One Lock Is No Longer Enough

There's encryption and then *there's encryption.*

Layered Encryption available only with BeachheadSecure®

01

LEAST ACCESS PRIVILEGE
Ensure Your Company's Crown Jewels Are Only 'Need-to-Know'

Imagine giving everyone in your company a master key to all data. Risky, right? That's exactly why least-privilege access (also called *data segmentation*) is so crucial. It ensures employees only access what they need to do their job—nothing more. Joe from Accounting shouldn't see HR files, and IT admins shouldn't be able to read your CEO's emails. This approach reduces security risks *and* complies with regulations/security requirements as specified in The FTC Safeguards Rule, CMMC 2.0, HIPAA, ISO 27001, NIST 800-171 and many others. Remember: when it comes to data access, less is more.

02

NETWORK ATTACKS
Are Only a Matter of 'When'

Every day, 1 in 200 PCs faces a network attack. System-level encryption alone isn't enough; when an authorized user logs in, all data becomes vulnerable. BeachheadSecure's layered encryption thwarts *even successful* system-level breaches. Our RiskResponder sentinel stops brute force attacks before they penetrate your defenses. Don't let your data be ripe for the taking.' With BeachheadSecure, you're protected against that 0.5% daily attack rate, keeping your sensitive information safe from threat actors who breach your firewall or infiltrate an unsecured wifi.

03

RANSOMWARE 2.0
The Growing Threat of Data Exfiltration

Modern ransomware attacks aren't just about locking you out. Threat actors are smart, and exfiltrate data *before* encryption—threatening exposure if demands aren't met. This leads to reportable breaches, exposed secrets, financial losses, fines, and damaged reputation. Even if you recover from backups, stolen data remains a risk. BeachheadSecure's unique layered encryption protects your data even if it's exfiltrated, preventing unauthorized access. Don't let your sensitive information become a bargaining chip - secure it at every level.

BEACHHEAD