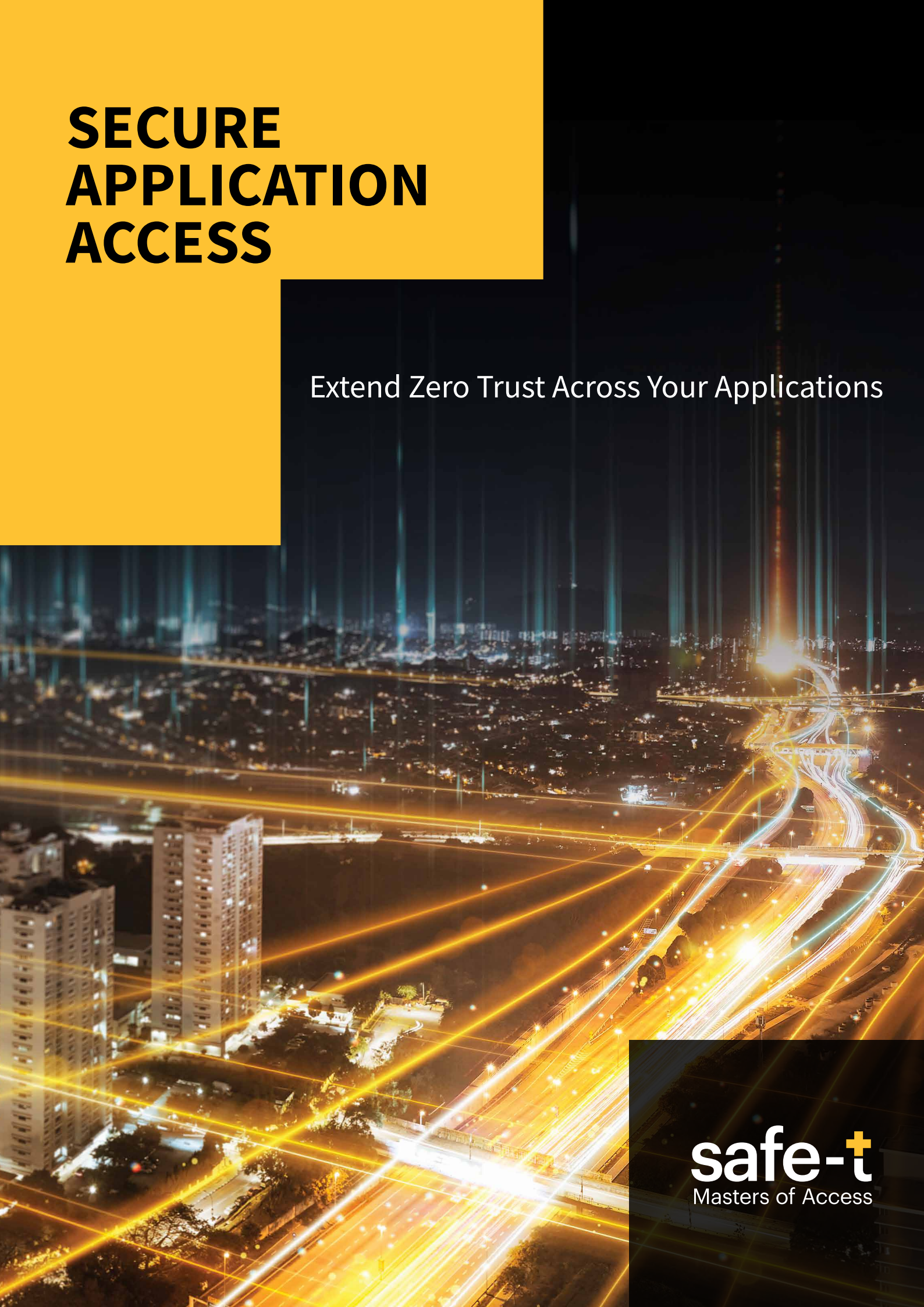
SECURE APPLICATION ACCESS

Extend Zero Trust Across Your Applications



safe-t
Masters of Access

The Dangers of Exposing Applications to the World

As organizations continue to “go digital” and become more connected, they open their networks and internal applications to remote employees, customers, business partners, 3rd party vendors, mobile devices, and connected devices.

Enhanced connectivity is necessary to remain business-relevant, but it comes at a cost; Research shows that six out of ten organizations around the globe have suffered at least one cyber-attack on their enterprise services.

This shouldn’t be the case in our technologically sophisticated world. But it is, because organizations typically expose their services to the internet in order to interact with their many 3rd party vendors and external partners. The fact is that organizations are still using legacy methods such as VPN and virtual desktop solutions of designing perimeter networks that don’t account for modern connectivity and application access challenges.

It is clear that organizations need a paradigm shift to overcome the challenges of providing simple, cost effective, and transparent access to internet facing services, while effectively combatting cyber-attacks and threats.

Introducing Safe-T Secure Application Access (SDP)

Safe-T’s Zero Trust Network Access (ZTNA) solution, Secure Application Access, is changing the way organizations grant secure external access to their services.

Safe-T’s Secure Applications Access offers secure and transparent access for all types of entities (people, applications, and connected devices) to any internal application, service and data, for example HTTP/S, SMTP, SFTP, SSH, APIs, RDP, and WebDAV.

Our solution implements Safe-T’s patented reverse-access (outbound) technology which eliminates the need to open incoming ports in the organization’s firewall.

The solution forces users to authenticate into resources first and then they are granted access by the solution. Configurable policies define the orchestrated authentication steps that each user or group member must perform. Now, backend services are not visible to unauthenticated users and the probability of suffering a successful attack is minimized. It's like we always say here at Safe-T: If you can't be seen, you can't be hacked®.

To prevent authenticated users from performing unauthorized operations, Safe-T's Secure Application Access provides user behavior analytics (UBA) capabilities that monitor the actions of protected applications. A dashboard displays security related events and aggregated statistics. Administrators use the dashboard to inspect details about anomalous behavior that can trigger alerts and identify suspicious activities.

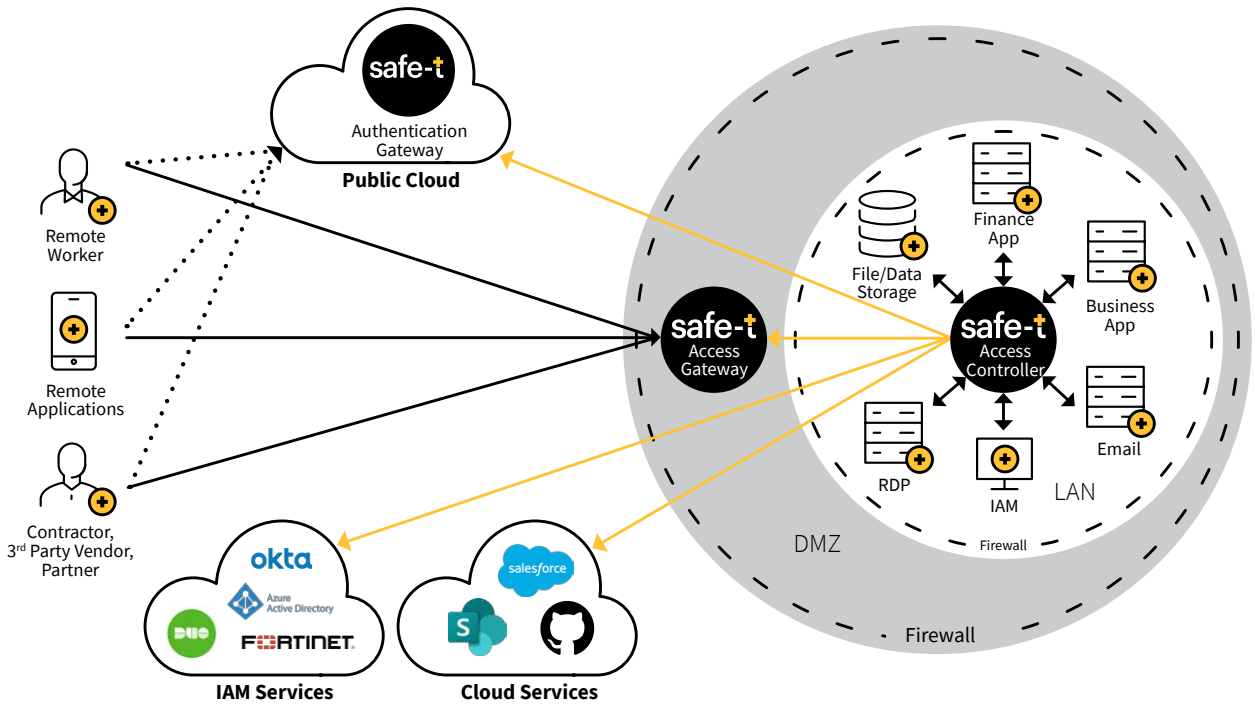
Features

Safe-T Reverse Access
Inside-out protection

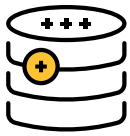
SMB Proxy Access
Encapsulated, exploit-safe SMB

User Behavior Analysis
Dynamic, AI-based behavior anomaly detection

Non web protocols ready
RDP, SFTP, SSH

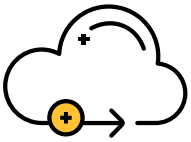


Benefits of Safe-T's Secure Application Access



Allows for any setup

Choose from on-prem, on cloud or hybrid deployment to best fit your organization's needs.



Supports total flexibility

Secure Application Access works with your VPN, in place of your VPN or next to your VPN.

Grants full network segmentation

Using Reverse Access patented technology , your network remains hidden from the outside at all times.

Prevents attacks before they happen

Our proprietary Telepath Behavioral Analytics tool detects malicious insiders and bots, catching them before they can do harm.

Scales precisely according to usage

SDP fits any type and number of users, and grows precisely with increasing or decreasing data demands. Any user - Client, client-less and IOT devices

With Safe-T's Secure Application Access, you can grant your users access to the applications and resources they need, without compromising on security.

safe-t
Masters of Access

support@safe-t.com | +972-9-866-6110
safe-t.com