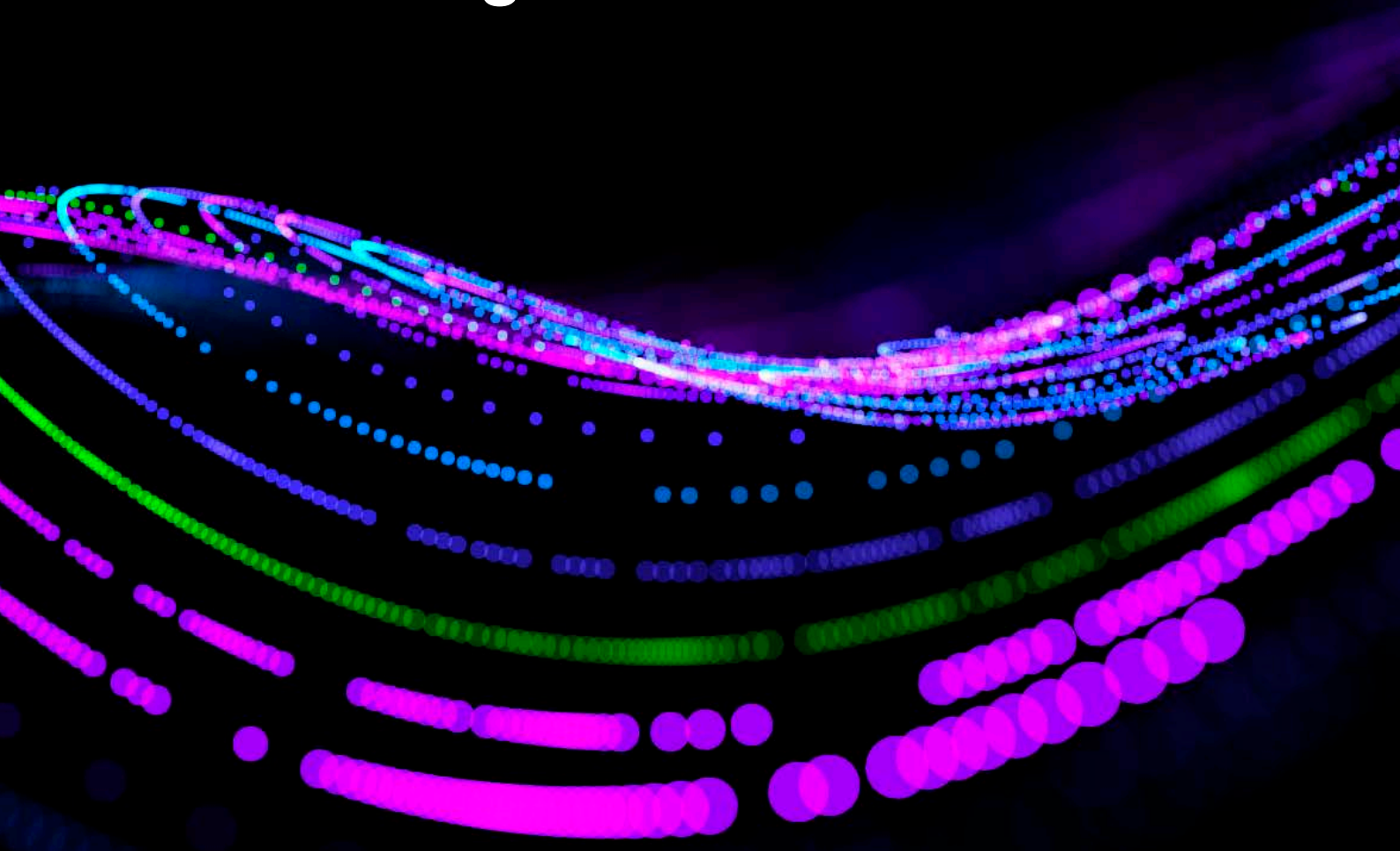
evolving NETWORKS™

WHITE PAPER

The evolving ZERO Platform



evolving.net.uk

Zero Trust starts at the LAN

WHITE PAPER

Secure Access Fabric for Everything (SAFE)

evolving ZERO™

Executive Summary

evolving ZERO is not just a network abstraction or zero-trust wrapper – it's a full-service platform for delivering integrated, policy-driven connectivity and security at scale. It merges traditionally siloed capabilities – ZTNA, Secure Web Gateway, CASB, next-gen firewalling, and advanced network optimisation – into a single composable service fabric.

This paper explains how **evolving ZERO** delivers what we call the **Secure Access Fabric for Everything (SAFE):**

- A platform architecture based on zero-trust enforcement, not perimeter assumptions
- A network fabric capable of encrypted, intelligent, multi-cloud connectivity
- A modular, open source system ready for "bring your own" extensibility
- An edge-to-cloud delivery system for secure access to apps and services – regardless of location

This is not theoretical zero-trust. This is operational infrastructure. And it's already live.

Introducing SAFE: Secure Access Fabric for Everything

SAFE is our model for a unified security and connectivity platform that works end-to-end.

SAFE stands for Secure Access Fabric for Everything, and also reflects the four layers of the platform architecture:

- **S – Stack:** Unified orchestration and policy
- **A – Access:** Identity-based Zero Trust access
- **F – Fabric:** Encrypted, intelligent routing layer
- **E – Edge:** Policy-enforcing connection points

It's both the name of the model and the structure of the platform.

ZERO stack	ZERO access	ZERO fabric	ZERO edge
• FWaaS	• ZTNA	• Encrypted Mesh	• EVX
• ACS	• Internet Access	• ZTNA	• Routing
• Monitoring	• Guest Gateway	• ZTNA Gateway	• Segmentation

A Trust-Defined Network

SAFE rewrites the relationship between the user, the device, and the network. In place of subnets and VLANs, it defines identity. Instead of forwarding rules or allow-lists, it enforces declarative policies. Instead of trusting the link or the provider, it encrypts and authenticates every flow by default.

This shift reclaims sovereignty. No implicit paths. No blind spots. No dependent brokers. SAFE treats the network as hostile – even the one you own – and makes it safe by design.

Modular, composable, distributed

One of the critical differentiators of SAFE is that it can be adopted incrementally. Start with access. Add edge. Extend the fabric. Integrate orchestration. SAFE does not require rip-and-replace or lift-and-shift. It can coexist, overlap, augment, and then eventually replace.

This composability gives customers agency. Each deployment reinforces policy coherence and zero-trust posture without forcing full migration from day one.

SAFE reflects the core values of **evolving ZERO:**

- Decentralised enforcement instead of centralised inspection
- Policy-as-intent, not configuration sprawl
- Identity as the new perimeter, not IP or subnet
- Traffic that is inert unless trust is proven

This is not consolidation. It's a return to principles. SAFE is zero-trust delivered as operational infrastructure.

Integrated capabilities

evolving ZERO offers a wide range of integrated security and networking capabilities, grouped across the four SAFE quadrants – Stack, Access, Fabric, and Edge. Each function represents a rethinking of how that service should operate in a zero-trust architecture: decentralised, policy-driven, identity-bound, and encrypted by default.

ZERO stack

- Evolving FWaaS
- Evolving NGFW
- Evolving DDoS Protection
- Evolving Secure Web Gateway
- Evolving CASB
- Evolving Monitoring + Analytics
- Evolving Identity Management

ZERO access

- Evolving Secure SWAN
- Evolving ZERO SWAN
- Evolving Internet
- Evolving Zero Trust Internet Access
- Evolving CaaS
- Evolving ZTNA
- Evolving Zero Trust Guest Gateway
- Evolving ZERO Cloud

ZERO fabric

- Evolving Secure Access Fabric
- Evolving Cloud VPN Connect
- Evolving Cloud Interconnect
- Evolving Cloud Direct
- Evolving Remote Access VPN

ZERO edge

- Evolving SWAN Edge
- Evolving ZERO Endpoint
- Evolving Network Segmentation
- Evolving Zero Trust Segmentation
- Evolving Advanced Routing
- Evolving Zero Trust Firewall
- Evolving ZTNA Gateway

STACK

The Stack layer powers the policy, orchestration, and analytics core of **evolving ZERO.** It consolidates legacy firewalling, monitoring, and access control services into a dynamic zero-trust enforcement layer.

- **Evolving FWaaS:** Delivers stateful and application-layer firewalling as a distributed service – policy-bound, identity-aware, and managed declaratively.
- **Evolving NGFW:** Replaces box-bound firewall appliances with context-driven rules embedded into EVX and platform.
- **Evolving DDoS Protection:** Prevents volumetric attacks at ingress through programmable thresholds and routing diversions.
- **Evolving Secure Web Gateway:** Provides inline, identity-aware web filtering and SaaS inspection without hairpinning to cloud brokers.
- **Evolving CASB:** Enforces conditional access to SaaS applications, monitors user behaviour, and prevents data leakage across trusted platforms.
- **Evolving Monitoring + Analytics:** Graphical flow telemetry in real time.
- **Evolving Identity Management:** Integrates with your IdP to deliver policy context, user tagging, MFA triggers, and session binding.

Together, these form a programmable, observability-rich control and security system that replaces the complexity and sprawl of traditional monolithic SASE stacks.

ACCESS

Access is where identity meets policy. It governs how people and workloads connect to the services they need – with Zero Trust rules and no assumptions.

- **Evolving Secure SDWAN:** Bandwidth aggregation, site to site access, and resilience features.
- **Evolving ZERO SDWAN:** Our signature overlay system for encrypted, dynamic, zero-surface connectivity.
- **Evolving Internet:** Resilient, high bandwidth, bi-directional QoS, internet capability.
- **Evolving Zero Trust Internet Access:** Secures and filters outbound web access through platform enforcement.
- **Evolving CaaS:** "Connectivity as a Service" – a fully managed multi-carrier network underlay service.
- **Evolving ZTNA:** Replaces VPNs with session-specific tunnels between authorised identities and resources.
- **Evolving Zero Trust Guest Gateway:** Provides guest Wi-Fi networks with secure internet access with no exposure of internal corporate networks.
- **Evolving ZERO Cloud:** Enables direct, secure, identity-verified access to public and private cloud applications without routing dependency on perimeter controls.

This quadrant makes zero-trust usable and flexible across workforce, third-party, and workload-to-service scenarios.

FABRIC

The Fabric quadrant handles encrypted routing between entities.

- **Evolving Secure Access Fabric:** A dynamic mesh of encrypted, policy-bound overlay tunnels that adapt to link and path performance.
- **Evolving Cloud VPN Connect:** IPsec or Wireguard internet overlays to your cloud tenancy.
- **Evolving Cloud Interconnect:** .Traditional dedicated interconnects such as ExpressRoute direct from the evolving ZERO platform.
- **Evolving Cloud Direct:** Physicall connect your private cloud or datacentre racks with NNIs into evolving ZERO.
- **Evolving Remote Access VPN:** Legacy-compatible, VPN tunnelling while you carefully move network segments to ZTNA.

The Fabric layer ensures that all transport is secure, policy-aware, and invisible unless permitted.

EDGE

The Edge quadrant brings enforcement physically closer to traffic origination and exit. It replaces the perimeter firewall with something faster, smarter, and truly secure.

- **Evolving SDWAN Edge:** Physical or virtual enforcement node that connects to multiple uplinks, routes based on policy, and forms part of the encrypted fabric.
- **Evolving ZERO Endpoint:** Full ZERO SDWAN enforcement point.
- **Evolving Network Segmentation:** Provides traffic isolation and segmentation with VLANs and VRFs.
- **Evolving Zero Trust Segmentation:** Single device subnets and zero east-west traffic to squash the attack surface.
- **Evolving Advanced Routing:** Full BGP/OSPF integration with path selection, failover, and load balancing.
- **Evolving Zero Trust Firewall:** Deny-all, segmentation aware, encrypted flows as default.
- **Evolving ZTNA Gateway:** Inline, distributed tunnel broker that validates identity and policy before any session is created.

The Edge quadrant is where the SAFE model becomes reality – every packet, every route, every session is earned, not assumed.

Deployment models

evolving ZERO offers multiple deployment models to suit the needs of organisations at different stages of network modernisation, cloud adoption, or zero-trust maturity. Each model supports incremental rollout or full-platform adoption, with consistent policy enforcement and observability.

EVX Edge

This is a hardware or virtual appliance deployed at physical sites (branches, data centres, retail locations) or in cloud edge environments. The EVX enforces the entire SAFE stack at the point of ingress and egress – handling routing, authentication, segmentation, encryption, and tunnel orchestration. It integrates with local BGP or OSPF, supports active-active uplinks, and provides deep visibility into all flows.

Secure client

Designed for end user devices, this lightweight identity-bound client enables dynamic, ephemeral tunnels directly to authorised destinations based on the user, device posture, and policy. It's commonly used to secure user-to-cloud traffic, developer environments, or remote users connecting to private resources.

Full Fabric-as-a-Service

In this model, Evolving delivers the entire SAFE platform as a managed overlay – spanning cloud interconnects, edge enforcement, traffic inspection, and observability. It's the fastest path to zero-trust adoption with minimal operational overhead. Ideal for distributed organisations or service providers looking to integrate secure access into their core offering.

Each deployment model is composable. Organisations can combine them or switch between them based on use case, lifecycle phase, or topology – without changing the policy model or connectivity logic.

Summary

evolving ZERO is the operational system for zero-trust and network security convergence. It replaces static infrastructure, fragmented products, and bolt-on tools with an integrated platform that is:

- Identity-aware
- Application-centric
- Cloud-native
- Secure by default
- Composable by design

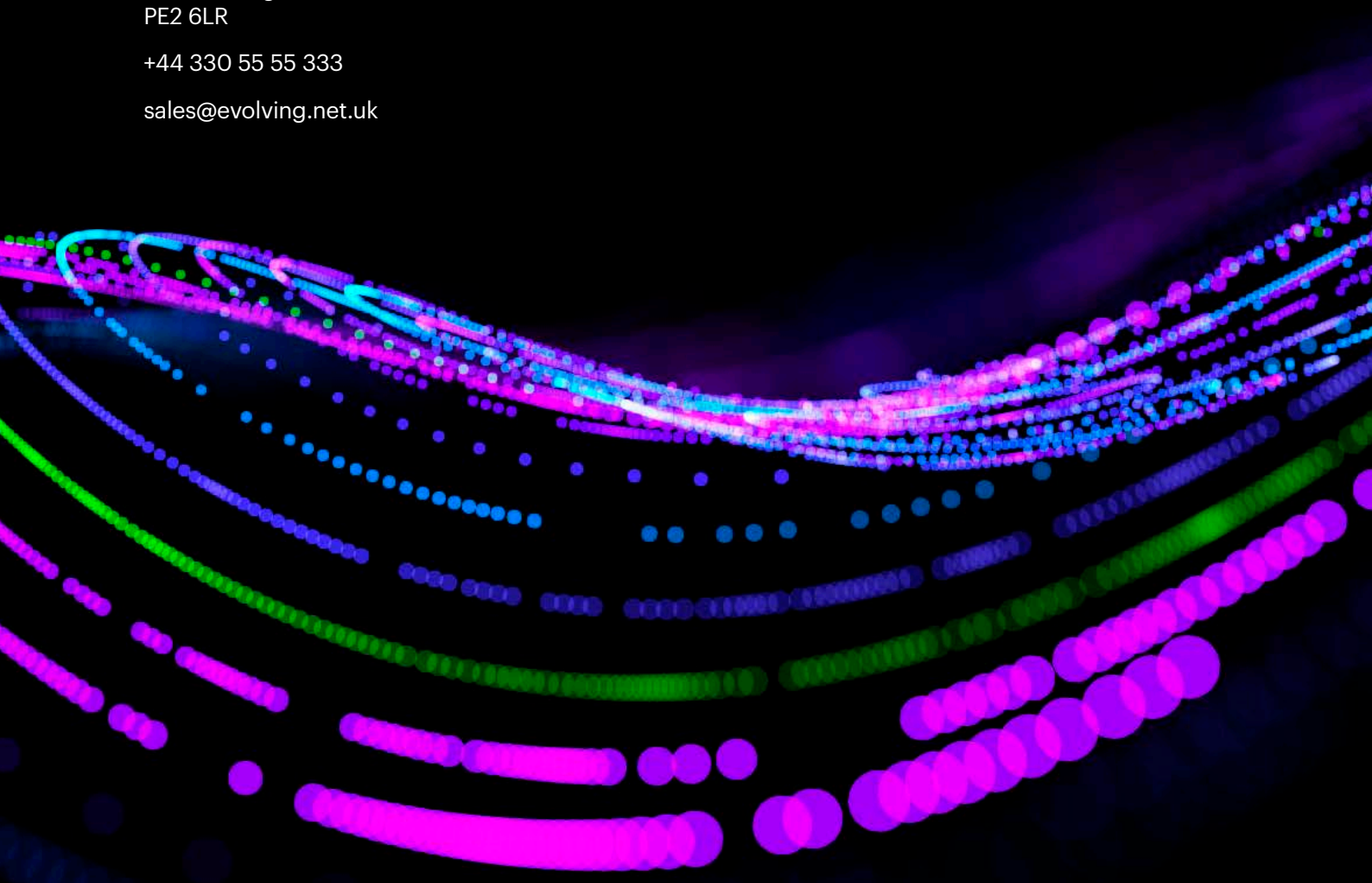
The SAFE model is more than a taxonomy. It's the next logical architecture.

Make Zero the default. Make SAFE the standard.

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

+44 330 55 55 333

sales@evolving.net.uk



evolving.net.uk