evolving NETWORKS™

WHITE PAPER

Redesigning SASE: evolving ZERO and the future of SAFE networking

evolving.net.uk

WHITE PAPER

Redesigning SASE: evolving ZERO and the future of SAFE networking

A Zero Surface Architecture for secure, adaptive connectivity

Executive Summary

The enterprise network is breaking. As organisations move to hybrid work, SaaS platforms, cloud-native development, and globally distributed teams, the legacy perimeter-based network model is no longer viable. VPNs, firewalls, SD-WANs, and access brokers create a patchwork of partial solutions – fragile, difficult to manage, and inadequate against modern threats.

evolving Networks has developed a different approach. **evolving ZERO** is a Zero Trust Network-as-a-Service (ZT-NaaS) that replaces implicit trust with policy-driven, identity-aware connectivity. It enables dynamic, encrypted, ephemeral access across people, applications, devices, and networks.

This white paper introduces the **Zero Surface Architecture** and the **SAFE** model that underpin **evolving ZERO,** explores its core principles, and describes how it supports a broad range of use cases – from site connectivity to developer security, SaaS access control, cloud workload segmentation, and beyond.

evolving ZERO is a Zero Trust Network-as-a-Service (ZT-NaaS) that replaces implicit trust with policy-driven, identity-aware connectivity.

The collapse of the perimeter

The traditional model – flat LANs protected by perimeter firewalls – was designed for a world where users, data, and applications were co-located. That world no longer exists. Today:

- Work happens everywhere: homes, airports, co-working spaces.
- Applications live in cloud providers, containers, and SaaS platforms.
- Third parties (partners, contractors, suppliers) require internal access.

Attempting to secure this environment with perimeter firewalls, VLANs, and VPNs introduces complexity and risk. VPNs extend the attack surface. Firewalls assume IP-based trust. SD-WAN overlays still rely on static tunnels and routing.

The result? A sprawling, expensive, and insecure system that struggles to support business agility.

What is Network-as-a-Service (NaaS)?

Network-as-a-Service (NaaS) is a new operational model for delivering network capabilities as a flexible, on-demand service. Rather than depending on hardware-based infrastructure and static configurations, NaaS platforms deliver dynamic, policy-driven connectivity that adapts in real time to changes in users, workloads, and topology.

NaaS abstracts routing, firewalling, encryption, segmentation, and access control into software-defined layers. It provides:

- Centralised orchestration with decentralised enforcement
- Built-in resilience through traffic aggregation and path redundancy
- Seamless integration with identity providers, observability stacks, and automation pipelines
- Integrated security directly in the transport layer
- Global scaling without managing hardware

evolving ZERO operates as a Zero Trust NaaS – fusing the NaaS delivery model with zero-trust principles, so that every connection is verified, encrypted, and ephemeral by design.

Zero-trust: principle vs practice

Network-as-a-Service (NaaS) is the modern approach to delivering network functions as cloud-native services. Rather than building and managing a complex stack of routers, firewalls, VPN concentrators, and monitoring systems, organisations consume connectivity as a service – on demand, policy-driven, and integrated with the rest of their infrastructure.

NaaS abstracts the physical and logical complexity of network design into a platform model.

evolving ZERO extends this concept by integrating zero-trust principles directly into the NaaS layer. Every connection is governed by identity, posture, and policy. No static configurations, no exposed surface, and no trusted core.

Zero-trust is often misunderstood.
It's not a product. It's a principle:

Never trust. Always verify. Enforce least privilege.

In practice, many vendors add zero-trust features to traditional products. The underlying architecture remains unchanged – trusted networks, static tunnels, manual firewall rules.

To fully realise zero-trust, we need a network model where trust is never assumed and where the **network itself is invisible unless permitted.**

This is the foundation of **evolving ZERO.**

What is evolving ZERO?

evolving ZERO is a new category: **Zero Trust Network-as-a-Service (ZT-NaaS).** It abstracts and unifies connectivity, encryption, access control, and observability under one platform.

Key characteristics:

- **Zero surface:** No exposed IPs, no open ports, no passive surface to scan or exploit.
- **Identity-based access:** Every connection is explicitly authorised based on user, device, role, and context.
- **Dynamic overlays:** Tunnels are ephemeral and policy-driven, not static or permanent.
- **Composable architecture:** Each component (policy engine, fabric, edge node) is modular.

It allows any identity – person, device, service – to connect securely to any permitted resource, without exposing anything else.

The SAFE model

The **evolving ZERO** platform is delivered as a **Secure Access Fabric for Everything (SAFE).** SAFE is more than branding – it defines how the platform works. Each letter corresponds to a foundational architectural layer:

Stack: Centralised policy and orchestration

Access: Identity-aware zero-trust access

Fabric: Encrypted, intelligent transport with dynamic failover

Edge: Enforcement points via EVX appliances or agents

SAFE is how the Zero Surface Architecture is enforced across users, applications, clouds, and devices.

Core Components

A key strength of **evolving ZERO** is its built-in aggregation and redundancy at every layer. Whether it's edge connectivity or backbone routing, the platform is designed for resilience and continuous availability. All major components support multi-path uplinks, active-active failover, and load-aware tunnel orchestration. This ensures that the system not only enforces zero-trust principles but also delivers high-performance, fault-tolerant connectivity as expected of any modern NaaS.

EVX

A zero-trust access appliance. Handles local policy enforcement, tunnel creation, and integration with routing (BGP/OSPF). Deployed at sites or in virtual form.

Controller

Central policy engine. Defines who/what can access what, under which conditions.

Authoriser

Real-time policy evaluation service. Verifies connection attempts and signs tokens for ephemeral tunnels.

Network Fabric Routers (NFR)

Distributed backbone routers that form the resilient core of the **evolving ZERO** fabric. Each NFR node supports redundant paths and traffic aggregation, ensuring packets can be routed based on health, latency, and load. This enhances fault tolerance and eliminates single points of failure in the service backbone.

Fabric overlay

The encrypted fabric dynamically stitches together authorised endpoints. Tunnels are formed using WireGuard, QUIC, or IPsec based on policy and network context. The fabric supports aggregated flows across multiple links, balancing traffic in real time and shifting between paths in the event of degradation. This makes the overlay not just secure, but adaptive and self-healing.

Zero Surface Architecture

This architectural stance eliminates exposure by default:

- There is no default network. Tunnels only form when policy permits.
- Nothing listens on public IPs. All communication is outbound and policy-authenticated.
- There is no lateral movement. Segmentation is built-in at the overlay level.

It turns the network from a trusted transport into a zero-visibility fabric where only approved connections are possible.

SAFE makes this model operational, tying access policy, transport, and observability into one cohesive system.

Benefits:

A defining strength of the Zero Surface Architecture is the elimination of passive exposure. Because nothing is reachable by default, attackers are deprived of the typical surface area they rely on – no open ports, no idle services, no exposed IP ranges to scan. This significantly reduces the opportunities for reconnaissance or exploitation.

Each connection is microsegmented by design, bound to the identity and intent of the communicating entities. Whether it's a device reaching out to an application or a workload accessing a backend service, the tunnel formed is unique, temporary, and scoped only to that connection. This segmentation is not a separate layer – it's part of the fabric.

Use cases

In every use case, **evolving ZERO's** aggregation and redundancy features underpin its ability to deliver uninterrupted service. Whether you're operating across multiple WAN links, connecting remote branches, or securing cloud-native applications, the platform automatically distributes and re-routes traffic to maintain optimal performance and availability.

A Branch connectivity without borders

- Replace MPLS or SD-WAN with encrypted overlays
- Dynamic failover across multiple uplinks
- BGP integration for seamless routing

B Universal access to internal tools

- No VPN or bastion required
- Access granted based on user + device posture
- Granular, scoped permissions per tool or environment
- Shortest path taken to apps without bandwidth hairpinning

D Third-party / partner access

- Provide contractors or suppliers scoped access
- Just-in-time, just-enough permissions
- Fully auditable and revocable

How It Works

1. **Authentication:** Identity is verified (via SSO, certificates, device posture, etc.)
2. **Authorisation:** Controller checks policy for the requested connection
3. **Connection:** Tunnel is formed between source and destination
4. **Observation:** Metadata is streamed to observability tools (SIEM, metrics, etc.)

Every connection within the **evolving ZERO** fabric is treated as a unique, fully isolated event. When a request to connect is made, it triggers a fresh policy evaluation – drawing on current identity, device posture, and contextual factors – to determine whether access should be granted. If approved, an encrypted tunnel is established specifically for that session, connecting only the necessary endpoints. This flow-specific model ensures high granularity, strong containment, and minimum exposure for every interaction.

Comparisons

Legacy Network	evolving ZERO
VPNs	Context aware, policy-driven tunnels
Static firewalls	Identity + posture-based policies
SD-WAN overlays	Dynamic encrypted overlays
Bastion hosts	Zero Surface access + ZTNA
Complex routing	Declarative control + BGP integration

Implementation

Many organisations begin their journey with **evolving ZERO** by solving a focused pain point. For example, a branch office suffering from flaky VPN access might deploy a single EVX node, replacing multiple static site-to-site tunnels with dynamic encrypted overlays. This change alone improves resilience and dramatically reduces the attack surface.

Another common entry point is internal application access. Instead of provisioning new VPN credentials for each dev or managing firewalls for segmented environments, teams use **evolving ZERO** to define access policies for a single app. A developer's device is authenticated and evaluated for compliance, and only then is a temporary tunnel granted for just that resource – nothing more.

Some organisations start by eliminating legacy VPNs altogether for specific user groups. A dev team, for instance, might go VPN-free overnight, using posture-aware, identity-driven access that eliminates the friction of logins, split tunneling, and manual routing while boosting security.

Each of these approaches delivers value independently, while also laying the foundation for a fully composable Zero Surface architecture.

Or go full-fabric

Organisations ready to fully embrace Zero Trust can deploy **evolving ZERO** across their entire infrastructure. With native support for uplink aggregation and multi-path routing, the platform ensures that enterprise traffic always follows the most resilient and efficient path – adapting dynamically to link failures, congestion, or provider outages. This is essential not only for security, but for **operational continuity at scale.** This means replacing traditional SD-WAN solutions with intelligent, encrypted overlays that adapt dynamically to network conditions and routing policies.

evolving ZERO ensures that access to services is based on identity, role, posture, and time – enforced in real time, logged for audit, and revocable on demand. This delivers a consistent security posture, whether users are on-premises, remote, or working across multiple clouds and partner networks.

A full-fabric deployment turns **evolving ZERO** from a tactical enhancement into a strategic operating model – one where connectivity and security are no longer separate concerns, but co-designed from the start.

- Delivered as a service with full lifecycle support
- Integrates with existing Identity Providers (IdP)
- Compatible with Mobile Device Management (MDM) solutions
- Works alongside your current infrastructure and observability stack

Strategic Fit

evolving ZERO supports a comprehensive, modern security posture by embedding security into the fabric of connectivity itself. By default, it prevents exposure, isolates flows, and enforces strict access boundaries – all without relying on traditional perimeter defences or layered appliances. Its built-in capabilities enable organisations to enforce fine-grained segmentation, ensure consistent access controls, and monitor access patterns continuously across distributed environments.

More than just a product, **evolving ZERO** represents an operational shift. It aligns networking and security with business intent, enabling teams to replace reactive defences with proactive, embedded protections that scale with modern infrastructure.

Conclusion

evolving ZERO turns networking inside out:

- Nothing is reachable unless permitted
- All access is encrypted, ephemeral, and observable
- The surface disappears unless explicitly allowed

evolving ZERO embodies the principles of zero-trust without compromise. It challenges the assumptions of legacy network design and replaces them with an architecture built for modern security demands – dynamic, contextual, and invisible by default.

By converging connectivity and access control into a single, unified framework, it eliminates unnecessary exposure, enforces policy at every touch point, and empowers organisations to operate securely without friction. This is more than a technology shift; it's a strategic realignment of how we build, manage, and trust the networks of tomorrow. This is connectivity, redesigned from the ground up.

Next Steps

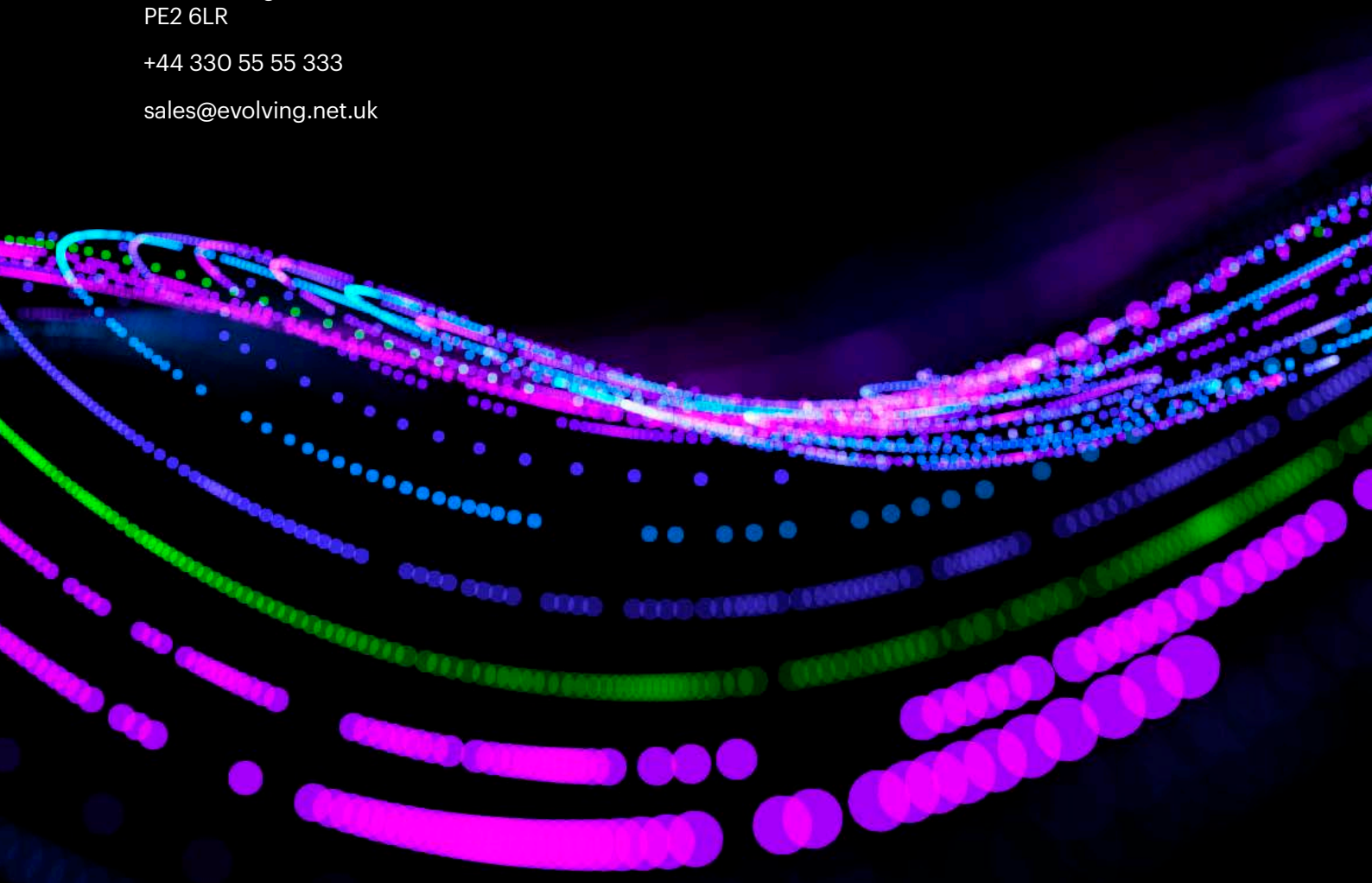
- Contact us for a demo
- Read the platform deep dive white paper
- Start a pilot project
- Replace VPNs or firewalls with EVX nodes

Zero-trust by design. SAFE by architecture

Evolving Networks
Nexus House
7 Commerce Road
Lynch Wood
Peterborough
PE2 6LR

+44 330 55 55 333

sales@evolving.net.uk



evolving.net.uk