SAFE-T

REVOLUTIONIZING ZERO TRUST WITH SOFTWARE-DEFINED PERIMETER

Securing your most sensitive data in a world of digital transformation

2019

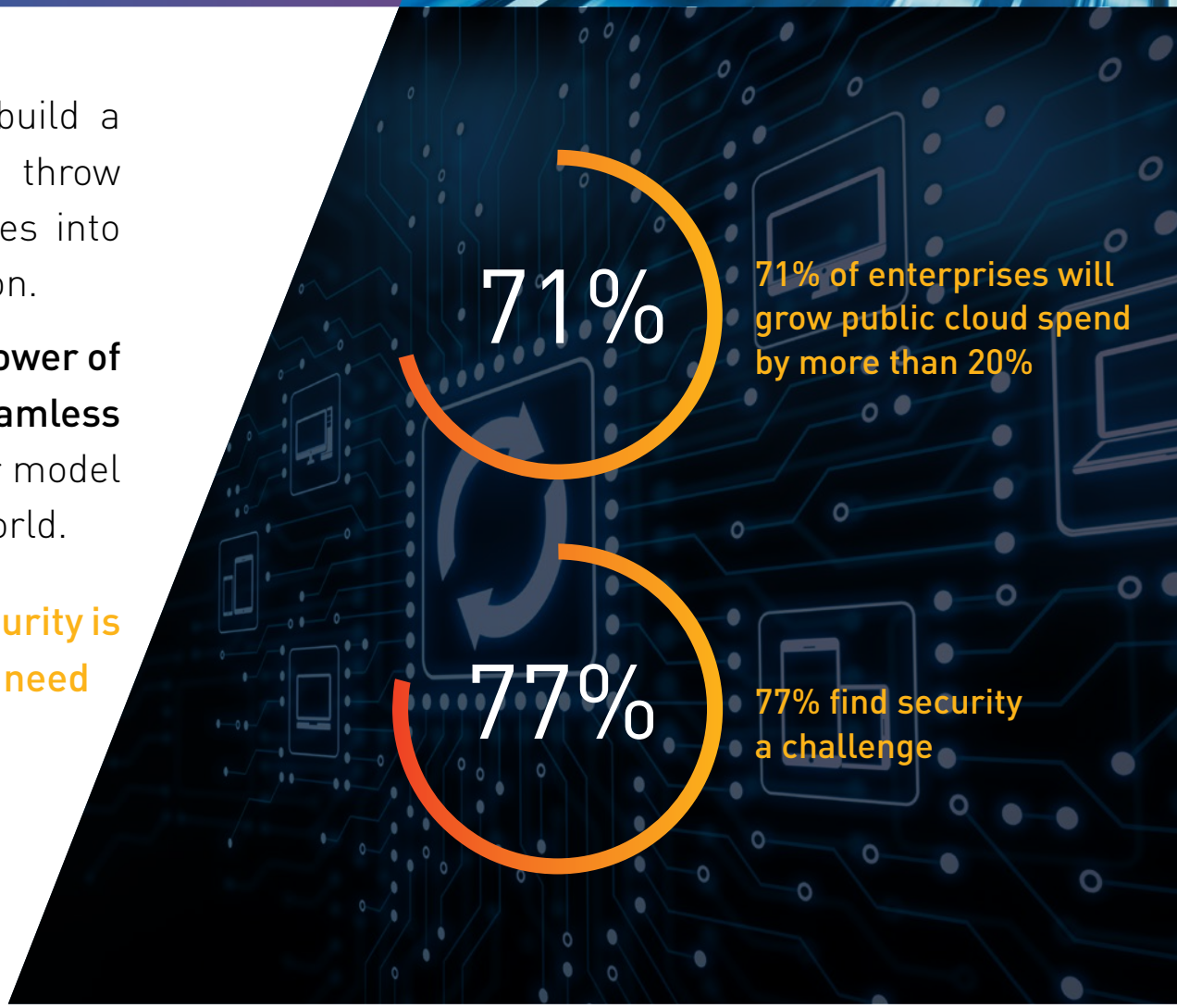
Keeping Data in the Right Hands

1 Security is **Changing**

The traditional security model was to build a wall around the corporate network and throw all the company's cybersecurity resources into defending it. But this is no longer an option.

Enterprises today want to leverage the power of cloud-based services, mobility, IoT and seamless collaboration. The old network perimeter model simply cannot exist in this new, fluid IT world.

In short: traditional perimeter-based security is no longer fit-for-purpose. Organizations need a new model.



2 Access Control is Evolving, but Current Solutions are Failing Customers

All of this digital transformation is designed to drive growth and success. But it also means increasing IT complexity: multiple platforms stretched across on-premise and hybrid cloud; and multiple internal and supplier teams. The growth in endpoints and IT complexity also expands the corporate attack surface.

Current solutions are failing. They aren't built for hybrid IT, they expose network connections and they are based on outdated notions of trust. This increases enterprise exposure to threats. Even worse, they're expensive to own and operate and difficult to segment.

Your access control solutions need to reflect the evolution taking place in the market.

3 A New Paradigm for **Network Security**

This evolution is leading us towards two new concepts that represent the future of cybersecurity:

SOFTWARE DEFINED PERIMETER

A new model proposed by Gartner. It holds that, instead of organizations exposing their services to the world and then layering security on top to prevent unauthorized access and DDoS, they should expose them only on-demand to authenticated users.

ZERO TRUST NETWORKS

An increasingly popular approach to network design devised by Forrester. It requires organizations to break down the network into smaller, secure segments. This prevents malware from moving laterally across the network, reduces exposure of vulnerable systems and protects sensitive data from unauthorized applications and users.

4 A Step in **the Right Direction**

These models finally offer enterprises a new approach to security which fits the push towards digital transformation.
By embracing the ideals of the Software **Defined Perimeter and Zero Trust Networks they can:**

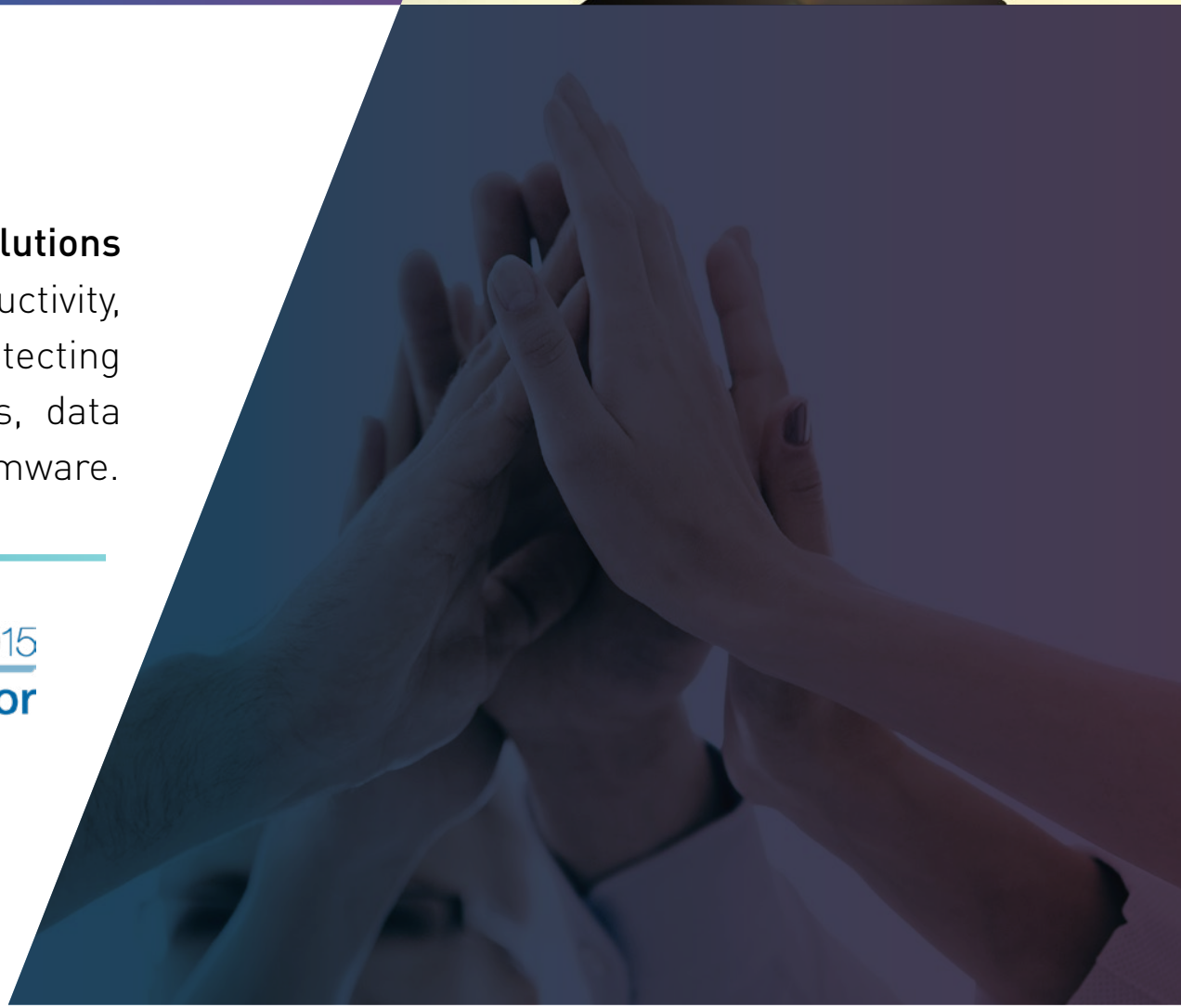
- Drive **business growth** through digital innovation
- **Support the requirements** of the modern workplace
- **Stay compliant in an** increasingly complex regulatory environment
- **Keep key customer data and** IP secure and core systems / services **up and running**

But while they're certainly a step in the right direction, these models can be improved.

5 Introducing **Safe-T**

Safe-T is an award-winning, cybersecurity company.

We provide software-defined access solutions designed to enhance operational productivity, efficiency, security, and compliance by protecting organizations from data related attacks, data exfiltration, leakage, malware, and ransomware.



6 Safe-T Software-Defined Access: **Zero Trust for the Data Access Lifecycle**

Safe-T's Software-Defined Access Suite takes SDP to the next level, revolutionizing Zero Trust network design. It's a patented, multi-layered solution that protects the entire data lifecycle in modern, complex hybrid cloud environments.

HOW DO WE DO THIS?

TRUSTED ACCESS

Safe-T protects and controls access by: separating the access layer from the authentication layer, transparently granting access only to authorized users, and by segmenting internal networks.

TRUSTED CONTROL

Internally, Safe-T controls data usage, preventing data exfiltration, leakage, malware, ransomware and fraud. Policy-based access controls help to manage data usage methods. Its all combined to unify and streamline business/security systems to drive efficiency and growth.

TRUSTED REPORTING

Safe-T provides the granular reporting and auditing you need per user and application for continuous compliance with most major regulations and frameworks.

7 Adaptive Access: The **On-Demand Perimeter**

Safe-T's Software-Defined Access hides your data at the perimeter, ensuring its accessible only to the right people, whether on-premise or in the cloud. This Adaptive Access solution is built on patented Reverse Access technology, offering a fully automated, dynamic on-demand perimeter that can:

- **Reduce your attack surface – if you can't be seen you can't be hacked**
- **Drive down TCO, via a single gateway and support for all protocols**
- **Ensure a seamless user experience**

How it works?

01 User logs into dedicated authentication portal published by the Authentication Gateway.

02 User enters credentials into portal

03 The Access Controller retrieves the credentials from the Authentication Gateway over a reverse-access connection, and then authenticates the user using - 3rd party IAM/IDP solutions (SecureAuth, Okta, DUO Security, etc), POST based login, Microsoft Active Directory, SAML, OTP, etc

04 After authentication, Access Controller instructs Authentication Gateway which applications to display to the user, and instructs Access Gateway to provide (reverse) access to the user to allowed applications.

05 User selects the application to access.

06 User redirected to the application's published IP address.

07 User accesses the newly published service.

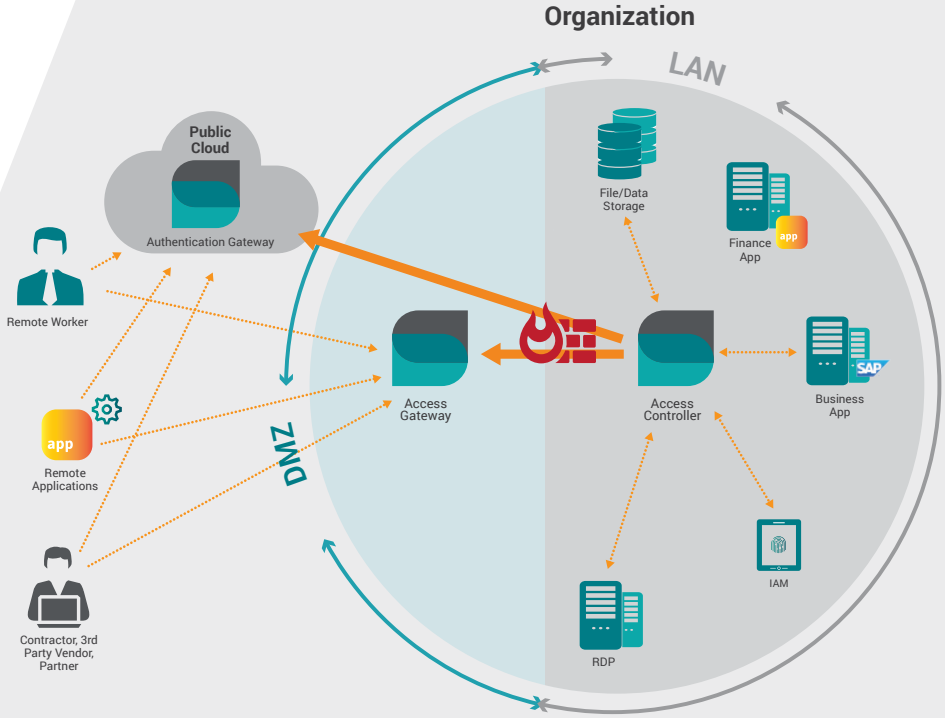
08 Once user is disconnected, Access Controller instructs Access Gateway to block access by that user to that application.

The Secret of **Reverse Access**

Safe-T's patented Reverse Access technology is at the heart of our revolutionary Adaptive Access model.

Here's how it works:

- Incoming requests from user/external application to internal application arrive at the Safe-T Access Gateway
- Safe-T Access Controller immediately pulls them into the LAN over an outbound connection
- Safe-T Access Controller uses the SecureStream engine to apply policy and workflow on traffic
- The request is sent to the internal application, and the reply is sent back to the user/external application



9 **Monitoring Data** Usage to Mitigate the Insider Threat

- Data leakage by employees, whether malicious or accidental, is now a major cyber risk for organizations. Insiders were blamed for over a quarter of breaches last year with human error a major contributing factor, according to Verizon. **That's why Safe-T not only secures external access but, unlike other SDP solutions, also provides powerful data usage controls.**

- **Safe-T SmarTransfer integrates seamlessly with existing file shares and enterprise authentication systems** to provide access and permissions control to any file types and content and prevent any unauthorized access or usage, including: upload, download, copy, open, delete, view, etc. It does this without relying on SMB protocol, instead using an HTTP/S connection from client to Safe-T. Clientless deployment is quick and easy.

10 **Security Everywhere** with Safe-T's Software Defined Perimeter

The Beauty of Safe-T's Software-Defined platform is that it can be used across the digital enterprise, from on-premise to hybrid cloud environments and even home users. This minimizes your TCO and maximizes protection.

Safe-T also outguns VPNs because it is:

- **Built for hybrid environments**
- **More cost effective to acquire, implement and manage**
- **Allows also IoT and "headless devices" to connect seamlessly to the organization**

Secure remote access is particularly important for modern organizations that need to support mobile working and complex partner/supply chain relationships. **With Safe-T, your home and remote users, partners and suppliers can benefit from industry-leading client-less, adaptive access technology without the need to install client software or a VPN.**

In fact, Safe-T is more secure than a VPN. Why? Because - unlike VPNs - it isn't based on the assumption of trust. **We operate a Zero-Trust,** authenticate-first-then-connect approach which ensures only authorized users are granted access. All applications and services will remain hidden to anyone else.

11 The Safe-T Promise: Zero Trust Access for the Digital World

Safe-T is committed to its global users.

We promise to:

- Reduce corporate attack surface
- Protect and control sensitive data
- Enable roll-out of digital business applications
- Support migration of applications to the cloud
- Save costs

Learn more about Safe-T and our Software-Defined Access Platform

Read our brochure

Get in touch to request a demo today

SAFE-T

Keeping Data in the Right Hands