Secured ILL

Brochure

Market Trends

SMEs Face 43% of Cyberattacks

With rising cloud usage and limited defenses, SMEs have become prime targets for cyber threats.

$9.2B Market by 2030

India's perimeter security market is growing fast - from $3.2B in 2023 to $9.2B by 2030, at a 14% CAGR.

Compliance Is Driving Action

Laws like the IT Act and CERT-IN guidelines are making perimeter protection mandatory for risk and reputation management.

Business Challenges

Exposure to Cyber Attacks Due to Weak Perimeter Security

Outdated infrastructure leaves networks vulnerable to breaches, malware, and targeted cyberattacks, putting critical business data at risk.

Risk of Non-Compliance with Government Regulations

Failure to comply with IT and data protection laws (e.g., CERT-IN, IT Act) exposes SMEs to legal and financial risks.

Compromised Security for Remote Users

On-premise setups are not equipped to protect remote employees, leading to security gaps in hybrid or distributed environments.

Poor Network Visibility

Limited insight into branch-level or multi-site network activity hinders the ability to detect, diagnose, and resolve issues efficiently.

Inefficient Network Optimization

Lack of intelligent WAN optimization and traffic prioritization results in poor bandwidth usage and inconsistent user experience.

Introducing Secured ILL

It is a comprehensive *networking and security solution* tailored for businesses of all sizes, ensuring seamless compliance with industry regulations *without the need to change existing IT infrastructure*. The solution bundles a fully managed, next-gen firewall with an Internet Leased Line (ILL) to provide enterprise-grade security, network resilience, and compliance readiness while maintaining operational efficiency.

Multilayered Security
Advanced threat protection built in.

Seamless Integration
Works with your current network.

Industry Compliance
Meets key IT security regulations.

Cost Effective as Delivered as a bundled OpEx model.

Unified Security
Covers office and remote users.

Single Solution
Protects against diverse cyber threats.

Key Features & Benefits

Built-in Next Gen Security

Includes an inbuilt firewall with Advanced Threat Protection (ATP) and User Threat Protection (UTP) capabilities.

WAN Resilience

Delivers uninterrupted connectivity through built-in auto-failover support for network continuity.

.

Unified Security

Enables secure access for all users across remote, hybrid, and on-premise work environments.

Stronger Perimeter

Protects the network using a managed firewall to ensure safety, compliance, and seamless uptime.

Privileged Access of Firewall

Provides flexible, on-demand access to configure and manage firewall settings within minutes..

Centralized Visibility

Offers a 360-degree dashboard to monitor network performance across all branch locations.

Future Ready

Supports easy scalability with options to enhance secure networking and branch connectivity.

Secured ILL – Product Variants

S.No.	Secured ILL Features	FortiCare	ATP	UTP	UTP+
1	Dedicated symmetric bandwidth (1:1)	✅	✅	✅	✅
2	Static IPv4 (/30 WAN & /29 LAN) and IPv6 IP (/126 WAN & /64 LAN) IP Pool	✅	✅	✅	✅
3	SLA: Network uptime 99.5% & MTTR <= 4 hrs.	✅	✅	✅	✅
4	Routing (Static & Dynamic) - supports RIP, OSPF, BGP	✅	✅	✅	✅
5	NAT (Source/Destination) configuration support	✅	✅	✅	✅
6	Fully managed services with proactive monitoring	✅	✅	✅	✅
7	Write access for immediate configuration changes (optional)	✅	✅	✅	✅
8	Industry-specific compliance guidance and best practices	✅	✅	✅	✅

Secured ILL – Product Variants

S.No.	Secured ILL Features	FortiCare	ATP	UTP	UTP+
9	Forti Manager & Forti Analyzer access (optional)	✓	✓	✓	✓
10	DoS (Denial of Service) protection policy with base rate limiting	✓	✓	✓	✓
11	Seamless auto-failover with other ISP links	✓	✓	✓	✓
12	IPSec and SSL VPN (Branch-to-Branch and remote user access)	✓	✓	✓	✓
13	Secure stateful firewall functionality	✓	✓	✓	✓
14	Basic and advanced firewall rules (Allow/Deny traffic)	✓	✓	✓	✓
15	Installation, firmware updates, and change management	✓	✓	✓	✓
16	Repair and replacement with 24×7 technical support (NOC expert teams)	✓	✓	✓	✓

Secured ILL – Product Variants

S.No.	Secured ILL Features	FortiCare	ATP	UTP	UTP+
17	Industry-compliant reporting	❌	✅	✅	✅
18	Deep Packet Inspection: Detects and blocks hidden threats in network traffic	❌	✅	✅	✅
19	SSL Inspection: Analyzes encrypted traffic to detect malware and attacks	❌	✅	✅	✅
20	IPS (Intrusion Prevention System): Blocks known and emerging cyber threats	❌	✅	✅	✅
21	Anti-Malware/Anti-Virus: Protects against viruses and malicious software	❌	✅	✅	✅
22	Identity-Based Security: Access control based on user roles and credentials	❌	✅	✅	✅
23	Application Control: Restricts usage of risky or unauthorized applications	❌	✅	✅	✅
24	Web & Video Filtering: Blocks access to harmful or non-business content	❌	✅	✅	✅
25	Email Link Scanning: Detects phishing by analyzing links in emails	❌	❌	✅	✅
26	Antispam Service: Filters spam and malicious email content	❌	❌	✅	✅

Secured ILL – Product Variants

S.No.	Secured ILL Features	FortiCare	ATP	UTP	UTP+
27	ZTNA: Secure access to corporate apps with user and device verification	❌	❌	❌	✅
28	Endpoint Security Posture: Real-time compliance check of device during session	❌	❌	❌	✅
29	Cloud Firewall: Web-based firewall with web filtering, IPS, and DNS security	❌	❌	❌	✅
30	CASB: Secures SaaS access and monitors shadow IT applications	❌	❌	❌	✅
31	Data Loss Prevention: Monitors and protects sensitive data from leakage	❌	❌	❌	✅
32	Multi-Device Support: Access on up to 3 devices per user	❌	❌	❌	✅

UTP+: Differentiators & Benefits

Key Differentiators	Customer Benefits
Enforces always-on security for all users and devices	• Zero tolerance for policy violations • Real-time threat detection and prevention • Strengthened data compliance
Secures data, apps, and remote workforce connectivity	• Protects critical applications • Seamless security access from any location • Secures data exchange and usage
Protects users, devices, and traffic across destinations, no VPN required	• Minimizes attack surface for enhanced protection • Secures traffic across all destinations • Authenticates both user and device
Provides full visibility into security threats and device health	• Full visibility into user and application traffic • Actionable insights through analytics • Proactive device health monitoring
Tracks and controls user activity regardless of location	• Blocks harmful applications • Monitors and controls user behavior • Centralized dashboard for unified oversight
Prevents data leakage with built-in endpoint protection	• Prevents data loss • Restricts unauthorized access to personal drives • Supports regulatory compliance

FAQs

1   **What is Secured ILL and what kinds of threats does it block?**

Secured ILL, with its perimeter firewall, protects against phishing, botnets, encrypted malware, and denial-of-service attacks. These threats typically enter through the internet before your LAN firewall can react.

2   **Why do we need a perimeter firewall?**

LAN firewalls are designed for internal security and are not optimized for edge-level threat detection. A perimeter firewall protects at the network boundary, blocking threats before they enter.

3   **Can our existing firewall block external threats?**

Not efficiently, because it's intended for internal segmentation and control. High-volume internet-based attacks often bypass or overwhelm these internal defences.

4   **Can't we just enable more features on our current firewall?**

You can, but activating features like IPS or SSL inspection will impact performance. These consume significant CPU power and may slow down your entire network.

FAQs

5 **What does the perimeter firewall do differently?**

It acts as the first point of defense at the ISP level, scanning traffic before it hits your network. This reduces the attack surface and keeps your core infrastructure safer.

6 **Is this bundled with Internet Leased Line?**

It is offered as part of the Secured ILL plan, which includes a managed perimeter firewall. This ensures multilayered security, integrated connectivity, and compliance in a single solution.

7 **Is it easy to manage?**

Yes, it's fully managed by our expert SOC and NOC teams 24x7. You also get a self-service portal to monitor traffic and access reports in real time.

8 **How fast is the deployment?**

Deployment is quick, smooth, and fully supported by our implementation team. From setup to configuration and go-live, we manage the entire process for you.

FAQs

9 **What is Secured UTP+?**

Secured UTP+ is a license-based security service designed for roaming and remote users. It protects users, devices, and application access, even when they are working outside office networks.

10 **What challenges does it address?**

It addresses the limitations of traditional VPNs and reduces the complexity of managing multiple hardware vendors. It also helps bridge the gap where internal security resources or skills are limited.

11 **How does Secured UTP+ help businesses?**

It secures all internet-bound traffic and controls user access to internal and cloud applications. It also enables detailed, policy-driven control for SaaS usage across your workforce.

12 **How is it priced?**

It is offered through a straightforward, per-user, per-year license model. This helps simplify procurement while ensuring predictable cost and scalability.

Thank you

www.tatatelebusiness.com

Your Trusted Smart Digital Solutions Provider