SASE/SSE EBOOK

Cloud Access Security Broker (CASB) overview

Protection from shadow IT

CATO NETWORKS | WINDSTREAM ENTERPRISE

The digital transformation has been the leading force in the evolution of the modern business. In particular, the adoption of cloud-based Software as a Services (SaaS) applications has been a prominent trend which is constantly expanding. Many of these SaaS applications are being adopted and used by employees without the enterprise IT and security departments' knowledge and approval. They can also hold sensitive enterprise information and intellectual property without IT's knowledge.

These unsanctioned applications constitute an additional attack surface which can compromise the information stored within them. They are collectively referred to as "shadow IT", as organizations' IT and security teams do not have insight into their usage and cannot control their access and properly protect from the threats they pose.

This is where the Cloud Access Security Broker (CASB) comes into play and helps organizations cope with the perils of shadow IT. Beyond unsanctioned applications, CASB helps organizations control access to sanctioned applications as well, making sure only authorized users, using authorized credentials, are granted access.

An effective CASB solution should cover these four steps: **Visibility, assessment, enforcement, and protection.**

Step 1

Visibility

The first step in dealing with shadow IT is gaining visibility into your organization's usage of SaaS applications.

Windstream Enterprise CASB, powered by Cato, solution monitors all enterprise SaaS-bound traffic and provides a detailed shadow IT report which details all applications, both sanctioned and unsanctioned, being accessed and used (fig. 1).

The dashboard provides a bird's eye view of aggregate SaaS usage including number of total and high-risk applications, list of the highest risk applications, number of users accessing them, distribution by risk, application type, sanctioned vs unsanctioned, as well as type of data transferred to and from SaaS apps and the geographic location of SaaS providers' headquarters.

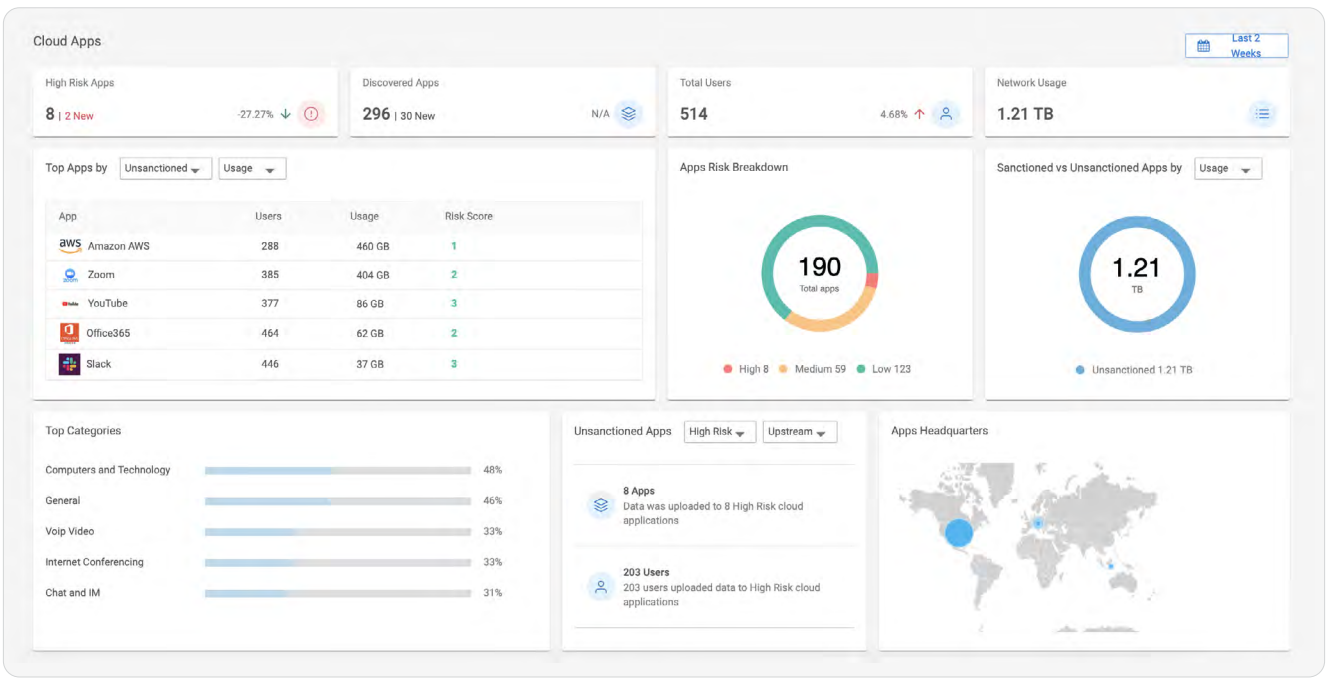


Figure 1: Shadow IT dashboard

Cato SASE/SSE Cloud's unique vantage point enables comprehensive and granular visibly into SaaS application usage. CASB provides detailed insight into each application's data consumption, users, geographic distribution, and other metrics for both inbound and outbound traffic. Each of the widgets containing this information can be further expanded to provide a deeper drill-down into the data with advanced filtering capabilities (fig. 2).

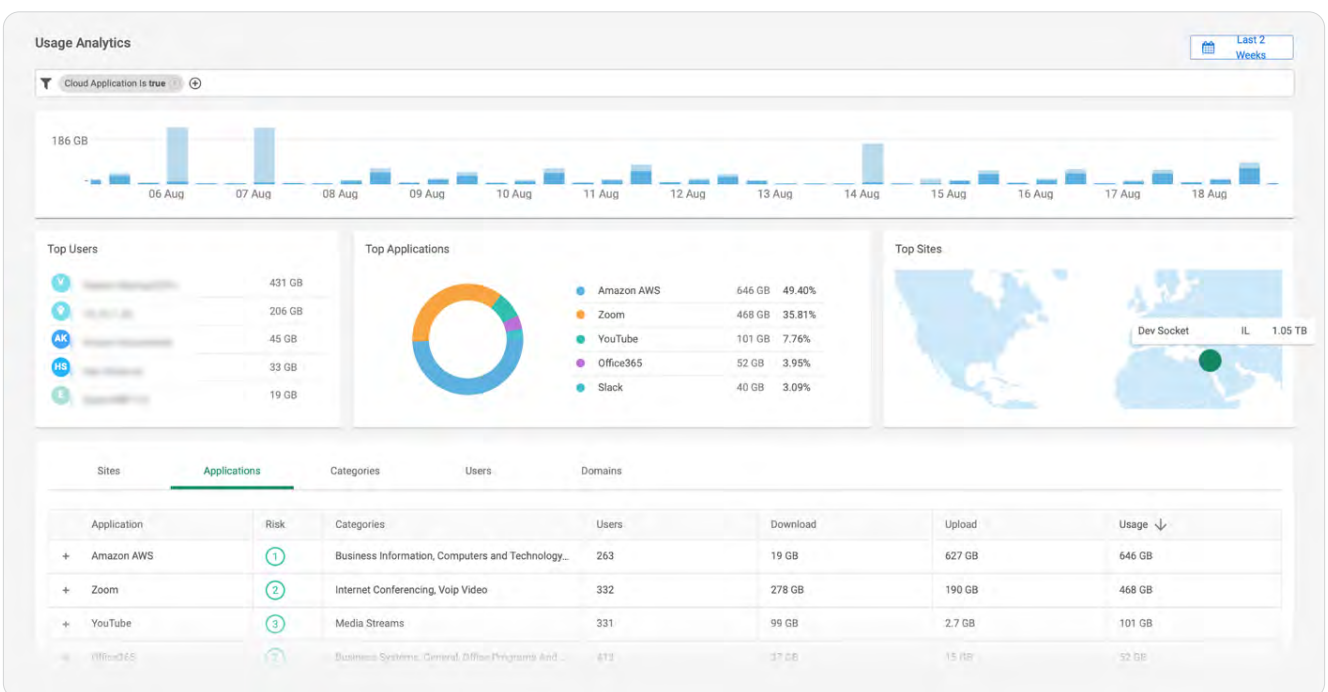


Figure 2: SaaS application drilldown

Step 2

Assessment

The second step in addressing shadow IT is performing a deeper analysis of specific application characteristics in order to better understand the potential risk it poses.

This analysis starts by collecting information about the application from several sources. Cato's CASB utilizes a unique Application Credibility Evaluator (ACE) which automates data collection and enables a quick and accurate assessment of each application's profile, resulting in an aggregated risk score (fig. 3). Cato CASB ACE saves substantial time and effort which would be otherwise needed to perform this process completely manually and improves security be providing a highly reliable analysis. The profile created by ACE provides insight into the application's purpose, publishers' credibility, degree of security or lack thereof, compliance, etc.

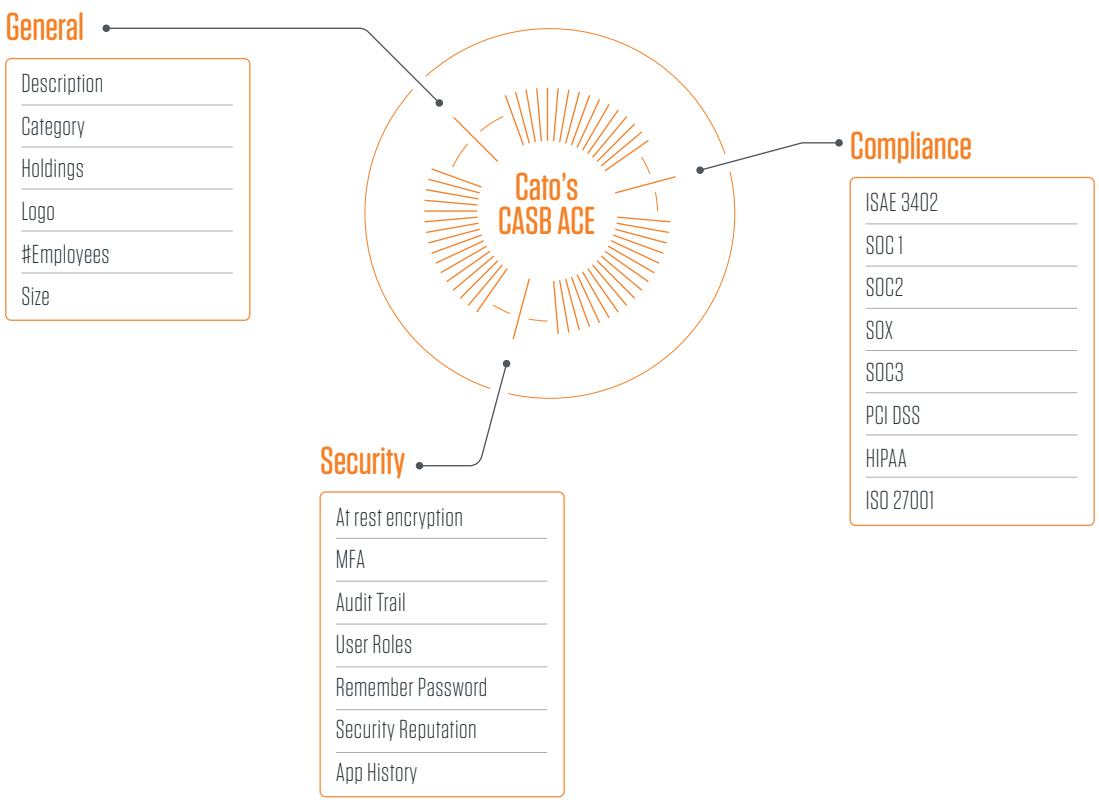


Figure 3: Application credibility engine

The ACE analysis result is shown in the Cloud Apps Catalog view (fig. 4). This enables IT teams to review each application and make a fully informed decision on whether, and how, they should enable employee access to it.

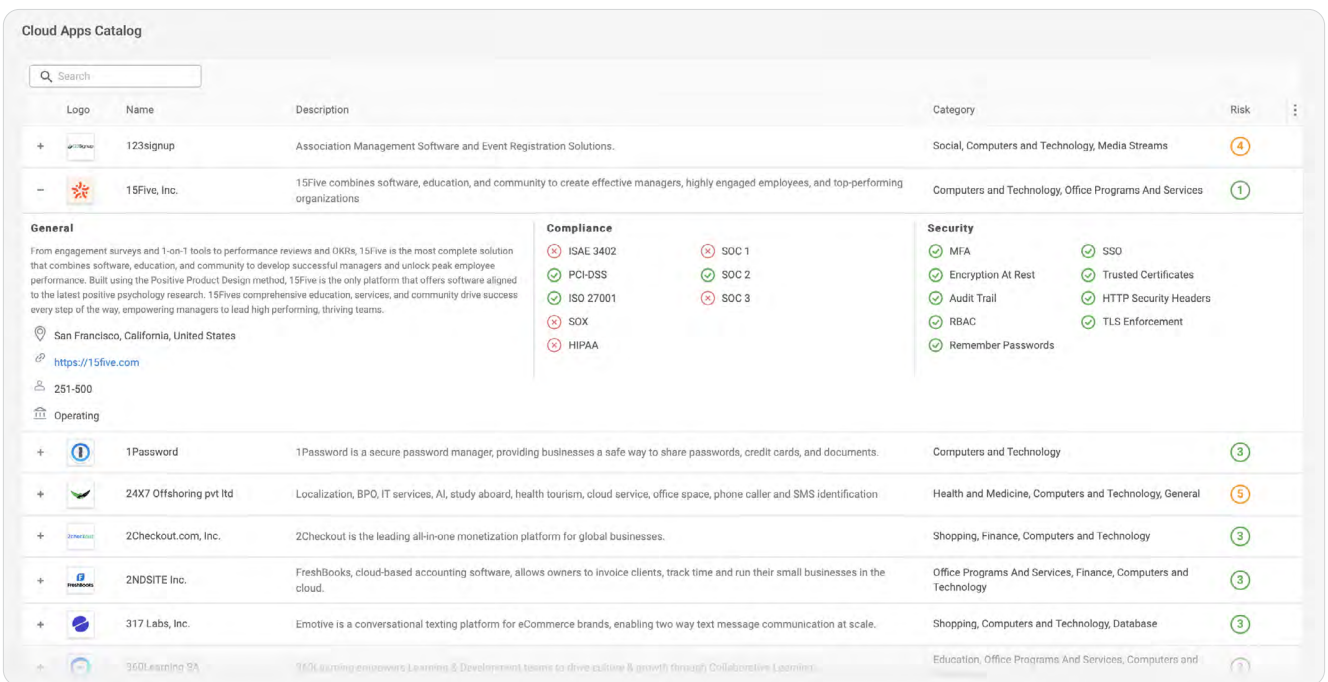


Figure 4: Cloud applications catalog

Step 3

Enforcement

The third step in dealing with shadow IT is controlling access to it.

Once the analysis phase is done and the required access policy is determined for each app, the rules which will enforce this policy can be defined via the Cato Secure Access Service Edge (SASE) with Security Service Edge (SSE) Cloud Management Application. The "CASB Policy Rules" view lists all defined rules with the applications they have been defined for, the matching criteria, the specified action to be taken in case the rule applies, the associated severity level and whether an alert or event should be generated (fig. 5). The list can be filtered to display a subset of rules with common criteria.

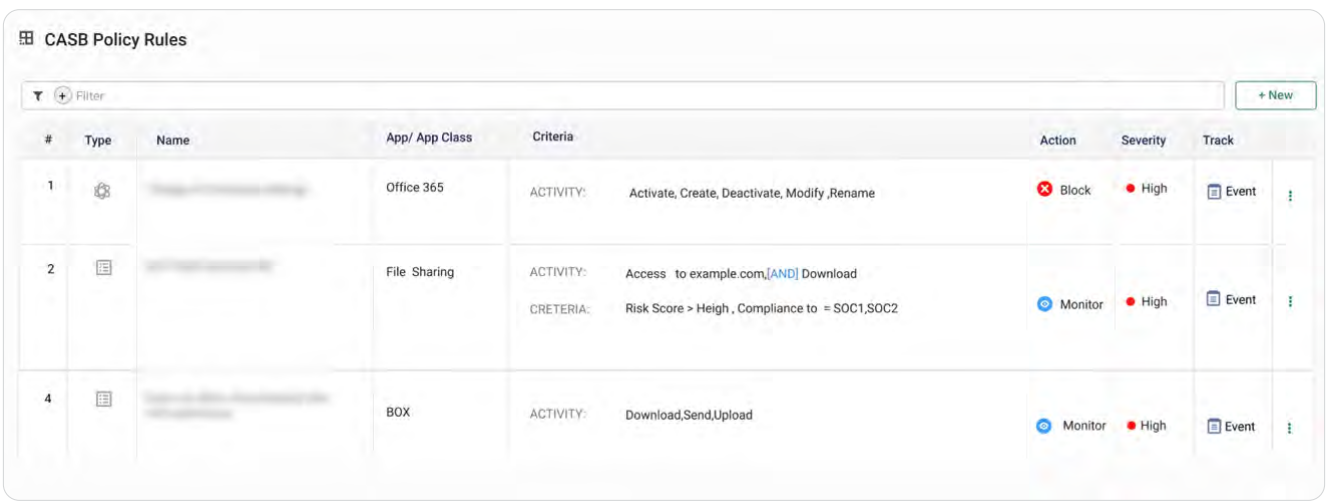


Figure 5: CASB policy rules view

Adding a new rule is a simple and intuitive process yet it offers high granularity and flexibility. By clicking the "+New" button on the top right side, we are presented with the "New Cloud App Rule" dialog which enables us to define rules for specific applications or application categories, the endpoint type (e.g., OS or user agent), defined device posture profiles, data profiles, time frames, type of actions requested, aggregate risk score as well as specific attributes (e.g., compliance or use of certain security services) (fig. 6).

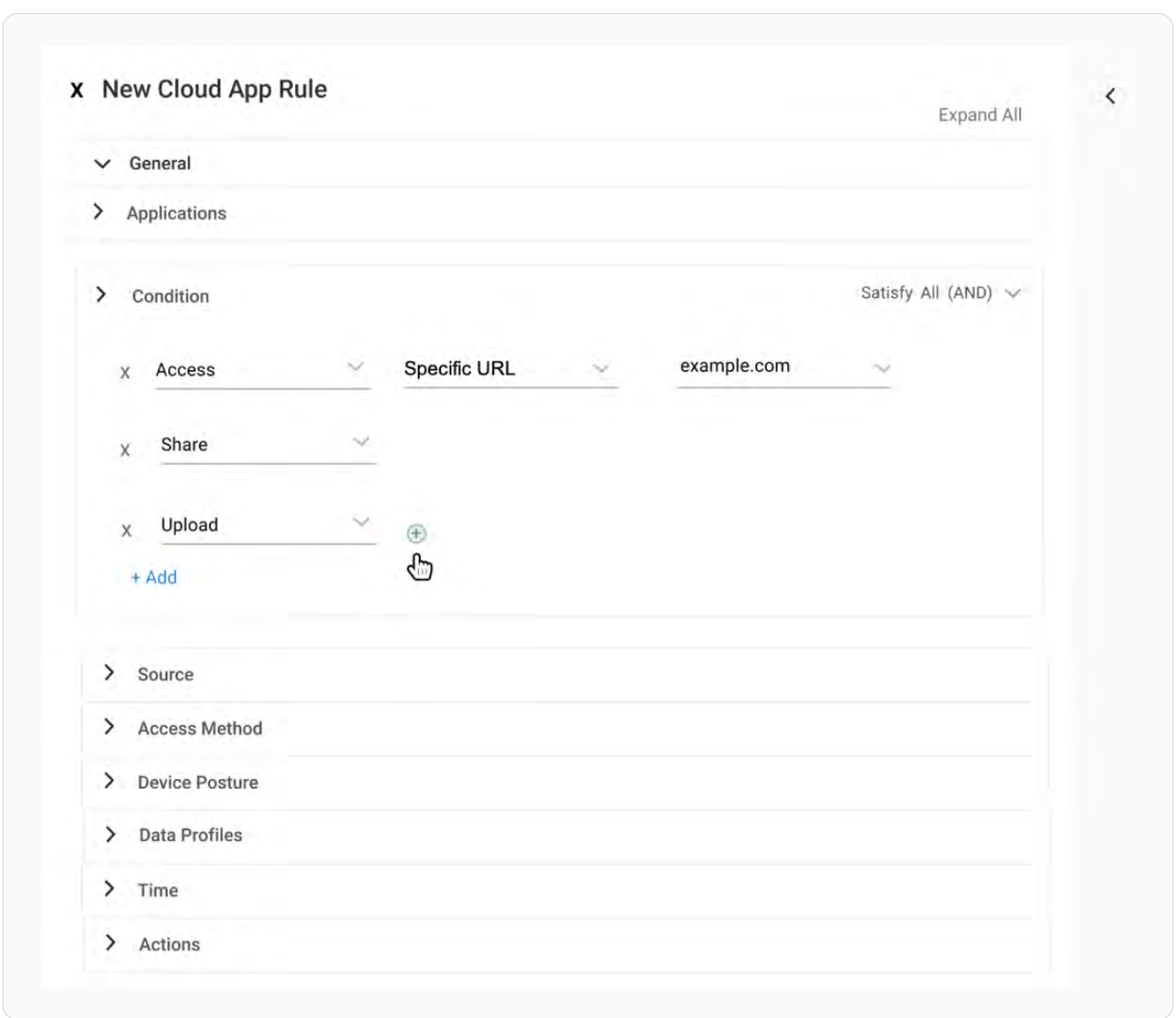


Figure 6: Defining new rules

This enables IT managers to define policies which cover a wide range of use cases, for example:

- Block access to file sharing applications which have been classified as high risk.
- Restrict Office365 access to corporate account only (block private accounts).
- Allow the sales department to use MS Teams chat, but not file sharing.
- Allow access to defined Dropbox accounts only.

Step 4

Protection

The last stage of dealing with shadow IT is to provide protection from threats which can compromise the enterprise's security.

Cato's converged security suite comes into play. By unifying all the security services in a single software stack running in each of our cloud PoPs, all SaaS traffic passing through the PoP is analyzed by all security services.

The security services include:

Next Generation Firewall (NFGW)

Secure Web Gateway (SWG)

Intrusion Prevention System (IPS)

Next Generation Anti Malware (NGAM), including real-time zero-day malware prevention

Data Loss Protection (DLP)

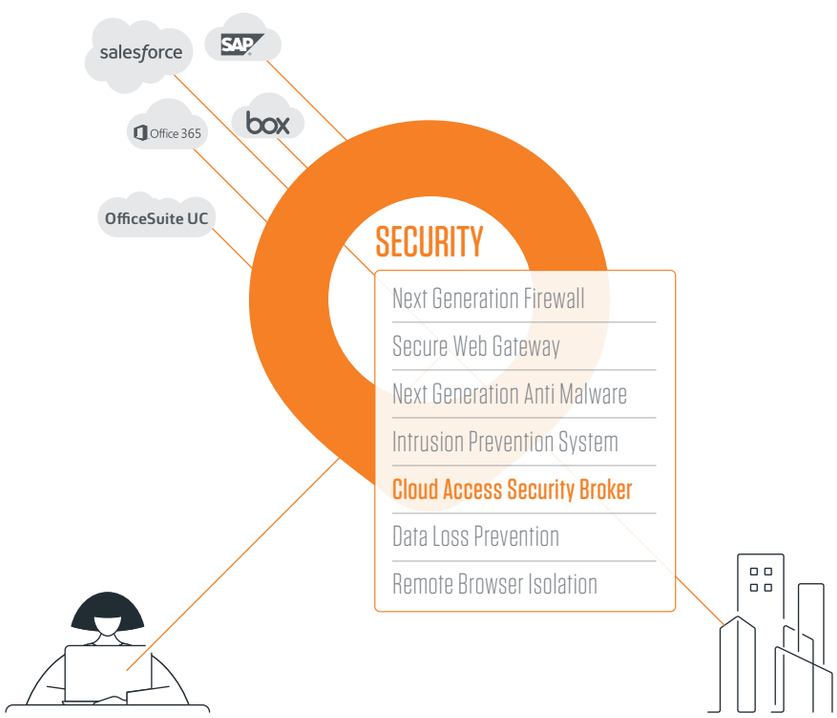
Combining the above security tools, CASB provides comprehensive protection for all SaaS traffic. In addition, since SASE/SSE Cloud includes a remote access solution (SDP/ZTNA) which is also embedded into each PoP, all the above security services are applied also to remote users accessing SaaS applications and providing full protection to employees working from anywhere.

The advantage of Windstream Enterprise SASE, powered by Cato

A CASB solution is critical tool for enabling enterprises to cope with SaaS usage and shadow IT. However, when deployed as a stand-alone product it requires integration with additional security solutions which can lead to increased complexity and lack of visibility.

Deploying CASB as part of a Windstream Enterprise SASE/SSE architecture simplifies the network and improves visibility and overall security by utilizing a fully converged security and networking software stack embedded into each PoP. Our SASE/SSE Cloud also leverages a private global backbone to optimize SaaS application performance by implementing prioritization, QoS, TCP optimization, and packet loss mitigation techniques, and offering resilient connectivity across the globe.

The converged software stack utilizes a unique Single Pass Architecture Engine (SPACE) which enables a unified view and decision process in contrast to the chaining of siloed stand-alone products. The same processing is applied to all traffic, including remotely connected users. Lastly, our SASE/SSE Cloud offers single-pane-of-glass management, covering all security and networking services in a unified console.



Our SASE solution

Windstream Enterprise is the first and only North American managed service provider to converge cloud-native network and security into a fully integrated Secure Access Service Edge (SASE) solution. This comprehensive architecture enables businesses to adapt to constantly shifting users, applications and work environments, while keeping application and security policies synchronized with these changing endpoints—all from a single pane of glass.

SASE Cloud with SSE