BeachheadSecure® PCs & MACs

Advanced Security for Windows & Mac PCs

Layered encryption, remote & automatic access-control for compliance and true PC data security

now includes Windows Security Management 10.2022

BeachheadSecure is an advanced web-based platform that makes it simple to enforce and manage encryption and access control on remote Windows & Mac PCs, USB Storage, Phones & Tablets and Windows Servers. BeachheadSecure protects organizations against insider risk, poor user security hygiene, compliancy violations and lost & stolen devices.

Encryption is just the beginning: RiskResponder measures & immediately responds to risk events as they happen

Encryption must be easy to manage and enforced under all conditions. You also need to be able to prove encryption is in place in the event that a device is lost, stolen or otherwise compromised. While encryption should be a cornerstone of your security strategy, it alone cannot protect data in circumstances where user credentials are compromised. Insider risk, lost credentials, and poor security hygiene all can undermine the best cybersecurity practices. Therefore, it's critical that you control access to sensitive data on PCs and Macs – remotely and instantly. With the BeachheadSecure administration console, you can do so with a simple button push. Or better yet, let BeachheadSecure's RiskResponder® measure risk in real-time and protect data instantly and automatically with pre-determined responses if risk exceeds acceptable thresholds – even when no one's looking.

RiskResponder: a deeper dive

Ransomware has brought to light the importance of a robust cybersecurity posture but, sadly, ransomware alone isn't the only threat to your data. Insider risk, former employees with malicious intent, compliancy violations, data exfiltration, compromised credentials and lost & stolen devices are all dangerous threats. Each of these vectors presents the possibility of business disruption, compliancy violations and data exposure. RiskResponder lets you determine when a PC's environmental or behavioral conditions constitute a risk, and allows you to pre-determine the appropriate and automatic countermeasure(s) as that risk escalates. Depending on the risk factors, these customized responses can range from simple notifications to your IT team, to a customizable message to the user, to complete and immediate revocation of access to your sensitive data. This risk assessment and deployment of pre-determined countermeasures will happen automatically and immediately, before members or your team (or even a SOC) has any clue there's a problem, 24/7/365. RiskResponder is your eyes and ears into the security conditions of your inventory of PCs and Macs, wherever they may be.

BeacheadSecure currently includes RiskResponder safeguards for addressing the following issues:

- ***Consecutive Invalid Logins:*** May suggest brute force or socially engineered attacks on device credentials
- ***Out of Contact:*** The device is no longer checking in, suggesting hardware is in unauthorized hands
- ***GeoFence Perimeter Violations:*** The device has moved outside of acceptable preset boarders
- ***Network-Borne Attacks:*** Unauthorized sites are attempting to access PC data
- ***Security Software Tampering:*** Unauthorized changes to local security tools (e.g. firewall, AV, encryption)

Beachhead will continue to build RiskResponder safeguards. What other PC environmental or behavioral conditions concern you? We'd love to hear your thoughts.

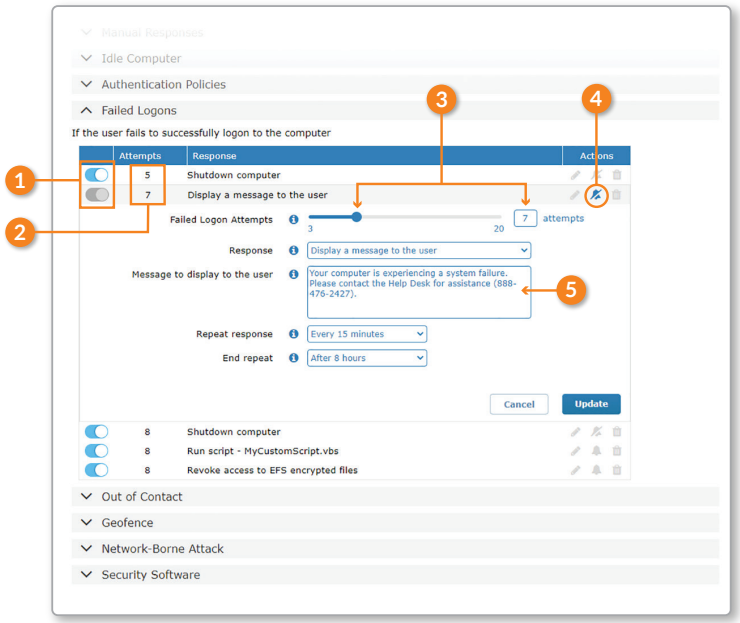
Currently-available automated responses/countermeasures for meeting any level of risk include: logging the event, sending alert(s) to IT team member(s) or security vendors, running a script, displaying a message to the PC user, shutting the computer down and removing the user's access to data (both at the file level and with lockout from BitLocker). Once a risk is removed, recovery to normal PC operation is achieved with literally a button push on the administration console.

2FA (Two-Factor Authentication)

Optionally, BeachheadSecure includes an enforceable 2FA (two-factor authentication) during the Windows boot process. A QR code is generated by the BeachheadSecure agent, which can be scanned by your preferred mobile security authentication application (e.g. Google, Microsoft Authenticator). The application will generate a pin code that is required at the PC boot screen. This second verification provides assurance that only authorized users will access your PC and its sensitive data!

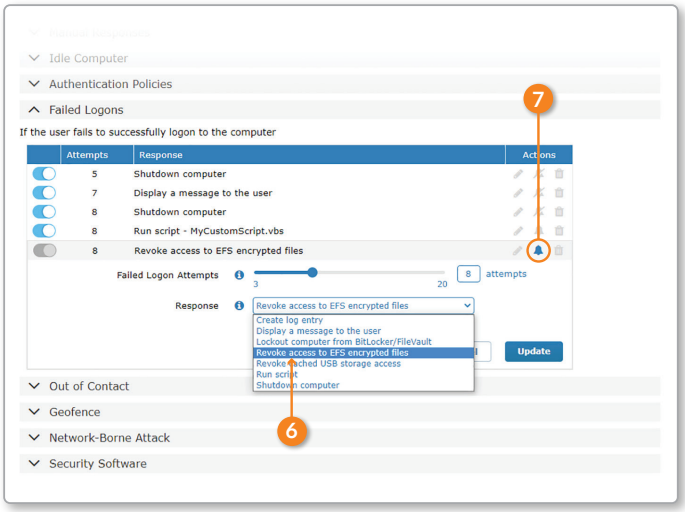
Anatomy of a RiskResponder (Failed Logons)

*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)

Protection for USB Storage Devices: Extended Encryption, Authentication Policy, Visibility and Access Control

Intimately coupled with PC & Mac security is the ability to enforce security policy to USB devices plugged into PCs. BeachheadSecure USB Storage will enforce encryption and an authentication requirement for any storage device holding your sensitive data. An installed communications module provides you with visibility and complete access control over that device, including the ability to deny access or kill compromised data. Flexible authentication settings will allow local authentication (user name & password), or require authentication to your administration console, giving you the ability to revoke authentication at any time. Flexible settings allow for credential caching, waiver of authentication requirements under certain circumstances, and much more. Backed by these features, BeachheadSecure USB Storage is the ultimate extension of data security on external devices.

Failure-to-Prove is failure-to-comply

Encryption must be proven to be in place at the time of the hardware compromise, or else it's not in compliance. Beachhead includes comprehensive reports that can be automatically generated at prescribed times and sent to designated recipients. The Compliancy Report, designed with input from some of the industries most knowledgeable compliancy experts, gives you the ability to produce an audit-worthy report with all the information necessary for demonstrating absolute compliance. While you may have lost hardware, you haven't allowed a breach. Now you can prove it!

Innovative from the cloud down

BeachheadSecure was the first, and still remains the most, comprehensive platform for addressing PC, USB, and device data security. BeachheadSecure either satisfies or partially satisfies 76% (69) of the entirety of the NIST Cybersecurity Framework requirements.

The best PC encryption and access control platform just got better. *Now manage Windows Security account-wide from BeachheadSecure!*

Centrally manage Windows Security tools like Defender, Controlled Folders and Firewall through Beachhead's Administration Console - at no additional cost! Defend your organization against virus, malware and ransomware threats with BeachheadSecure as a stand-alone option or layered with another Advanced Threat Protection (ADP) tool for even greater protection. Coupled with Beachhead's RiskResponder and you'll have nearly unlimited response options appropriate for every level of risk.

Protect your business with first-in-class data security

BeachheadSecure PCs & Macs protects your devices and crucial data with the only web-based security platform able to enforce encryption and security policy. Factoring in RiskResponder's fully-included automated threat mitigation and Compliancy Report for provable audit-proof compliance, BeachheadSecure safeguards your business from just about every device-based risk attackers might throw at it.

BEACHHEAD

For more information call
408.496.6936 or email
info@beachheadsolutions.com