evolving NETWORKS™

WHITE PAPER

Rethinking network topology in a Zero Trust world

evolving.net.uk

Rethinking network topology in a Zero Trust world

Executive Summary

Legacy network topologies like hub-and-spoke and mesh models were designed for a world where devices inside the perimeter could trust one another by default. But in a Zero Trust world, trust is never implicit, and network communication must be policy-enforced, identity-driven, and isolated by design. This paper introduces a new conceptual model – the Up and Out Topology – to define how Zero Trust networks should be built from the ground up. This topology is a key structural element of the broader Zero Surface Architecture, underpinning multiple products in the evolving ZERO portfolio, including Zero Trust Segmentation, ZERO SDWAN, and the Zero Trust Guest Gateway.

Why traditional topologies no longer work

In a hub-and-spoke topology, devices (spokes) connect to a central point (the hub), and by default can communicate freely via that hub to all the other spokes. Mesh topologies attempt to optimize redundancy and resilience by allowing peer-to-peer routing. Both assume lateral communication is normal and even desirable.

However, these models break down under Zero Trust assumptions:

- **Lateral movement is a risk, not a feature.**
- **Network location is not identity and is only one facet of posture.**
- **Perimeter-based trust models are obsolete.**

Using outdated terms to describe Zero Trust networks leads to confusion and potentially dangerous misconfigurations.

Introducing the Up and Out Topology

Up and Out is a Zero Trust network topology where:

- Each endpoint exists in isolation (e.g., in a /32 subnet).
- All traffic is routed up to a centralised policy enforcement point.
- Traffic is only allowed out to explicitly authorised destinations.
- No peer-to-peer or lateral traffic is permitted between endpoints.

This topology prioritizes identity, policy, and directional control over proximity or network location.

An upstream-only topology, its structure is inherently asymmetric: endpoints initiate connections upward to a gateway, but do not receive traffic from other endpoints or even from the gateway itself unless explicitly authorised by carefully considered administrative policy. The default is zero.

Communication is always outbound from the isolated node to the platform, where

access decisions are made before allowing traffic to continue. This zero peer principle breaks the assumption of mutual reachability that underpins traditional topologies.

It may turn the traditional notion of a LAN on its head, but in a Zero Trust mindset, access is changed radically. The physical topology remains the same, with switches and cables still enforcing hub-and-spoke at Layer 1. But by abstracting – one of the most important lessons of the software-defined era – we can create network separation to give a level of security not conceived by the original framers of LAN networking.

The broader Zero Trust picture

A new topology is not only desirable in the Zero Trust context, it's required for its full realisation. Zero Trust is more than just a security model – it's a rethinking of how connectivity, exposure, and control should be structured. Clear, intuitive language like "up-and-out" allows organisations and their technical leaders to engage with these ideas without requiring an exhaustive reeducation effort.

Most Zero Trust journeys today begin with ZTNA – introducing access brokers, identity checks, and posture-aware decision-making at the application edge. But that addresses only part of the surface. The physical and logical structure of the network itself must also reflect Zero Trust principles.

As organisations begin to see the value of a Gate and State model – where ephemeral overlays are established by ZTNA gateways based on who and what is requesting access – it becomes equally important to apply the same rigor at the network layer. Up-and-out complements ZTNA by enforcing Zero Trust in LANs, SDWAN overlays, and guest networks. It ensures that every packet has a purpose, a route, and a policy.

True Zero Trust isn't just about conditional access. It's about re-architecting the default assumptions of your network so that nothing can happen implicitly. Up-and-out makes that structural change real – on every LAN, everywhere.

The Zero Surface Architecture

The up-and-out topology is one foundational element of the broader Zero Surface Architecture:

- Default deny inbound.
- Zero routing by default.
- Zero lateral flows by default.
- ZTNA flows control access to apps.
- Internet access is one way, and filtered heavily.
- Every flow is intentional, observable, and minimally scoped.

This architecture spans LAN, WAN, cloud, and guest networks. It moves beyond "secure access" toward a state where the very structure of the network enforces Zero Trust.

Product Applications

1. Zero Trust Segmentation

- Microsegmentation within sites or zones.
- Devices are isolated from one another and can only route to upstream policy cores.
- Ideal for OT, IoT, and sensitive environments.

2. ZERO SDWAN

- Extends up-and-out principles across multisite WANs and cloud edges.
- Identity-based overlay routes connect trusted edges via centralized enforcement.
- Eliminates lateral risk even across encrypted tunnels.

3. Zero Trust Guest Gateway

- Provides strict, upstream-only internet access for unmanaged or guest devices.
- Blocks access to internal resources entirely.
- Fully policy-enforced.

Language Matters

Using legacy language like "hub and spoke" introduces conceptual debt – an accumulation of misaligned assumptions that make Zero Trust harder to communicate and implement. Security teams must constantly re-explain what Zero Trust isn't, rather than building understanding around what it is.

A new network model – Up and Out – gives us the language to describe Zero Trust topologies accurately, without compromise. It's visual, directional, and aligned with the principles that modern networks demand.

Conclusion

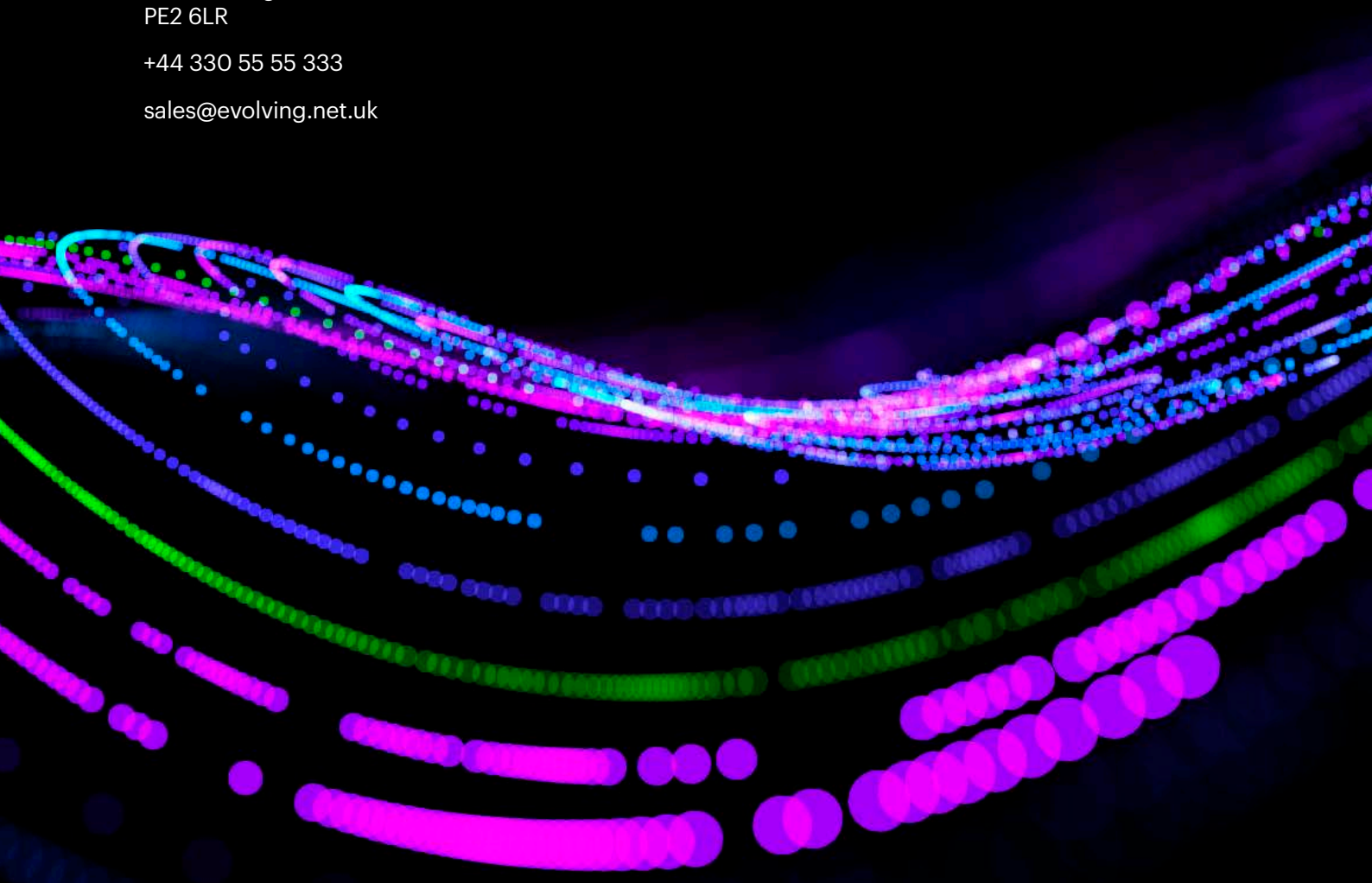
Up-and-out is the right topology for a Zero Trust world.

It rejects lateral movement, redefines routing around trust, and fits naturally into the Zero Surface Architecture. As Zero Trust evolves from buzzword to baseline, we must evolve the way we think, speak, and build. This is the topology to match.

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

+44 330 55 55 333

sales@evolving.net.uk



evolving.net.uk