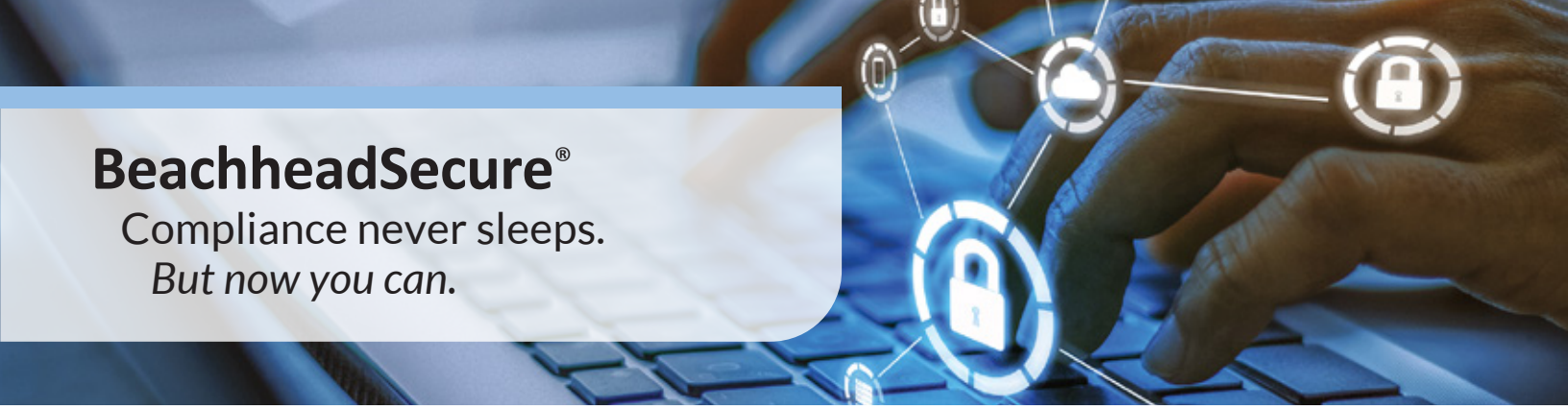


BeachheadSecure®

Compliance never sleeps.
But now you can.

Your data. Your control. No exceptions. BeachheadSecure's 68 advanced access and security controls don't just protect your data—they prove it with audit-ready documentation and reporting for CMMC levels 1 & 2, HIPAA, FTC Safeguards, CIS, ISO 27001, NIST CSF, PCI and 800-171. More than 800 compliance requirements, automatically enforced and instantly provable.

Modern compliance demands complete control.

Today's compliance requirements demand more than the basics. AV, encryption, and firewalls? They're now table stakes. CMMC, HIPAA, FTC Safeguards and other mandates require extensive controls to not only address the latest malware but also address data exposure from stolen devices, insider risks, poor security hygiene, and unauthorized access. BeachheadSecure doesn't just check boxes. It *actively* manages and documents every security measure, proving your holistic protection is working 24/7.

Encryption that protects against today's (and tomorrow's) threats

Why layer encryption? Because attackers don't quit. BeachheadSecure's layered encryption on Windows PCs blocks both network-borne attacks and data exposure. With 70% of ransomware payments now going toward preventing a threat-actor from exposing the victim-firm's exfiltrated data (per HHS reports), this protection isn't optional. (Or said another way: you can't afford not to have it.) Our layered approach shrinks your threat surface and enforces least-privilege access—exactly what today's compliance frameworks require.

Automatic defense, 24/7

Control your data anywhere, automatically. Our built-in RiskResponder® technology watches your PCs and Macs 24/7, monitoring for any compliance-critical threat behaviors or environmental anomalies. It spots and reacts to risks (geofence isolations, invalid login attempts, etc.) before they become compliance violations. Responses are pre-set, automatic, and instant based on your customized preferences—from subtle user warnings, to alerting staff, to complete data lockdown. No manual monitoring. No delayed response. Just constant protection that moves as fast as threats do.

A proven path to proven compliance.

Turn security requirements into verifiable compliance. BeachheadSecure's advanced encryption, MFA and comprehensive remote access controls to address emerging and more heavily enforced compliance requirements. With 68 security controls actively protecting and documenting your business, you'll prove your compliance status at every audit. Ready to see it in action? Let's set up your evaluation today.

A comprehenisve & holistic approach to security

PCs & Mac	Security	Description
COMPLIANCE CONTROLS	68 Required Compliance Controls	BeachheadSecure provides 68 software controls that satisfy over 800 security control numbers of CMMC Level 1 & 2, FTC Safeguards, HIPAA and several others
COMPLIANCE REPORTING	Documentation of Compliance Posture	ComplianceEZ™ 1.0 maps BeachheadSecure to each compliance mandates control number requirements. Compliancy report is audit-worthy evidence of compliance when device is lost/stolen
ENCRYPTION	Superior Encryption Management	System-level and user-level "layered" encryption protects data from network-borne attacks and may be the only protection available to secure "exfiltrated" data. System-level encryption (Filevault) avail with Mac OS only
REMOTE ACCESS CONTROL	Manual Access Controls (Remote data) "quarantine" or wipe	Push button remote data access control from the console (quarantine is recoverable, wipe is permanent).
MFA	MFA (Multi-factor authentication)	QR code-based prompt for authentication app scan (Mac and Windows)

A comprehenisve & holistic approach to security

PCs & Mac	Security	Description
RiskResponder®	RiskResponder Automatic Access Controls	Monitors environmental & behavioral risk conditions and will trigger pre-determined threat mitigation responses appropriate for the level of risk. • Invalid logon attempts • Time out-of-contact • GeoFence perimeter violations • Network-borne attacks • Security Software tampering
ASSET TRACKING & GEOFENCING	GeoTracking/ GeoFence	Track devices worldwide with automatic RiskResponses™ as they travel beyond acceptable boundries
USB STORAGE + ENCRYPTION + AUTHENTICATION	USB Storage Encryption, Authentication & Full Access Control	Enforces 256K AES encryption, USB authentication policy (several) and provides ability to quarantine or kill.
WINDOWS SECURITY	Windows Security Management	Manage MS Defender individually or schedule "Layered" Defender scans in addition to chosen AV tool. Windows Firewall Windows Controlled Folders

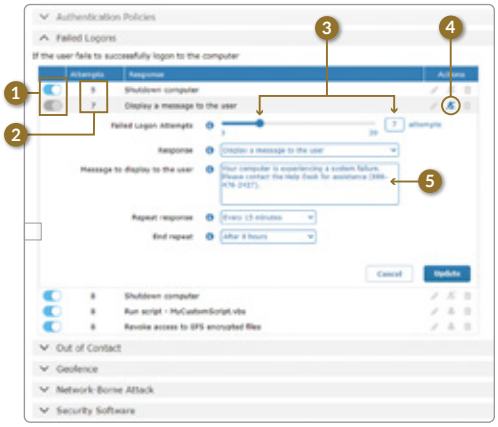
Phones & Tablets	Security	Description
ENCRYPTION	Encryption Management	Enforcement of native encryption
REMOTE ACCESS CONTROL	Manual Access Controls (Remote data) "quarantine" or wipe	Push button remote data access control (quarantine is push-button recoverable, wipe is permanent).
AUTHENTICATION	Authentication & Access Controls (password policy enforcement controls)	Data is encrypted behind authentication. Enforce password length, strength, frequency and device lock-out.

Window Server	Security	Description
ENCRYPTION & MFA	Encryption & Authentication Control	System-level encryption (Bitlocker) with MFA

Anatomy of a RiskResponder (Failed Logons)

Our RiskResponder is your "eyes and ears" across your client's entire inventory of PCs and Macs. Beyond just monitoring environmental and behavioral risks, it *automatically mitigates* threats with responses appropriate to the level of risk, 24/7/365. Compliance never sleeps—but you can.

Creating/editing automated response to display ***custom user message*** *at 7 consecutive invalid logon attempts*



1. Is the Responder *ON* or *OFF*
2. Risk threshold that triggers the automated response
3. Easily set the risk threshold where the response is triggered
4. Determine whether an alert(s) is sent to designated recipient(s)
5. Flexible, customizable messages to user

Creating/editing automated response to ***revoke data access*** *at 8 consecutive invalid logon attempts*

6. Selected Response - in this case user will not be able to access PC data after 8 consecutive invalid logon attempts
7. Determine whether an alert(s) is sent to designated recipient(s)

Report & Document with ComplianceEZ™ (version 1)

Using the NIST Cybersecurity Framework (CSF) for guidance, our ComplianceEZ v1.0 maps 68 BeachheadSecure controls to 800+ requisite controls across NIST 800-171, CIS, PCI DSS, ISO 27001, HIPAA and the FTC Safeguards Rule. Augment your compliance expertise with tools that don't just "check compliance boxes"—they enable you to actively manage and document every security measure for those – like you – who demand a superior security posture.

BEACHHEAD

For more information call
408.496.6936 x.2 or email
sales@beachheadsolutions.com