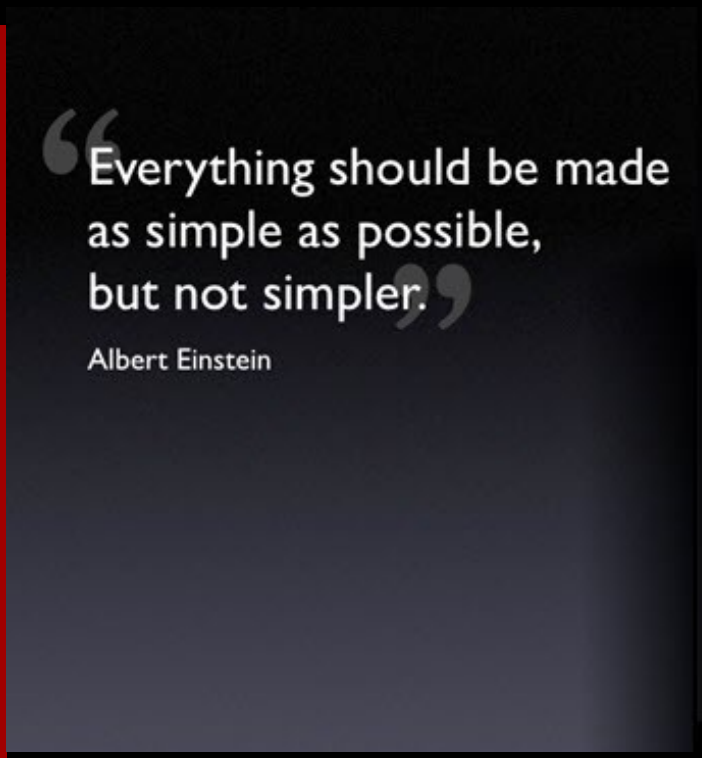
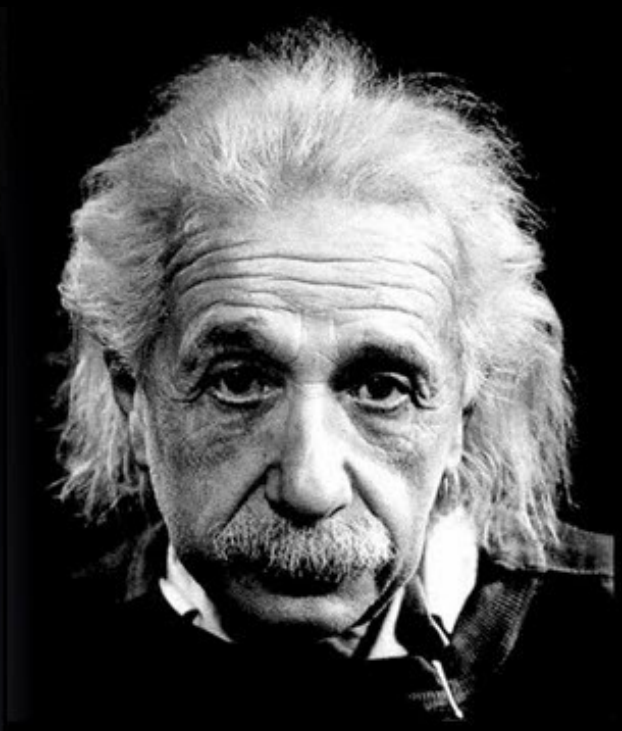
ZAFEHOUZE

ZAFEHOUZE INC / ZAFEHOUZE APS
www.zafehouze.com
info@zafehouze.com



# ZafePass VPC

## (Virtual Private Connectivity Intro & Fact Sheet)

An agile technology platform, supporting your organisations transition process, leveraging and extending the feature-sets of;

**Cloud Security Alliance’s SDP** (*Software Defined Perimeter)*
***Gartner Group’s SASE****: (Secure Access Service Edge)*
*and* ***Forrester’s ZT (EX)****: (Zero-Trust Employee eXperience*)

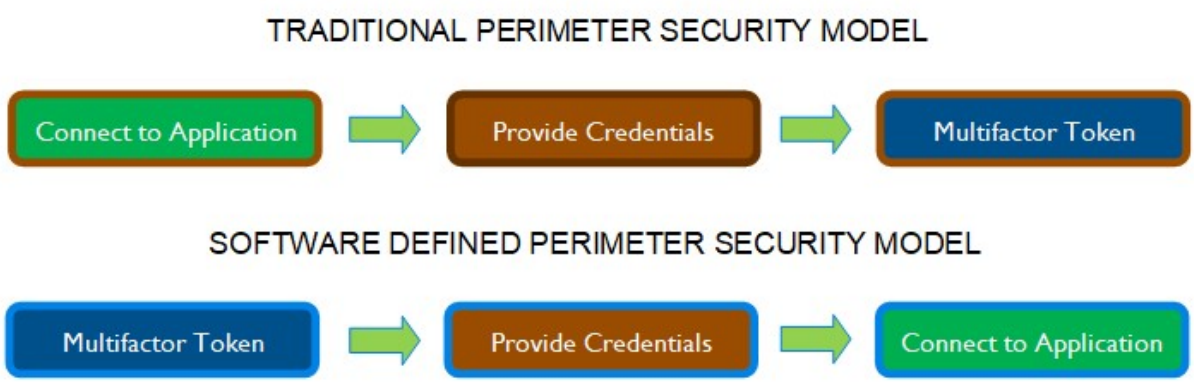
An all-in-one End-2-End simplifying and securing access to any IT-resources, services, applications and/or data.

# BACKGROUND

The main principles behind the technologies ZafePass leverage and is created around, are not entirely new. They are typically implemented in “classified IT organisations” like Department of Defense (DoD) and Intelligence Communities (ICs).

To these principles (Software Defined Perimeter and Zero-Trust / SASE) we have added unique functionalities, taken from the ‘secure communication’ patent we filed in 2005. The result is a design capable of ‘hiding’ IT-resources, services, applications and data behind a “ZafePass Access-Point” to which, a user MUST ‘authenticate’ before being presented with a list of entitled virtual private micro-segmented ‘resources’.

It’s neither complex nor expensive. Where most other solutions provide Zero-Trust Network access, ZafePass VPC provide direct application and service access. This helps in simplifying the security-stack and increase user productivity and user-experience. This design has many advantages over traditional IP-network access and security as the current model, were trust is presumed and based on “connect first—authenticate second”, can easily be misplaced. In todays hyper-connected and highly adversarial threat landscape, the traditional model is both outdated, and puts an organisation at risk.




## THE PROBLEM SHORT: “Implicit Trust”

Unless you have a “perimeter-less IT design” - your implicit trust design is akin to someone knocking on your front door, being let in, and only then you ask who they are and what they need. This method leave you organisation exposed to:

- ***Infrastructure reconnaissance scans***
- ***Unauthenticated users being able to exploit servers***
- ***Unauthorized users consuming unauthorized resources***
- ***Denial of Service & Man-in-the-Middle (MitM) attacks***
- ***Code-injection and brute-force attacks***
- ***Lateral Movement attacks***
- ***Large attack surface—as many solutions are needed to work together***
- ***High Costs of Operation, Administration and Management***

“Legacy, perimeter-based security models are ineffective against attacks. **Security and risk professionals must make security ubiquitous throughout the ecosystem.”** (*Forrester*)

ZafePass Empirical

# IT'S TIME TO PHASE IN A NEW MODEL

Driven by the mobile and cloud era, a modern 'business and its workforce' require simple and seamless access to IT-resources, services, applications and/or information. Its a daunting task for IT-teams to manage devices, juggle risk, compliance and regulations, managing data (that has 'left the building'), users who go around IT when deploying new applications, support legacy SCADA/OT requirements, mobility and we haven't even touched upon delivering, protecting and managing the many point security solutions using certificates, the IP address configurations, firewall management of rules, detect / response services etc. No surprise, IT-teams are left with a lack of visibility and control.

In addition, the IT-team responsiveness has to be faster than ever—and in a time where the IT-infrastructure and the way to protect it, looks like a museum of past IT-decisions, the end result is often that the business is not getting what they want from their IT, and in some cases, business circumvent IT all together.


If a conclusion should be drawn up, it is that the IP based network access legacy and complexity, are keeping IT from satisfying these new demands, that in the end fuels frustration.

The Software Defined Datacentre has been around for a while, so has Software Defined Perimeter, and its about time for the two to join together.

## CO-EXISTENSE & PRESERVE IT INVESTMENTs

To overcome these challenges, ZAFEHOUZE developed ZafePass VPC for providing Enterprises a modern, user-centric, simple and secure **V**irtual **P**rivate **C**onnectivity to any IT-resource, meeting and exceeding Software Defined Perimeter, SASE / Zero-Trust and API-SEC principles. On top are added features and functionalities for simple and effective administration of large environments.

ZafePass is de-coupled from the physical network topology, allowing simultaneous private micro-sessions between the resource-side and the user-side as the network and infrastructure is utilized as a simple backbone. This design has many advantages;

- full control with the environment from IT, due to ...
- easy and real-time on-/offboarding of resources, services, applications, users and ...
- control of user access based on security policies can be enforced in real-time, it …
- only takes seconds (one step) no matter if you have 2 or 2 million users, the …
- cost is a fraction of your current set-up / TCO (guaranteed)

Its time to empower your IT-team, your users, contractors and alike, with a solution rooted in SDP and ZT, added a range of unique obfuscating techniques that will leave Cyber-criminals in the dark and empty-handed trying to gain access to, and compromise your, business.

ZafePass offer a no-risk parallel phased-in implementation supporting your existing setup, and users can be converted one-by-one, group-by-group meeting any resource plan. Stat with the most critical first and then add as convenient.

It is important to emphasise—a ZafePass VPC environment will become yours (the licensee), as SafePass IS NOT hosted by ZAFEHOUZE, there's NO data-traffic re-routing to a ZAFEHOUZE data-centre, there's NO hardware to manage … and for TRULY meeting Zero-Trust principles, there is NO 3rd party point-security solution and NO certificate dependencies.

ZAFEHOUZE

# ZAFEPASS ARCHITECTURE

The ZafePass architecture is made up of only two components;

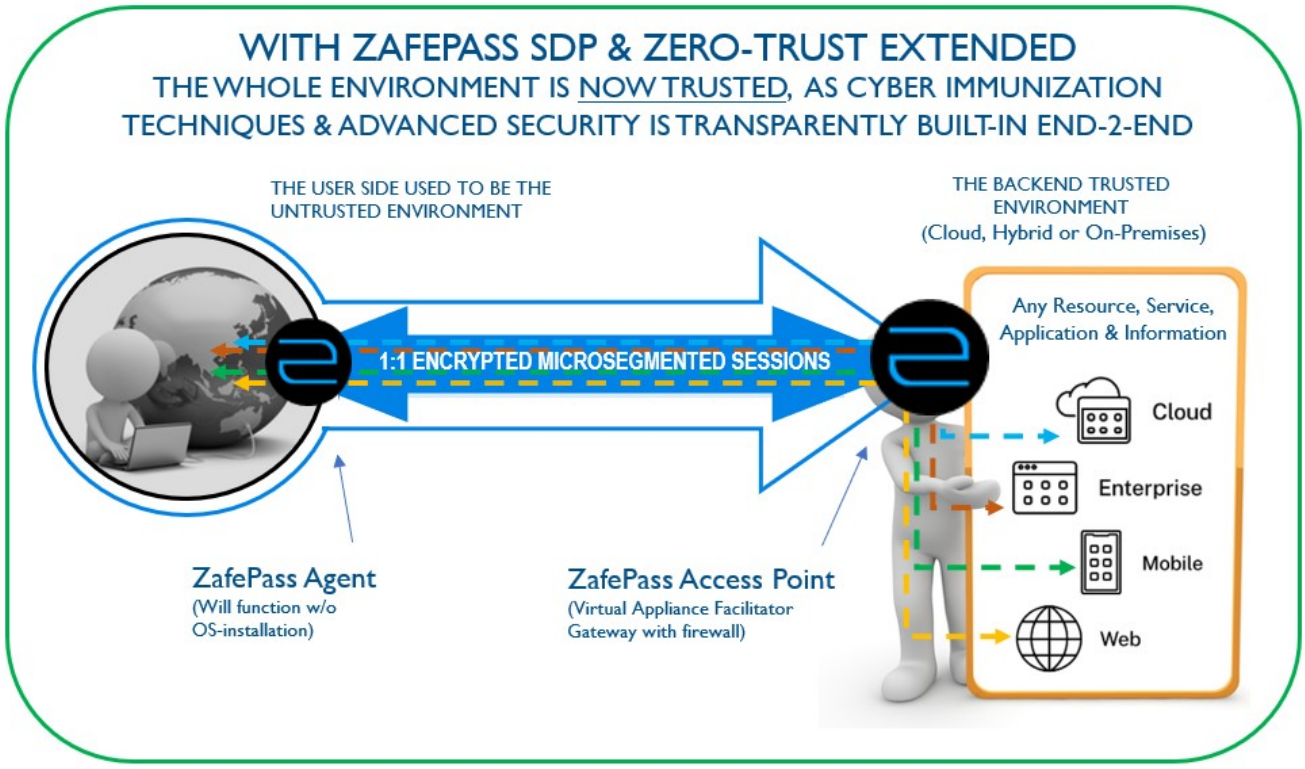
(1) A "**ZafePass Agent**", 'running' (optionally installed) on any user's device.

(2) A "**ZafePass Access Point**", (or multiple) 'running' on a Virtual Machine (VM)

Agents can be easily distributed (the security problem is taken care of) and reside and launch, or auto-launch from any media; a laptop, phone, tablet, USB key, read-only media, a web-site etc.

Access Points can easily be distributed to a datacentre and/or service provider, supporting on-prem, hybrid and public cloud out of the box. A centralized admin console helps IT-teams to configure, change, provision any elements i.e. on-/offboarding anything … users, resources, apps and app-deployment options, security policies and enforcements based on activity, geolocation, white-/black-listing etc.

ZafePass VPC is designed for agility, scalability, easy and time efficient management of any size environment—its an end-to-end solution, cryptographically secured together with a range of obfuscation techniques, using methods that has never been breached nor compromised.




The above figure represents a simplified layout of ZafePass Virtual Private Connectivity solution. The Access Point (gateway / proxy) can easily be placed in AWS, Azure, Google, Alibaba, IBM cloud environments etc. — or reside with your local cloud service provider.

ZafePass has a range of other use-cases that can be requested by contacting us.

**"A ZafePass deployment** can be a catalyst for changing how users access and how security is accomplished across the entire enterprise— **both on-premises and cloud"** (*Cloud Security Alliance*)

# ZAFEPASS Business Value of "Perimeter less"

At the end of the day, its not what ZafePass VPC adds to your business, but much more interesting what it removes.

Financials are often the first in line, and you can expect cost-savings on both CAPEX and OPEX. Some cases see cost savings above 50% of the IT-security budget from;

- *Reduced licensing, support and labor savings.*
- *Higher Efficiency, Effectiveness and Productivity from your organisation.*
- *Increased agility of IT operations, meeting business requirements faster.*
- *Governance, Risk & Compliance will experience reduced risk as network attacks and exploitations are prevented. PII data can be shielded off.*
- *Compliance scope increase as data collection, reporting, auditing is highly improved through centralized control of connections. ISO recertifications require less time etc.*
- *Secure cloud computing by rapidly, confidently and securely adoption of cloud architectures by reducing the cost and complexity of the required security architecture to support required applications in data-centres, public-cloud, private–cloud or hybrid.*

The outcome is greatly reduced attack-surface, impacting positively on risk and operational resiliency. Cyber-criminals will not be able to use the TTPs or attack-tactics, techniques and procedures, as ZafePass VPC 'offers them nothing' to work with. ZafePass leaves NO artefacts, and is completely resistant to Denial of Service, Man in the Middle attacks, and brute force, code injection as well as lateral movement attacks are either NOT possible or highly unlikely to happen.

ZafePass VPC provide the option for eliminating the need for point-security based on X.509 (VPN, PKI, TLS/SSL etc.). Also add-on crypto, IDS, IPS, IAM, PIM/PAM, CASB, Secure Web Gateways, DLP can be optional, especially for smaller enterprises. Larger enterprises should consider especially IAM and integration to SIEM / SOAR services, DNS and mail traffic scans as well as infrastructure monitoring, although ZafePass VPC is immune to infrastructure vulnerabilities.

## ABOUT ZAFEHOUZE

ZAFEHOUZE own all Intellectual Property (IP) rights to the ZafePass technology, and was founded by 4 Cyber-security guardians, as we became frustrated with the in-ability to secure organizational IT-infrastructure no matter how much we implemented. The foundation and the ZAFEHOUZE mission is to help organizations become Cyber-crime immune.

Allow us to quote a former colleague of ours — Mr. Bruce Schneier, American cryptographer, cyber-security professional and a very passionate privacy specialist and writer.

*People make security trade-offs based on feelings.*

*Here are two options for considerations:*

*There are people who just make you feel secure, and hope you never notice you're not, and there are people that can actually make you secure and hope you notice.*

*Who you work with is up to you!*

ZAFEHOUZE

Ph.: +46 40 644 4611 / +45 9363 1300

info@zafehouze.com

https://zafehouze.com

ZafePass Empirical

# WHY SELECT ZAFEPASS; Additional Considerations

## SIMPLIFYING IT OPERATIONS

**ZafePass** help you adjust to business requirements faster, easier and with less intervention from IT, the service/help desk and even external 'advisors'. Simplifying the amount of solutions, support the rapid changes needed for meeting digital transformation, without sacrificing security and compliance goals. In addition current changes in network topologies, on-/off-boarding of users and resources would have to take place in multiple systems. ZafePass change that, so you can stay agile, fast, responsive and flexible meeting future organisational requirements.

## ZERO-TRUST eXtended feature set (ZTX)

**Zero-Trust;** a hyped new buzz-word in the cyber-security industry. You'll hear vendors talk about ZT for Network Access (ZTNA) and literately labelling ZT to 'everything' security related. It is to a large extend fine. ZafePass have taken the ZTX approach—as the feature sets go beyond 'Zero-Trust', hence taken the Forrester abbreviation 'Zero-Trust eXtended' enhanced functionality.

## COMPLIANCE

**ZafePass** will help enterprises address many of the common compliance controls. Being able to reduce the scope of an audit, ZafePass can often decrease the overall cost and complexity of the engagement as there are fewer systems to evaluate. Because of the unified security policies and controls, it will help lower the management workload, as less audit variables need to be tested and evaluated.

## AUGMENT EXISTING SECURITY SOLUTIONS

**How to efficiently** finding a needle in a haystack. Security Service Providers offering Managed SOC or Detection & Response services as well as your inside SOC operation team will benefit from ZafePass being implemented. Your "haystack" will be reduced, attack flanks eliminated, and effectively you'll find the 'needle' much faster. Another challenge is the detection of lateral movement—in ZafePass lateral movement is impossible. Integrations with the most types of enterprise class security solutions, will support you overall security posture as using ZafePass is not an 'all-or-nothing' solution.

## ELIMINATE USER CONFUSION

**Different access solutions** have different functionality, inevitably leading to a situation where users will wonder why they can access certain IT resources ad perform certain operations from one location or device, but cannot do it from another. VPNs are often conflicting with home-Wi-Fi or when 'on the road' not functioning. The reason for this is lack of parity between the capabilities of different methods in different scenarios. ZafePass will apply consistency and a superior user experience—as connections are user transparent and managed automatically by ZafePass.

## HIGH LEVEL OF SECURITY

**Enforcing uniformly granular security policies** and handling events in a heterogenous environment is almost impossible. Organisations using the "implicit trust model" inevitably reach a point where the organisational security policies are not enforced properly, opening various IT resources to the risk of attack, breaches and data loss. ZafePass is able to solve these kind of challenges.

## ADAPTIVE RISK-BASED CONTROLS

**ZAFEPASS enable you to know exactly who** is attempting to access a ZafePass Access Point, from where, which device, what authentication methods to be used (2FA/3FA/biometric or other, or in random). The sensitivity of the application being accessed from various service and resource points in combination with identity-centric access to the right user, from the right location, using the right device, with the right patch level—you are simply able to tune security policies and your posture up and down meeting even the most rigid requirements.