BeachheadSecure® for MSPs
Compliance never sleeps.
But you and your clients can.

Make compliance your competitive differentiator. BeachheadSecure for MSPs' 68 advanced access and security controls don't just protect your clients' data—they prove your 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 to every client.

**All things mobile.
BeachheadSecure**

Phones

Servers

Tablets / Pads

PCs & Laptops

Macs

USB Drives

Basic security won't satisfy new compliance demands

The days of winning clients with basic security services are all but over. AV, encryption, and firewalls? They're now table stakes that everybody offers. Today's compliance-focused clients require more—comprehensive protection against stolen devices, insider risks, poor security hygiene, unauthorized access, and more. BeachheadSecure for MSPs doesn't just check boxes. It enables you to actively manage and documents every security measure, proving your holistic protection is working 24/7.

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

Why layer encryption? Because attackers don't quit. BeachheadSecure for MSPs' 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: your clients 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 that makes it easy to showcase your value

Monitor every client 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 you and your client agree on. No manual monitoring. No delayed response. Just constant protection that moves as fast as threats do.

Build a premium practice

Stop competing on price. Start winning on value. While other MSPs offer basic security packages, BeachheadSecure for MSPs lets you

deliver and document comprehensive protection that compliance-focused clients demand. Every feature—from layered encryption to automated responses—proves you're not just another MSP. You're a security and compliance leader that is ready for tomorrow's threats.

A proven path to MSP leadership

Transform security requirements and compliance into long-term client value. BeachheadSecure for MSPs' advanced 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 clients' businesses, you'll prove your premium value at every audit. Ready to stand out? Your free evaluation starts 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).

A comprehensive & holistic approach to security

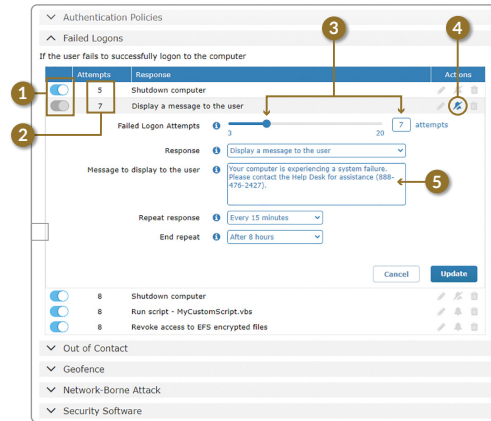| PCs & Mac	Security	Description
MFA	MFA (Multi-factor authentication)	QR code-based prompt for authentication app scan (Mac and Windows)
RiskResponder®	RiskResponder Automatic Access Controls	Monitors environmental & behavioral risk conditions and will trigger pre-determined threat mitigation responses 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

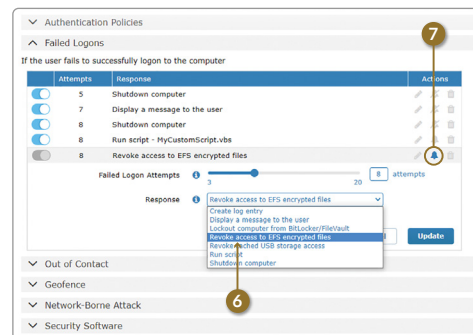## Anatomy of a RiskResponder (Failed Logons)

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. Share this capability with clients to prove you're a cut-above-MSP who understands that today's security demands a holistic approach. Compliance never sleeps—but you and your clients 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)
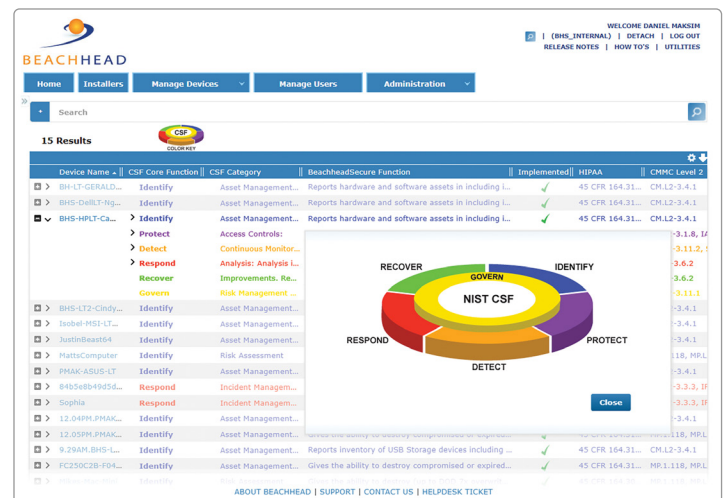5. Flexible, customizable messages to user

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. Distinguish your practice with built-in compliance expertise and tools that don't just "check boxes"—they enable you to actively manage and document every security measure for regulated clients or those demanding a higher security posture.