SAFE-T
Accelerating Safe Business

Safe-T Secure Data Access

Isolating applications from world, while providing secure and transparent access

Recent researches show that six out of ten organizations around the globe have suffered at least one Cyber-attack incident on their enterprise services which are exposed to the Internet.

This statistic is made possible, since the need of exposing enterprise services to the world (in order to interact with 3rd party vendors or partner), combined with the old way of designing perimeter networks (e.g. DMZ segments) and application access (VPNs, RDP, open firewalls), is no longer working. Attackers are still getting through.
It is clear then, that a paradigm change is needed in order to overcome the challenges of providing simple and transparent access to internet facing services, while effectively combatting cyber-attack and threats.

Safe-T's Secure Data Access (SDA), a component of the Safe-T High-risk Data Security solution, is an advanced software-defined perimeter (SDP) and logical segmentation solution, purpose built to create a bulletproof data center perimeter, protecting all applications while enabling access.

Built on top of Safe-T's disruptive and breakthrough secure reverse-access technology as well as Safe-T's Integrated Data Security Platform, Safe-T SDA:

- ✓ **Isolates applications, services and networks from attackers**
- ✓ **Prevents un-authorized access to data, applications, networks, or APIs**
- ✓ **Controls and manages access to your applications and data**
- ✓ **Eliminates the need for VPNs, removing network access, allowing only application access**
- ✓ **Close all incoming firewall ports**

Safe-T's Integrated Data Security Platform consists of four components:

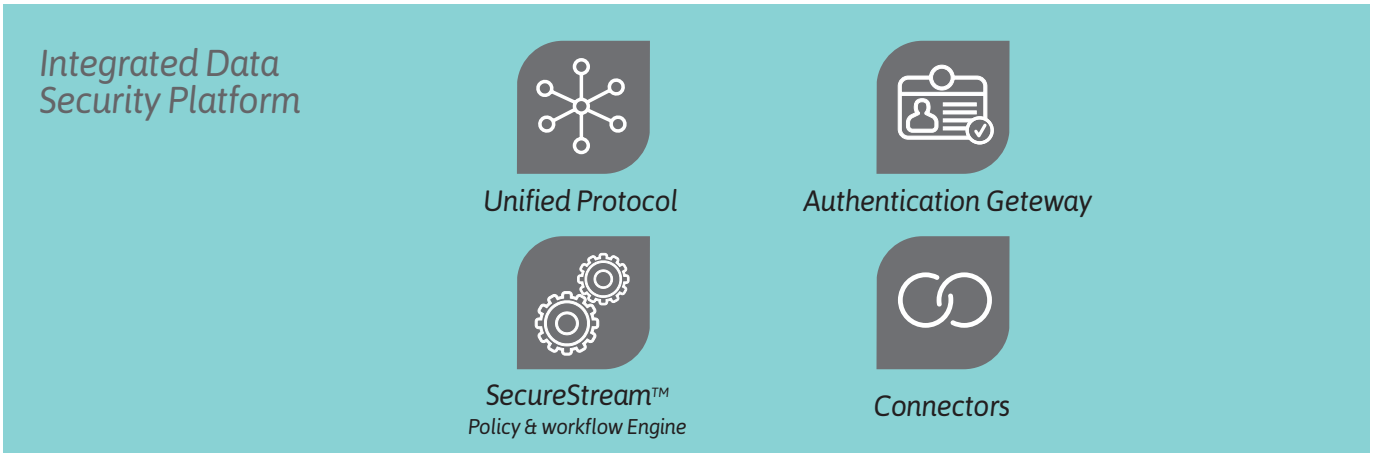

Figure 1 - Safe-T Integrated Data Security Platform

Unified Protocol

- ✓ Native and SDK based support for all common enterprise file transfer and business applications' protocols
- ✓ Easily integrate new RFC protocols or modifying existing ones
- ✓ Real-time application/protocol conversion (HTTP to SFTP, SQL to DropBox)

Authentication Gateway

- ✓ Built-in multi-factor authentication and authorization (MFA) engine
- ✓ Integrate Safe-T products with any number of authentication and authorization systems

SecureStream™ policy and workflow engine

- ✓ Broker traffic to 3rd party security (DLP, AV, Antimalware) and IAM products
- ✓ Automatically enforces security policies on outgoing/incoming data exchange flows
- ✓ Easily create multi-factor authentication and authorization as well as data exchange workflows

Connectors

- ✓ Dozens of Safe-T Connectors to enterprise applications, storages, cloud storage solutions/services, security solutions, authentication solutions, encryption solutions, and more

Dual Node Technology

Safe-T SDA is a dual node patented technology, which removes the need to open any ports within a firewall, while allowing secured application access between networks (through the firewall).

- ✓ **External SDA Node –** installed in the DMZ / external / non-secured segment
- ✓ **Internal SDA Node –** installed in the internal / secured segment

Located in the organization's DMZ (on-premise or cloud), the role of the external SDA node is to act as a front-end to all services/applications published to the Internet. It operates without the need to open any ports within the internal firewall and ensures that only legitimate session data can pass through into the internal network.

The role of the internal SDA node it to pull the session data into the internal network from the external SDA node, authenticate the user, scan the data for malware and viruses, pass the data to 3rd party security solutions for scanning, and only if the session is legitimate, pass it to the destination application server.

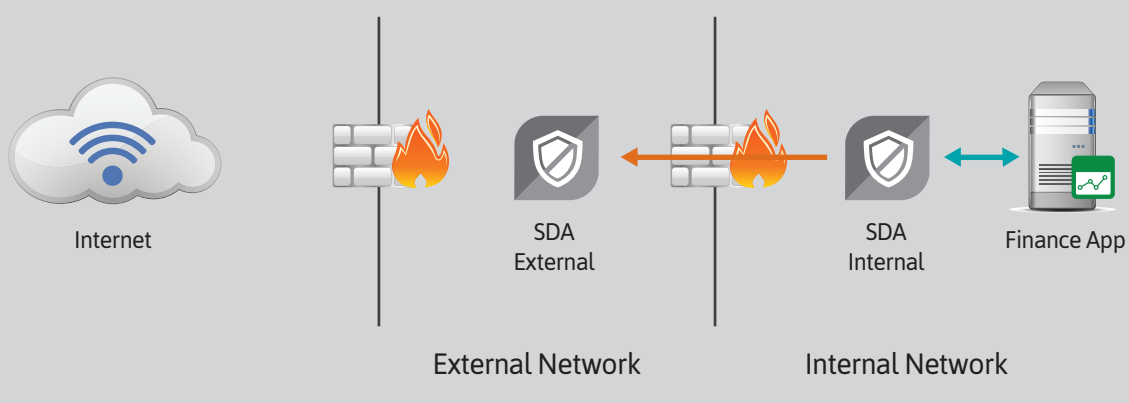

Figure 2 - Safe-T Secure Data Access Technology

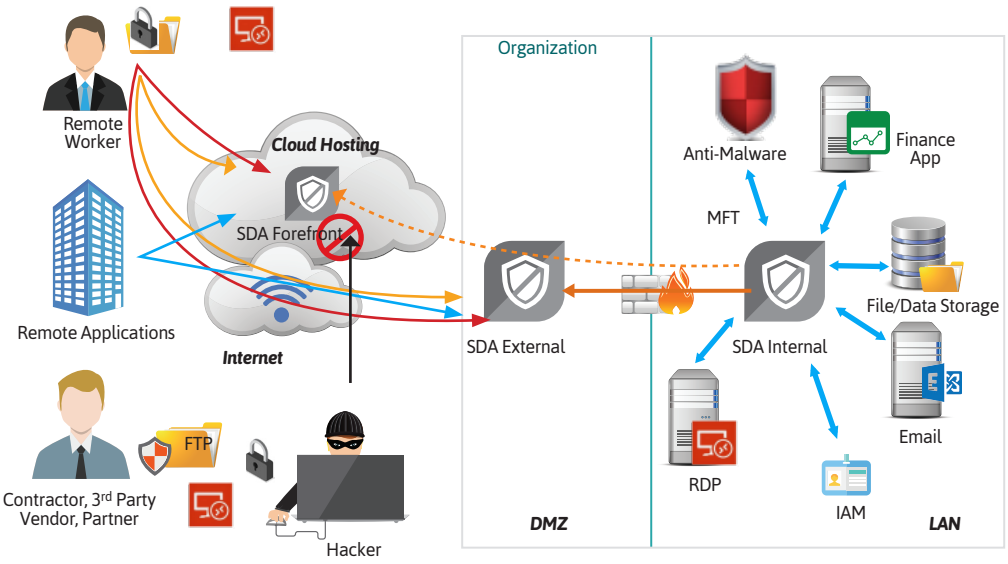

Figure 3 - Safe-T Secure Data Access as Software-Defined-Perimeter

Secure Data Access (SDA) Features

- *Patented Reverse-Access proxy*
- *Multi-factor authentication*
- *Deep packet inspection*
- *SecureStream™ policy and workflow engine*
- *Broker traffic to 3rd party security and IAM products*
- *Dynamic URL rewriting supporting multi-domain applications*
- *Publish multiple internal applications on a single IP*
- *Client-less and VPN-less application access*

Robust Secure Access Use Cases:

Software-defined Perimeter (SDP)
provide secure access to your entire organization's data center with a one-of-a-kind software-defined-perimeter solution. Completely hide your organization's true location and architecture from external users and attackers.

Secure Partner Access
provide secure, authenticated, and scanned direct-access to any application for your business partners and providers, without opening any ports in the firewall, or needing to provide VPN client-software.

Logical Network Segmentation
logically segment your network, deploying a Zero Trust model, to reduce the risk of cyber-attacks from reaching internal network segments, or laterally moving throughout your network.

Secure Application Access
provide secure, authenticated, and scanned direct-access to any application for your business users, without opening any ports in the firewall.

Security Services Consolidation
consolidate all of your security solutions into one cyber dome, ensuring all data access flows are managed, and get scanned with the appropriate security solution.

SAFE-T
Accelerating Safe Business

About Safe-T

Safe-T® Data is the provider of solutions designed to mitigate attacks on business-critical services and data for a wide range of industries, including: financial, healthcare, government, etc.

Safe-T's High-risk Data Security (HDS) Solution mitigates data threats: un-authorized access to data, services, networks, or APIs; as well as data, related threats, including data exfiltration, leakage, malware, ransomware, and fraud.

Safe-T is a cyber security company dedicated to preventing unauthorized access and use of high-threat services and data, inside and outside the organization perimeter. Enterprises and businesses around the world trust Safe-T's High-threat Data Security solution to secure their data, applications, and networks from insider and external data threats.

Focused on providing security solutions for the enterprise market, Safe-T enables organizations to benefit from enhanced productivity, efficiency, heightened security, and improved regulatory compliance.

Safe-T has offices in North America, APAC, Africa, Europe, and Israel.

*For more information, visit **www.safe-t.com**.*

Secure Data Access (SDA) Benefits

- Reinforce firewalls to isolate applications, services and networks from attackers
- Drive down costs through simplification, operational efficiency and decommissioning of DMZ components
- Permit only authorized access to data, services, networks, and APIs
- Deploy on-premise or as a hybrid-cloud DMZ (DMZaaS)
- Remove the need for VPN
- Prevent network access, allow only application access
- Provide direct application or human access