The Challenge of Cloud Security

Why CASB is not enough

What is SecureCloud?

Coronet SecureCloud is an autonomous, all-in-one cloud based service that enables every business to effortlessly secure its cloud operations such as SaaS, private and public cloud services, and access to infrastructure such as Azure, Google and AWS.

Coronet simplifies security by including all needed features to secure the cloud operations, including BYOD/BYON and all other elements outside of the traditional perimeter. SecureCloud eliminates the need for VDI/Container, MTD, DPM, CASB, access GW, Proxies, and the integration of those systems into a SIEM system.

SecureCloud removes the need for heavy implementation, integration, on-going maintenance and operation of multiple solutions. Thus, providing full implementation of cloud security in less than an hour for a fully automatic operation with no need for operators or SIEM solution.

Businesses need to protect the full cloud security chain, not just part of it

CASBs protect cloud data usage only when in fact, there are three other links in the security chain that could jeopardize the entire cloud security operation. The identity of the user and devices accessing the platform, the security posture of the device being used, and the security posture of network through which the connection is made. Securing an organization's cloud operations, with services such as Office 365, Dropbox, Salesforce, Box, G-Suits and others, can only be done by treating all parts of the security chain equally.

By activating a trust-based model, Coronet SecureCloud ensures that only trusted users, using trusted devices, connecting through trusted networks to trusted cloud services, can access corporate data. Any other solution that does

not encompass the full security chain, CASB included, will leave the operation vulnerable to data leaks, stolen credentials, and malicious software such as ransomware and malware.

Why is CASB not enough

For example, CASB will allow a user to use a rooted device that might damage the entire cloud operation due to its vulnerability. It will also allow a user to connect to the cloud using a compromised hotel WiFi network leading to credentials or data theft. , CASB will allow access from a public or temporary device that does not belong to the user or the enterprise having no knowledge of ransomware, malware, keyloggers, etc. that might compromise such device. Not only will CASB allow all of the above (and more), it will have no visibility into the potential risks and threats.

Therefore, it should be clear that in order to secure cloud operations, there is a need to handle the full security chain (user, device, network and service) and to provide visibility, access control and data control, rather than just use CASB which handles the data usage control on the service side.

The importance of having good visibility into all security aspects

To accurately detect threats that put corporate data and reputation at risk, all activities along the cloud security chain need to have clear visibility, access control and data control. An automatic actionable assessment needs to be made in the context of user identities, security posture of the devices they use, the networks they connect to and service properties. Real visibility for the full cloud security chain (user-device-network-service) must be a priority for an organization's security operation in order to meet most regulatory requirements and leading security practices. Only when achieving such visibility, risks can be identified and mitigated in real time. Using a CASB, which only has visibility into a user's actions on the service itself, provides a very limited point of view that cannot satisfy security compliance and leaves organization exposed.

Better visibility equals better control

Only with granular visibility into the whole chain one can set access control rules to provide access to specific user identities and the terms of its access, e.g, authorized device and network, as well as location based (geo-fencing) rules limiting access from specific locations.

> **For example, certain information and services can be used just in the office. Combining detailed visibility with easy-to-operate access control eliminates the threats of malware and ransomware infiltrating the cloud infrastructure, and prevent cloud data leakage through the device or network used.**

The final step to ensure a well-protected work process with cloud services does not end after access is granted, but only after it is guaranteed that the user is using corporate data safely. It needs to be set up in advance and monitored to understand what activities are allowed by whom, to prevent sensitive information from getting leaked or transferred, prevent malicious and unauthorized activities, identify malicious actors on services etc. While most CASBs excel the field of data control within the cloud services, they do not support access control (which user, device, and network are secured and authenticated to access the service), and rarely provide reasonable visibility, if any.

Integrated solution vs. all-in-one

Integrating all four factors of the security chain; user, device, network and cloud, through multiple security systems such as MTD, containers, proxies, gateways as well as CASBs requires substantial time, budget, and effort, as well as trained, dedicated teams to operate it. While the modern IT needs keep on growing this becomes impossible to maneuver, both from the personnel and the financial point of views. In a world where “simplicity is king”, this primitive way of combined services just doesn’t cut it. If it is not simple, it simply will not work. Only a fully automated system, connecting all four parts of the chain, can truly supply full end-to-end protection. A Single and strong engine controlling all cloud security aspects is the only way to eliminate the need for multiple systems implementation. The entire operation should be pre-integrated to all popular SaaS and IT tools and have a “set it and forget it” state of mind, shifting from anomaly detection to compliance and trust declaration.

Summary

CASBs protect cloud data usage only, when in fact, there are three other links in the security chain that could jeopardize the entire cloud security operation. CASB has no visibility into the potential risks and threats in the device, the network, or the user. Having visibility only into a user’s actions on the service itself provides a very limited point of view that cannot satisfy security compliance leaving organizations exposed.

The following chart compares CASB capabilities to SecureCloud, illustrating exactly where CASBs capabilities fall short.

	CASB	SecureCloud
Threat Analysis & visibility		
Malware/ransomware protection	✓	✓
IP based access threat identification	✓	✓
Geofencing based access identification		✓
identify threats due to device posture		✓
Identify threats due to network posture		✓
Identify threats due to behaviour analysis		✓
Identify threats due to impossible travel (geo-location based)		✓
Identify threats due to impossible travel (IP based)	✓	✓
Governance		
PII/PCI/EDR information control	✓	✓
Custom information control	✓	✓
IP based service filtering	✓	✓
Geofencing of services		✓
Document sharing	✓	✓
Certificate sharing	✓	✓
Geofencing of Admin activities		✓
Custom file type control	✓	✓
Behavior control	✓	✓
Sharing control	✓	✓
Admin activities control	✓	✓
GDPR compliance		✓
SOX compliance	✓	✓
HIPAA compliance		✓
Chinese regulation support		✓

	CASB	SecureCloud
Security		
Control access based on authorized devices		✓
Control access based on devices security		✓
Control access based on authorized locations		✓
Control access based on authorized networks		✓
Control access based on networks security		✓
Enforce context aware access control		✓
Enforce context aware data sharing control		✓
Control access based on suspicious login process	✓	✓
Operation in China		✓
Block spread of malware/ransomware		✓
Incident response management		✓
Infrastructure support		
Access control for Azure as PaaS/IaaS	✓	✓
Access control for Google as PaaS/IaaS	✓	✓
Access control for AWS as PaaS/IaaS	✓	✓
Cross border regulations support		✓