BeachheadSecure® for MSPs

ComplianceEZ®: Your New Competitive Edge in Compliance-as-a-Service

BeachheadSecure gives MSPs a clear way to differentiate by delivering real compliance-as-a-service—without hiring compliance specialists or adding operational overhead. It's the only platform that both manages and documents 68 technical controls required across today's major frameworks. With ComplianceEZ built in, you can centrally manage your clients' PCs, Macs, phones, tablets, USB devices, and servers while supporting CMMC Levels 1 & 2, HIPAA, FTC Safeguards, CIS, ISO 27001, NIST CSF & 800-171, PCI DSS, and more.

More than 800 requirements are automatically enforced, continuously monitored, and fully documented. You're alerted the moment something drifts out of compliance, and you can produce audit-ready reports whenever needed—helping you maintain your role as a trusted, consultative partner.

Give Your Clients What Modern Compliance Really Requires

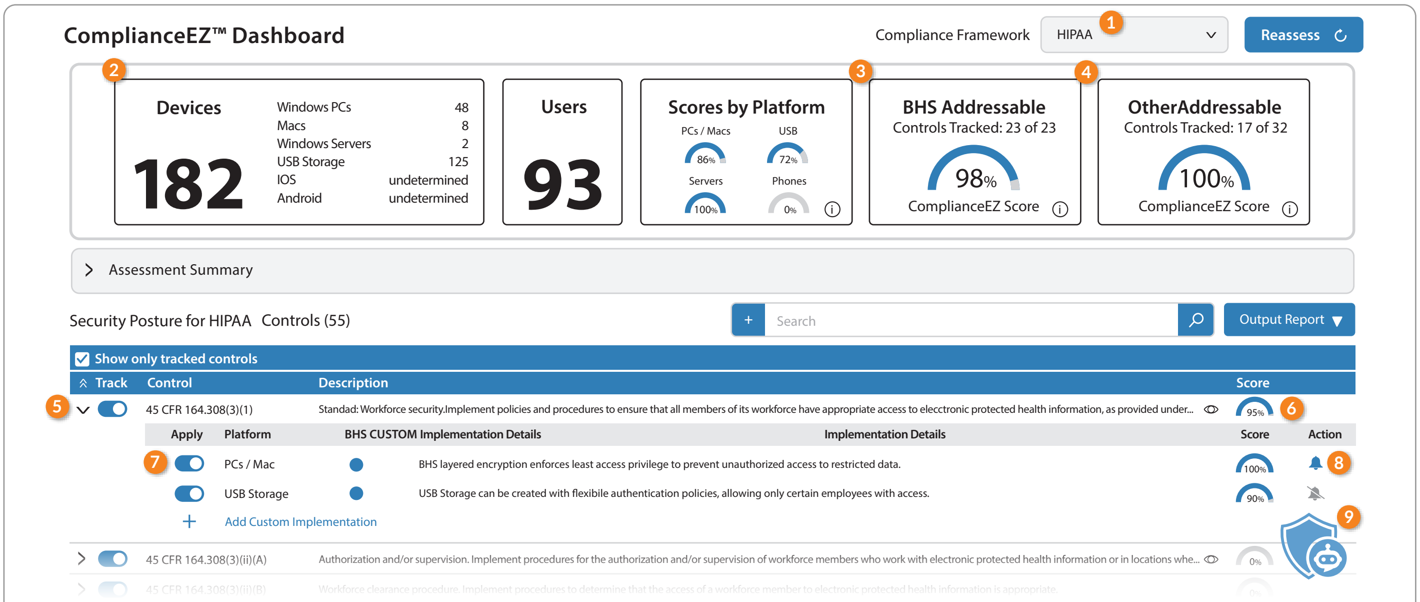
Most customers think AV, encryption, and firewalls equal "security." For compliance, those basics are just the starting point. Today's regulations demand controls that address stolen or lost devices, insider threats, poor security hygiene, unauthorized access, and the full range of data-exposure risks. BeachheadSecure lets MSPs show they're covering all of this—while quietly managing and documenting each control in the background. It's a simple way to raise the value of your security offering and clearly stand apart from competitors.

ComplianceEZ: Built-In Expertise You Can Deliver as a Service

ComplianceEZ makes compliance understandable and actionable. It explains each requirement in plain language, shows exactly how BeachheadSecure satisfies it, and includes an AI chatbot focused exclusively on compliance questions. It automatically maps and scores 68 BeachheadSecure controls and lets you document any additional tools or processes you rely on. The result is a complete, auditable compliance program across the devices and data you're already managing.

With round-the-clock monitoring, instant alerts, and on-demand reporting, you can walk into any QBR, audit, supply-chain questionnaire, or cyber-insurance renewal with confidence—and a service you can easily monetize.

Anatomy of ComplianceEZ



ComplianceEZ™ Dashboard

Compliance Framework: HIPAA (1)

(2) Devices 182

Windows PCs	48
Macs	8
Windows Servers	2
USB Storage	125
IOS	undetermined
Android	undetermined

Users 93

(3) Scores by Platform: PCs / Macs 86% · USB 72% · Servers 100% · Phones 0%

(4) BHS Addressable — Controls Tracked: 23 of 23 — 98% ComplianceEZ Score

OtherAddressable — Controls Tracked: 17 of 32 — 100% ComplianceEZ Score

› Assessment Summary

Security Posture for HIPAA Controls (55)

☑ Show only tracked controls

Track	Control	Description	Score
(5) ●	45 CFR 164.308(3)(1)	Standad: Workforce security.Implement policies and procedures to ensure that all members of its workforce have appropriate access to elecctronic protected health information, as provided under...	95% (6)

Apply	Platform	BHS CUSTOM Implementation Details	Implementation Details	Score	Action
(7) ●	PCs / Mac	●	BHS layered encryption enforces least access privilege to prevent unauthorized access to restricted data.	100%	🔔 (8)
●	USB Storage	●	USB Storage can be created with flexibile authentication policies, allowing only certain employees with access.	90%	
+	Add Custom Implementation				

Track	Control	Description	Score
●	45 CFR 164.308(3)(ii)(A)	Authorization and/or supervision. Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations whe...	0%
●	45 CFR 164.308(3)(ii)(B)	Workforce clearance procedure. Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	0%

(9)

1. Chosen compliance mandate/framework. Others include CMMC Levels 1 & 2, CIS, FTC Safeguards, NIST CSF & 800-171, Cyber Essentials, PCI DSS, and ISO 27001.
2. Device numbers for this account.
3. Controls that Beachhead can satisfy (tracked & automatically documented).
4. Controls not satisfied by Beachhead but can be documented as part of comprehensive compliance posture.
5. List of all controls for chose compliance mandate/framework. HIPAA includes 55 total Technical Control requirements.
6. Total score is an accumulation of all platform scores that are tracked.
7. Platform that a BeachheadSecure offers that can address a control requirement automatically document for BHS, manually documented for other vendor tools.
8. Alert on/off. Alerting & instruction when compliance falls below selected threshold.
9. AI Chatbot for more information on compliance frameworks and BeachheadSecure capabilities.

Layered Encryption: Ransomware Protection Your Customers Can't Ignore

BeachheadSecure gives you a unique advantage: a layered encryption architecture for Windows PCs that most competitors simply can't match. With 70% of ransomware payments now driven by threats of leaking or selling exfiltrated data, twice-encrypted data will render it inaccessible. BeachheadSecure enforces Least Access Privilege, a requirement for most compliance frameworks and with ComplianceEZ you'll be able to document client compliance . Whether a device is on-network or not, protection stays fully enforced—making you the MSP who can actually prove your clients' data is safe.

RiskResponder®: Set-and-Forget Threat Response for MSPs

RiskResponder watches your clients' devices 24/7 for behaviors and conditions that matter to compliance. From geofence violations to repeated bad logins to network-borne attacks, RiskResponders respond immediately to mitigate the threat and assure compliance. That might mean showing a user warning, sending alerts back to your helpdesk team, or locking down data entirely—all automatically. No manual monitoring. No chasing issues after the fact. Just continuous, automatic protection that lets you deliver premium security without increasing your workload.

Where Security Meets Compliance

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	Automatically mapping and scoring all 68 BHS controls, ComplianceEZ also lets you document and manage additional controls outside the BeachheadSecure platform—creating a complete, auditable compliance picture. With 24/7 monitoring.
ENCRYPTION	Where Security meets Compliance	System and user-level encryption on Windows PC protects exfiltrated data from exposure and meets today's compliance standards.
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)	Supports both OTP/authenticator applications AND FIDO2 hardware for PCs & Macs.
RiskResponder®	RiskResponder Automatic Access Controls	Monitors environmental & behavioral risk conditions and will trigger pre-determined threat mitigation responses approprate for the level of risk. • Invalid logon attempts • Time out-of-contact • GeoFence perimeter violations • Network-borne attacks • Security Software tampering

Where Security Meets Compliance

PCs & Mac	Security	Description
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

Set Yourself Apart—and Stay Ahead of Customer Expectations

With BeachheadSecure and ComplianceEZ, MSPs gain an easy, scalable way to offer compliance-as-a-service, strengthen client relationships, and keep customers ahead of rising regulatory and insurance requirements. You're not just providing another tool—you're delivering confidence, expertise, and proof of protection your clients can't get anywhere else.

BEACHHEAD

For more information call
408.496.6936 x.1004 or email
channelteam@beachheadsolutions.com