<BeachheadSecure®> by <your name>

Compliance demands around-the-clock vigilance.

Our solutions let you rest easy.

Compliance is just one of our many differentiators and why <your name> isn't just like every other MSP out there. With 68 advanced access and security controls, we don't just protect your data, we prove our value 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.

Basic security doesn't satisfy new compliance demands

Anti-virus, encryption, and firewalls? Table stakes everybody offers and insufficient on their own. Today's compliance-focused businesses require more—comprehensive protection against stolen devices, insider risks, poor security hygiene from employees, unauthorized access, and more. <BeachheadSecure> doesn't just check boxes. It enables us to actively manage and document every security measure, proving we're providing you with holistic protection 24/7.

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

Why layer encryption? Because attackers don't quit. <BeachheadSecure> 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 a targeted business'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 24/7/365: preset risk responses for whatever comes next

Monitor and respond to every potential threat, automatically. Our built-in <RiskResponder®> technology watches 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—from subtle user warnings, to alerting staff, to complete data lockdown—based on the customized preferences that are right for your organization. No manual monitoring. No delayed response. Just constant protection that moves as fast as threats do.

We don't match other MSPs—we set the new standard for comprehensive, compliance-focused managed security

<BeachheadSecure's> advanced layered encryption, MFA, and comprehensive remote access controls address emerging compliance demands that basic MSPs can't touch. With 68 security controls actively protecting and documenting your businesses, we prove our premium value at every audit. Contact us to learn more about how we can transform your security posture.

A comprehenisve & holistic approach to security

PCs & Mac	Security	Description
HIPAA 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 approprate 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

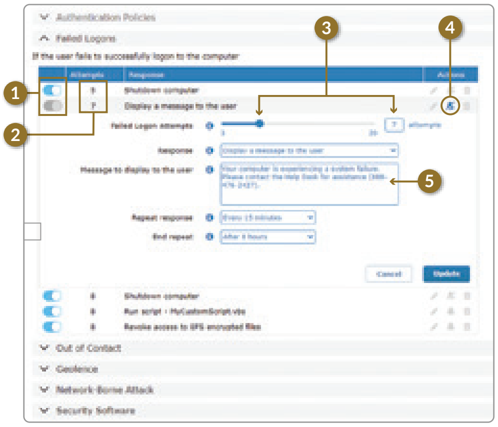
Phones & Tablets	Security	Description
ENCRYPTION	Encryption Management	Enforcement of native encryption
REMOTE ACCESS CONTROL	Manual Access Controls (Remote data) "quarantine" or wipe	Push button remote data access control (quarantine is push-button recoverable, wipe is permanent).
AUTHENTICATION	Authentication & 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 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. We understand that today's security demands a holistic approach. Compliance never sleeps—but you can.

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



Authentication Policies
Failed Logons
If the user fails to successfully logon to the computer

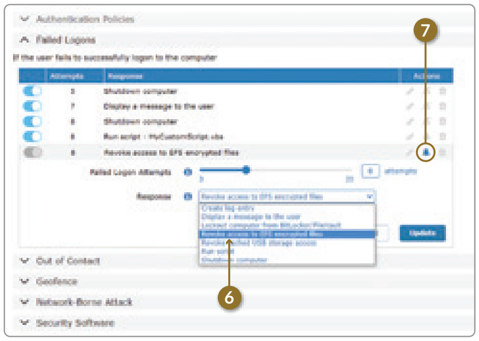
	Attempts	Response	Actions
●	5	Shutdown computer	
○	7	Display a message to the user	

Failed Logon attempts: 7 attempts
Response: Display a message to the user
Message to display to the user: Your computer is experiencing a system failure. Please contact the Help Desk for assistance (888-876-2437).
Repeat response: Every 15 minutes
End repeat: After 8 hours

	Attempts	Response	Actions
●	8	Shutdown computer	
●	8	Run script : MyCustomScript.vbs	
●	8	Revoke access to EFS encrypted files	

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*



Authentication Policies
Failed Logons
If the user fails to successfully logon to the computer

	Attempts	Response	Actions
●	5	Shutdown computer	
●	7	Display a message to the user	
●	8	Shutdown computer	
●	8	Run script : MyCustomScript.vbs	
○	8	Revoke access to EFS encrypted files	

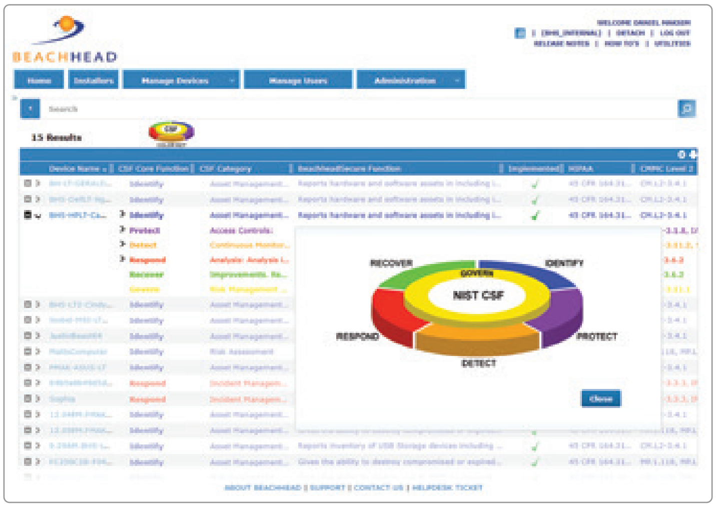
Failed Logon Attempts: 8 attempts
Response: Revoke access to EFS encrypted files

Create log entry
Display a message to the user
Lockout computer from BitLocker/Filevault
Revoke access to EFS encrypted files
Revoke/limited USB storage access
Run script
Shutdown computer
Update
Out of Contact
Geofence
Network-Borne Attack
Security Software
6
7

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. <Your name> doesn't just "check boxes"—we actively manage and document every security measure for you, whether your regulated or just demanding a higher security posture.



<Your Logo>

For more information:
call 123.456.7890
info@your_url.com