

ENCRYPTAGUARD LLC: STRATEGIC INFRASTRUCTURE & PERFORMANCE-OPTIMIZED EDGE SECURITY

Founder & Lead Architect: Tanner Sutherlin

Executive Summary

In an increasingly complex threat environment, small and medium-sized enterprises (SMEs) are frequently compromised due to a reliance on vulnerable ISP defaults. Standard configurations often lack the necessary encryption and filtering required to protect sensitive data streams and maintain high-performance connectivity. **EncryptaGuard LLC** provides a "Drop-In" Managed Edge Gateway that integrates a hardened, hardware-based security layer into existing infrastructure.

Our architecture prioritizes **On-Premise Edge Processing** and **Outbound Privacy** to deliver a secure, high-speed network environment with zero data sovereignty compromise.

Core Security Framework

EncryptaGuard LLC establishes a standardized security posture through three foundational pillars.

1. In-Line Traffic Hardening

We implement an **In-Line Security Architecture**, positioning our gateway as a dedicated intermediary between the ISP Modem and the Internal Router. This ensures that all traffic is filtered and encrypted at the hardware level before it enters or leaves the core business network, securing the internal environment against unauthorized data collection.

2. Bandwidth Reclamation & Telemetry Suppression

By neutralizing background telemetry, trackers, and "invisible weight" at the gateway level, we reclaim significant bandwidth for production-critical applications. This centralized policy enforcement allows mission-critical services to operate on clean, high-priority paths, providing a browsing experience that is up to **3x faster**.

3. Managed Resilience & Lifecycle Management

Modern network defense requires continuous adaptation. Our managed nodes utilize 24/7 health monitoring and automated, "Zero-Touch" security patching. This ensures that every deployment remains resilient against emerging global vulnerabilities without requiring manual intervention or specialized IT staff on-site.

Technical Specifications & Architecture

High-Performance Edge Computing

To maintain absolute data privacy, all security processing occurs locally at the **Network Edge** on industrial-grade **Protectli Vault** hardware running hardened Ubuntu. Unlike traditional cloud-based filters that introduce latency and route sensitive metadata through third-party servers, EncryptaGuard ensures that all filtering decisions are made on-premise.

Encrypted Outbound-Only Management

Fleet integrity is maintained via **Outbound-Only Encrypted Tunnels**. By utilizing a WireGuard-based mesh architecture, the internal network remains entirely invisible to the public internet, as no inbound ports are ever opened on the primary firewall.

Operational Standards

- **Hardware:** Fanless, solid-state industrial appliances with dedicated multi-core processing.
 - **Data Integrity:** All DNS requests are encapsulated via **DNS-over-HTTPS (DoH)** to prevent ISP-level snooping.
 - **Privacy:** On-premise processing ensures zero-logging of internal browsing behavior by external entities.
-

Strategic Consultation

EncryptaGuard LLC provides a sophisticated defense-in-depth solution for businesses that prioritize uptime, speed, and privacy.

Contact for Technical Assessment: Visit www.encryptaguard.com or connect with our engineering team via [LinkedIn](#) for a strategic consultation regarding your unique network environment.

**Secure Your Edge with EncryptaGuard LLC Hardened Architecture. Enterprise-Grade Privacy.
Professionally Managed.**