

EncryptaGuard: Proof of Value & Risk Mitigation Report (2026)

1. The Executive Summary: The Invisible \$3.31 Million Threat

In 2026, the average cost of a data breach for a small business has surged to **\$3.31 million**. While many business owners believe they are "too small to target," small to medium enterprises (SMEs) actually account for **43% of all cyberattacks** annually.

The stakes are terminal: **60% of small businesses close their doors permanently within six months** of a significant cyber incident. EncryptaGuard is not just a hardware upgrade; it is a **Liability Shield** designed to physically isolate your business from these existential threats.

2. The Direct Cost of a Breach (Small Business Baseline)

When a breach occurs, the government investigates the crime, but the business pays for the recovery. Taxpayer money does not cover the private forensic and legal costs required to get your business back online.

Category	Estimated Cost (SME)	Impact Description
Forensic Investigation	\$15,000 – \$30,000	Mandatory private audit to prove the scope of the breach to insurers and regulators.
Ransomware Recovery	\$25,000+	Cost to extract, restore, and verify lost data, even if a ransom isn't paid.
Legal & Defense Fees	\$50,000 – \$100,000	Average litigation costs as nearly every breach now triggers customer lawsuits.
Revenue Loss	\$8,000 – \$20,000 / Day	Direct lost sales and employee downtime during system restoration.

3. The Regulatory Nightmare: Virginia (VCDPA)

Operating in Virginia carries specific legal liabilities under the **Virginia Consumer Data Protection Act (VCDPA)**. Failing to maintain "reasonable" security practices can lead to devastating civil penalties.

- **The \$7,500 Multiplier:** The Virginia Attorney General can impose fines of up to **\$7,500 per individual violation**.
 - **Exposure Calculation:** For a local office with just **500 client records**, a single breach could represent a theoretical liability of **\$3.75 million** in regulatory fines.
 - **Mandatory Notification:** Virginia law requires businesses to notify every affected resident "without unreasonable delay." The global average cost for breach notification alone is **\$390,000** per incident.
-

4. Operational ROI: Recovering the "Invisible Weight"

Beyond security, EncryptaGuard pays for itself by optimizing your existing infrastructure and labor.

Bandwidth Recovery

Modern trackers and advertising scripts "steal" up to **40% of your bandwidth** for background telemetry. EncryptaGuard physically removes this weight at the edge, handing you back the full value of the internet speeds you are already paying for.

Productivity Gains

Minor technical lags—slow app loads, DNS hangs, and "spinning wheels"—cost employees an average of **10–15 minutes per day**.

- **For a 10-person firm:** This is **~40 hours of lost labor per month**.
- **The Solution:** Our RAM-cached edge processing serves your most frequent requests instantly, delivering a browsing experience up to **3x faster**.

5. The EncryptaGuard Advantage

We replace the "Open Door" of standard ISP routers with a **Hardened Gateway Layer**.

1. **Physical Isolation:** We sit between your modem and your access point, creating a physical barrier that prevents "lateral movement." Even if a guest's device is compromised, it has no physical path to your core business data.
2. **Invisible Presence:** Using an outbound-only **VPN tunnel**, your network becomes invisible to hackers scanning the public internet. A hacker cannot attack what they cannot find.
3. **Insurance Readiness:** Comprehensive edge security and microsegmentation can reduce your cyber insurance premiums by **15% to 30%**.

Lead Engineer: Tanner Sutherlin **Website:** www.encryptaguard.com