ...the relationship 'between Shadow IT and CASB is found within the extra contextual information that can be leveraged for an organizational perimeter'
  - …that Shadow IT is addressed by applying cloud indexes and fine-grained policies
  - ...overhead can be mitigated through ease of onboarding, implementation and adjusting to an organizational structure