Eliminating EnterpriseNetwork Risks,One Blind-Spot at a Time

Discover How with ACT Enterprise Secure Internet Leased Line

Modern enterprises operate in an environment where connectivity is inseparable from risk. Take for instance, industries such as fintech, healthcare, e-commerce that run almost entirely on real-time digital transactions. A few minutes of downtime – or a single successful breach – can erode customer trust, expose sensitive data, and halt operations. Globally, the average cost of a data breach globally reached $4.67 million in 2025. The healthcare industry witnessed the highest breach costs, with the total breach costs touching $11.3 billion in 2025.

Yet, while businesses have accelerated their digital transformation, security practices have often remained reactive. Attack surfaces have expanded across SaaS platforms, hybrid workforces, and cloud applications, giving threat actors more entry points than ever before. The challenge for enterprises today is simple to state but hard to achieve: **Reduce blind spots across the network so threats can be detected before they become incidents.**

The Growing Demand For Timely Threat Intelligence

Cyber risks no longer arrive as isolated events. Malware, ransomware, phishing kits and credential-harvesting tools are increasingly automated and AI-assisted. Enterprises that rely only on periodic audits or manual monitoring are always a step behind.

What forward-looking enterprises truly need is **continuous visibility** – the ability to see what is entering and leaving their network at all times. The fewer blind spots an enterprise has, the better it can navigate complex, multi-vector attacks. Timely threat intelligence is therefore not a luxury; it is the foundation of business continuity.

This visibility must begin at the gateway itself – the point where the enterprise network meets the internet. For most enterprises, 90–95% of business activity today depends on internet connectivity, from collaboration tools and ERP systems to customer-facing applications. If that gateway is not secured and intelligently monitored, every digital initiative rests on fragile ground.

Security Starts with Proactive Monitoring

Enterprises often assume that buying a high-speed connection is enough. In reality, connectivity without protection simply opens a faster highway for malicious traffic.
What they additionally need is proactive monitoring of their threat landscape: identification of abnormal patterns, blocking of harmful content, and immediate response to suspicious behaviour.

Traditionally, enterprises have approached this in two ways:

1.Purchase a firewall from a global OEM and manage it internally.

2.Rely on their connectivity provider to bundle and manage the firewall as a service.

For many small and mid-sized enterprises, the first option quickly becomes complex and expensive. Beyond the hardware cost lies the need for skilled specialists, 24x7 monitoring, timely firmware upgrades, policy management, and replacement during failures. These are capabilities that few growing businesses can maintain in-house.

Secured Internet Leased Line: Connectivity with Built-In Defence

ACT Enterprise Secured Internet Leased Line is designed precisely to remove these blind spots. It combines a high-reliability leased line with a fully managed enterprise-grade firewall, delivered as a single service.

Unlike broadband connections, leased lines are meant for mission-critical operations where downtime directly impacts revenue and reputation. ACT Enterprise delivers Secured Internet Leased Line over fibre with dedicated, symmetrical bandwidth – the speed subscribed is the speed experienced, for both uploads and downloads. This stable foundation becomes the platform for stronger security.

The managed firewall acts as the **first line of defence** between the enterprise's internal network – employee devices, servers, SaaS platforms – and the open internet. It blocks malware, ransomware, trojans and attempts by threat actors to access sensitive data, while also preventing users from inadvertently reaching malicious domains.

What differentiates ACT Secured ILL is not just the device but the **managed experience** around it. ACT Enterprise handles installation, configuration, policy changes, patch updates, and even hardware replacement, taking away the anxiety of day-to-day security operations. For SMEs and growing campuses that lack dedicated security teams, this becomes a force multiplier.

Adding intelligence at the Device Level

Today's threats evolve too quickly for rule-based controls alone. That is why ACT Secured Internet Leased Line brings together a modern firewall solution integrated with AI-powered capabilities at the device level **–** to detect network anomalies, recognise new attack signatures, and respond automatically before damage occurs.

This embedded intelligence transforms the gateway from a passive filter into an active sentinel. Suspicious downloads can be quarantined, command-and-control traffic can be blocked, and risky user behaviour can be flagged in real time. The result is a dynamic defence that learns continuously rather than waiting for manual intervention.

More Than Technology – Experience Matters

In the managed security space, the real differentiator is **customer experience –** how quickly issues are resolved, how proactive the monitoring is, and how confident customers feel in everyday operations.

ACT Enterprise focuses on:

- Fibre-based last-mile delivery for higher uptime
- Guaranteed dedicated speeds
- Rapid response support
- Lifecycle management of firewall infrastructure
- Proactive alerts and configuration assistance

This approach allows enterprises to focus on innovation instead of infrastructure, knowing that their digital perimeter is continuously guarded.

Closing blind spots, enabling growth

Every enterprise leader today faces the same paradox: digital expansion increases opportunity while simultaneously increasing risk. Eliminating every threat is impossible; **eliminating blind spots is not.**

ACT Secured Internet Leased Line gives enterprises a clear, monitored gateway to the internet – where connectivity, security and intelligence operate as one service. By reducing unknowns at the network edge, businesses can adopt cloud tools, remote work and customer-facing platforms with far greater confidence.

In a world where the next attack is always around the corner, resilience begins with visibility. And visibility begins with a secure, intelligently managed connection.