WHITE PAPER

Redesigning connectivity and security: the Zero Surface Architecture

evolving.net.uk

WHITE PAPER

Redesigning connectivity and security: the Zero Surface Architecture

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) platform 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** that underpins **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) platform 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 traditional tools such as 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.

ZTNA isn't enough

With the rise of Network-as-a-Service (Naas) and now the start of the serious adoption of Zero Trust across the business world, new models are needed for the provision of modern secure networking.

While many providers and businesses push ZTNA as a practical and viable Zero Trust option, it's becoming clearer that this isn't the end of the Zero Trust story.

In fact, there is a risk that organisations feel a false sense of protection, thinking that by deploying ZTNA, they are ticking the Zero Trust box and need do no more.

Zero Trust: principle vs practice

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, but 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 premise of the Zero Surface Arcitecture.

Zero Surface Architecture

What if instead of allow-all and hub-and-spoke – inherently trust based in their design – an architecture was concevied that started with all of the Zero Trust principles from the word go.

Such a model would drastically and dramatically reduce the attack surface, often eliminating it entirely. The perimeter as we know it would become irrelevant. The days of the default meshed topology would be numbered.

The Zero Surface Architecture 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. Micro-segmentation is built-in at every level.
- Hub-and-spoke is replaced with up-and-out, a zero-peer, upstream only topology.

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

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.

How It Works

First, the network is made inert. Instead of allow-all, deny-all is the starting point. No flow across the network, whether LAN or WAN is allowed.

User devices themselves are isolated within their own microsegmented network – only allowed access to the upstream gateway, and not to their peers on the LAN, or on the WAN.

Then, Universal ZTNA is employed for users and compatible devices. The Zero Trust fabric underpinning this application access is allowed across the network, so long as the authenticaion, authorisation and posture checks come back clean.

Every application flow is encrypted, dynamic, and controllable. Access is ephemeral, and based only on policy and dynamic checks.

Internet access follows the same model, through the Zero Trust overlays once authorised, and straight to a Secure Web Gateway, controlling, monitoring and restricting all internet use.

IoT and OT are then treated with pinpoint accuracy. VoIP handsets are allowed tailored access to hosted VoIP and only on the specific ports required. All traffic is encrypted across the ISP circuits, and exits to the internet via Next Generation Firewalling.

Printers and scanners are treated in a similar manner, favouring an up-and-out topology, and 1:1, port to port, IP to IP rules. If ZTNA can be employed to govern their access, then it is. ZTNA gateways or app connectors can sit in front of individual or groups of ZTNA-unready tools and devices even on the LAN, controlling access per user and microsegment, and still with posture checks.

The Zero Surface Architecture is exactly what it says – a way to replace the traditional any-to-any network model, where every device is exposed and compromise can spread freely, with a true Zero Trust environment where access is explicitly granted, lateral movement is blocked, and nothing is reachable by default.

Implementation

Many organisations begin their journey with Zero Surface Architecture 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 the fully composable Zero Surface Architecture.

Or go full-fabric

Organisations ready to fully embrace Zero Trust can deploy Zero Surface Architecture 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.

A Zero Surface Architecture 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 models 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, the Zero Surface Architecture 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

A Zero Surface Architecture 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 boundary, 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 secure 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

Make zero the new default.

evolving
NETWORKS™

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

+44 330 55 55 333

sales@evolving.net.uk

evolving.net.uk