

EncryptaGuard: Enterprise-Grade Managed Security for the Modern SMB

Author: Tanner Sutherlin, Founder & Lead Architect

Date: December 2025

Executive Summary

Most small businesses operate on "dirty" networks where critical operations share the same unencrypted space as guest traffic and employee distractions. EncryptaGuard is a "Drop-In" Secure Business Gateway that replaces vulnerable ISP defaults with a hardened, containerized security layer.

By optimizing **Time-to-Content (TTC)** and eliminating the "invisible weight" of trackers, EncryptaGuard provides a browsing experience that is up to 3x faster while physically isolating business assets from external threats.

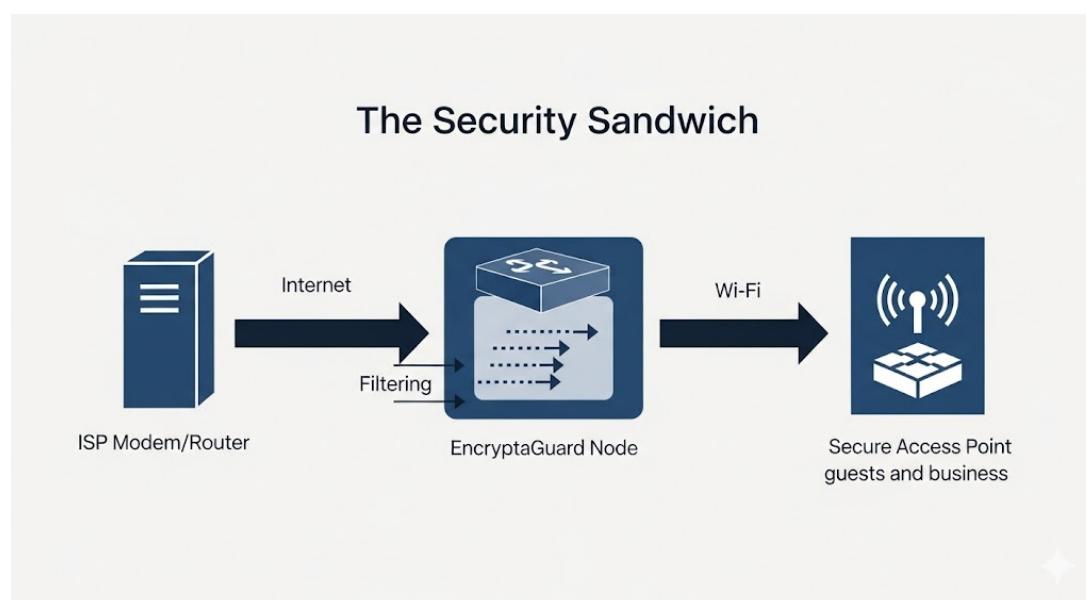
The Technical Architecture

1. Edge Computing Advantage

Unlike cloud-only filters that add latency, EncryptaGuard processing happens at the **Edge** on dedicated **Protectli Vault** hardware. This ensures zero latency increase and absolute data privacy, as filtering occurs on-premise before data ever leaves the building.

2. The "Security Sandwich" (Isolation Logic)

EncryptaGuard utilizes a physical isolation model. The node sits between the ISP Modem and a dedicated Secure Access Point (AP). This creates a "Security Sandwich" that prevents lateral movement—even if a guest device is compromised, it has no physical path to the core business network.



3. Hardware Specifications

- **Platform:** Protectli Vault (Fanless, Solid-State).
 - **Efficiency:** Industrial-grade components with ultra-low power consumption.
 - **Connectivity:** Multi-port physical separation (WAN/LAN/Management).
-

Operational Excellence

Zero-Trust Connectivity

EncryptaGuard nodes utilize an **outbound-only Tailscale VPN tunnel**. No ports are opened on the customer's firewall, keeping the internal network completely invisible to the public internet while allowing for 24/7 secure remote management.

The "Clean Pipe" Metric

By blocking ad and tracker telemetry at the gateway level, we physically prevent up to **20-40% of background "noise" data** from entering the network. This reclaims bandwidth for business-critical applications like VoIP and Point-of-Sale (POS) systems.

Data Privacy Compliance

EncryptaGuard is built on a "Privacy-First" philosophy. All DNS filtering happens on-premise. No user browsing traffic is sent to third-party clouds for analysis, ensuring 100% data sovereignty for the business owner.

Business Impact

- **Reclaimed Productivity:** Enforce a security baseline that blocks high-distraction services (TikTok, Netflix) at the network level.
 - **Reduced Liability:** Proactively block malware and phishing attempts before they reach employee devices.
 - **Managed Reliability:** 24/7 monitoring ensures your security layer is always up to date with the latest global threat intelligence.
-

Ready to secure your business? Visit www.encryptaguard.com or contact tanner.sutherlin@encryptaguard.com.