PREVENT-FIRST
NON-EXPOSURE SECURITY

A Comparative Analysis & Regulatory Framework Alignment Report

Prepared with reference to:

prevent-first.eu | zafehouze.com | zafepass.com

May 2026

PREVENT-FIRST
— NON-EXPOSURE SECURITY —

Executive Summary

The cybersecurity industry has long operated under a reactive paradigm: deploy defenses, detect intrusions, and respond to breaches. Even the most advanced frameworks – Zero-Trust, SASE, and Software-Defined Perimeter – reduce risk but do not eliminate exposure.

Prevent-First Non-Exposure Security represents a categorical departure from this approach.

This report provides a structured comparative analysis of Prevent-First Non-Exposure Security as articulated by the European Prevent-First Alliance (prevent-first.eu) and operationalized by Zafehouze through the ZafePass Prevent & Protect platform.

It contrasts this paradigm with conventional cybersecurity vendors – and in this report Check Point, ESET, and Morphisec, are representing network centric security vendors in 3 main categories – firewall vendors, end-point detection & response and end-point execution prevention.

Further it maps Prevent-First principles against the major global regulatory and security frameworks: CMMC 2.0, NIST SP 800-53, NIST SP 800-171, ISO 27001, NIS2, and others.

> *Core finding: Prevent-First Non-Exposure Security does not merely improve on existing models — it eliminates the conditions under which attacks can succeed. By making resources invisible, unreachable, and ephemerally connected, it removes the attack surface entirely rather than hardening it.*

Key conclusions of this report:

- Traditional 'prevention-first' claims by network-centric vendors address Layer 3/4 security but leave the attack surface structurally intact.
- Prevent-First architecture, as implemented in ZafePass, operates above the network layer at the session and resource level, achieving a null state where no standing exposure exists.
- The Prevent-First model natively satisfies the intent – not merely the letter – of CMMC 2.0, NIST 800-171, ISO 27001, NIS2, and related frameworks, often exceeding their requirements.
- The ZafePass platform has undergone a decade of adversarial testing and external security validation, with zero successful breaches recorded.

1. The Problem with Network-Centric 'Prevention'

1.1 The Reactive Paradigm

Conventional cybersecurity architecture — including next-generation firewalls, endpoint detection and response (EDR), SIEM platforms, and Security Operations Centres (SOCs) – is built on a fundamentally reactive logic: threats exist, intrusions happen, and the system's job is to detect and respond as quickly as possible.

This model accepts that the attack surface is visible. Adversaries can scan IP ranges, enumerate open ports, probe endpoints, and conduct reconnaissance. The assumption is that defenses will catch them before or shortly after they gain a foothold. In practice, the average dwell time for attackers in enterprise environments has remained measured in days or weeks – time during which enormous damage can be done.

1.2 Why Zero-Trust Is Necessary But Insufficient

Zero-Trust, introduced by Forrester Research in 2010 and endorsed by CISA, NIST, and NATO, is widely considered the gold standard of modern security architecture. Its core principles — 'never trust, always verify, least privilege' – represent a significant advancement over perimeter-based security.

However, Zero-Trust has a fundamental limitation: it operates within the network. It verifies access requests, but the resources being requested – and the infrastructure through which requests are routed – remain visible and potentially targetable. A Zero-Trust implementation still exposes:

- IP addresses and resolvable hostnames
- Open ports and services (even if authentication-gated)
- Cloud edge infrastructure subject to reconnaissance
- VPN concentrators and identity provider endpoints

> *Zero-Trust reduces the blast radius of a compromise. Prevent-First removes the conditions for compromise to begin.*

1.3 SASE and SDP: Progress, But Still Exposed

Secure Access Service Edge (SASE) converges network and security capabilities — SD-WAN, cloud-delivered firewalls, CASB, and Zero-Trust Network Access (ZTNA) — into a unified cloud service. Software-Defined Perimeter (SDP) cloaks resources behind authenticated access brokers. Both represent meaningful progress.

Yet both retain structural exposure. SASE traffic routes through cloud points of presence that are themselves scannable and subject to zero-day attack. SDP enforces access at the perimeter layer, meaning the perimeter itself remains a target. Neither achieves true invisibility at the resource level.

2. The Prevent-First Non-Exposure Security Paradigm

2.1 Philosophical Foundation

Prevent-First Security was formally articulated by the European Prevent-First Alliance (prevent-first.eu) as a next-practice extension of Zero-Trust. Its central proposition is philosophical as much as technical: if an asset cannot be seen, it cannot be attacked. If a session does not persist, it cannot be hijacked. If there is no network path, there is no lateral movement.

The framework draws intellectual lineage from the Jericho Forum's 2004 'deperimeterization' project – recognizing that network perimeters are dissolving in a hyper-connected world.

Prevent-First takes this further: rather than defending a disappearing perimeter, it creates new perimeters at the most atomic level – the individual session, the individual user, the individual resource.

2.2 The Five Pillars of Prevent-First

Pillar 1: Micro-Perimeters

Every protected resource – data repositories, applications, services, and operational technology assets – is isolated within its own enforcement boundary. Access to one resource grants zero access to any other. Lateral movement is structurally impossible, not merely monitored.

Pillar 2: Null State & Ephemeral Connectivity

Resources exist in a 'null state' e.g. non-exposed / unreachable) – until a validated user makes an authenticated request. Connectivity is established ephemerally for the duration of the authorized session and disappears entirely when session ends. No standing connections or residual pathways.

Pillar 3: Session & Resource Segmentation

Users do not access networks. They access single, explicitly authorized resources. Each session is unique, cryptographically isolated, and fully logged. Compromise of one session cannot propagate to others.

Pillar 4: Guard-Railed Access Control

Every access decision is continuously validated against a multi-dimensional policy engine incorporating user identity, device posture, defined geo-specifications, time-of-day, network context, environmental and behavioral attributes. Access is never granted by default – it must be explicitly earned against all policy dimensions simultaneously.

Pillar 5: Virtual Private Connectivity (VPC)

Rather than VPNs – which create broad, shared network tunnels – Prevent-First establishes one-to-one encrypted tunnels between a verified user and a single entitled resource. No shared access, no broad reach, no leak paths.

> *The result: the enterprise becomes a null state — invisible, unreachable, and uncompromisable. Attackers cannot reconnoitre what they cannot see. They cannot exploit what they cannot reach.*

3. Comparative Analysis: Prevent-First vs. Conventional Vendors

3.1 Architectural Comparison

The following table provides a structured comparison across key architectural and security dimensions. Note that Check Point, ESET, and Morphisec each represent different layers of conventional cybersecurity – network security, endpoint protection, and endpoint runtime protection respectively – yet all share the fundamental limitation of operating on a visible, standing attack surface.

Criteria	Check Point	ESET	Morphisec	ZafePass (Prevent-First)
Security layer	L3/L4 Network	L3/L4 Network	Endpoint/Process	**Session & Resource**
Attack surface	Reduced	Reduced	Reduced	**Eliminated**
Adversary recon possible	Yes	Yes	Yes	**No — Null State**
Lateral movement	Mitigated	Mitigated	Limited	**Structurally Impossible**
Standing network exposure	Present	Present	Present	**None**
VPN / SASE dependency	Often required	Often required	Coexists	**Replaced entirely**
Core model	Detect & Block	Detect & Block	Prevent-at-Execution	**Never-Expose**
Ephemeral connectivity	No	No	No	**Yes — by design**
Zero-Trust compliant	Partial	Partial	Partial	**Full + Extended**
Backdoor risk	Present	Present	Present	**Architected out**
CMMC 2.0 support	Partial	Partial	Partial	**Comprehensive**
NIS2 alignment	Partial	Partial	Partial	**Native**

3.2 Narrative Assessment

Check Point (representing leading firewall and network access vendors)

Check Point's CloudGuard and Quantum platforms are mature, enterprise-grade solutions. Their 'prevention-first' positioning refers primarily to blocking known and unknown threats at network ingress/egress points using AI-based threat intelligence. Resources behind the perimeter remain networked and discoverable. SOC operations are required to detect anomalies post-ingress.

ESET (representing end-point detection & response + execution prevention vendors)

ESET emphasizes proactive endpoint protection, leveraging machine learning and behavioral analysis to block threats before execution. Their prevention-first posture is endpoint-centric – stopping malicious code from running — but does not address the broader issue of network-level exposure or lateral movement pathways.

Morphisec (representing a sophisticated level of end-point execution prev. vendors)

Morphisec's Moving Target Defense technology is technically innovative, randomizing memory allocation to prevent exploit code from locating its targets. This is genuine prevention at the execution layer. However, it operates post-ingress: an attacker has already reached the endpoint. The network path, IP address, and initial attack vector remain exposed.

ZafePass by Zafehouze (Prevent-First)

ZafePass operates at a fundamentally different layer. By wrapping every protected resource in an authenticated, ephemeral, one-to-one session — and returning all resources to null state when sessions are not active — it removes the preconditions for attack entirely. There are no exposed IPs to scan, no ports to probe, no VPN concentrators to target. The attack surface is not reduced: it is eliminated.

4. Why VPN and NAC Cannot Deliver Authentic Zero Trust

4.1 The Formula One Tyre Problem

Road tyres fit a Formula One car. The wheel hubs are compatible, the bolts thread correctly, and the car will move. But the compound is wrong, the contact patch is wrong, and the thermal behaviour under racing conditions is entirely mismatched. You can complete a lap — but you cannot win the race.

This is precisely the relationship between VPN/NAC and authentic Zero Trust. VPN and Network Access Control technically fit inside a Zero Trust strategy. The architecture moves. The vendor slide decks read correctly. The compliance checkbox gets ticked. But the fundamental property that makes Zero Trust meaningful — no standing trust, ever — is violated at the most basic structural level.

> *The industry has been selling road tyres to Formula One teams for fifteen years and calling it performance. Most security practitioners never notice, because the car does move — just not fast enough to win.*

4.2 The Original Zero Trust Intent

John Kindervag's 2010 Forrester Research paper, and the Jericho Forum's deperimeterization work that preceded it, were built on one philosophical bedrock: trust is a vulnerability. The moment you trust a connection, a session, a network segment, or a device state, you have created an assumption that an adversary can exploit. Zero Trust was designed to eliminate standing trust entirely. Its three principles — never trust, always verify, least privilege — are not checkboxes. They are a continuous operating mode. Verification must happen at every access decision, for every specific resource, in real time. Not once at session establishment. Not once at device admission. Every time.

4.3 Why VPN Violates Zero Trust at the Architectural Level

A VPN creates a persistent, authenticated tunnel — and then hands the authenticated user a network. Not a resource. Not a door to one room. A key to the entire floor.

Once inside, the user has standing access to an IP range, potentially for hours or days. The VPN concentrator itself is a publicly visible, permanently exposed target — a routable address that can be scanned, probed, and attacked.

The session is not ephemeral: it is a long-lived channel that can be hijacked, credential-stuffed, or traversed laterally.

This is the structural opposite of Zero Trust. It is trust encoded in persistence. The connection itself is the grant of trust — and once granted, it persists independently of whether the user, the device, or the context remains legitimate.

- The VPN concentrator is permanently exposed on the public internet — an always-on attack surface.
- Authentication happens once, at tunnel establishment. Every subsequent packet inherits that trust.
- The authenticated user receives network access, not resource access — the blast radius of a compromised credential is the entire network segment.
- Session persistence gives an attacker time: dwell time in enterprise environments measured in days means a VPN-based breach is a slow, thorough, damaging one.

4.4 Why NAC Has the Same Structural Problem

Network Access Control verifies device posture at the point of admission — then grants the compliant device access to a network segment. The verification happens once. The access persists.

Device state drifts. Patches are missed. Certificates expire. Malware loads after admission. A device that was clean and compliant at 9am can be compromised by 10am — and the network segment is still open to it because NAC already made its decision.

NAC also operates at Layer 2/3. It controls which VLAN a device joins, not which specific resources within that VLAN it can reach. The granularity is a blunt instrument applied to a precision problem.

Granting access to a VLAN grants access to everything addressable within that VLAN, regardless of whether the user has any legitimate reason to reach those systems.

- NAC is a point-in-time admission check, not a continuous access control mechanism.
- Device state between checks is unknown — NAC trusts the snapshot, not the current reality.
- VLAN-level access control is network-centric, not resource-centric. It cannot express least privilege at the resource level.
- Lateral movement within a VLAN is structurally possible — NAC does nothing to prevent it.

Architectural property	VPN / NAC	Claimed Zero Trust	Prevent-First (ZafePass)
Connection model	Persistent tunnel	Standing gateway	Ephemeral, session-scoped only
What access is granted	Network segment (IP range)	Narrowed zone — still network	One specific resource, nothing else
Attack surface	Concentrator + full segment	Gateway + reduced zone	None — null state when idle
Adversary recon	IP visible, ports probeable	Gateway scannable	Nothing to discover or probe
Lateral movement	Possible within segment	Reduced but possible	Structurally impossible
Session persistence	Hours or days	Persistent	Vanishes on session close
Device trust model	Verified once at admission	Periodic re-check	Continuous multi-dim validation
Never trust principle	Violated — trust persists	Partially honoured	Fully honoured — no standing trust
Kindervag compliance	No	Partial	Yes — and extended beyond

4.5 The Three Failure Modes in Plain Language

Failure Mode 1 — Trust by Persistence (VPN)

The VPN grants network access once, then trusts the connection indefinitely. Every packet sent through that tunnel is trusted because the tunnel itself was authenticated — not because each packet represents a legitimate, currently valid access request. The principle 'never trust' is directly contradicted: the tunnel is trusted, continuously, for its entire lifetime. When the tunnel is compromised — through credential theft, session hijacking, or a man-in-the-middle attack — the adversary inherits that persistent trust wholesale.

Failure Mode 2 — Deferred Trust (NAC + ZTNA Marketing)

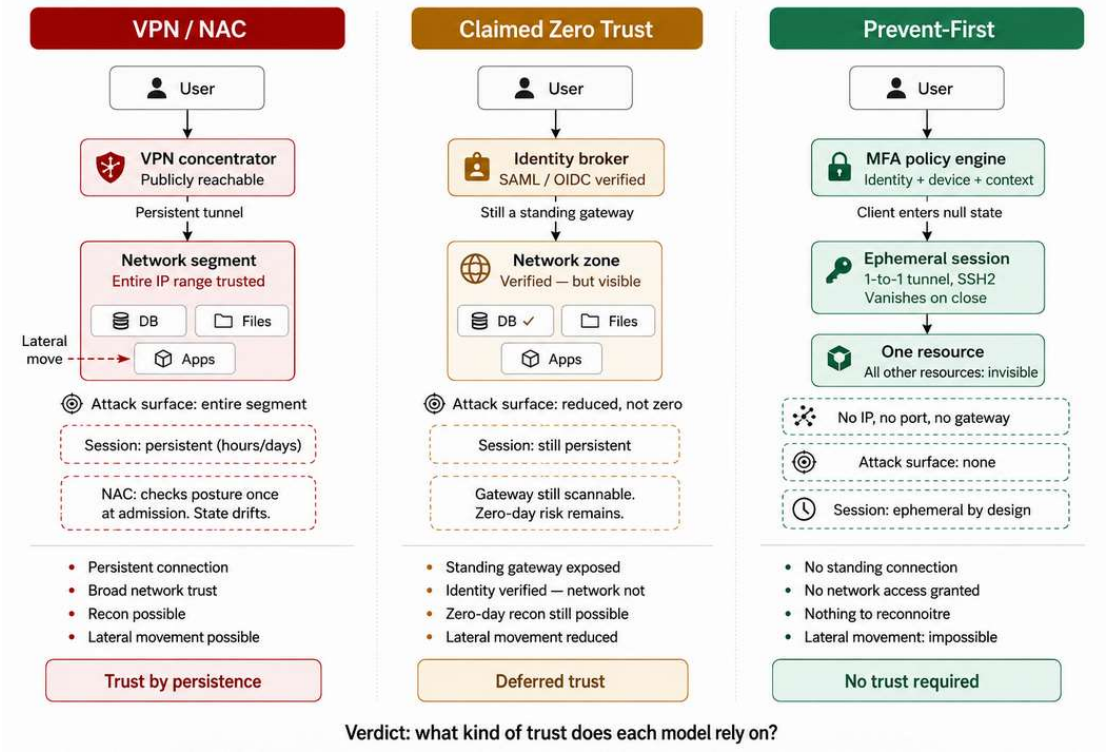
The identity broker may be excellent. SAML and OIDC verification may be thorough. But the gateway is still a permanently present, publicly scannable target. The device was clean when admitted — it may not be now. The verified identity is real — but the session that identity opened persists long past the moment of verification. This is not 'never trust, always verify.' It is 'verify once, then trust until the session expires.' Deferred trust is still trust.

Failure Mode 3 — Network-Level Thinking in a Resource-Level Problem

Both VPN and NAC are architecturally network-centric. They control which network a user or device can reach, not which resources within that network are accessible. Zero Trust's requirement for least privilege — access only to what is needed, only when it is needed — cannot be expressed at the network level. A VLAN is not a resource. An IP range is not a permission. Genuine least privilege requires resource-level enforcement, session-level granularity, and ephemeral rather than standing access. VPN and NAC cannot provide any of these things, because their architecture does not operate at that layer.

4.6 The Three Security Trust Models in Operation

The below diagram actually explains a very important architectural difference that many organisations completely miss. The image compares three fundamentally different security models and, more importantly, the kind of trust relationship each model depends on.



1) Traditional VPN / NAC security – 2) “Claimed” Zero Trust architectures and 3) Prevent-First Non-Exposure Security.

The core question is: “***What kind of trust does each model rely on?***”, “***What do you require?***” . and clearly visualize the difference between old and modern cybersecurity architectures.

4.6.1 VPN / NAC — “Trust by Persistence”

This is the traditional enterprise security model. Even if segmentation exists: the network itself is still exposed and interactable. How it works:

A user - authenticates,
- connects through a VPN gateway,
- and receives access to a network segment.

Once connected:

- the connection remains persistent,
- the user becomes part of the network,
- and many systems become reachable.

Key Characteristics

Persistent tunnel. The connection remains active for **hours, days or until manually disconnected.** Broad network trust. The user is trusted because:

- they successfully connected.

Entire IP range becomes reachable. This means:

- scanning is possible,
- reconnaissance is possible,
- lateral movement is possible.

Main Problem

Even though access control exists: ... attackers can still interact with the environment.

If:

- credentials are stolen,
- a laptop is compromised,
- or malware executes,

then the network is already reachable. The attack surface still exists.

4.6.2 Claimed Zero Trust — “Deferred Trust”

This is where many modern vendors position themselves today. It improves significantly over VPN. But the diagram argues it still leaves exposure behind. How it works:

The user:

- authenticates through an identity broker,
- MFA is verified,
- identity is validated,
- access policies apply.

This is much stronger than traditional VPN.

BUT: there is still:

- a standing gateway,
- a visible service,
- a reachable infrastructure component.

Key Improvement: Instead of trusting the whole network:

- trust becomes identity-based.

That is good. Lateral movement is reduced.

Main Limitation

The environment is still discoverable, reachable and interactable = EXPOSED.

Meaning:

- gateways and environments can still be scanned,
- zero-days can still target exposed services,
- attack paths still exist.

So ... although, the attack surface is reduced – cyber-criminal activity is not eliminated.

That is why the diagram calls it:

“Deferred Trust”

Trust still exists.

It just happens later in the process.

4.6.3 Prevent-First — “No Trust Required”

This is the architectural shift the diagram tries to explain. The idea is ... do not expose a standing environment in the first place. How it works

The client starts in **a “null state”** meaning**;**

- ***no network access,***
- ***no broad visibility,***
- ***no standing tunnel.***

Only after; identity, device, policy and context are verified does:

- ***a temporary,***
- ***ephemeral,***
- ***one-to-one connection***

get created.

Key Difference

The user does NOT enter a network, gain subnet visibility or access a segment. Instead – the user gets access only to ONE specific resource. Nothing else exists from the user perspective.

Important Architectural Concepts and main differentiator from the others are **Ephemeral Sessions.** These sessions, exists temporarily, disappears on close and leaves no persistent tunnel.

No Standing Gateway

The diagram argues - there is no persistent reachable infrastructure exposed to attackers. Meaning:

- **no IP to scan,**
- **no visible ports,**
- **no exposed gateway,**
- **no persistent attack target.**

No Network Trust

The user is not trusted 'as a result of' joining a network. The network itself becomes largely irrelevant. Trust becomes session-specific, resource-specific, policy-driven and temporary.

Why This Matters

The image is fundamentally arguing: "*Traditional cybersecurity protects exposed environments*". While: "***Prevent-First attempts to reduce or eliminate unnecessary exposure itself***". That is the core philosophical difference – but it is also important to emphasise the diagram is NOT saying firewalls are useless, VPNs are useless or Zero Trust is bad. It doesn't... instead it argues:

"... the closer you move toward eliminating persistent exposure, the smaller the operational opportunities become for attackers".

That means:

- *less reconnaissance, fewer attack paths, less lateral movement, less dependency on detection and fewer persistent targets.*

The Most Important Line in the Diagram are At the bottom:

Model	Trust Type
VPN/NAC	Trust by persistence
Claimed Zero Trust	Deferred trust
Prevent-First	No trust required

That is actually the entire story. The diagram argues:

- VPN trusts users because they connected,
- Modern Zero Trust delays that trust,
- Prevent-First removes the need for broad trust relationships entirely.

VPN: "Here's the whole building. Please behave**." Zero Trust: "**Show ID first — then you can enter parts of the building**." Prevent-First:** "You never enter the building. You only get handed exactly the things you need – temporarily."

4.7 What Authentic Zero Trust Actually Demands

Kindervag's original principle — 'never trust, always verify' — only holds if every access decision is made at the moment of access, for that specific resource, validated continuously. That demands:

- No standing network access — only session-scoped resource access
- No persistent tunnels — only ephemeral, purpose-built connections that dissolve when the session ends
- No broad VLAN or subnet trust — only one-to-one, policy-evaluated resource entitlement
- Continuous validation, not point-in-time admission — device posture, user identity, context, and behavioural signals re-evaluated at every access event
- No permanently exposed infrastructure — no VPN concentrator, no NAC gateway, no standing attack surface

This is precisely what the Prevent-First architecture delivers. ZafePass resources exist in null state — invisible and unreachable — until a validated user makes an authenticated request against the full multi-dimensional policy engine. The connection is established ephemerally for that session only, carries only that user to only that resource, and dissolves without residue when complete. There is no persistent tunnel to hijack, no gateway to scan, no segment to traverse laterally.

> *Zero Trust is not a product category. It is not a VPN with MFA bolted on. It is not a NAC that checks device certificates. It is a continuous operating principle: no trust is ever granted without being earned, re-earned, and scoped precisely to the task at hand. Prevent-First is the first architectural paradigm that makes this principle structurally enforceable rather than aspirationally documented.*

4.8 Implications for Security Teams and Procurement

The practical consequence of this analysis is that organisations using VPN or NAC as the foundation of a Zero Trust strategy are not implementing Zero Trust. They are implementing a better perimeter — which is a meaningful improvement, but a categorically different outcome.

Security teams evaluating their Zero Trust posture should ask these diagnostic questions:

- Does our access control grant network access or resource access? If the answer is network access, Zero Trust has not been implemented.
- Are our sessions ephemeral or persistent? If sessions persist beyond the duration of a specific task, standing trust exists.
- Is our authentication infrastructure permanently exposed on the public internet? If so, it is an attack surface — regardless of how strong the authentication is.
- Can a user who authenticates successfully reach resources they are not authorised to use? If lateral movement is possible, least privilege has not been achieved.
- Does our device posture validation happen once (at admission) or continuously? Point-in-time admission checks are not Zero Trust.

If any of these questions reveals a gap, the architecture is built on road tyres. The car moves — but it cannot win the race. Prevent-First Non-Exposure Security, as implemented in ZafePass, addresses every one of these diagnostic criteria by architectural design, not by policy configuration.

> *The industry has spent a decade calling VPN-plus-MFA 'Zero Trust.' It is not. The difference is not cosmetic — it is the difference between reducing your attack surface and eliminating it. Only the latter constitutes true prevention.*

5. ZafePass Technical Architecture

5.1 Gateway Architecture

ZafePass is built on a transit gateway model using FreeBSD UNIX as the gateway operating system — the same foundation used by Netflix, WhatsApp, and Juniper Networks. Each gateway speaks only SSH2, meaning it presents exactly one protocol to the outside world: the most scrutinized and hardened secure communication protocol in existence.

To authenticate against a ZafePass gateway, an attacker would need to simultaneously possess a valid username, a matching password (which is not the user's actual credential), and a machine-generated private key stored only in encrypted memory on the client. Even quantum computing capability would not help: three unknown, machine-generated secrets must be simultaneously guessed.

5.2 Multi-Factor Authentication Policy Engine

ZafePass MFA is not merely 'something you know + something you have.' The policy engine validates access against a multidimensional matrix:

- Device identity (hardware identifiers, not just certificates)
- User credentials (separate from device identity)
- Public and private IP context
- Machine serial number and MAC address
- Time of day and day of week
- Defined IP address match (or address net)
- Device approval status (manual or automated enrolment)

This multi-dimensional validation provides stronger assurance than TOTP authenticators or SMS OTP, without requiring any additional action from the end user.

5.3 Data Islands & Peer-to-Peer Connectivity

Once authenticated, the ZafePass client receives a list of authorized resources and then goes to null state — the connection to the central authentication system closes entirely. When a user requests a resource, a direct peer-to-peer connection is established between the client and the specific gateway serving that network segment, bypassing the central infrastructure entirely.

This 'Data Islands' model means that each network segment is cryptographically isolated. Ransomware, malware, or an attacker who gains access to one segment has no pathway to any other. The structural impossibility of lateral movement is not a policy configuration: it is an architectural property.

5.4 No Third-Party Dependencies & No Backdoors

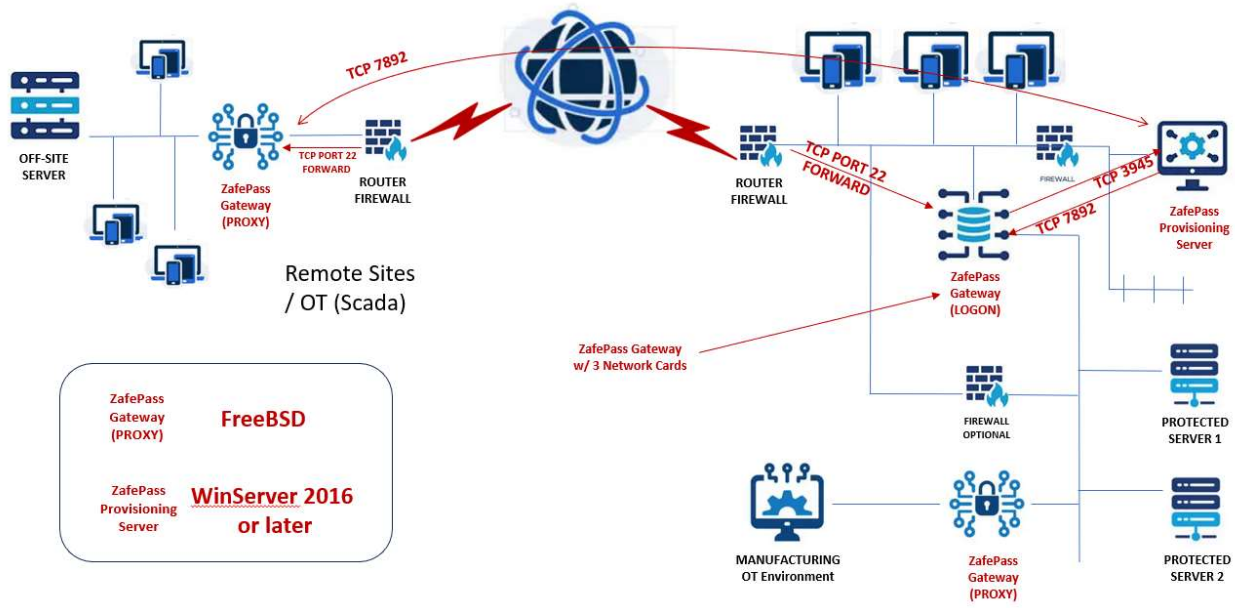
ZafePass does not use x.509 PKI certificates - the standard Certificate Authority infrastructure that underlies most web security. Instead, it generates all cryptographic key-pairs fresh at installation.

Neither Zafehouze nor any third party retains knowledge of these keys. No government, intelligence agency, or law enforcement body has any means of compelling access - because no access mechanism exists to compel.

5.5 Validation Record

Over twelve years of active development and deployment, ZafePass gateways are probed hundreds to thousands of times daily. Zero successful breaches have been recorded. Independent external validation over a ten-month engagement confirmed that no practical or theoretical attack path could be identified — even with access to the back-end source code.

The foundational architecture:



5.6 Connectivity Architecture: VPC, Dual-Reverse Proxy and Null-State (Ephemeral)

ZafePass replaces network-level connectivity (VPN/IPsec) with application-centric Virtual Private Connectivity (VPC). Users see resources, not networks. Applications, services and policy-controlled access points is exposed in the ZafePass launchpad – only after all checks and validations have succeeded. Key properties of VPC:

- No layer-3 network overlay, no IP routing tables pushed to endpoints.
- Each resource is associated with its own logical micro-channel and policy set.
- Connectivity is bound to specific processes via the Network Socket Gateway engine in the client.

The ZafePass Proxy Gateway operates as a Dual-Reverse / SOCKS5 proxy and application enabler. Tunnels are established over SSH/SSH2 with an additional encrypted virtual channel for application payloads. Only configured resources are reachable; everything else is implicitly denied.

Null-state extends across the connectivity stack. When a task completes, Connector instances and gateway engines disconnect, destroy keys and reset internal state.

No unsolicited event can “wake up” a dormant module: there are no idle listeners beyond the pre-shared, and generated on a per-installation basis hardened entry point(s), and no reusable session context. This is materially different from traditional “stateless” services, which still respond to arbitrary incoming packets.

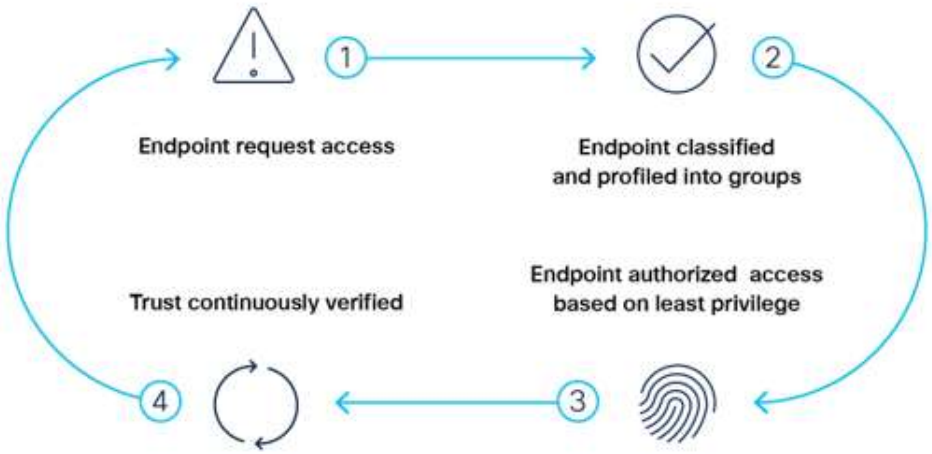
5.7 Identity, Device, Policy and Comply-to-Connect

ZafePass enforces device adoption before user identity is even considered. Adoption binds a device cryptographically to a user account using a combination of device fingerprinting, key material and internal identity stores. Copying the client binary to another host yields no usable access; the binding is not portable.

Authentication uses MFA, device identity, ephemeral session tokens and certificate validation. ZafePass employs a double keypair model in its provisioning infrastructure – one hard-coded keypair for signing authenticity and one rotating keypair for session key exchange. Long-lived cookies or browser tokens are not used; session keys are discarded at teardown.

The Policy Engine combines role-based and attribute-based access control. Policy evaluation occurs both at session establishment and continuously for operations such as application launch, resource selection, file access, clipboard/print actions and protocol initiation. This is deeper than network ACLs or static group entitlements, and directly aligned with the concept of least privilege.

Comply-to-Connect (CtC) gates connectivity on device posture, key validity, adoption status and contextual constraints (location, time, origin, risk signals). If CtC fails, no tunnel is established, no session container is created, and no partial access is granted. D&R tools typically observe non-compliant devices after the fact; ZafePass never allows them to reach the protected surface.



5.8 Data-Plane Security: Virtual File System (VFS) and Unified File System (UFS)

Virtual File System (VFS)

(Local, encrypted, session-bound storage anchored inside the ZafePass micro-perimeter)

ZafePass **Virtual File System (VFS)** is a **policy-controlled, emulated secure drive** that behaves like a physical storage volume but is actually an **encrypted container file** stored beside the ZafePass client itself.

1. **Local encrypted storage vault, session bound perimeter enforced file access**
    - VFS is a virtual drive containing all stored data inside a single encrypted file co-located with the client (e.g., a portable drive or workstation) only accessible **after successful ZafePass authentication. Unmounts** once the session ends.
    - VFS access is governed by ZafePass **guard-railed policies –** meaning, only approved applications and/or users can access the drive. Windows Explorer can be restricted. Application-restricted mode is available.

Unified File System (UFS)

(Unified, policy-driven access layer for remote, hybrid, and heterogeneous storage systems: SMB, NFS, S3, SFTP)

ZafePass **Unified File System (UFS)** extends secure storage from local endpoints to distributed or cloud environments. It presents a **virtualized abstraction of network file systems**, where the user sees consistent folder-like structures, but data resides remotely on shared drives or cloud objects.

UFS is designed to give system owners **full control of cross-environment file access**, without exposing backend systems directly to user devices.

UFS consists of three major components:

1. **UFS Manager, UFS Proxy and ZafePass Client UFS interface**
    - Defines mappings, policies, and share exposure.
    - Handles encryption for cloud storage such as S3 (all uploaded objects are transparently encrypted; bucket contents cannot be directly downloaded outside ZafePass)
    - **UFS Proxy** *(for SMB, NFS, and local-folder backends)* a secure relay, reachable only through ZafePass gateways. Users never communicate directly with file servers.
    - **ZafePass Client UFS Interface**. Presents a list of "shares" as folders.
    - Provides zero-installation access; mappings update dynamically without endpoint changes.

6. Regulatory Framework Alignment

6.1 CMMC 2.0 (Cybersecurity Maturity Model Certification)

CMMC 2.0 is the US Department of Defense's mandatory certification framework for defense contractors handling Controlled Unclassified Information (CUI). It defines three maturity levels, with Level 2 requiring full implementation of all 110 practices drawn from NIST SP 800-171.

The table below maps Prevent-First/ZafePass capabilities against CMMC 2.0 Level 2 domain requirements:

CMMC 2.0 Domain	Requirement Summary	ZafePass Coverage	Notes
Access Control (AC)	Limit system access to authorized users; control remote access	✓ Full	Guard-railed, policy-driven access; P2P ephemeral sessions replace VPN
Identification & Authentication (IA)	Authenticate users, devices, and services	✓ Full	Multi-dimensional MFA; device + user + context validation
Configuration Management (CM)	Establish baseline configs; control changes	✓ Covered	Synchronizer auto-manages gateway config and ACLs continuously
Audit & Accountability (AU)	Create, protect, and review audit logs	✓ Full	Per-user firewall logging; rSyslog with RHEL to SIEM in near real-time
System & Comm. Protection (SC)	Monitor, control, and protect communications	✓ Full	SSH2 transit gateways; no exposed interfaces; one-to-one encrypted tunnels
Risk Assessment (RA)	Periodically assess risk to operations	✓ Covered	Null state eliminates the primary risk categories; residual risk near zero
Incident Response (IR)	Establish capability to respond to incidents	◑ Partial	Prevention focus reduces IR need; recommend pairing with IR playbook
Media Protection (MP)	Protect CUI on system media	✓ Covered	Local encrypted storage; no data traverses uncontrolled paths
Personnel Security (PS)	Screen individuals; enforce termination procedures	◑ Partial	Access revocation immediate; personnel vetting is organizational scope
Physical Protection (PE)	Limit physical access to systems	◑ Partial	Out of ZafePass scope; organizational controls required

> *CMMC 2.0 Assessment: ZafePass directly and comprehensively addresses 7 of 10 Level 2 domains, partially supports 3 organizational domains (IR, PS, PE) that require complementary policy controls. Overall CMMC 2.0 alignment: High.*

6.2 NIST SP 800-53 (Security and Privacy Controls)

NIST SP 800-53 Rev. 5 provides the most comprehensive catalog of security and privacy controls available, used by US federal agencies and widely adopted internationally. It comprises 20 control families. The following maps ZafePass against the most security-critical families:

Control Family	Key Controls	ZafePass Alignment
AC – Access Control	AC-2 Account Mgmt, AC-3 Enforce, AC-17 Remote Access, AC-20	✓ Native
IA – Identification & Auth	IA-2 MFA, IA-3 Device ID, IA-5 Auth Mgmt, IA-8	✓ Native
SC – System & Comms	SC-7 Boundary, SC-8 Confidentiality, SC-28 Data at Rest	✓ Native
AU – Audit & Accountability	AU-2 Events, AU-3 Content, AU-9 Protection, AU-12 Generation	✓ Native
CM – Config Management	CM-2 Baseline, CM-6 Settings, CM-7 Least Functionality	✓ Covered
SI – System Integrity	SI-3 Malware, SI-4 Monitoring, SI-10 Input Validation	✓ Covered
SA – System Acquisition	SA-8 Security Engineering Principles	✓ Native
IR – Incident Response	IR-4 Handling, IR-5 Monitoring, IR-6 Reporting	◑ Partial
RA – Risk Assessment	RA-3 Risk Assessment, RA-5 Vuln Scan	✓ Covered
CA – Assessment & Auth	CA-7 Continuous Monitoring, CA-9 Internal Connections	✓ Covered

> *NIST 800-53 Assessment: The Prevent-First architecture natively satisfies the intent of the AC, IA, SC, AU, and SA families – the five families most directly related to access control and exposure management. These represent the highest-impact control families for breach prevention.*

European PREVENT-FIRST Alliance

6.3 NIST SP 800-171 (Protecting CUI in Non-Federal Systems)

NIST SP 800-171 defines 110 requirements across 14 requirement families for protecting Controlled Unclassified Information. It forms the basis of CMMC Level 2. The most demanding families from a technical implementation standpoint are:

Requirement Family	# Requirements	ZafePass Direct Coverage	Coverage Level
3.1 Access Control	22	22 of 22	✓ Full
3.3 Audit & Accountability	9	9 of 9	✓ Full
3.4 Configuration Management	9	8 of 9	✓ Full
3.5 Identification & Authentication	11	11 of 11	✓ Full
3.6 Incident Response	3	1 of 3	◑ Partial
3.9 Personnel Security	2	0 of 2	◑ Partial
3.10 Physical Protection	6	0 of 6	◑ Partial
3.13 System & Comm Protection	16	16 of 16	✓ Full
3.14 System Integrity	7	6 of 7	✓ Covered

> *NIST 800-171 Assessment: ZafePass directly addresses approximately 73 of 110 requirements (66%) through its technical architecture. The remaining requirements relate to organizational, personnel, and physical security domains that are complementary to – not in conflict with – the ZafePass platform.*

6.4 ISO/IEC 27001:2022

ISO 27001 is the international standard for Information Security Management Systems (ISMS), now aligned with Annex A controls drawn from ISO 27002:2022. It is the most globally recognized information security certification, with over 70,000 certificates issued worldwide. Zafehouze Solutions holds ISO 27001 certification.

ISO 27001 Annex A Domain	Key Controls	ZafePass Alignment
A.5 Organizational Controls	Policies, roles, threat intelligence, supplier relationships	✓ Covered
A.6 People Controls	Screening, training, remote working	◑ Partial
A.7 Physical Controls	Physical security perimeters, equipment	◑ Partial
A.8.2 Privileged Access Rights	Privileged access management	✓ Native
A.8.3 Information Access Restriction	Least privilege, need-to-know	✓ Native
A.8.5 Secure Authentication	MFA, secure log-on	✓ Native
A.8.6 Capacity Management	Resource monitoring	✓ Covered
A.8.12 Data Leakage Prevention	Prevent unauthorized data exfiltration	✓ Native
A.8.15 Logging	Event logging, log protection	✓ Native
A.8.20 Network Security	Network controls, segmentation	✓ Native
A.8.22 Segregation of Networks	Isolate sensitive environments	✓ Native
A.8.26 Application Security	Secure development, app access control	✓ Covered

> *ISO 27001 Assessment: ZafePass's architecture natively addresses the technical and network control domains of Annex A. Zafehouze itself is ISO 27001 certified, meaning the organizational management layer is also demonstrably in place.*

6.5 NIS2 Directive (EU Network and Information Security Directive 2)

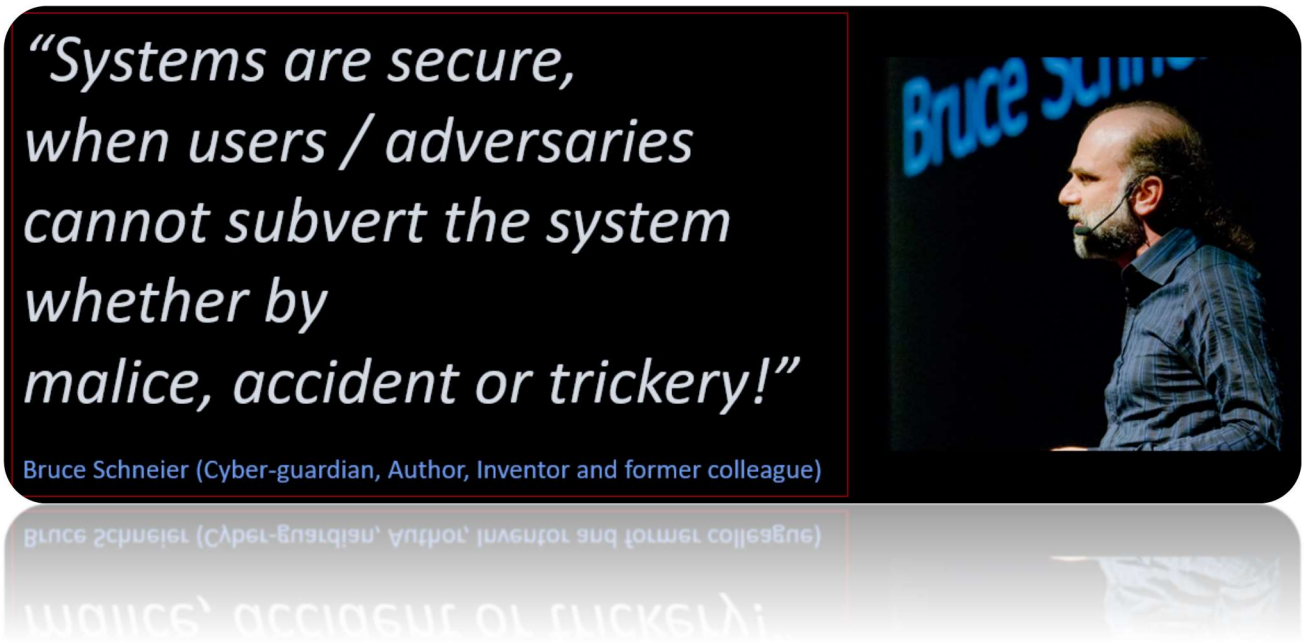
The NIS2 Directive (EU 2022/2555), effective from October 2024, significantly expands the scope and requirements of its predecessor. It applies to essential and important entities across 18 sectors, mandating risk management measures, incident reporting, supply chain security, and board-level accountability. Non-compliance carries fines up to €10 million or 2% of global turnover.

NIS2 Article / Requirement	Mandate Summary	ZafePass / Prevent-First Coverage
Art. 21 – Risk Management	Implement appropriate and proportionate technical measures	✓ Native — null state eliminates primary risk categories
Art. 21(2)(a) – Policies	Risk analysis and information system security policies	✓ Covered — policy engine codifies all access rules
Art. 21(2)(b) – Incident Handling	Incident prevention, detection, response, recovery	◑ Partial — prevention comprehensive; IR requires complement
Art. 21(2)(e) – Supply Chain	Security in supply chain and third-party relationships	✓ Native — same policy applies to partner/contractor access
Art. 21(2)(f) – Acquisition Security	Security in network/IS acquisition and development	✓ Covered — European-built, ISO 27001 certified, no backdoors
Art. 21(2)(g) – Vuln Disclosure	Policies for vulnerability handling and disclosure	✓ Covered — external validation; responsible disclosure policy
Art. 21(2)(h) – Cryptography	Use of cryptography and encryption	✓ Native — PGP/RSA/ECC; FIPS 140-2 inspired design; SSH2
Art. 21(2)(i) – HR Security	Human resources security, access control	✓ Full — multi-dimensional MFA; immediate access revocation
Art. 21(2)(j) – MFA	Multi-factor authentication requirement (explicit)	✓ Native — MFA policy engine core to ZafePass architecture
Art. 23 – Incident Reporting	72-hour reporting to national authority	◑ Partial — logging supports reporting; process is organizational

> *NIS2 Assessment: Prevent-First and ZafePass are exceptionally well-aligned with NIS2's risk management and access security mandates. Notably, NIS2 Article 21(2)(j) explicitly requires MFA – which ZafePass delivers as a core architectural feature, not an add-on. Supply chain security (Art. 21(2)(e)) is also natively addressed by extending the same access policy to partners and subcontractors.*

6.6 Additional Framework Alignment

Framework	Scope & Applicability	Alignment Level	Key Mapping
CIS Controls v8	18 controls, prioritized for SME to enterprise	✓ Full	Controls 1–7 (Asset, Vulnerability, Access, Logging) natively covered
GDPR (EU)	Data protection, privacy by design, breach notification	✓ Covered	No-exposure prevents data breaches; encrypted storage; no 3rd party keys
SOC 2 Type II	Security, Availability, Confidentiality trust criteria	✓ Covered	CC6 (Logical Access), CC7 (System Ops), CC9 (Risk Mitigation) addressed
IEC 62443 (OT/ICS)	Industrial control system security	✓ Covered	Zone-and-conduit model maps to Data Islands; OT assets protected without exposure
DORA (EU)	Digital operational resilience for financial sector	✓ Covered	ICT risk management, operational resilience, third-party risk all addressed
HIPAA Security Rule	US healthcare data protection	✓ Covered	Access controls, audit controls, transmission security all natively satisfied
PCI-DSS v4.0	Payment card industry data security	✓ Covered	Network segmentation, access control, logging requirements addressed
UK Cyber Essentials+	UK government baseline certification	✓ Full	Firewalls, access control, malware protection, patch management all satisfied



6. Business Case & Cost Efficiency

6.1 Total Cost of Cyber Risk Control

A central business argument for Prevent-First is economic as well as security-driven. Detection-centric architectures generate significant operational cost: SOC staffing, SIEM license and ingestion costs, incident response retainers, breach remediation, and regulatory penalties. These costs scale with threat volume – and threat volume is increasing.

Prevent-First economics work differently. By eliminating the attack surface, the number of detectable events drops dramatically. SIEM ingestion volumes shrink. SOC tier-1 noise is reduced. Breach-related remediation costs trend toward zero. Regulatory confidence is higher, reducing audit burden.

6.2 Quantified Risk Reduction

The Prevent-First framework projects a greater than 95% reduction in exposure, which directly correlates with breach probability reduction. ZafePass's twelve-year zero-breach operational record across a continuously probed environment provides empirical support for this projection.

6.3 Operational Efficiency

ZafePass is deployed as a 100% software platform – no hardware required. Deployment is achievable within a single day. The platform's automated gateway management and ACL synchronization significantly reduce the engineering overhead typically associated with VPN and network segmentation management. Customers report substantial reductions in support ticket volumes and engineering time.

6.4 Supply Chain Security Extension

One of the most compelling business benefits of Prevent-First is the ability to extend identical access policies to partners, contractors, and subcontractors – the supply chain – without requiring those parties to implement separate security infrastructure. This directly addresses the supply chain security requirements of NIS2, CMMC, and ISO 27001, which have become among the most difficult compliance obligations for organizations to satisfy.

7. Conclusions & Recommendations

7.1 Summary of Findings

This report has established the following findings:

- Conventional cybersecurity vendors – including those that market 'prevention-first' positioning – operate at the network layer and leave the attack surface intact. Their security models are fundamentally reactive, even when they include proactive threat intelligence or endpoint runtime protection.
- The Prevent-First Non-Exposure Security paradigm, as articulated by the European Prevent-First Alliance, represents a genuinely distinct security philosophy: eliminating exposure rather than defending against exploitation of exposure.

- ZafePass by Zafehouze Solutions is the leading commercial implementation of Prevent-First principles, with a technically validated architecture, a zero-breach twelve-year operational record, ISO 27001 certification, and Made-in-Europe sovereignty assurances.
- ZafePass natively and comprehensively addresses the intent of CMMC 2.0, NIST SP 800-53, NIST SP 800-171, ISO 27001, NIS2, and a broad range of additional global frameworks – often exceeding their requirements rather than merely satisfying them.
- The economic case for Prevent-First is compelling: lower CAPEX/OPEX, reduced SOC burden, near-zero breach-remediation-cost, and a demonstrably stronger regulatory compliance posture.

7.2 Recommendations

For Enterprise Security Teams

- Evaluate current architecture against the Prevent-First framework to identify residual exposure that Zero-Trust, SASE, or SDP implementations are leaving open.
- Conduct a ZafePass proof-of-concept deployment, which can be completed within a single day on a software-only basis with no disruption to existing infrastructure.
- Reassess SIEM and SOC investment strategy: Prevent-First architecture reduces the event volume that drives SIEM costs, enabling reallocation of budget to prevention.

For Compliance & Risk Officers

- Map current CMMC 2.0 or NIS2 gap analysis against ZafePass capabilities – the platform addresses the highest-risk technical control families directly.
- Use the Prevent-First framework as an evaluation lens for third-party and supply chain security assessments.
- Consider the reputational and regulatory risk differential between a 'detect-and-respond' posture and a 'no-exposure' posture when communicating cyber risk to boards and regulators.

For Boards & Executives

- Demand clarity from security teams on whether current investments reduce exposure or merely improve response time to exploitation of standing exposure.
- Recognize that Prevent-First Non-Exposure Security is now commercially available, practically deployable, and empirically validated – it is no longer a theoretical ideal.
- Factor supply chain security obligations under NIS2, DORA, and CMMC into vendor selection: only Prevent-First architectures extend identical protection to the supply chain without requiring partners to rebuild their own infrastructure.

> *The next practice in cybersecurity is not faster detection. It is no exposure. Prevent-First Non-Exposure Security – as implemented in ZafePass – makes the enterprise invisible, unreachable, and uncompromisable.*

9. Pioneers Before Their Time: The Intellectual Origins of Prevent-First

9.1 A Concept Twelve Years Ahead of the Industry

The cybersecurity industry attributes the formal articulation of Zero Trust to John Kindervag's Forrester Research paper published in 2010. The Jericho Forum's deperimeterization commandments preceded it by six years, in 2004. Both are rightly credited as intellectual milestones.

What is less widely known is that the core architectural principles now embodied in Prevent-First Non-Exposure Security were conceived, engineered, and filed as a United States patent in 2003 – seven years before Zero Trust entered the industry lexicon. The inventors were not researchers or analysts. They were practitioners who had spent decades building, breaking, and securing real enterprise networks, and who recognised the structural inadequacy of perimeter-based security long before it became a consensus view.

> *US Patent Application US20050262343A1, filed 2003 and published 2005, describes a pervasive, user-centric network security architecture built on dynamic datagram switching, on-demand authentication, and mobile intelligent data carriers. It is the direct intellectual ancestor of what is today called Prevent-First Non-Exposure Security.*

9.2 The Patent: US20050262343A1 – EMCADS

The patent, known internally as EMCADS (Encrypted Mobile Communications and Dynamic Switching), carries the full title: 'Pervasive, user-centric network security enabled by dynamic datagram switch and an on-demand authentication and encryption scheme through mobile intelligent data carriers.'

Published by the United States Patent and Trademark Office in 2005, the patent describes methods and systems for:

- Providing secure, stable network connections supported by an improved client-server architecture that moves decisively beyond static perimeter models
- A dynamic datagram switching schema enabling per-session, per-resource routing – the architectural precursor to what is now called ephemeral connectivity and null-state access
- Mobile intelligent data carriers enabling on-demand authentication and encryption – effectively the first patent-protected formulation of what became device-bound, context-aware, multi-dimensional MFA
- Targeted delivery of applications to authorised users only – controlling access not merely to data, but to the applications themselves, anticipating the resource-centric access model central to Prevent-First
- Biometric and multi-factor authentication methodologies integrated at the session layer – not the network layer – establishing the principle that trust must be established at the point of resource access, not the point of network entry

The patent's central insight – that security must be pervasive and user-centric rather than network-centric and perimeter-bound – is identical to the principle that Forrester's Kindervag would independently articulate seven years later as Zero Trust. The difference is that the Prevent-First founders had already engineered it, filed it, and received patent protection for it.

9.3 The Founders: Niels E. Anqvist & Jimi T. Jorgensen

Niels E. Anqvist and Jimi T. Jorgensen, Co-Founders of Zafehouze, are the inventor and patent-holders behind EMCADS. Niels' professional biography reads as a map of the security disciplines that converged to make Prevent-First possible:

- 40 years in information technology; 30 years in information and cybersecurity
- eMBA; Cert. SOC Architect; Cert. Security and Deep Packet Inspection systems specialist
- Cloud Security Alliance Chapter President
- Serial inventor: Ultra-RAID (1992), first Bluetooth applications (1998), EMCADS (2005)
- Enterprise experience spanning Intel, HP, IBM, Deloitte, Network Instruments, and Autonomy/Darktrace

The Ultra-RAID invention of 1992 preceded widespread RAID adoption in enterprise storage. The Bluetooth application work of 1998 predated Bluetooth's mass-market emergence by nearly a decade. The EMCADS patent of 2003–2005 predated Zero Trust by seven years. The pattern is consistent: Anqvist and the Prevent-First founders do not react to trends. They originate them.

9.4 What EMCADS Got Right That the Industry Took a Decade to Understand

A precise reading of the EMCADS patent against the subsequent evolution of the cybersecurity industry reveals that its core claims anticipated four major architectural shifts that the industry spent the following fifteen years slowly and incompletely working toward:

Dynamic datagram switching → ephemeral connectivity

The EMCADS patent's dynamic datagram switching schema – routing network sessions dynamically, per-request, rather than through standing connections – is architecturally identical to what is now marketed as ephemeral connectivity and just-in-time access. The industry arrived at this conclusion through Zero Trust, ZTNA, and SDP. The EMCADS patent had it in 2003.

Mobile intelligent data carriers → device-bound identity

The concept of mobile intelligent data carriers enabling on-demand authentication is the direct precursor to modern device-bound credentials, hardware security keys, and the concept that identity is inseparable from the device presenting it. Modern approaches to authentication and hardware-rooted trust trace the same intellectual lineage. EMCADS described this in 2003.

User-centric architecture → resource-level access control

The patent's 'pervasive, user-centric' framing directly challenges the network-centric orthodoxy of its era. Rather than asking 'which network should this user access?', EMCADS asked 'which resources should this specific user access, from this specific device, under these specific conditions?' This is the question that NIST SP 800-207 (the Zero Trust Architecture standard) formalised in 2020 – seventeen years after EMCADS was filed.

On-demand authentication and encryption → continuous validation

The 'on-demand' qualification in EMCADS is critical. Authentication and encryption are not performed once and then trusted. They are invoked at the point of demand – at the moment of access – and are tied to the specific session, the specific resource, and the specific user context. This is the architectural definition of 'always verify' as Kindervag would later describe it. EMCADS described it first.

9.5 From Patent to Platform: The ZafePass Lineage

The ZafePass platform is not merely inspired by the EMCADS patent. It is the direct commercial realisation of it, refined over twelve years of adversarial testing, platform development, and customer deployment. The journey from the 2003 filing to the current ZafePass architecture represents one of the longest-running, most consistent research and development trajectories in cybersecurity:

Year	Milestone	Industry context at the time
2003	EMCADS patent filed: dynamic datagram switching, on-demand authentication, user-centric resource access	Industry orthodoxy: firewall perimeters, VPN remote access, static network segmentation
2004	Jericho Forum publishes deperimeterization commandments — first mainstream challenge to perimeter thinking	First peer recognition that perimeters are dissolving; no commercial solution yet
2005	US20050262343A1 published by USPTO	Forrester, Gartner, and IDC still publishing reports on next-generation firewalls as the primary security evolution
2008	First Zafepass gateway prototypes deployed and adversarial testing begins	Zero Trust concept not yet coined; VPN remains the gold standard for remote access
2010	Forrester's Kindervag coins 'Zero Trust' — independently reaching the same architectural conclusions as EMCADS	Industry begins 15-year journey toward architectures EMCADS had already patented
2014	ZafePass platform enters active enterprise deployment	ZTNA, SDP, and SASE frameworks begin appearing in Gartner and Forrester research
2016	Platform survives sustained, professional adversarial testing over 10-month engagement with full source code access	Major enterprise VPN breaches begin accumulating (Juniper, Fortinet, Cisco)
2020	NIST publishes SP 800-207 Zero Trust Architecture — formalising what EMCADS described in 2003	US federal government mandates Zero Trust adoption following SolarWinds breach
2022	Zafehouze formalises Prevent-First framework with European Prevent-First Alliance	NIS2 Directive enacted; supply chain security and MFA become regulatory mandates
2024–2026	ZafePass deployed across critical infrastructure: defence, healthcare, energy, government	Industry consensus: Zero Trust is necessary but insufficient; exposure elimination becomes next frontier

European PREVENT-FIRST Alliance

9.6 Why Founding Pedigree Matters for Enterprise Procurement

In cybersecurity procurement, it is common to evaluate vendors on their current product capabilities, compliance certifications, and reference customers. Less commonly evaluated — but equally important — is the intellectual depth and time-horizon of the founding team's thinking.

Vendors who are implementing Zero Trust concepts today are implementing ideas that were mainstream by 2015 and patent-protected by 2005. They are iterating on an established paradigm. Zafehouze and the Prevent-First founders are not implementing Zero Trust. They invented it independently, before it had a name, and have spent twenty years stress-testing and refining the commercial implementation.

This matters because security architecture is not a product that is replaced on a three-year refresh cycle. It is infrastructure that organisations will live with for a decade. The question is not only whether a vendor can pass the CMMC or ISO 27001 audit today. It is whether their architectural thinking is two years ahead of the threat landscape, or twenty.

The EMCADS patent, the ZafePass platform's zero-breach twelve-year record, the independent validation with full source-code access, and the Prevent-First Alliance's framework articulation collectively establish that the founders of Zafehouze have been ahead of the threat landscape not by a product cycle, but by a generation.

> *The industry coined 'Zero Trust' in 2010. The Prevent-First founders patented it in 2003. The industry is still catching up to where they were twenty years ago – and ZafePass is already beyond that, implementing what the industry will be calling 'next practice' for the next decade.*

References & Further Reading

Prevent-First Alliance: https://prevent-first.eu

Zafehouze Solutions: https://zafehouze.com

ZafePass Platform: https://zafepass.com

Regulatory & Framework Sources:

- CMMC 2.0 Model Documentation – US DoD Office of the Under Secretary of Defense for Acquisition & Sustainment
- NIST SP 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-171 Rev. 2 – Protecting Controlled Unclassified Information in Nonfederal Systems
- NIST SP 800-207 - foundational cybersecurity guideline defining Zero Trust Architecture
- ISO/IEC 27001:2022 — Information Security Management Systems
- EU Directive 2022/2555 (NIS2) — Network and Information Security (2nd version)
- EU Regulation 2022/2554 (DORA) — Digital Operational Resilience Act
- IEC 62443 — Security for Industrial Automation and Control Systems
- PCI DSS v4.0 — Payment Card Industry Data Security Standard
- CIS Controls v8 — Center for Internet Security
- Jericho Forum — Commandments and Deperimeterization Principles (2004)