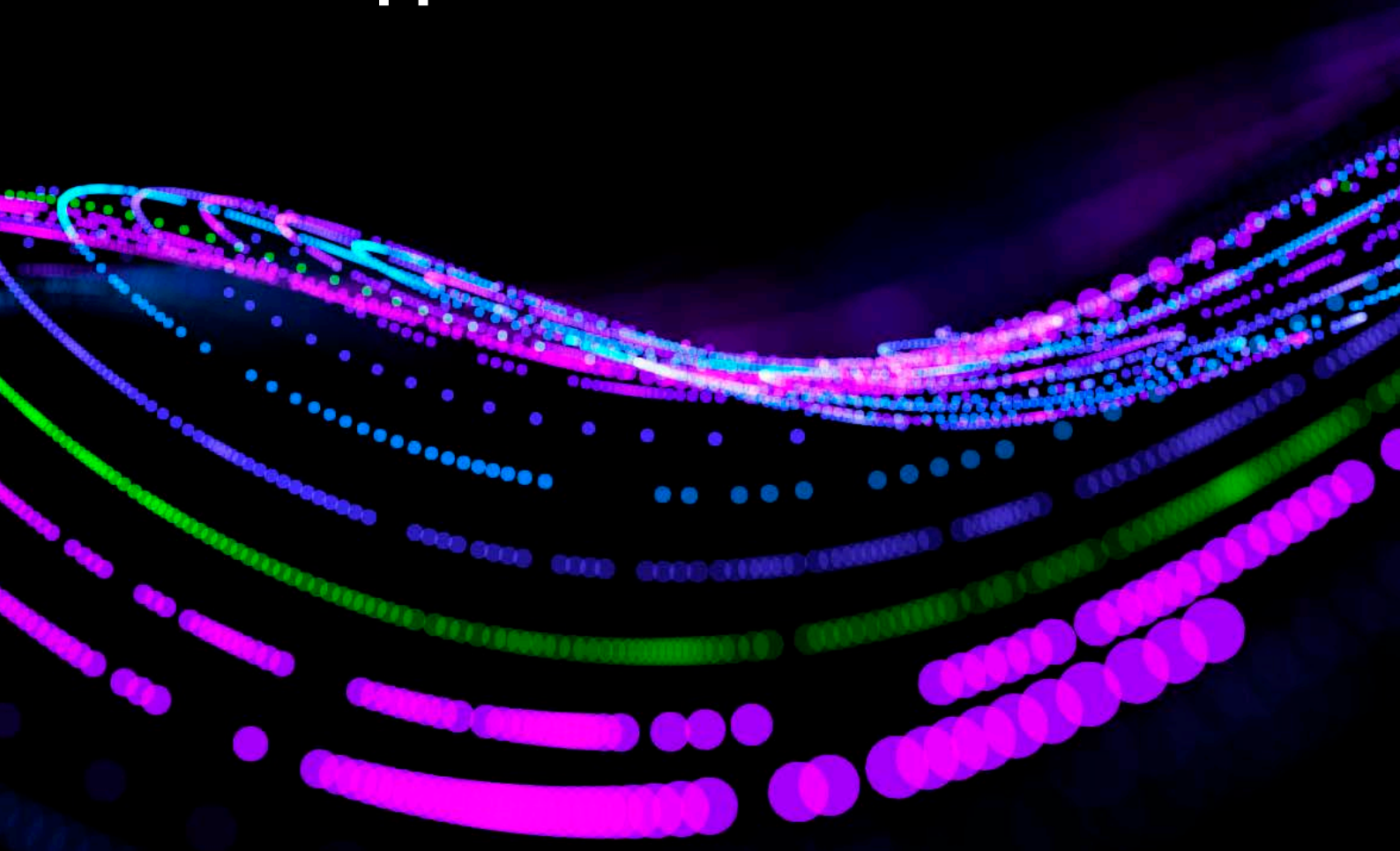
evolving NETWORKS™

WHITE PAPER

A new approach to Zero Trust



evolving.net.uk

A new approach to Zero Trust

Evolving beyond SASE: why SD-WAN needs a zero approach

Executive Summary

Zero Trust has become the security mantra of the decade, but the industry's response has been to centralise, layer, and bolt-on. The result is a bloated stack that misinterprets the intent of Zero Trust and overloads modern networks with unnecessary inspection and complexity.

At Evolving Networks, we believe in a ground-up redesign. Not more layers. Not more boxes. A new baseline.

Our vision – **evolving ZERO SD-WAN** – rebuilds the network around the idea that no route, flow, or connection should exist unless explicitly permitted by identity, posture, and policy. This is a platform-native interpretation of Zero Trust. It starts not at the perimeter, but at the packet.

This paper outlines why Secure Access Service Edge (SASE), while a step in the right direction, doesn't go far enough. It explains why a **Zero Surface Architecture** – a foundational shift in network design – is the only viable basis for Zero Trust in a world where cloud, mobility, and decentralisation are the norm.

The failure of SASE to deliver on Zero Trust

SASE was supposed to simplify. Instead, it centralised. It brought the stack to the cloud, but it didn't unpick the assumptions behind it. SASE vendors advertise Zero Trust, but in practice, they route all traffic to cloud enforcement points, apply traditional inspection methods (DPI, CASB, proxies), and reintroduce the very perimeter models Zero Trust aimed to eliminate.

Problems with current SASE-based Zero Trust:

- **Centralisation of Control & Inspection**
- **Stack Bloat with Full Inspection**
- **Dislocated Policy Enforcement**

Crucially, while SASE eventually incorporated **ZTNA,** nothing fundamentally changed in the firewalling layer. The firewall remained a static perimeter construct, enriched with cloud analytics perhaps, but still operating on the same assumptions: trust the internal, inspect the edge, control the outside.

Zero Trust became a bolt-on.

ZTNA vendors often criticise traditional firewalls – rightly pointing out that they assume trust based on IP and location. But ironically, many ZTNA solutions still sit on top of those very same firewalls, consuming network access policies that haven't evolved. They shift access control to the identity layer but leave the network architecture untouched.

This approach doesn't fix the model. It just masks it.

Zero Trust is not ZTNA (and it's not SASE either)

Zero Trust was never meant to be a bolt-on.

The original model, defined in 2010 by John Kindervag at Forrester Research, was a direct critique of how firewalls and network trust were being misapplied:

> "All interfaces should have the same trust and it should be zero. And that's really where Zero Trust comes from. It's a pushback against how we were building firewalls."

Kindervag's Zero Trust model was built around one premise: **eliminate implicit trust.** All traffic should be inspected, logged, and verified, regardless of its origin.

Over time, this intent was diluted. Zero Trust became a feature list, dominated by identity brokering and ZTNA. When Gartner first introduced the SASE framework in 2019, ZTNA wasn't even included – it was added later as remote work pushed demand.

The market absorbed Zero Trust as a compliance checkbox, delivered by gluing ZTNA onto an unchanged underlay. The outcome: networks that still route based on static rules, and overlays that assume encryption equals security.

But Zero Trust is not a product. It's a **philosophy of design.**

The problem with SASE-centric Zero Trust

SASE promised convergence – merging networking and security – but instead delivered consolidation: boxed products stacked in the cloud. It's created a generation of complex, opaque, and centralised architectures that are the opposite of what Zero Trust intended.

Key issues:

- **Over Centralisation:** Enforcing trust decisions through a central choke point introduces latency and dependency on cloud PoPs.
- **Stack Bloat:** Heavy reliance on full-payload inspection, DPI, CASB and proxies that often recreate legacy perimeter patterns.
- **Increased Latency:** Cloud-first doesn't mean context-first. Trust decisions often happen far from where the user or device is, taking the traffic with them on the journey.

The result: most SASE deployments simulate Zero Trust on top of a traditional wide-area network. They don't replace it.

Back to first principles: what Zero Trust was always meant to be

The Zero Trust model was never about proxies, brokers, or cloud firewalls. It was about a mindset:

- **No implicit trust.**
- **Always verify.**
- **Trust no network, even your own.**

Evolving Networks has reinterpreted this for the SD-WAN era:

- No pre-assumed routes unless identity and posture justify it.
- No reliance on firewalls as a control plane.
- No belief that private infrastructure is inherently safe – even dedicated private ExpressRoute connections.

Instead, we introduce:

- **Inline ZTNA Gateways** embedded into EVX appliances.
- **Distributed Policy Enforcement,** not cloud choke points.
- **Contextual Visibility** through nDPI and flow telemetry.

And above all:

Encryption By Default: Trust No Underlay

Even in private leased lines or MPLS networks, our platform assumes no trust. The ISP is not trusted. The carrier is not trusted. The backbone is not trusted.

Every flow across our SD-WAN fabric is encrypted and authenticated, regardless of cost, path, or provider. This is not paranoia. It's Zero Trust applied to the WAN.

What is evolving ZERO SDWAN?

ZERO SDWAN is the Evolving Networks implementation of secure, policy-driven WAN architecture, rebuilt for the Zero Trust era.

It combines our SD-WAN fabric with identity-aware, posture-enforced session control, and ephemeral pathing. It retains the performance benefits of bandwidth aggregation, traffic shaping, and QoS – but within a model where no traffic flows unless explicitly authorised.

Key capabilities of ZERO SDWAN:

- **Default is zero**
  The Zero Surface Architecture – zero traffic flow without policy, identity or authorisation.
- **Inline ZTNA Gateways**
  Each EVX appliance enforces Zero Trust Access at the edge. No need to hairpin to cloud brokers or sacrifice performance or bandwidth.
- **Distributed policy enforcement**
  Policies are decentralised and enforced at the point of ingress, reducing round trips and cloud reliance.
- **Context-aware telemetry**
  We use nDPI to capture real-time metadata and flow classification – not full-payload inspection – allowing lightweight, high-fidelity visibility and adaptive policy response.
- **Encrypted by default**
  Whether site-to-site, cloud-to-user, or edge-to-datacentre, all flows are encrypted and authenticated.
- **Device-level segmentation**
  No lateral flow, not just between sites on the WAN, but between devices on the LAN.

The Zero Surface Architecture

Our architecture eliminates unnecessary exposure. There are:

- No routable IPs unless authorised
- No discoverable services unless explicitly permitted
- No implicit internal network zones

In short: **No Surface To Attack.**

Zero Surface means:

- You cannot scan the network
- You cannot route unless authorised
- You cannot see what you don't earn the right to see

This is the architectural embodiment of Zero Trust.

Why the market needs this

The market is moving. Cloud-native apps. Remote-first teams. Hybrid access models.

Yet most WAN solutions are still rooted in assumptions from the MPLS era. Even newer offerings that brand themselves as SASE or ZTNA often build on these assumptions – just relocating them into the cloud.

Customers are facing:

- Unmanageable network complexity as hybrid becomes the norm.
- Fragmented trust enforcement between cloud, edge, and branch.
- Poor visibility and control over east-west and outbound traffic.
- Legacy networks that assume trust by IP, subnet, or VLAN.

What customers need:

- A network that has no assumptions.
- Access that is granted based on who, what, and why – not where.
- Routing that is conditional, encrypted, and minimal.
- A platform that simplifies rather than expands the attack surface.

This is the problem evolving ZERO SD-WAN solves.

Conclusion: the future of networking is the past, done properly

Zero Trust is not a new idea. It's a long-standing principle that was overlooked, diluted, and then re-marketed as a set of loosely integrated tools.

The path forward isn't about adding more layers or consolidating outdated models. It's about returning to what John Kindervag originally outlined: eliminate implicit trust, enforce everything, inspect continuously.

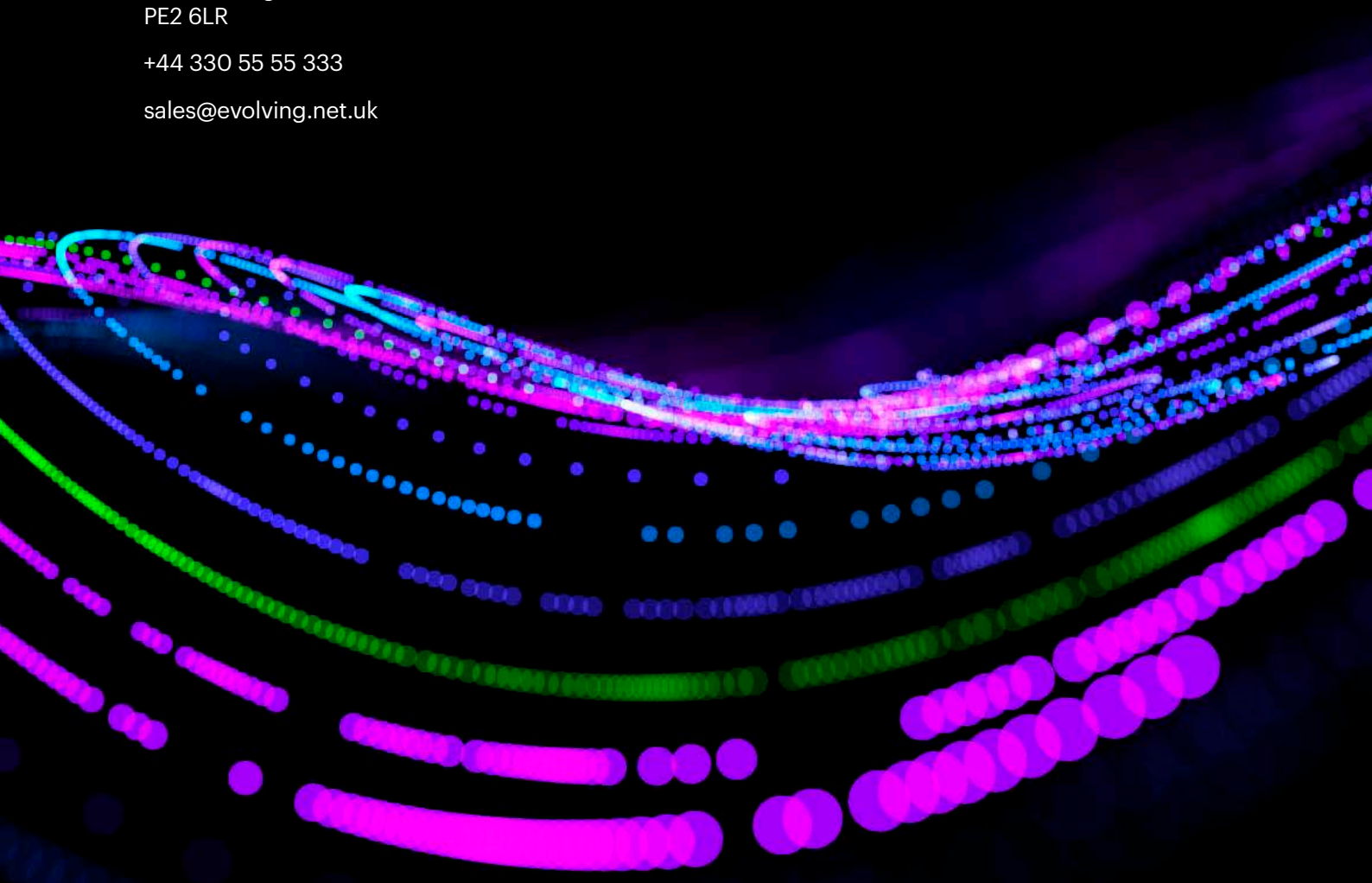
At Evolving Networks, this isn't a philosophy we pay lip service to – we built our next generation SD-WAN fabric around it. With encrypted overlays, identity-verified flows, and an architecture that exposes nothing by default, ZERO SDWAN reflects Zero Trust as it was intended: comprehensive, foundational, and deeply embedded.

Not just an access feature. Not an add on to your traditional firewall. A principle applied at every layer of the network.

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

+44 330 55 55 333

sales@evolving.net.uk



evolving.net.uk