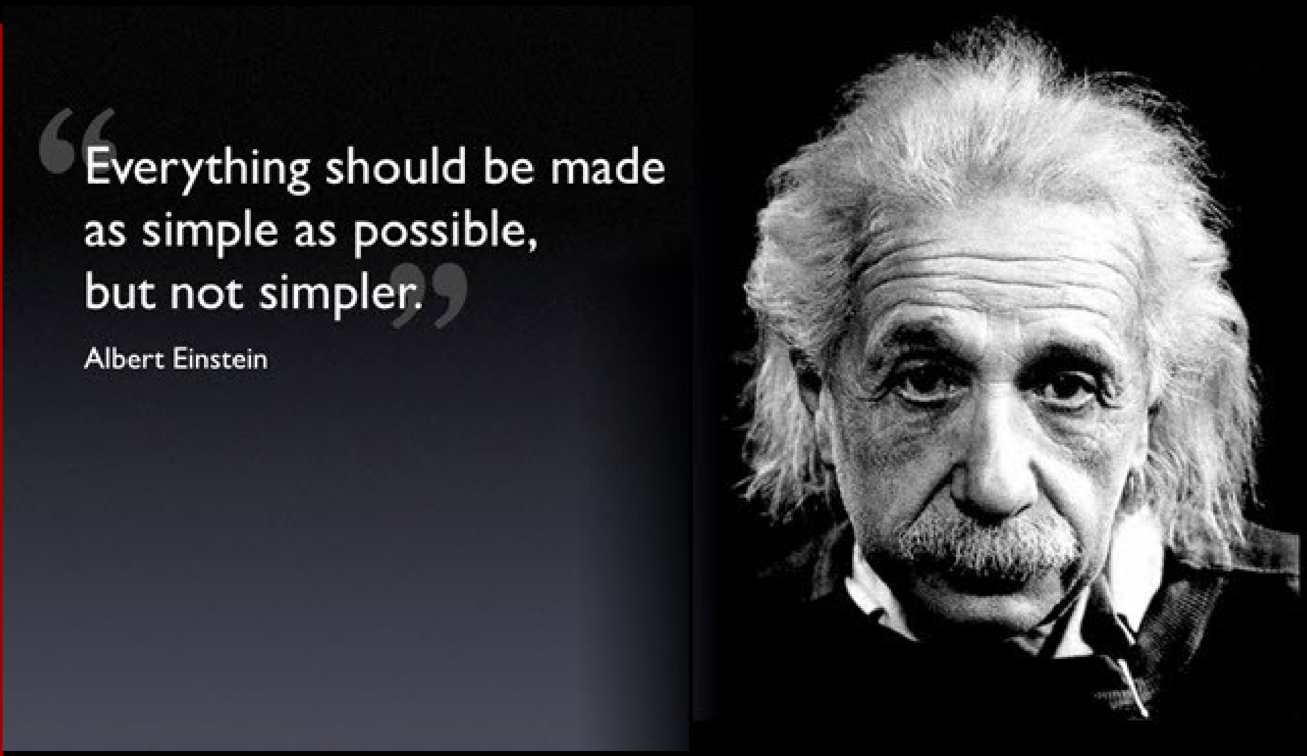
ZAFEHOUZE

ZAFEHOUZE Inc. / ZAFEHOUZE ApS www.zafehouze.com info@zafehouze.com



> “Everything should be made as simple as possible, but not simpler.”
>
> Albert Einstein

ZafePass VPC

(INTRO FACT SHEET)

Is an agile technology platform, supporting your organisations future requirements, leveraging and extending the feature set of;

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

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

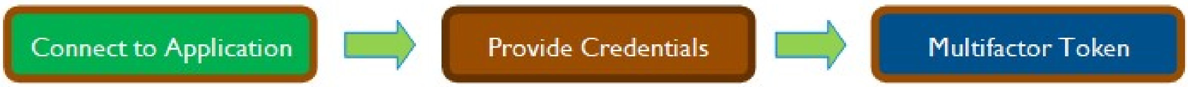
BACKGROUND

The principles behind ‘the ZafePass technology’ are not entirely new, but typically implemented in “classified IT organisations” like Department of Defense (DoD) and Intelligence Communities (ICs).

Principles and even more extreme ones rooted in our patent in secure communication, that are implemented in the ZafePass architecture, 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’.

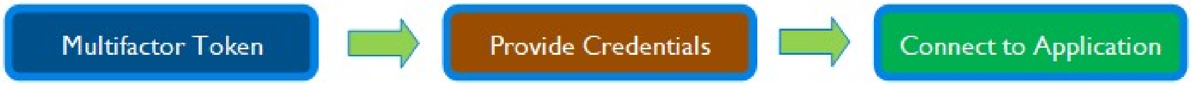
It doesn't sound very simple—but ZafePass VPC is not even close to the complexity you have today using technologies with a 30 year old cumbersome legacy. ZafePass VPC is simple, user-friendly, smart, cheap, secure and highly efficient. This design has many advantages over traditional IP-network access and security using a “connect first—authenticate second” model. A model were trust is presumed and easily be misplaced.

TRADITIONAL PERIMETER SECURITY MODEL



Connect to Application → Provide Credentials → Multifactor Token

SOFTWARE DEFINED PERIMETER SECURITY MODEL



Multifactor Token → Provide Credentials → Connect to Application

In todays hyper-connected and highly adversarial threat landscape, the traditional model is both outdated, and puts any organisation at risk, because of the predicated isolation (separation) of users and networks.

We’ll come back to the Software Defined Perimeter / Zero-Trust Security model later.

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 them 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 attacks, Man-in-the-Middle (MitM) exploits and Lateral Movement***
- ***Large attack surface—as many solutions are needed to work together***

High Costs of Operation, Administration and Management

.. and this was just six selected out of a larger list.

> “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 this mobile and cloud era we're in, the modern 'business and its' workforce' require simple and seamless access to IT-resources; the variety of services, applications and/or information. It's a daunting task for IT-teams to manage devices, juggle risk, compliance and regulations, managing data that has officially '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 rules on a global scale. 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 this IP based network access legacy and complexity, that keeps IT from satisfying these new demands, that in the end fuels frustration.

The Software Defined Datacenter has been around for a while, so has Software Defined Perimeter. It's time for the two to come together, joined by Zero-Trust EX.

CO-EXISTENSE & PRESERVE IT INVESTMENTs

To overcome these challenges, ZAFEHOUZE developed ZafePass VPC for providing users with modern, simple and secure **V**irtual **P**rivate **C**onnectivity to any IT-resource, following specifications outlined by Cloud Security Alliance for Software Defined Perimeter and Forrester for Zero-Trust EX (Employee eXperience). There are elements of Secure Access Service Edge, defined by Gartner Group and elements of API security.

ZafePass is de-coupled from the physical network topology, allowing simultaneous private micro-sessions between the resource-side (trusted) and the user-side (untrusted) - utilizing the network and infrastructure as a simple backbone. This 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, ZT-ET added a range of unique obfuscating techniques that will leave Cyber-criminals in the dark and empty-handed trying to compromise your business.

The first step is a transition towards 'a perimeter-less environment' can be phased-in in parallel with your existing setup, lowering any concerns you might engaging on ZafePass VPC for users to securely consume your organisations IT-resources.

ZafePass VPC goes beyond the specifications of SDP, SASE and ZT. A ZafePass VPC solution will become yours (licensee). Its 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.

ZAFEPASS ARCHITECTURE

The ZafePass architecture is made up of only two components;

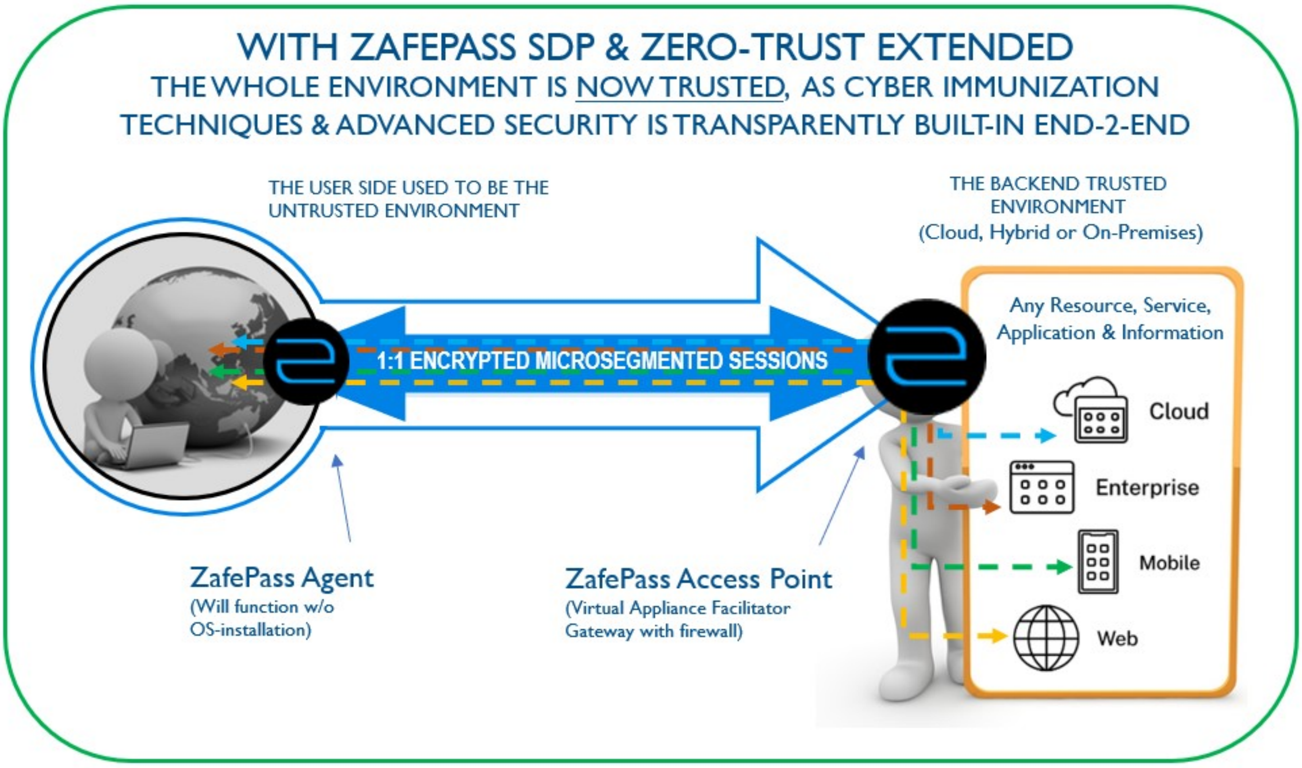
(1) A "**ZafePass Agent**", 'running' (optionally installed) on any user's device.

(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-2-end platform, cryptographically secured together with a range of obfuscation techniques, using methods that has never been breached or compromised.



WITH ZAFEPASS SDP & ZERO-TRUST EXTENDED

THE WHOLE ENVIRONMENT IS NOW TRUSTED, AS CYBER IMMUNIZATION TECHNIQUES & ADVANCED SECURITY IS TRANSPARENTLY BUILT-IN END-2-END

THE USER SIDE USED TO BE THE UNTRUSTED ENVIRONMENT
THE BACKEND TRUSTED ENVIRONMENT (Cloud, Hybrid or On-Premises)
1:1 ENCRYPTED MICROSEGMENTED SESSIONS
Any Resource, Service, Application & Information
Cloud
Enterprise
Mobile
Web
ZafePass Agent
(Will function w/o OS-installation)
ZafePass Access Point
(Virtual Appliance Facilitator Gateway with firewall)

The above figure represents a simplified layout of ZafePass Virtual Private Connectivity solution. The Access Point can easily be placed in AWS, Azure, Google, Alibaba, IBM cloud environments—or at a 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-centers, public-cloud, private–cloud or hybrid.*

The outcome is a massively reduced attack-surface, impacting risk and the operational resilience. Cyber-criminals will not be able to use their attack-tactics (MITRE ATT&CK), 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 even happen.

ZafePass VPC eliminate the need for VPN and many network security components based on X.509 (VPN, PKI, TLS/SSL etc.), add-on crypto, IDS, IPS, IAM, PIM/PAM, CASB, Secure web Gateways and DLP. A small organisation haven’t a need for these costly solutions—where larger organisations could benefit from IAM, have a need for XDR (cross-detection and response), Intrusion Detection, and most likely monitoring solutions like a SIEM (cloud be managed) or a Managed Security Operation Center setup.

ABOUT ZAFEHOUZE

ZAFEHOUZE own all Intellectual Property (IP) rights to the ZafePass technology, and have reduced supply chain risks by eliminating dependencies to 3rd party vendors and certificate issuers.

ZAFEHOUZE was started by 4 Cyber-security guardians, becoming frustrated with the inability to secure an organisations IT-infrastructure. The basic mission of ZAFEHOUZE is to help any organisation to become Cyber-crime immune.

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

> *People make trade-offs based on the feeling of security—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.*

ZAFEHOUZE

Ph.: +46 40 644 4611

info@zafehouze.com

https://zafehouze.com

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.