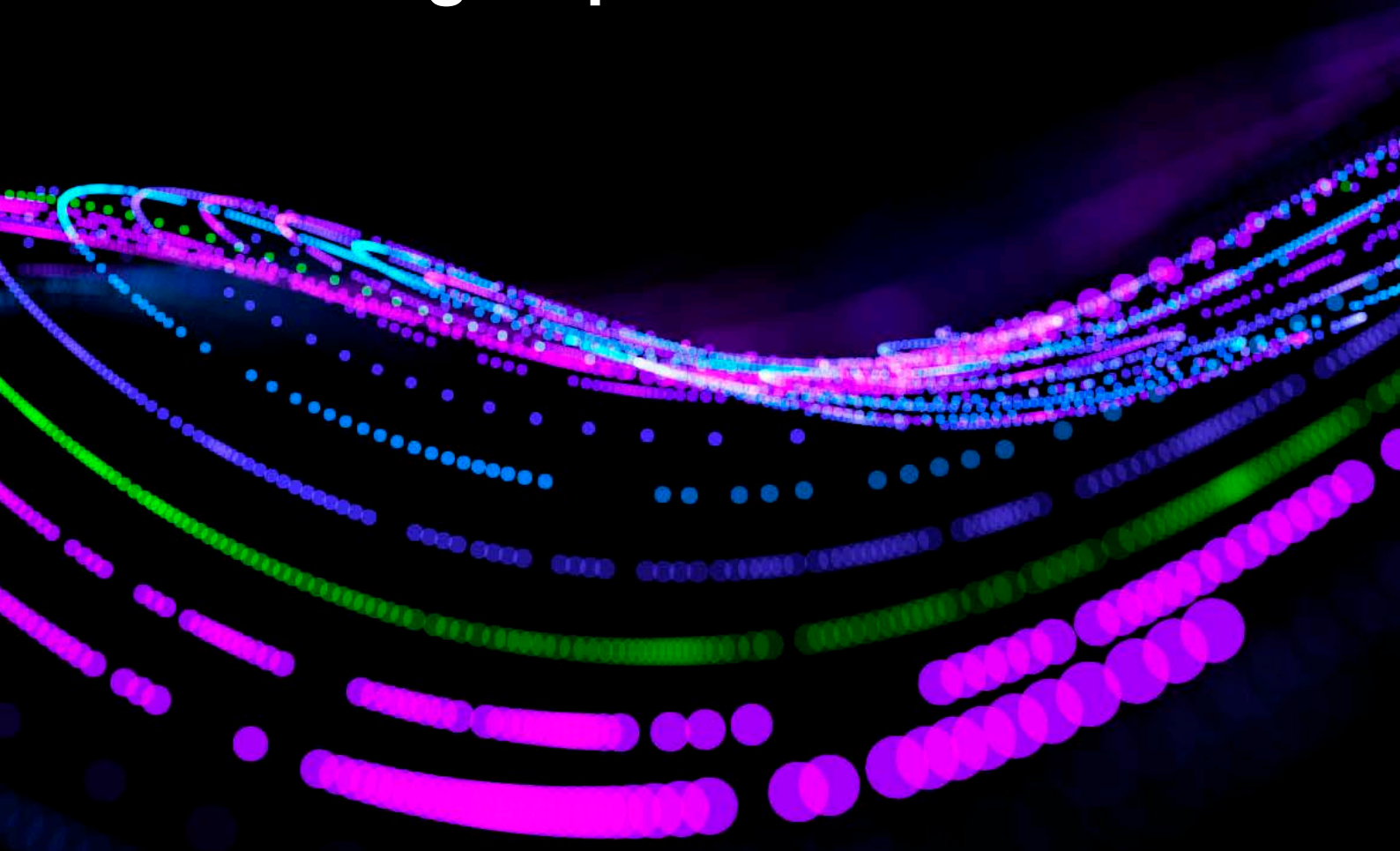
evolving NETWORKS™

WHITE PAPER

Redefining the perimeter



evolving.net.uk

Redefining the perimeter

Why trust – not infrastructure – is the foundation of modern network security

WHITE PAPER

Executive Summary

For decades, enterprise security revolved around the perimeter – a static boundary between the trusted internal network and the untrusted external world. But in today's digital-first, cloud-native, work-from-anywhere reality, that perimeter no longer exists. Users connect from anywhere, devices are increasingly mobile, and applications reside far beyond the walls of the private data centre.

In this environment, a modern approach is required – one that redefines the perimeter not around infrastructure or IP addresses, but around something more adaptive, enforceable, and meaningful: trust. This white paper explores how enterprises are embracing a trust-centric model to secure users, devices, and data across distributed environments. It introduces **evolving ZERO,** a Zero Trust platform that applies identity and context as the new perimeter – and enforces it where it matters most: at the edge.

A modern approach is required – one that redefines the perimeter not around infrastructure but around something more adaptive, enforceable, and meaningful: trust.

The perimeter has collapsed

The traditional perimeter model relied on the assumption that what resided inside the network could be trusted by default. Firewalls and VPNs established boundaries, and users or devices inside those boundaries were implicitly granted access. This model worked in an era where all resources, users, and infrastructure were centralised within physical offices and data centres.

However, this model has broken down in the face of digital transformation. Enterprises are now globally distributed. Employees, contractors, and third parties regularly access critical applications from remote locations. Cloud adoption has shifted applications away from data centres. Devices are often unmanaged or personally owned. Trusting by location not only no longer maps to reality, but has ceased to be an option.

As a result, the perimeter – once a definable security control zone – has collapsed. In its place, enterprises must embrace a model where trust is defined dynamically, based on who is requesting access, what they are using, and how they are behaving.

A necessary paradigm shift

Security models must evolve to reflect the fluidity of today's digital operations. Trust must become dynamic, contextual, and continuously evaluated. Rather than relying on network location, modern security frameworks use a combination of identity, device posture, context, and policy to determine access.

This is the essence of the Zero Trust model: never assume trust based on where a user or device is, but always verify who or what they are, their current posture, and whether they should have access to a given resource.

In a trust-based perimeter model:

- Identity is verified using robust, federated systems
- Device health and posture are assessed in real time
- Access is granted through ephemeral, policy-bound tunnels
- All flows are policy-evaluated at the point of entry

This enables organisations to enforce least privilege, contain risk, and drastically reduce lateral movement potential.

evolving ZERO: enforcing the new perimeter

In contrast to hypercentralised cloud security architectures, **evolving ZERO** shifts enforcement to the network edge. Rather than routing application traffic through a remote broker, it applies policy where the traffic originates – locally, at the EVX or at the user. This reduces latency, eliminates dependency on external infrastructure, and reduces bandwidth.

Hypercentralised platforms claim to eliminate the attack surface – but in reality, they relocate it. The broker itself becomes the new perimeter: a globally reachable service that must accept unauthenticated requests from any IP address. **evolving ZERO** avoids this by design. Nothing is exposed. No service is reachable. The attack surface isn't just minimised – it's removed until trust is proven.

evolving ZERO is a platform designed to enforce this redefined perimeter. It applies Zero Trust principles not as an abstract goal, but as a practical, deployable architecture. Unlike traditional SASE platforms that centralise decision-making in the cloud, Evolving Zero enforces trust where it matters most: at the edge.

With **evolving ZERO,** every device, user, and application is considered untrusted by default. The EVX sits at the network edge and acts as a local enforcer. Traffic is not routed unless it originates from a verified identity with the appropriate posture and access policy. There are no implicit paths. There is no default gateway. Instead, access is explicitly granted via dynamic overlay tunnels tied to user, device, and policy context. Zero is the new default.

This architecture ensures traffic never flows unless it's earned. Trust becomes a condition, not a location. The result is a network that is inert unless activated by validated trust signals.

A platform built for today's enterprise

evolving ZERO consists of four composable components:

- **ZERO Edge** is the enforcement layer, deployed as the EVX. It inspects and routes traffic only when trust conditions are met. It enables enforcement at the edge – on-premises, at branches, or in virtual infrastructure.
- **ZERO Access** is the endpoint client that enforces posture and identity. It combines ZTNA and Secure Web Gateway capabilities, ensuring outbound and private access traffic is always tied to identity and device posture.
- **ZERO Fabric** is the encrypted network overlay. It dynamically creates context-aware overlay tunnels between endpoints and resources. These tunnels exist only while needed, and only for authorised flows.
- **ZERO Stack** is the modular security services layer. It delivers pluggable security components such as IAM integration, FWaaS, ZTNA gateways, SWG and CASB.

Together, these components create a system where trust is enforced continuously, locally, and contextually – and where policy is composable and vendor-neutral.

Built on open standards, designed for modular deployment, and architected for interoperability – Evolving Zero allows you to integrate your own security modules and IAM. Unlike vendor-locked platforms that enforce a single stack, evolving ZERO embraces defence-in-depth and gives you control. You choose what to run, where to enforce, and how to secure – without compromise.

evolving ZERO vs the old guard: decentralised by design

Another core distinction lies in the traffic path itself. With broker-based models such as Zscaler Private Access (ZPA), application traffic from the user device is routed to the cloud broker – often far from the user – before being relayed to the destination server.

These hypercentralised architectures introduces unnecessary hairpin latency, consumes additional edge bandwidth, and makes session integrity dependent on the broker's availability.

In contrast, **evolving ZERO** allows authorised users to establish direct, identity-bound tunnels from client to application – with all policy checks enforced at the endpoints. This architecture improves performance, reduces cloud dependency, and avoids introducing the broker as a man-in-the-middle chokepoint.

Zero is the new default

By decentralising enforcement, **evolving ZERO** avoids the architectural weaknesses introduced by broker-first models. It ensures that access decisions are both faster and more secure, and that no part of the network becomes a standing invitation to unauthenticated traffic. Where hypercentralised platforms concentrate risk in a few visible endpoints, **evolving ZERO** distributes enforcement to the edge – eliminating single points of exposure.

With **evolving ZERO,** the perimeter is no longer a place. It is a dynamic condition that must be satisfied before any connection is made. Trust becomes the only currency. The network enforces that trust at its edge, in real time, and with full auditability.

Organisations gain a security model that works just as well on-premises as it does in the cloud. Access becomes justifiable, observable, and enforceable. The days of implicit trust fade into history, replaced by transparent, accountable access control.

Security teams benefit from simpler policy design, real-time enforcement, and a reduction in risk surface befitting the modern era. End users benefit from seamless, identity-based access wherever they work.

Conclusion

Trust is no longer a byproduct of location. It is the perimeter itself. By redefining access around verified identity and dynamic context – and enforcing those decisions at the edge – organisations can fully realise the promise of Zero Trust.

evolving ZERO provides the foundation for this transformation. It brings policy, identity, and control to the forefront – and ensures that the network, at every point, obeys the principle of: **no trust, no traffic, no assumptions.**

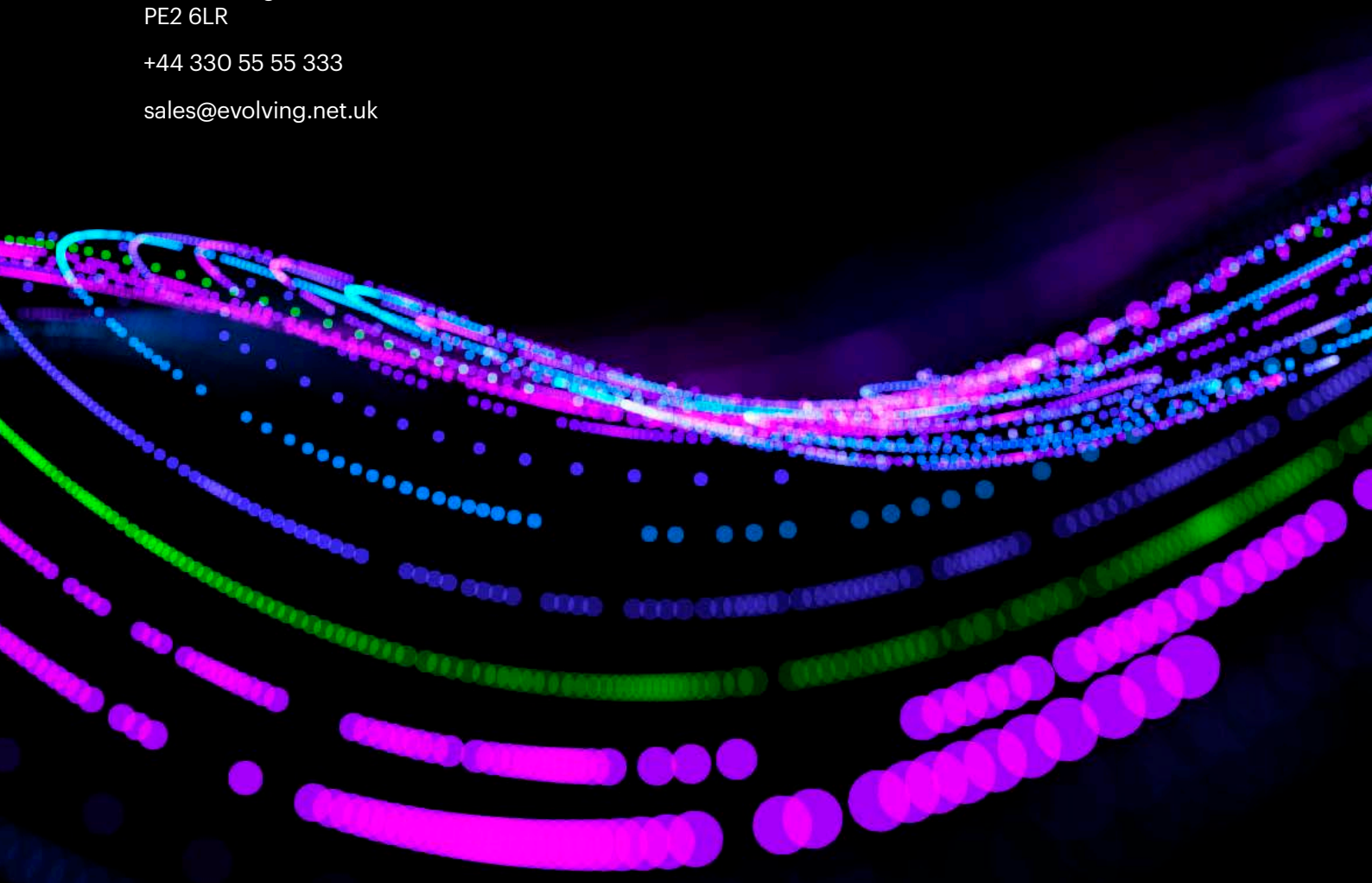
In contrast to hypercentralsed stacks that treat cloud presence as a requirement, **evolving ZERO** empowers enterprises to regain control, enforce locally, and reduce platform risk – delivering a resilient, sovereign security posture across edge and cloud alike.

Evolving Networks. Make zero the new default.

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

+44 330 55 55 333

sales@evolving.net.uk



evolving.net.uk