secureaccess.com

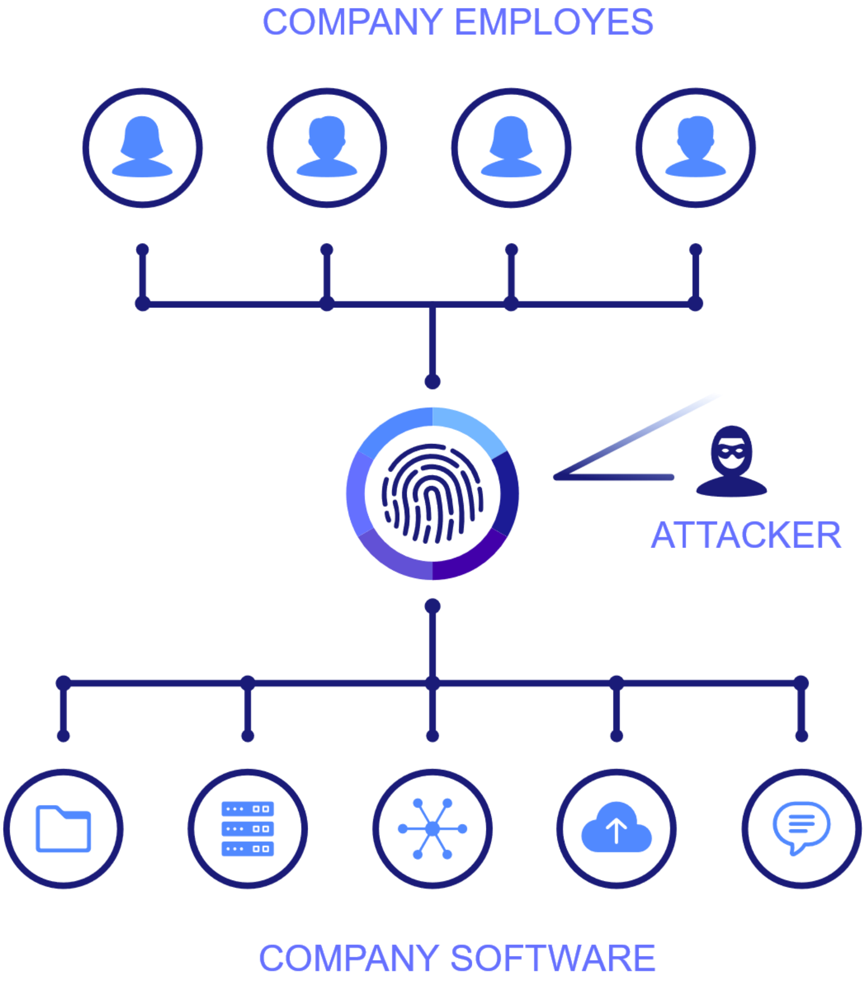
WHITE PAPER

APRIL 2019

INDEX OF CONTENTS

1. INTRODUCTION

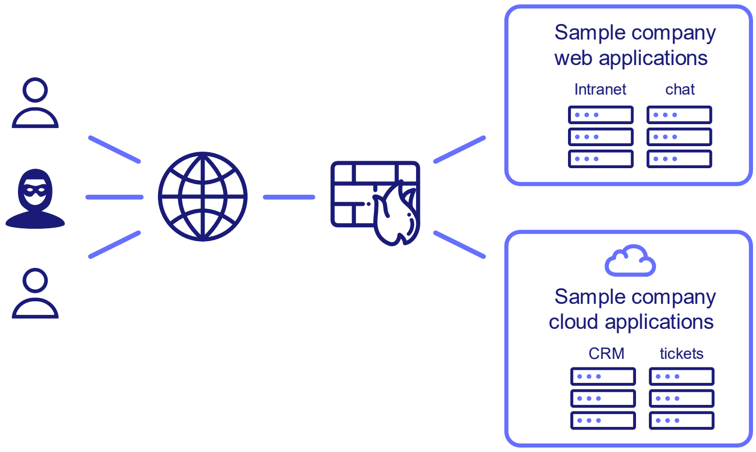
Any web application or website exposed to the Internet is susceptible to attacks. In many cases companies have no choice but to expose these web applications to the internet, so that employees, remote workers and partners can access them.



2. PRODUCT DESCRIPTION

2.1. Current problem

In most companies, internal web applications are placed behind a firewall to isolate them from the internet. This firewall needs to allow legitimate users to the web application, so rules are created for this to happen. Poor setup, bad configuration and new exploits in firewall firmware and software mean that many firewalls do not work as intended and web applications are exposed to the internet with the subsequent security risk that this entails. Due to the complexity of maintaining the firewall, some companies don't bother with them at all and choose convenience over security. New vulnerabilities are detected and published each day. This can affect the software that runs on the exposed servers and automatically poses a risk to the security of all information and corporate infrastructure.


Sample company web applications
Intranet
chat
Sample company cloud applications
CRM
tickets

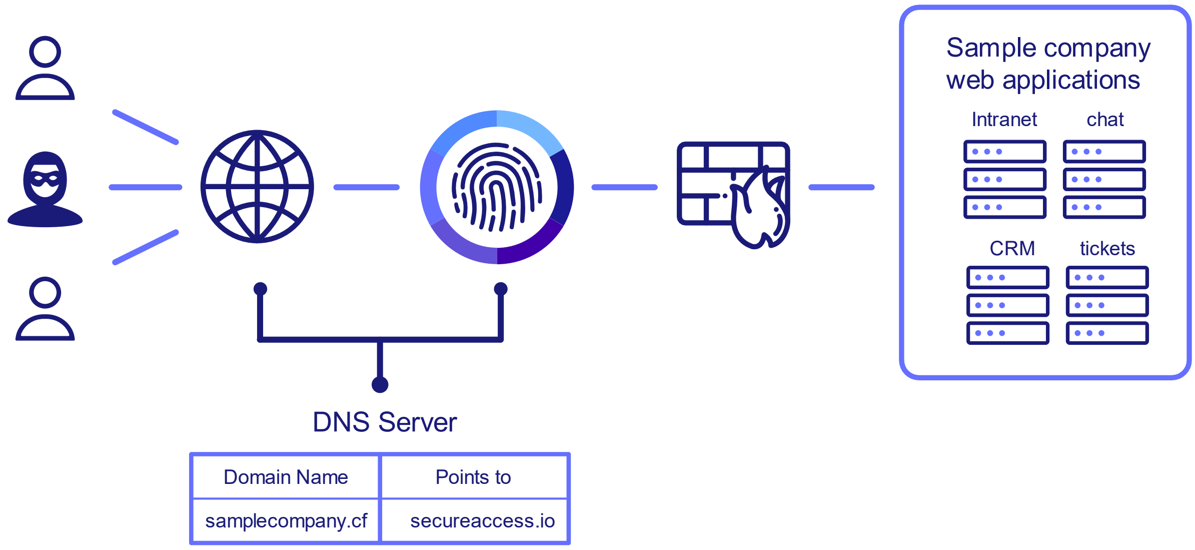
One solution to this problem is to completely isolate internal web applications and create a VPN that allows users to access from outside the internal network. Unfortunately, this is a complex and difficult to maintain system.

2.2. SecureAccess® CLOUD as a solution

SecureAccess® CLOUD is a cloud-based access control service. It provides an additional layer of security to Internet facing web applications.

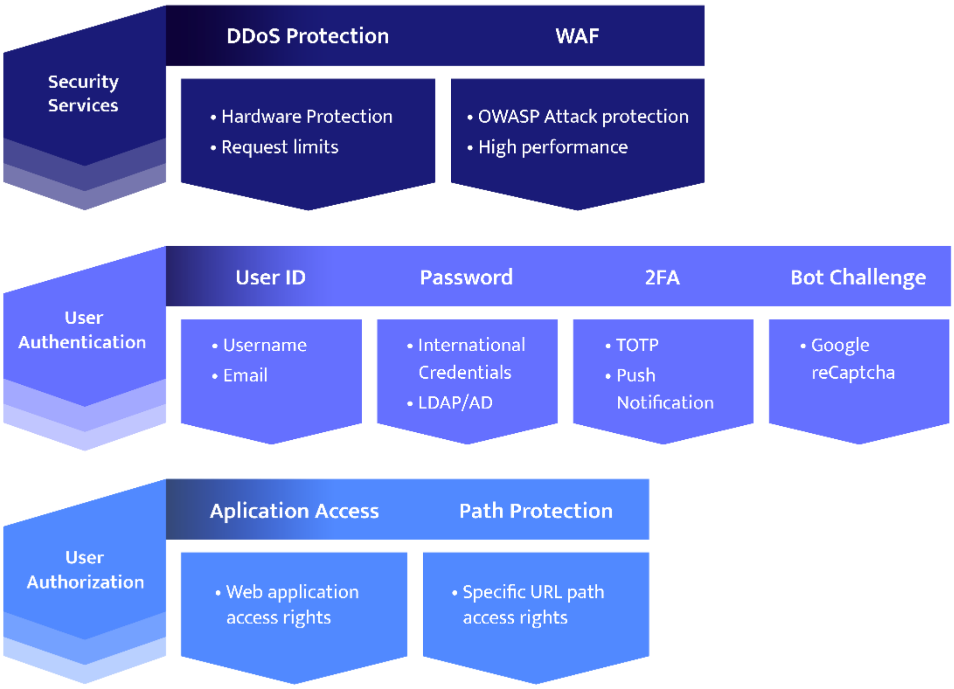
To tackle this problem, SecureAccess® CLOUD proposes a simple but effective solution that doesn’t involve complex VPN setup and maintenance. It acts as an access control layer between corporate web applications and the internet.

Users can not access the final web application without first going through the process of validating their credentials in SecureAccess® CLOUD. If users cannot pass the validation, they will be unable to access the web application and attackers will be unable exploit any vulnerabilities in the web application.

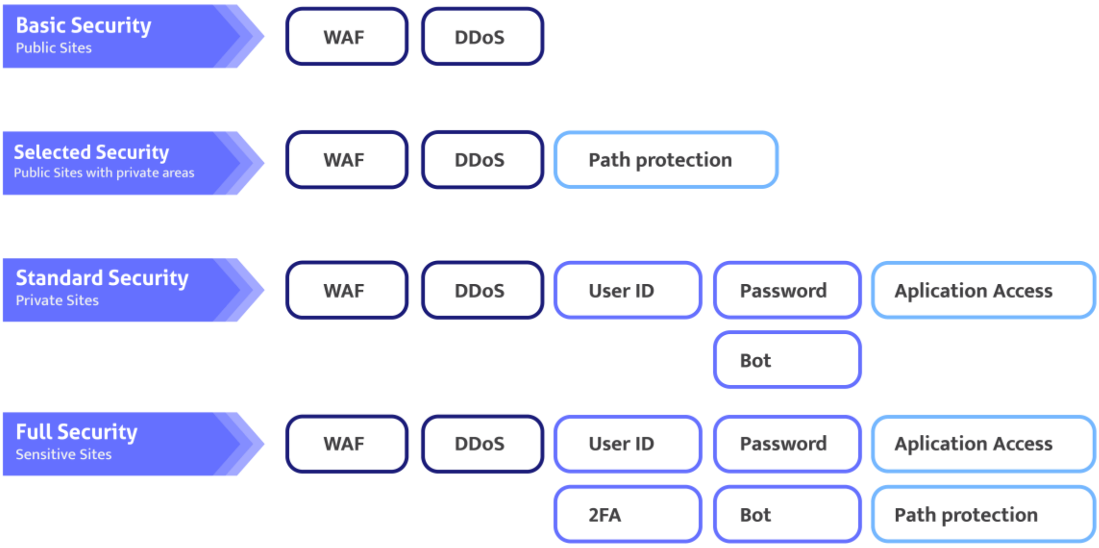


Domain Name	Points to
samplecompany.cf	secureaccess.io

Placing SecureAccess® CLOUD between end users and your servers brings multiple security features that are distributed in a configurable multilayer architecture. These features are distributed in three layers: Security Services, Authentication and Authorization.



Each one of the contain several modules that can be enabled to obtain the level of security required for each protected web application:



2.3. SecureAccess benefits

SecureAccess® CLOUD can integrate every type of web application: from project management tools, corporative wikis, CRM / Intranet, to error-monitoring systems and panel administrations for any type of network. Moreover, SecureAccess® CLOUD does not require installation of additional software or complex configurations.

SecureAccess® CLOUD further enhances security with double factor authentication, introducing its own phone application: SecureAccess ® 2FA. It prevents the access of non-legitimate users to the corporate web applications. It offers a full access control service without the need for extra authentication providers.

SecureAccess® CLOUD allows organisations to protect their web applications simply and cost effectively whilst ensuring scalability and granularity in access control. All this is managed from a simple intuitive configuration panel and with data visualisation of the use of the platform.

SecureAccess® CLOUD integrates a WAF that follows a set of configurable rules to allow genuine requests to pass and blocks malicious requests from reaching the final web applications.

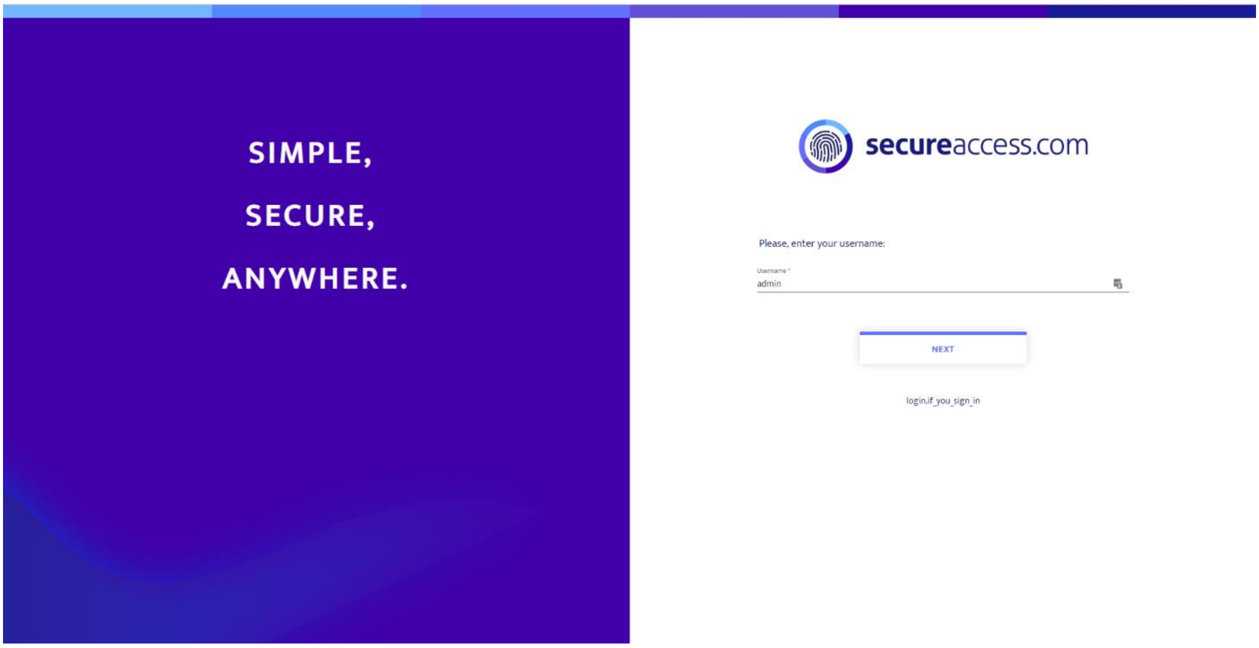
SecureAccess® CLOUD encrypts all traffic without affecting the company's performance or connection speed.

SecureAccess® CLOUD generates HTTPS certificates for free and offers the possibility to install your own certificates through the administration panel.

3. MAIN FEATURES

3.1. Unified Secure Access

To access the web applications protected by SecureAccess® CLOUD, users must enter their credentials in the access screen and go through the user-friendly login process.

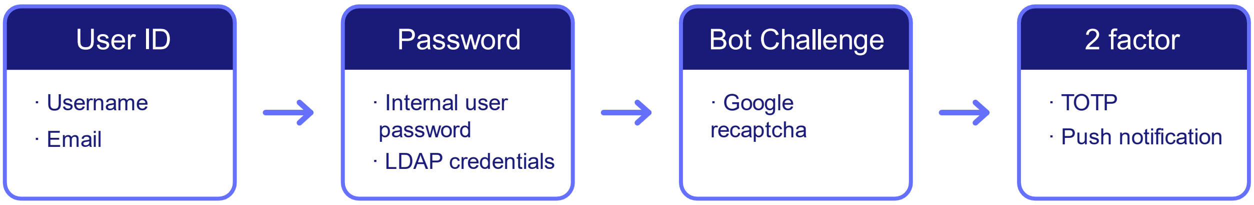


Please, enter your username:

Username *
admin

This process is designed to avoid providing unnecessary information to malicious users trying to brute force their way into the platform. Even when a user fails one of the challenges (such as username or password) the next one is prompted and in the end the authentication will fail leaving the attacker unable to know which element of the process they failed.

The user must face a set of configurable challenges in order to prove its identity. The following is an example of SecureAccess´s secure login flow:



User ID
· Username
· Email

Password
· Internal user password
· LDAP credentials

Bot Challenge
· Google recaptcha

2 factor
· TOTP
· Push notification

3.2. Two Factor Authentication

SecureAccess® CLOUD allows you to configure a second factor of authentication in the user’s identification process. With this integration it is possible to keep attackers out of your web applications even when user's credentials are compromised. SecureAccess® CLOUD offers three different 2Factor mechanisms out of the box:

- **TOTP (Time-Based One-time Password).**
- **Push notification.**
- **U2F hardware key**

For TOTP or Push mechanisms users can use SecureAccess® 2FA Mobile application to generate the TOTP access token or receive the push notifications on their mobile devices.

SecureAccess® CLOUD is compatible with FIDO U2F and FIDO 2 security keys.

3.3. Security features

Data for each customer is stored in different **independent databases**, guaranteeing that configuration, user and platform usage data is protected and safe from unwanted access.

If you don't have your own **SSL certificate**, SecureAccess® CLOUD allows you to generate them automatically and transparently, which helps you navigate securely among your web applications.

Additionally, in order to protect your web applications SecureAccess® CLOUD offers an integrated **Web Application Firewall (WAF),** that enables you to enter a set of configurable rules to allow genuine requests to pass and blocks malicious requests from reaching the final web applications.

SecureAccess® CLOUD customers are automatically **protected against Denial of service attacks** levering the hardware infrastructure the platform is running on.

3.4. Secure and fast communications

All communications between internet users, SecureAccess® CLOUD and the final web application are made through HTTPS connections, assuring the confidentiality of the data throughout the transmission.

The administrative user responsible for configuring SecureAccess® CLOUD can include corporate certificates or use the out of the box feature to automatically generate valid certificates from the dashboard.

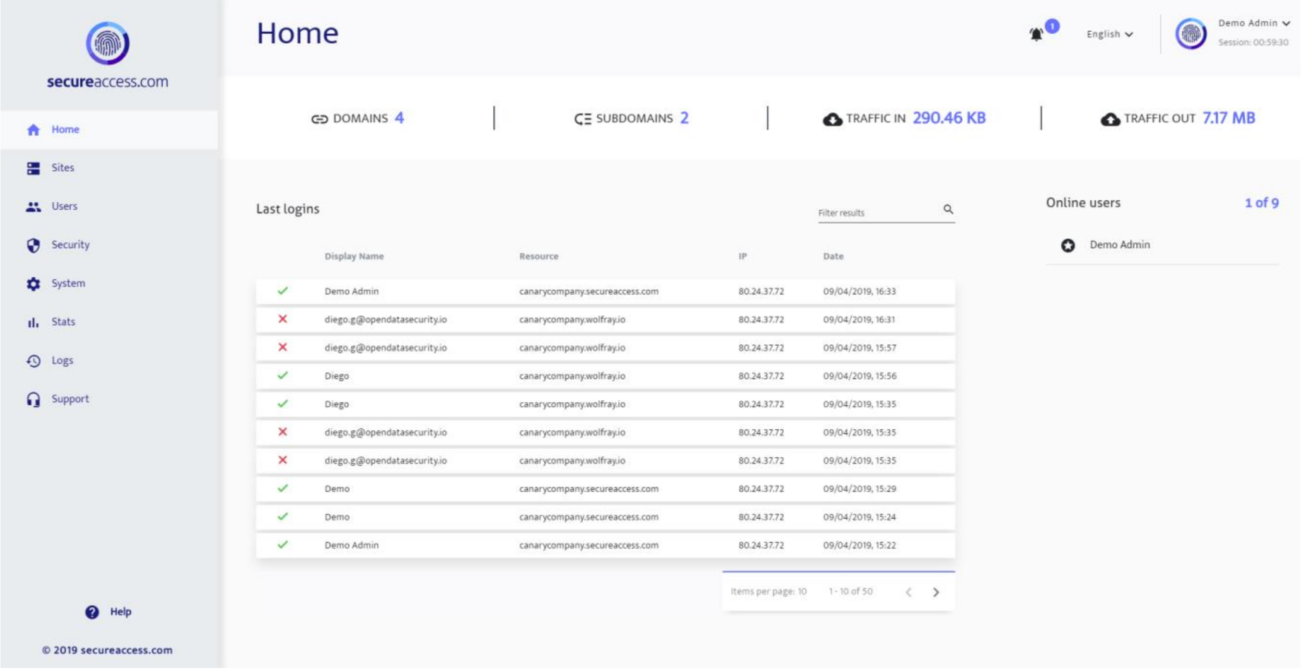
3.5. Scalability and high availability

SecureAccess® CLOUD is a cloud service that guarantees the availability of the service through redundancy mechanisms both at the server and database level. To be able to support large numbers of concurrent users, SecureAccess® CLOUD has an intelligent configuration that automatically increases the infrastructure in which it runs based on the current user demand.

3.6. Administration panel

SecureAccess® CLOUD allows the system administrators to easily configure everything related to users and control access to web applications. You can also monitor the use of the platform with data in real time.

3.6.1. Data monitoring

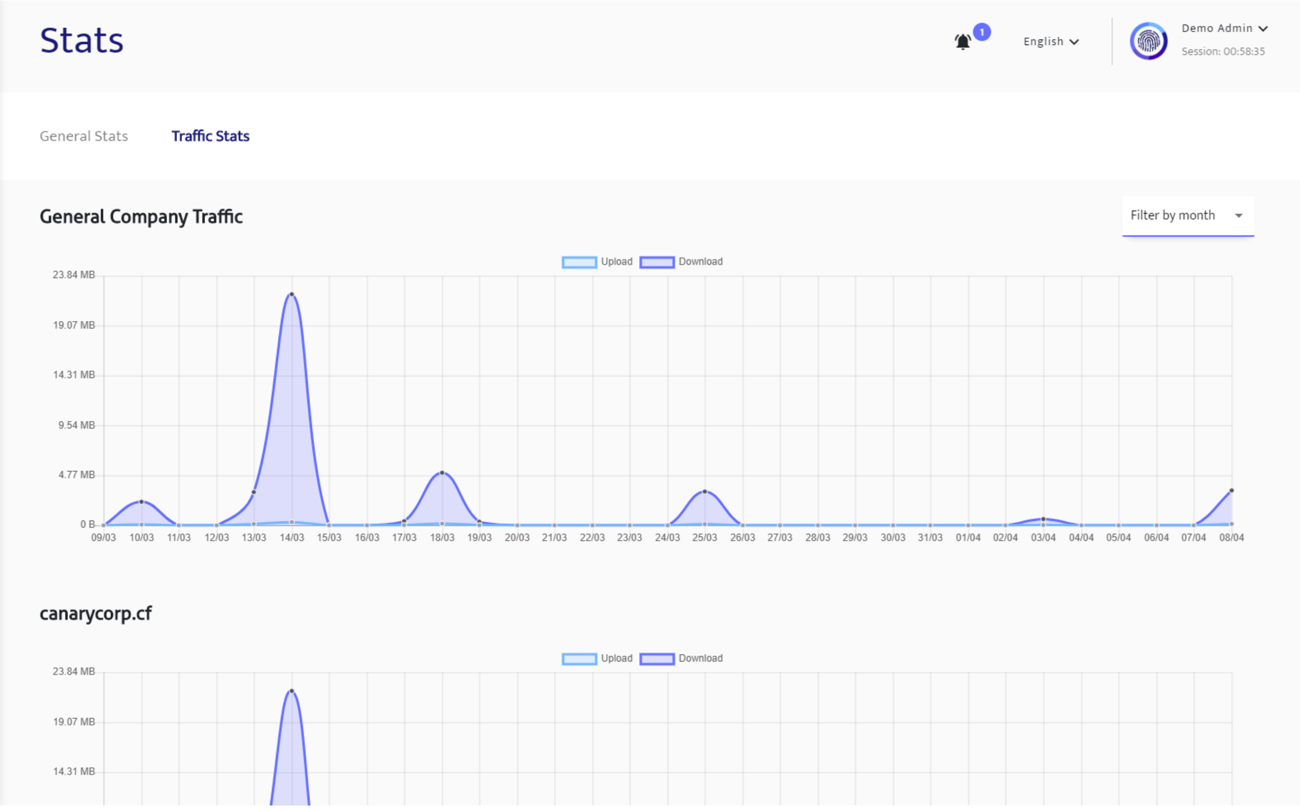


Last logins

	Display Name	Resource	IP	Date
✓	Demo Admin	canarycompany.secureaccess.com	80.24.37.72	09/04/2019, 16:33
✗	diego.g@opendatasecurity.io	canarycompany.wolfray.io	80.24.37.72	09/04/2019, 16:31
✗	diego.g@opendatasecurity.io	canarycompany.wolfray.io	80.24.37.72	09/04/2019, 15:57
✓	Diego	canarycompany.wolfray.io	80.24.37.72	09/04/2019, 15:56
✓	Diego	canarycompany.wolfray.io	80.24.37.72	09/04/2019, 15:35
✗	diego.g@opendatasecurity.io	canarycompany.wolfray.io	80.24.37.72	09/04/2019, 15:35
✗	diego.g@opendatasecurity.io	canarycompany.wolfray.io	80.24.37.72	09/04/2019, 15:35
✓	Demo	canarycompany.secureaccess.com	80.24.37.72	09/04/2019, 15:29
✓	Demo	canarycompany.secureaccess.com	80.24.37.72	09/04/2019, 15:24
✓	Demo Admin	canarycompany.secureaccess.com	80.24.37.72	09/04/2019, 15:22

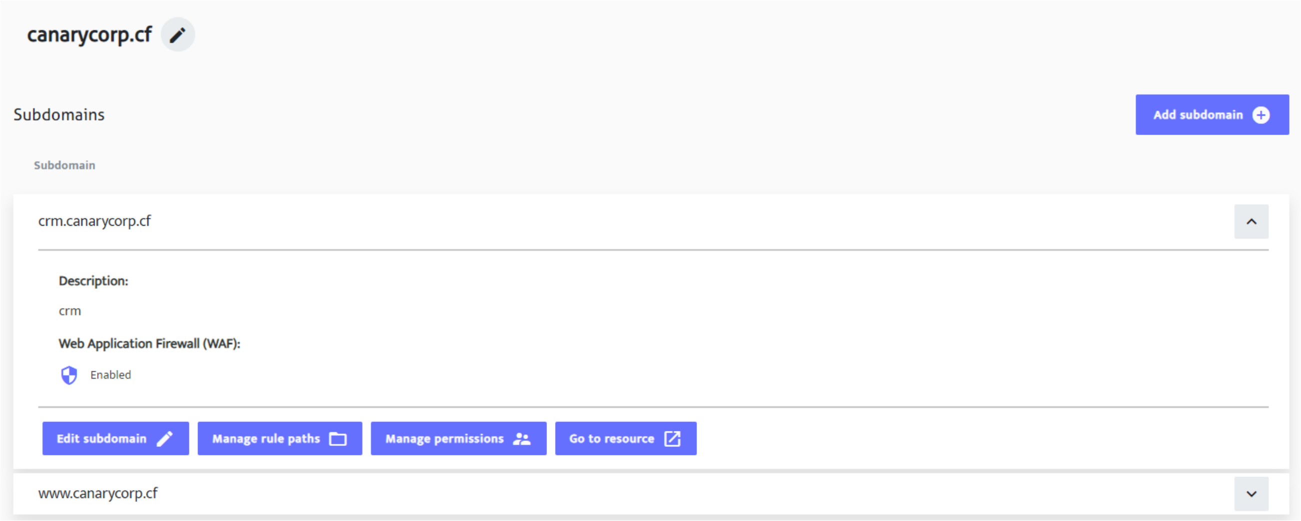
The SecureAccess® CLOUD administration panel shows real-time data accesses to the final web applications to allow the monitoring of which valid and invalid requests are made, at any time. It also shows information about the location, devices and browsers from which users access.

SecureAccess® CLOUD provides system administrators with tools to monitor the bandwidth consumption of each web application through interactive graphics in a specific time period or in real time.



3.6.2. Access configuration

In the administration panel you can register multiple domains and subdomains that point to the corporate web applications. For each of these web applications you can define access permissions at the group level or individual users allowing granularity when controlling authorisations.



crm.canarycorp.cf

Description:
crm

Web Application Firewall (WAF):
Enabled

www.canarycorp.cf

3.7. Always updated

Thanks to the fact that it is cloud-based, all SecureAccess® CLOUD customers receive the latest updates immediately. We always guarantee retroactive compatibility between new versions to ensure that the service continues to work for all our customers.