# The Safe-T +

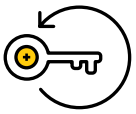
safe-t
Masters of Access

## It’s all about the unique features and our innovative, customizable approach to SDP.

You’ve got more than a few choices when it comes to SDP solutions. That’s actually a great thing in today’s threat-laden data access landscape. SDP is proving to be a game changer for provisioning Zero Trust access in ever-changing network conditions. **So what makes the Safe-T approach unique? How do we stand out in a crowded space? We like to think of the Safe-T advantage as our one-of-a-kind +, how we give you more.**

## So what is this +?

### Reverse Access



Our totally unique dual-server patented technology removes the need to open any ports within a firewall while allowing secure application access between networks (through the firewall).

Located in the organization’s DMZ (on-premise or cloud), the role of the Access Gateway 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, therefore ensuring that only legitimate session data can pass through into the internal network. What’s more, the Access Gateway performs TCP offloading, allowing it to support any TCP based application without the need to perform SSL decryption.

The role of the Access Controller it to pull the session data into the internal network from the external SDA node, and only if the session is legitimate, perform layer 7 proxy functionality (SSL offloading, URL rewrite, Deep Packet Inspection, etc) and pass it to the destination application server.

#### Benefits of our Reverse Access technology include:

- Access to applications/networks without opening incoming holes in the firewall.
- Supports any TCP based application.
- Bi-directional traffic is handled on outbound connections from the LAN to the outside world.
- Client-less and VPN-less application access.
- Logically segment networks.

### User Behavior Analysis (UBA)

Using Big Data and Machine Learning principles, UBA detects the presence of bots and authenticated malicious insiders to effectively stop fraudulent activities. You’ll get highly actionable data to help you recognize and tamp down dangerous threats before they have the opportunity to cause harm. It’s anomaly detection that is specifically designed to work with a software defined perimeter solution, providing the most comprehensive solution to evolving access challenges.

#### Safe-T User Behavior Analysis gives security teams:

- Actionable intelligence regarding emerging threats
- Comprehensive forensics capabilities
- Insights into sophisticated attacks
- The ability to stop fraudulent activities by understanding normal behaviors

## Multiple Deployment Options

At Safe-T, we believe that you know your infrastructure best. You don't need anyone to tell you where and how to deploy your SDP. Got a VPN you'd like to keep? With Safe-T SDP, that's not a problem—you can put whichever user group you want, such as risky third party contractors, onto SDP, and leave the rest on your VPN. Want to explore the world of SDP in a gradual way, without uprooting your existing access structure? Only Safe-T makes that a possibility with a customizable deployment that puts you in the driver's seat.

## Can Be Used By Regulated Organizations

While the cloud is all anyone can talk about, some high-risk organizations cannot freely make use of it. Thanks to Safe-T's on-prem SDP deployment options, now even highly sensitive organizations such as CI providers, government agencies, and financial institutions can get granular, need-to-know access to applications, without exposing themselves to the inherent dangers of the cloud.

## Secure NTFS File Share and Access with Internal and External Entities

Secure File Access (SFA) gives internal and external users transparent access to secure storage. What appears as a standard mapped network drive is actually a secure, encrypted and access-controlled channel to interact with files – upload, download, copy, open, delete, etc. while not relying on vulnerable protocols such as SMB.

### The benefits of SFA include:

- Transforms standard network drives to a secure, encrypted and access-controlled drive
- Sensitive information is exposed on a "need to know basis" and permissions
- Users are granted specific permissions to perform actions, etc.
- Secure access to sensitive information is gained over HTTPS protocol
- All user actions are controlled and audited
- Fully integrated with Safe-T Secure Application Access solution