WHITEPAPER

Enterprise-Grade Cybersecurity for the SMB Market

How Network Operators Can Increase SMB ARPU and Reduce Churn with SecureConnect

Intelligently Connected™

veea.com

Ubiquitous Connectivity has become a commodity.

Across global markets, network operators are under sustained pressure from price competition, declining margins, and increasing customer churn, particularly in the small and mid-sized business (SMB) segment.

At the same time, SMBs are facing a sharp escalation in cyber threats driven by cloud adoption, distributed work, AI-enabled attacks, and increased reliance on digital payment and operational systems.

Cybersecurity Insights

- Despite growing awareness of cyber risk, most SMBs remain underprotected.
- Enterprise-grade security solutions are too complex, too costly, and too fragmented for SMB environments.
- Managed Security Service Providers (MSSPs) struggle to scale economically across this segment.
- The gap is widening between risk exposure and practical adoption of cybersecurity.

Strategic Opportunity

Operators already own the customer relationship, the access network, the billing relationship, and the operational lifecycle.

SecureConnect enables operators to embed enterprise-grade security directly into connectivity, transforming broadband into a cybersecure, value-added service delivered as a managed subscription.

Operator’s Advantages

By adopting SecureConnect, operators can increase average revenue per SMB, reduce churn through service stickiness, simplify operations by replacing fragmented security stacks, and establish a scalable platform for future edge, IoT, and digital services.

© 2018 – 2026 by Veea Inc. and its subsidiaries. All rights reserved.

The SMB Security Gap

SMB's In The Market

SMBs represent the backbone of modern economies, accounting for a significant share of employment, GDP contribution, and local economic activity. Yet they are disproportionately targeted by cyberattacks due to limited security maturity, reliance on basic connectivity, and lack of dedicated IT resources.

Market Findings

Market research and operator experience consistently show that most SMBs rely on consumer-grade routers, unmanaged Wi-Fi, and stand-alone software tools that provide limited protection against modern threats.

Critical business systems — point-of-sale terminals, customer databases, inventory systems, and cloud applications — are frequently exposed.

Current Security Models

Existing security models fail SMBs for structural reasons. Enterprise security platforms are designed for specialised teams and complex environments. MSSPs require custom integration, ongoing engagement, and cost structures that do not align with SMB economics. As a result, even security-aware SMBs struggle to act.

This creates a '**complexity gap**': awareness of cyber risk is high, but the ability to deploy, manage, and sustain effective security remains low. The consequences include increased downtime, data breaches, regulatory exposure, and growing support burden for operators.

Operators' Positioning

Network operators are uniquely positioned to close the SMB security gap. Unlike over-the-top vendors or standalone security providers, operators already manage connectivity, service provisioning, billing, and customer support at scale.

Limitations & Perceptions

However, traditional approaches (reselling security products or relying on third-party MSSPs) have delivered limited results. Attach rates remain low, sales cycles are long, and margins are diluted. Security is perceived as an optional add-on rather than a core service.

Solution

Embedding cybersecurity directly into connectivity fundamentally changes this dynamic. When security becomes part of the network service itself, adoption increases, operational complexity decreases, and value creation shifts upstream to the operator.

This model enables operators to differentiate their broadband offerings, strengthen customer relationships, and reposition themselves as trusted digital service providers rather than commodity connectivity suppliers.

Data Breaches &
Ransomware Infections

Downtime and transaction
delays / loss

Increased security upgrade
and repair costs

Increased support burden
including possible regulatory
exposure

© 2018 – 2026 by Veea Inc. and its subsidiaries. All rights reserved.

veea SecureConnect™

SecureConnect is an entirely new category in cybersecurity. By engineering the industry's first hardware platform with security embedded at every layer - from silicon to software.

SecureConnect delivers ultra-reliable 5G-based fixed wireless access with enterprise grade cybersecurity in a single, integrated solution that eliminates the complexity and cost of traditional IT deployments.

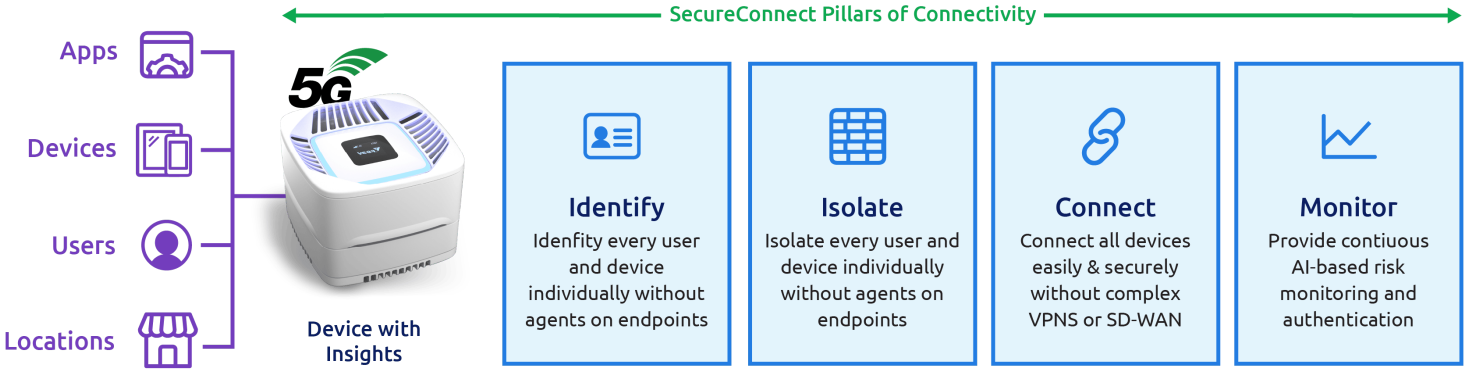
This comprehensive, category-defining platform enables service providers to deliver advanced cybersecurity protection to SMB and SME customers at accessible price points - transforming enterprise-grade security from a premium offering into a scalable market opportunity. SecureConnect combines secure broadband access, Zero Trust Network Access (ZTNA), next-generation firewalling, SD-WAN capabilities, and cloud-managed lifecycle control.

Unlike fragmented security stacks, SecureConnect is delivered via a single device and a unified management platform

- This enables plug-and-play deployment and remote operation at scale.
- This simplicity is critical for SMB environments and operator economics.

Operators retain full lifecycle ownership, from provisioning and policy management to upgrades and service evolution.

- By design, SecureConnect also provides a foundation for future edge services, enabling operators to introduce additional digital capabilities without re-architecting customer environments.



Identify
Idenfity every user and device individually without agents on endpoints

Isolate
Isolate every user and device individually without agents on endpoints

Connect
Connect all devices easily & securely without complex VPNS or SD-WAN

Monitor
Provide contiuous AI-based risk monitoring and authentication

SecureConnect combines Wi-Fi, optional 5G, AI-driven cybersecurity and automated policy enforcement into one edge device and provides a consistent and policy driven way to identify, isolate, encrypt and monitor every device and connection across legacy and new environments.

© 2018 – 2026 by Veea Inc. and its subsidiaries. All rights reserved.

See how SecureConnect Compares

	Fortinet FortiGate-50G-5G	Peplink Pepwave BR1 Pro 5G	Teldat Be.Safe Pro SSE	Veea SecureConnect
Zero-Trust Architecture No device connects without granting permission with the app.	✓	✗	✓	✓
Agentless Assesments All connected devices secured, without loading software on devices.	✗	✗	✗	✓
Edge Computing Able to run other secure apps on the same hub, such as CCTV.	✗	✗	✗	✓
Mesh Networking Full in-building WI-Fi coverage with seamless roaming.	✗	✗	✗	✓
IoT & Legacy Device Support All IoT devices secured by segmenting traffic and isolating threats.	✓	✓	✗	✓
DNS Filtering Blocks access to malicious sites at DNS-lookup stage before the client connects.	✓	✓	✗	✓
Continous Monitoring Security and connectivity run concurrently.	✓	✓	✓	✓

© 2018 – 2026 by Veea Inc. and its subsidiaries. All rights reserved.

Commercial Impact For Operators

SecureConnect enables operators to move beyond low-margin connectivity by introducing premium, security-enabled service bundles. These bundles increase average revenue per SMB while remaining cost-effective compared to traditional enterprise security solutions.

Churn Reduction

Churn reduction is a critical benefit. Security services embedded into the network create natural stickiness, increasing switching costs and reducing customer attrition.

Once security policies and operations are integrated, customers are far less likely to change providers.

Operational Efficiency

Operational efficiency improves through platform consolidation. SecureConnect reduces vendor sprawl, lowers support ticket volumes, and minimises on-site interventions.

Remote management and standardised deployments lower operational expenditure.

Future Monetisation

Finally, SecureConnect establishes a scalable platform for future monetisation, including IoT, analytics, compliance, and industry-specific digital services.

SecureConnect vs The Status Quo

Why the traditional SMB security model no longer scales.

Traditional SMB Security Model

- **Fragmented Security Stack:**
  Multiple vendors, separate consoles, inconsistent policies.
- **Manual Integration:**
  Custom configuration and on-site complexity.
- **MSSP Dependency:**
  Third-party reliance reduces operator control and margin.
- **Low Attach Rates:**
  Security treated as optional add-on.
- **Price-Driven Retention:** Limited switching friction.

veea SecureConnect™

- **Integrated Platform:**
  One device. One management layer.
- **Operator-Controlled:**
  Full lifecycle ownership and branding.
- **Scalable Deployment:**
  Standardised, plug-and-play architecture.
- **Built-in Monetisation:**
  Premium bundles with higher ARPU.
- **Structural Stickiness**
  Security embedded into daily operations.

The difference is not incremental. It is architectural.

	Traditional Model	SecureConnect
Deployment	Multi-vendor	Plug-and-play
Control	Limited	Operator-owned
Economics	Margin dilution	ARPU expansion
Scalability	Low	Designed for SMBs

© 2018 – 2026 by Veea Inc. and its subsidiaries. All rights reserved.

What's in it for you?

Veea is engaging network operators, ISP's and partners to explore commercial opportunities, define pilot programs while validating ARPU and retention impacts in real-world deployments.

SecureConnect is designed specifically for network operators to move beyond connectivity and capture greater value from the SMB markets. This unique pilot-first approach allows you to assess SecureConnect's commercial and operational value with minimal risk, while laying the foundation for a scalable deployment.

Contact Veea Sales to learn how you can start a SecureConnect pilot.

Visit www.veea.com/contact-us or mail us at sales@veea.com

Intelligently Connected™

Veea, Veea Logo, Veea Shield Logo, VeeaHub, vMesh and vTPN are registered trademarks of Veea Inc. Other trademarks and trade names are those of their respective owners. Arm and Cortex are trademarks or registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. Zigbee Alliance's trademarks and logos, and all goodwill associated therewith, are the exclusive property of the Zigbee Alliance. Thread Group, Thread, Built on Thread and Thread Certified Component word marks and logos, are registered and/or unregistered trademarks and service marks of Thread Group in the United States and/or other jurisdictions. Wi-Fi is a registered trademark of Wi-Fi Alliance®. The SD, SDHC, miniSDHC, microSDHC, SDXC and microSDXC Logos are trademarks of SD-3C LLC. Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries. Docker, Inc. and other parties may also have trademark rights in other terms used herein.

© 2018 – 2026 by Veea Inc. and its subsidiaries. All rights reserved.

Intelligently Connected™

Veea Inc. 164 E 83rd Street | New York, NY, 10028

sales@veea.com

© 2018 - 2026 Veea Inc. All Rights Reserved. Specifications subject to change without notice.
Veea and VeeaHub are trademarks of Veea Inc. All other trademarks and tradenames are the property of their respective owners.