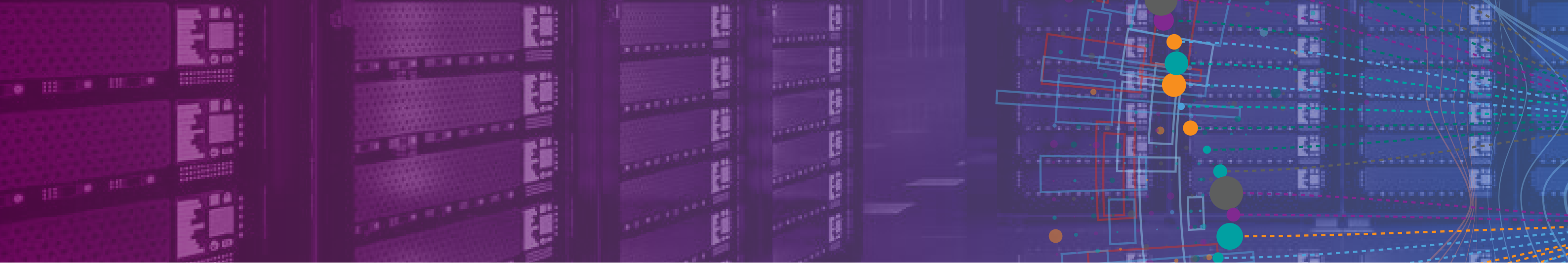
SAFE-T

Keeping Data in the Right Hands

Anonymous Application Access

Product Brief

Contents



Introduction

With the move to the digital enterprise, all organizations regulated or not, are required to provide customers and anonymous users alike with access to applications, to upload files. Examples include:

- ✓ **Bank customers, transfer an image of scanned check from a mobile app to a backend service**
- ✓ **Job applicant uploads a CV file to a jobs portal**
- ✓ **Insurance company customers, uploading a signed contract into the insurance company's CRM system via a portal**
- ✓ **Healthcare practitioner uploading an X-ray image to the HMOs system**

However, if the digital service is not deployed with access lifecycle and security considerations in mind, the organization risks exposing itself to external attacks such as network DDoS, malware, ransomware, application level attacks, etc.

In addition, if monitoring of the flow is not implemented, visibility into the user's usage of the service cannot be achieved, and resolution of usage error becomes a lengthy and complicated process.

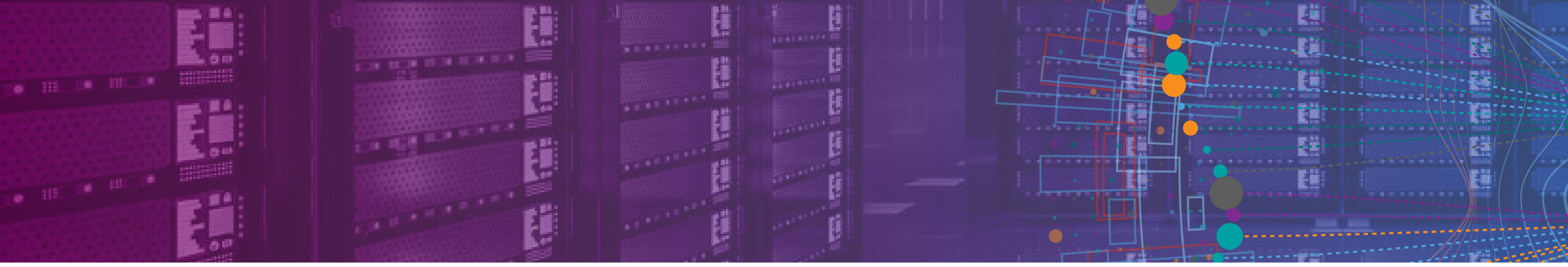
The Safe-T Solution

Safe-T Software Defined Access offers organizations the means and technology to easily and securely offer new file upload scenarios for both customers and anonymous users.
Built on Safe-T's Software Defined Perimeter technology and Integrated Data Security Platform, Safe-T allows greatly simplify the launch of new services without compromising on security, compliance on regulation, or end user ease of use.

How It Works

As can be seen in figure 1 below, the Safe-T Anonymous Application Access solution is composed of an access component and a data exchange component. The solution is deployed in multiple tiers within the organization:

- **DMZ tier –** includes an Access Gateway which is located after the organization's portal to which the user uploads the file
- **Anti-Malware tier -** includes an Access Controller, Data Exchange Server, and an Access Gateway. The Data Exchange Server connects to the organization's anti-malware solution
- **Lan tier -** includes an Access Controller and Data Exchange Server. The Data Exchange Server connects to the organization's backend application.



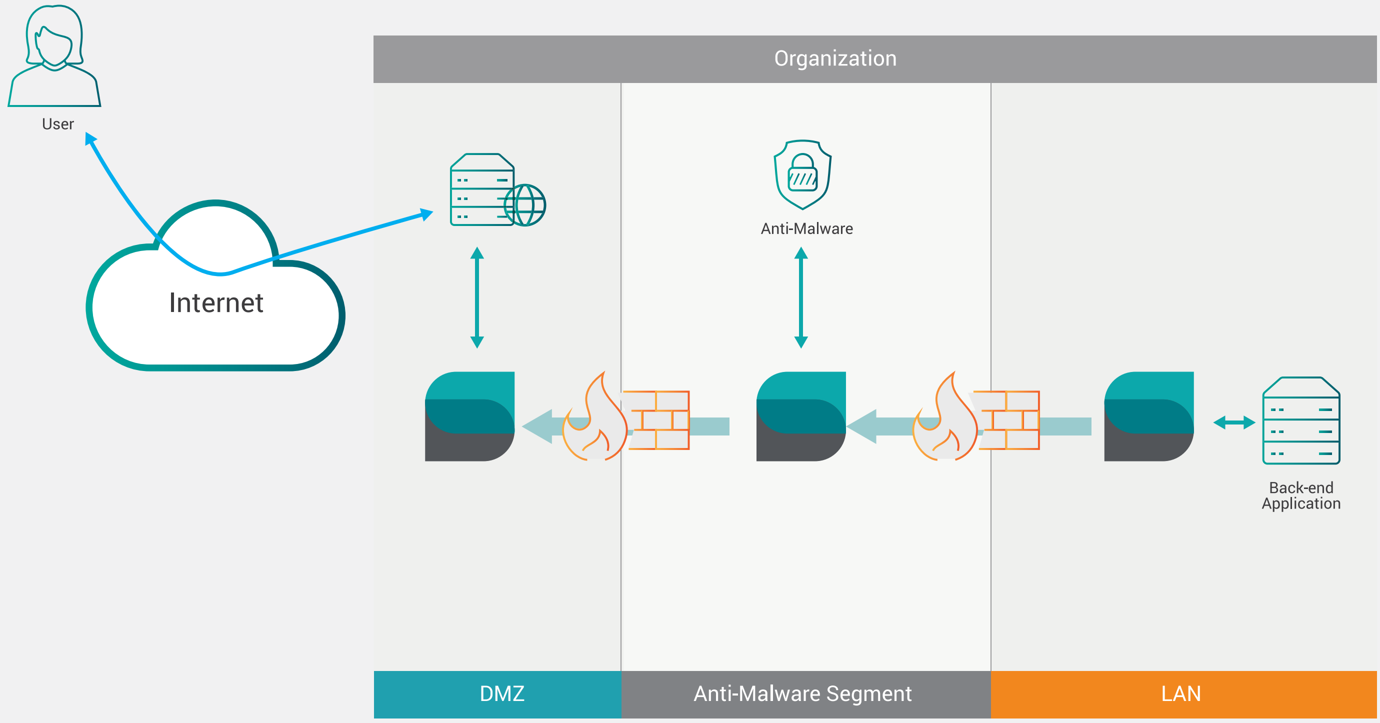


Figure 1 - Safe-T Anonymous Application Access

1 User access organization Web portal and uploads a file

2 The upload stream continues from the web portal to the **DMZ Access Gateway.**

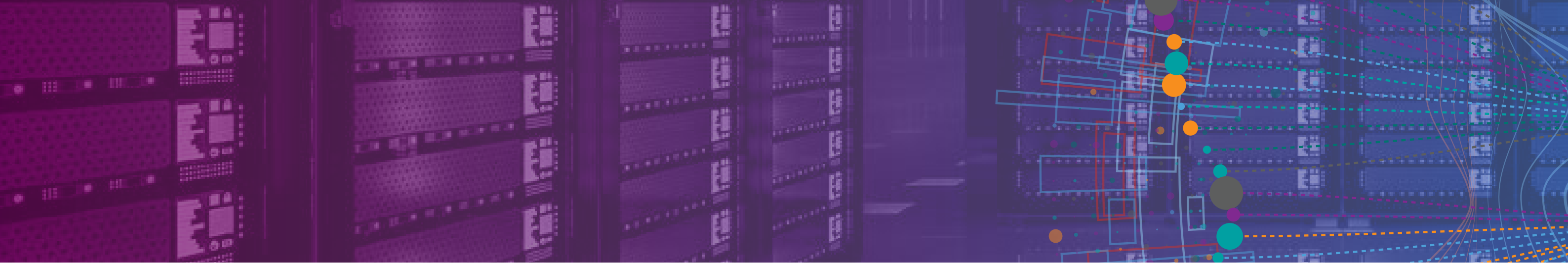
3 The **Anti-Malware Access** Controller continually polls the **DMZ Access Gateway**, pulling the upload stream (over an outbound port on the DMZ firewall), and passing it to the **Anti-Malware Data Exchange** Server.

4 **The Anti-Malware Data Exchange** Server passes the upload stream to the **Anti-Malware server** for it to scan the file.

5 The clean file is returned to the Anti-Malware Data Exchange Server, which passes it to the **Anti-Malware Access Gateway**.

6 The **LAN Access Controller** continually polls the **Anti-Malware Access Gateway**, pulling the upload stream (over an outbound port on the LAN firewall), and passing it to the LAN Data Exchange Server.

7 **The LAN Data Exchange** Server, stores the file in the back-end application / storage.



Capabilities

Deploying Software Defined Access for anonymous application access and file upload offers following capabilities:

- Support user, mobile, or API based access
- Support registered and anonymous access
- Monitor end-to-end user access and uploaded file lifecycles
- Support unlimited, parallel, multi-step workflows using Safe-T SecureStreamTM policy, workflow, and API engine
- Firewall is constantly in deny-all state, no open ports required for access
- Allow client-less access to applications
- Perform incoming file scanning in a secure zone
- Hide DMZ components which can be hacked and utilized to access the network
- Highly scalable solution

Benefits

The benefits of providing application access via Safe-T's Anonymous Application Access:

- ✓ **Greener technology through paperless services**
- ✓ **Improvement of customer experience and service**
- ✓ **Short time to market when rolling out of new customer facing services**
- ✓ **Fully automated application access**
- ✓ **End-to-end monitoring of access and file upload flows**
- ✓ **Support all types of users**
- ✓ **Gain ROI by consolidating file upload and API based flows**

Feature List

Access Component

Feature	Comments
System Level Features	
High availability (HA) **Ability to perform high availability/ clustering mode in the same data center and between data centers**	Safe-T Access Gateway and Controller can be setup in HA using an external load balancer or application delivery controller
Disaster recovery **Ability to failover to another data center in the event of application unavailability or site disasters**	Safe-T Access Gateway and Controller can be setup in a disaster recovery architecture using an external load balancer or application delivery controller
Patented Reverse-Access technology	Safe-T's reverse-access technology is patent protected. The Reverse-access technology is a dual node technology, which removes the need to open any ports within a firewall, while allowing secured application access between networks (through the firewall)
Access Features	
Patented Reverse-Access technology	Safe-T's reverse-access technology is patent protected. The Reverse-access technology is a dual node technology, which removes the need to open any ports within a firewall, while allowing secured application access between networks (through the firewall)
Support any TCP based application / service	Safe-T Access Gateway and Controller can support any TCP based application / service, applying reverse-access to it
Logical Network Segmentation	Logically segment the network, deploying a Zero Trust model, to reduce the risk of cyber-attacks from reaching internal network segments, or laterally moving
HTTPS Proxy	Safe-T Access Gateway and Controller supports HTTP/S based applications / services
SSL Off-loading	Safe-T Access Gateway and Controller support terminating SSL client connections destined to an application / service

Feature List

Access Component

Feature	Comments
Multi-factor authentication	Safe-T Access Gateway and Controller supports authenticating and authorizing users with multi-factor identity management tools before service requests to back-end applications can take place. • Authentication via the organization’s LDAP or Active Directory systems, • Authentication using OTP as 2nd factor for NTLM or Kerberos • Integration with 3rd party authentication solutions
Client-less and VPN-less application access	Safe-T Access Gateway and Access Controller do not require any client application to be installed on the end-user’s machine

Management and Operation

Using a Web for full management	Yes
System logs	Yes
External Provisioning	Yes, via TCP API for reverse-access rules

Data Exchange Component

Feature	Comments
Server base platform to host the server application	-Virtual Machine -Windows Server
64-bit Application Support	Safe-T products are 64-bit compatible - Server Management Console - SmarTransfer (Windows extensions) - Web UI
High availability **Ability to perform high availability/ clustering mode in the same data center and between data centers**	Safe-T Data Exchange Server connects to a remote SQL DB server and can provide storage over the LAN, administrators can have more than one Safe-T Data Exchange Server installed on the premises to provide DR capabilities

Data Exchange Component

Feature	Comments
Disaster recovery **Ability to failover to another data center in the event of application unavailability or site disasters**	Safe-T Data Exchange Server connects to a remote SQL DB server and can provide storage over the LAN, administrators can have more than one Safe-T Data Exchange Server installed on the premises to provide DR capabilities
Users database **Location where user information is stored**	Safe-T Data Exchange Server uses an SQL database
Configuration database **Location where configuration settings are stored**	Safe-T SDE uses an SQL database. Safe-T supports multiple protocols including NTFS/NFS, thus allowing customer to work directly with existing data centers
Database Encryption of sensitive information inside local SQL/MySQL database with which Safe-T Data Exchange Server works.	All sensitive information is encrypted including contacts, passwords, emails, packages, messages, etc. Encryption is done using AES 256-bit.
Full Web access interface for internal users	Yes

Secure Email Features

Ability to send file or folder	Yes, local or network directories
Ability to designate directories for automatically sending of files from different application	Yes (command line and automated flow)
Splitting large files/directories	Yes
Control extension file type	Any type. You can control which files type of files are allowed or blocked
Policy engine based attachment scanning **Ability to perform applied policy scanning on an incoming attachment**	Yes
Policy override **Ability to enforce policy on any file type or size**	Yes

Feature List

Data Exchange Component

Feature	Comments
Ability to expire attachments	Yes - by download times - by date/hours/minutes
Ability to compress attachments (file, folder)	- Zip - RAR -AES --etc
Ability to encrypt the attachment	Yes, AES 256 or any other type of external encryption
Attachment encryption level	Internal (128bit AES, 256bit AES), External HSM.
Body encryption for secure messaging	Yes
Ability to restrict so that only intended recipients can download the attachments	Yes, done by combining security methods: 1) Turn ON OTP via Text Message [SMS] 2) Limit max downloads 3) Create a short expiry time for sent messages (few hours)
Ability to archive email together with original attachment	Yes, supports archiving solutions: - Symantec Enterprise Vault - CommVault Archiving
OTP via mobile or SMS on email	Yes
File encryption at rest	Yes
File encryption in transit	Yes
HTTPS secured connection	Yes
Ability to sign files with certificates	Yes, and as SDK
Data manipulation (external tools)	Yes
Secure File Upload	Yes
Integration to mobile devices	Yes

Feature List

Data Exchange Component

Feature	***Comments***
Integration to Web Portals	Yes
Integration to Applications	Yes
System Health Monitoring	Yes
Workflow auditing and logging	Yes
Integration with Storages	Yes

Management and Operation

LDAP integration **Ability to manage users via Active Directory**	Yes
Ability to manage passwords of Active Directory and non- Active Directory users	Yes, using Active Directory policy and built-in password management policy for non- Active Directory users
Using a Web for full management	Yes
Storage management of occupied space of uploaded files with the ability for easy delete	Available (Disk Quota Management)
File archiving	Yes
Users/group control integrated through Active Directory	Yes
Ability to manage and limit file and disk size and enforce volume quota per user	Yes
Report generation	Yes, detailed, simple, summary, etc.
Auditing - ability to track all email attachments records and administrative changes	Yes

Feature List

Data Exchange Component

Feature	Comments
Ability to schedule the generation of reports	The following reports can be scheduled for generation (manually or via SDK): - Generate report when an email is sent/ received– manager and user level - Generate report detailing the total sent/ received files and sizes – manager and user level - Safe-T allows generating manager and user level reports
Policy on group and individual users	Yes
Policy regards file types allowed/not allowed	Yes
External Provisioning	Yes, via REST API
Safe-T Connectors Protocols	
Active Directory	Yes
WebDAV	Yes
HTTP/S based applications	Yes
NAS	Yes
NTFS	Yes
SAN	Yes
SFTP	Yes
SMTP	Yes
SOAP/WSDL	Yes
SSH	Yes
SQL	Yes

Feature List

Data Exchange Component

Feature	Comments
Applications	
Enterprise Applications	- Oracle - SAP - IBM AS400 - SharePoint
Antivirus and Anti-Malware solution integration	- Check Point Sand Blast - AVG (Client/Server) Server - Gate Scanner - RE-SEC - OPSWAT - ODI - McAfee - Symantec SEP - Trend Micro OfficeScan - WinClam - SDK
Consumer Cloud Storage	- Box - DropBox - OneDrive - Google Drive
DLP integration	- Symantec - WebSense - McAfee - SDK
PDF Encryption	Yes
PDF Sign	Yes