Stop breaches from spreading with Zero Trust segmentation across workloads and endpoints

Modern estates are increasingly complex – spanning multiple datacentres and public clouds, hosted environments, and partner networks. This means you're defending a broader attack surface with ample opportunity for breaches, making prevention extremely difficult, if not impossible.

Additionally, endpoints remain one of the most vulnerable aspects of your environment. Zero-day attacks mean that endpoint security solutions can still leave you vulnerable to lateral movement before they can adapt to the new attack vector.

Reducing the 'blast radius' using segmentation is a foundational tenet of Zero Trust security, but segmentation using traditional methods is expensive, labour-intensive, and difficult to manage once implemented.

Stop the reach of the breach

Zero Trust segmentation is a modern security approach that minimises the impact of breaches and ransomware. It mitigates the spread of breaches by continually visualising how your workloads and endpoint devices are communicating, creating granular policies that only allow wanted and necessary communication, and automatically isolating breaches by restricting lateral movement.

Our Managed Micro-Segmentation Security service is created by combining our managed service wrap with Illumio's Zero Trust Segmentation platform, the industry's top technology partner for managed micro-segmentation security. It allows you to outsource your network segmentation management to us, meaning you can be confident that your micro-segmentation policies are set up and working correctly.

Benefits of our managed micro-segmentation service

See risk
Visualise all communication and traffic between workloads and endpoints across the entire hybrid attack surface.

Set policy
Easily ringfence, micro- or nano-segment your estate to control communication and only allow necessary and wanted traffic.

Stop the spread
Automatically push policy to isolate compromised areas or endpoints to stop the spread of an active attack.

Secure endpoint exposure
Isolate cyber attacks to a single device – even before the attack is detected by your endpoint security tools.

Total Economic Impact study*
- Return on investment (ROI) of 111%
- Benefits of $10.2m over three years
- Payback period six months

*Total Economic Impact of Illumio Zero Trust Segmentation, Forrester Consulting, March 2023
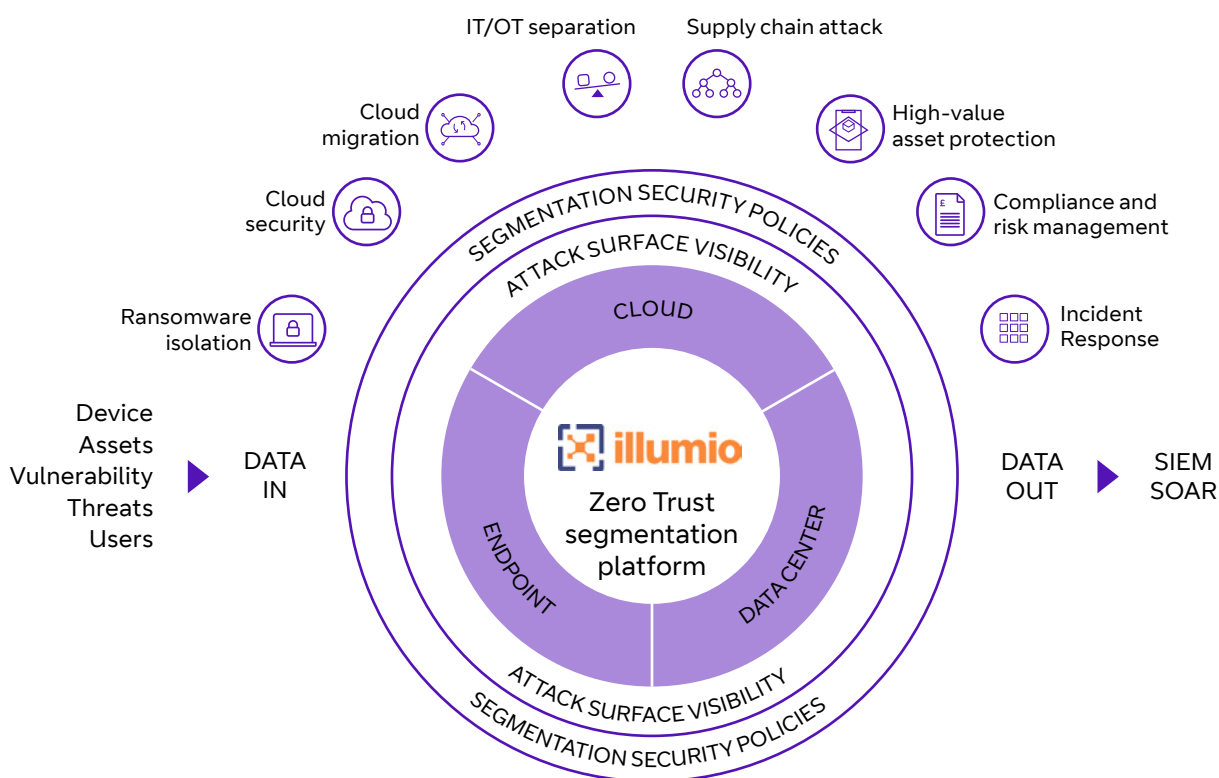
Visualisation, management, and proactive monitoring

We have many workloads under our management. Our experts will ensure your micro-segmentation policies are correctly configured.

We'll then proactively monitor your set-up to ensure your service is running smoothly.

You'll get reports so you can be confident that legitimate traffic is not being mistakenly blocked.

We're available round-the-clock if you need to create a new policy based on what you're seeing. We can also help with moving individual nodes into existing policies.

Why work with us?

We're a trusted global partner with expertise in delivering security services across different verticals in all geographies.

We were the first managed security services provider (MSSP) to offer a fully managed Illumio micro-segmentation service, and we have thousands of workloads under our management.

We have accredited Illumio professionals who will manage the design, set up, deployment, and management of our micro-segmentation service.

Our Advisory Services Visibility Assessment offers you an easy way to trial the service and get visibility into your workload vulnerabilities before a full deployment.

What could Managed Micro-Segmentation do for you? Visit bt.com/security