PRODUCT BRIEF

CLOUD ACCESS **SECURITY BROKER**

Discover your cloud applications and take control of your shadow IT.

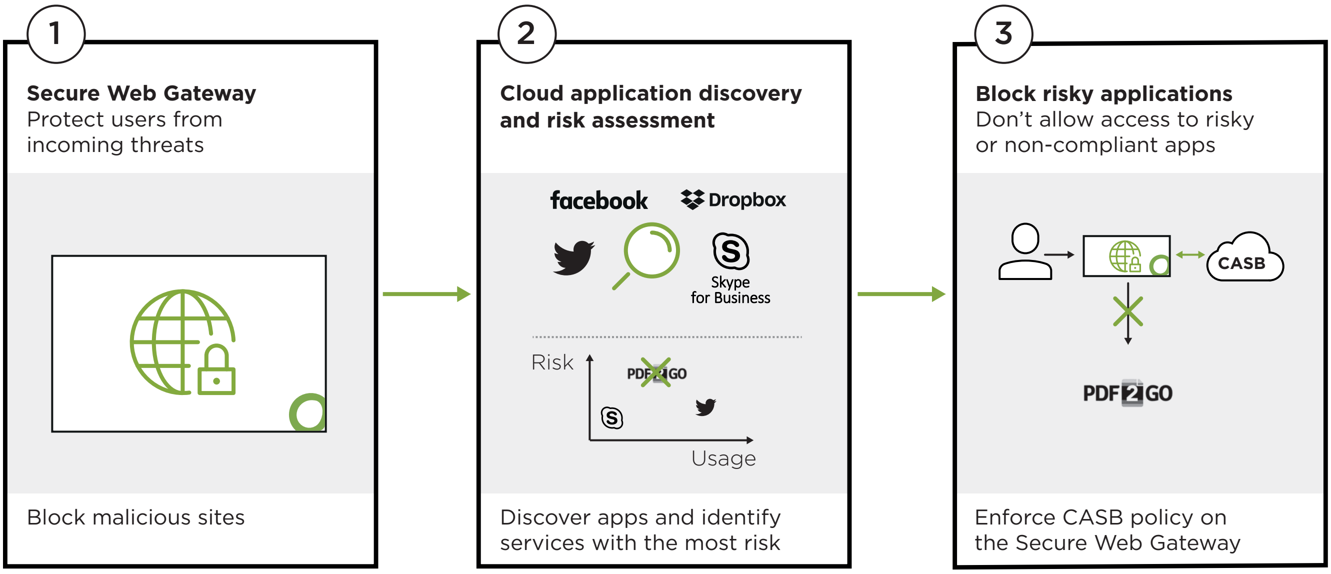
Get visibility across your cloud app landscape

With all types of cloud applications – those supported by IT and those brought in by users – now ubiquitous in the enterprise, organizations need a cloud access security broker (CASB) to confront data security and governance challenges. After all, the use of cloud applications by your workforce inevitably means that more of your sensitive data is now in the cloud.

Secure access to public cloud resources

The Open Systems CASB service smartly connects the Open Systems Secure Web Gateway with Microsoft Cloud Application Discovery and Security. You're able to continuously discover and monitor cloud application usage in your network and receive detailed risk assessments of current activity. In addition, you can use that information to enforce global CASB policies to block access to risky and non-compliant cloud apps on the Secure Web Gateway directly.

How CASB enables the cloud security journey



1

Secure Web Gateway
Protect users from incoming threats

Block malicious sites

2

Cloud application discovery and risk assessment

Discover apps and identify services with the most risk

3

Block risky applications
Don't allow access to risky or non-compliant apps

Enforce CASB policy on the Secure Web Gateway

Why the Open Systems CASB Solution?

SEAMLESSLY INTEGRATED

Benefit from CASB without suffering from the usual performance and security drawbacks.

INDUSTRY-LEADING TECHNOLOGY

Get access to best-of-breed CASB features that are seamlessly tied to your existing SASE services.

ADAPTED TO YOUR NEEDS

Get insights into your risk landscape and adapt your CASB policies to precisely match your needs.

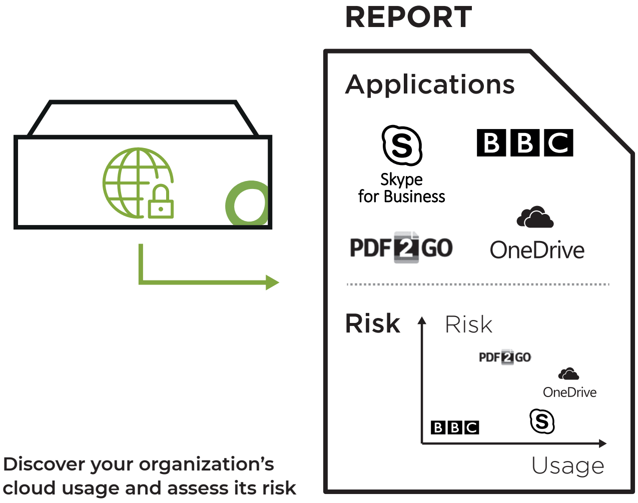
LEVERAGE INVESTMENTS

Make use of existing investments as CASB builds on Microsoft Cloud App Discovery and Security.

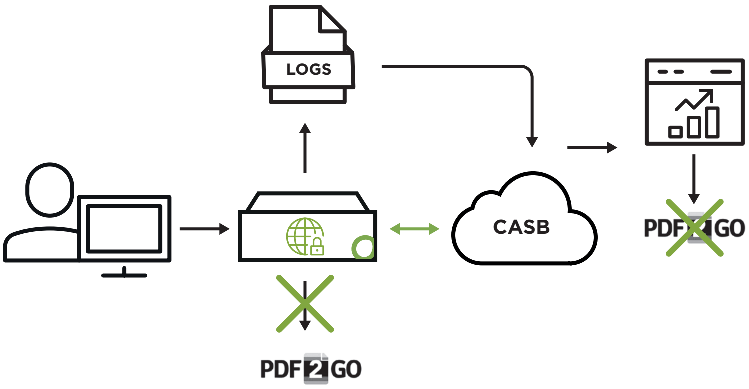
How does the Open Systems CASB work?

Cloud Application Discovery – free of charge

- Continuous overview of the risk score – and therefore the enterprise readiness – of cloud applications in use
- With an adequate license, get access to the cloud application discovery and security portal by Microsoft where you see all details of the application usage and the implied risk
- An overall risk level which can be customized to your company is calculated to express the overall risk of your cloud application usage
- Basis to take decisions on cloud application usage and data sharing policies



Discover your organization's cloud usage and assess its risk



Block access to risky or non-compliant cloud applications on Secure Web Gateway directly

Cloud Application Policy Enforcement

- Combination of the Open Systems Secure Web Gateway (SWG) and the third-party CASB product (Microsoft)
- SWG on the SASE edge: User authentication, malware and threat protection policies are enforced locally on the Open Systems SASE edge device (SWG)
- CASB enforced on the SASE edge: whenever a cloud app is declared as unsanctioned, it can be blocked on the Open Systems SASE edge device (SWG)
- Consulting for cloud application access policies is provided by the TAMs based on predefined use cases

Note: To benefit from Open Systems CASB Discovery or Policy Enforcement, the following preconditions apply:

- Open Systems Secure Web Gateway needs to be part of your portfolio – either as part of Managed SASE Enterprise, Enterprise+ or as a standalone service.
- Microsoft Cloud App Discovery or Microsoft Cloud App Security needs to be licensed. These are, for example, part of Microsoft 365 E3 and E5 or of Azure AD Premium Plans.

Open Systems connects and protects users, apps, and data everywhere they reside with a comprehensive, unified easy-to-use technology platform combined with an excellent 24x7 Managed SASE service.

Discover more at open-systems.com | Approved for public use.