



PRODUCT SPEC

# Zero Trust Firewall (ZTFW)

Essential network  
protection

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

+44 330 55 55 333  
sales@evolving.net.uk

[evolving.net.uk](https://www.evolving.net.uk)

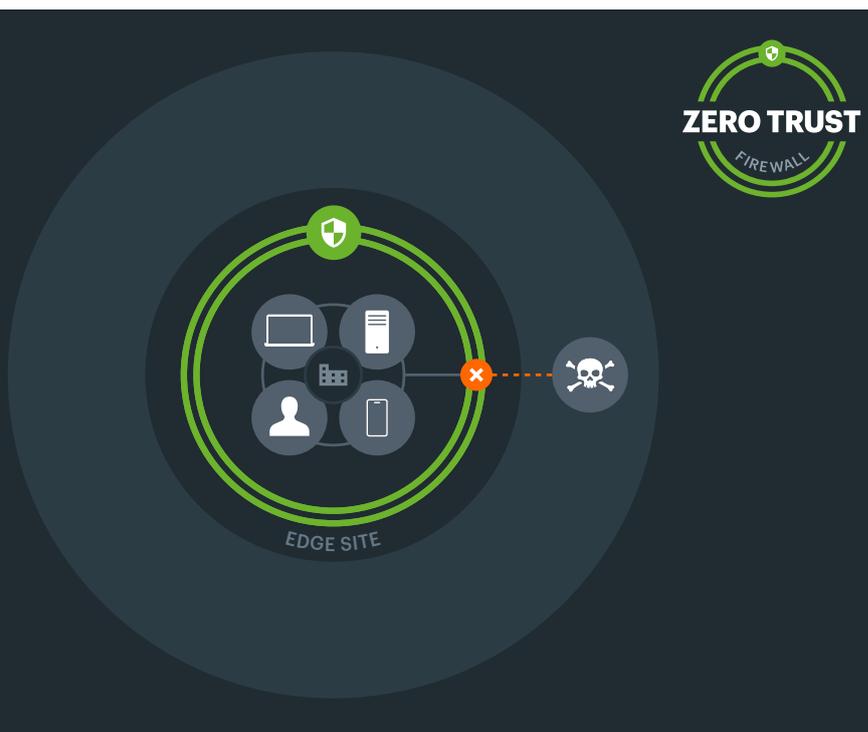
# Zero Trust Firewall (ZTFW)

Essential network protection delivered with simplicity and efficiency

## Overview

This on-board, lightweight, perimeter firewall is designed to deliver essential network protection with simplicity and efficiency. Built on Linux with industry trusted, open source tools, it seamlessly integrates into existing systems and provides first-defence firewalling for businesses of all sizes.

Built to complement ZTNA and endpoint security strategies, where the modern workplace obviates the need for NGFW, it delivers fully managed, low cost, and customisable network security that fits seamlessly into Zero Trust architectures.



## PRODUCT SPEC

### Feature list

#### Deployment

On board

#### Access control

Deny all, with explicit rules based engine for granular control

#### VLAN capable

Yes, and secured with inter-VLAN policies

#### Inbound port forwarding

Yes

#### NAT gateway

Yes

#### Secure access to private, public & cloud networks

Yes

#### DHCP services

DHCP server and DHCP relay

#### High availability

Yes, when paired with EVX HA (minimum 2 appliances)

Seamlessly integrates into existing systems and provides first-defence firewalling

## Key features

- **No additional hardware:** On board edge EVX appliances, so no additional footprint or power, and immediately integrated into Ultimate Internet and Network as a Service.
- **Enterprise-grade without enterprise cost:** No licence fees, no hardware renewal costs, no vendor lock in.
- **Defence-in-depth:** Choose best of breed security solutions and augment EDR and ZTNA.
- **Proven track record:** Software trusted by governments, enterprises, and tech giants worldwide.
- **Automatic updates & patching:** Managed, proactive patch management.
- **Zero Trust:** Default deny all plus powerful rules engine for access control.

## Typical use cases

- Businesses requiring firewalling at the edge.
- IT environments prioritising quick setup and straightforward management.
- Modern workplaces scaling back their Next-Gen Firewalls, and focusing on endpoint security and Zero Trust.
- Cloud first companies, where advanced security is delivered off-premise.

