BEACHHEAD
Whitepaper

Defend Data and Devices with Automatic Threat Responses Customized to Risk Severity

Using BeachheadSecure's RiskResponder® For Preemptive Security 24/7/365

October 2021

The breadth of threat vectors with the potential to compromise a company's systems and data continues to accelerate. Nothing less than truly comprehensive device security is effective to avoid crippling breaches and their devastating consequences. In today's world, this means leveraging modern solutions that can detect threats as they happen and deliver proactive, automated and immediate risk mitigation responses. Comprehensive security also means adopting zero trust practices to account for attackers who have gained control of a device, or in situations where a device's employee user may have evolved into an insider threat.

While many security products report on risk incidents, the damage is usually already inflicted by the time a manual investigation begins. Businesses require solutions fully capable of invoking accurate, automatic, and immediate risk mitigation procedures in response to active threats.

Encryption is the First Step

Implementing effective data security protections begins with encryption, but it certainly cannot end there. Solutions must allow businesses to seamlessly deploy and manage encryption across *all* devices with access to sensitive organization or customer data, whether that means PCs and Macs, USB drives, or phones and tablets, and whether the device is company- or employee-owned.

From a regulatory compliance perspective, businesses have their reputations on the line. You're likely subject to enforcement actions if you cannot provide irrefutable evidence that compulsory data encryption measures are active. If compromised data is effectively rendered unreadable through encryption measures, then in the eyes of regulators there has been no breach. Therefore, when a device is lost or stolen, or when a regulatory audit occurs, provable and persistent encryption is absolutely essential.

For example, BeachheadSecure® includes Compliancy Report, a comprehensive reporting tool that provides audit-grade records delineating all security measures enforced on specific devices. With Compliancy Report, businesses can hand auditors a complete record of the data encryption standards in place, as well as all further access controls and automated protective mechanisms safeguarding data on a device. This provable record leaves no doubt in the minds of regulators that security practices and compliant, enabling peace of mind for your firm.

Danger Scenarios: Remote Access Control and Automated Defenses are More Critical Than Ever

Businesses must retain access control over all devices able to access client data – wherever those devices may be – from a remote admin console. At the same time, businesses must have a sentinel solution on those devices that can not only report and alert admins to threats, but also take decisive and automated action to mitigate threats as they escalate. That solution must also offer business flexible features so they can tailor effective automated responses as they see fit based on usage patterns, company policies and employee behavior and practices. When an incident occurs at 3AM, sensitive data cannot wait for investigators to manually respond to alerts, but instead needs instant and automated mitigation to kick into action. Such automation enables businesses to anticipate and get ahead of issues by setting up predetermined countermeasures aligned with the severity of potential risk. This preparation allows businesses to neutralize threats if and when they arise, and before data exposure, fines, reputational harm or business disruptions can result.

Remote access controls and robust EDR capabilities that go beyond encryption are requisite for complete data protection across numerous scenarios, including:

- **Device loss or theft.** If a device is lost or stolen during an active credentialed session, encryption cannot prevent unauthorized access to data.

- **Poor user practices.** Employees remain the greatest risk to data security through their own behaviors. Poor password hygiene, writing login credentials on sticky notes attached to devices, clicking on phishing emails, visiting high-risk websites: each of these all-to-common practices circumvent basic data security protections. The rise of work-from-home policies, accelerated by the pandemic and likely a new normal going forward, has also made employees more likely to engage in risk behaviors such as sharing devices and passwords with others in their homes.

- **Insider threats.** Sometimes threats created by employees are no accident. A customer relayed to us this all-to-familiar story of a mortgage company where an employee literally tried to steal the business. This employee copied all of the company's most sensitive customer data to a USB drive, intent on using it to start a company of his own. He ultimately took that data to a competitor, and his actions are the subject of an active court case. Simple security tools like encryption are simply not prepared to recognize and thwart such nefarious actors. Examples like this – and we've heard many – go to show how necessary it is for business to leverage advanced security features operated with a zero-trust approach.

Use RiskResponder to get ahead of risks before they become a catastrophic issue

Beachhead RiskResponder™, part of the BeachheadSecure platform, delivers EDR capabilities enabling organizations to prepare, customize, and execute powerful risk mitigation responses across a comprehensive list of potential threat conditions. As soon as threats are detected, RiskResponder instantly and automatically executes preset actions appropriate to the risk.

That response could mean logging active events, alerting appropriate personnel to investigate risk activities, running a script, presenting the device's user with a dialog alert, or immediately removing data access from a protected device. RiskResponder’s intuitive UI design allows admins and other IT professionals to easily define responses to particular circumstances, getting ahead of issues as soon as they arise and before they have the chance to develop into huge headaches.

Specifically, businesses can customize RiskResponder to automatically respond to invalid login attempts; for example, sending a warning dialog alert to the employee after a certain number of failed logins, and quarantining data after a certain number of attentional attempts. Admins can similarly set time-based limits, forcing sessions to time out and authorized users to reenter their credentials. RiskResponder also features geofencing-enforced security rules, which admins can use to send warnings and (if needed) disallow data access if a device travels outside of normal work locations and boundaries. Any attempts to remove security features from a device – from encryption to firewall to anti-virus protections – is met with immediate detection and countermeasures. Network-borne attacks earn the same instantaneous responses.

BeachheadSecure’s robust capabilities for remotely revoking data access from at-risk devices and quarantining any client data present – even in circumstances where a device is offline and out of visibility – also enable organizations to practice strict, effective zero trust policies. If and when a device is back in-hand and no longer at risk, admins can easily and seamlessly restore data access.

Using these tools, businesses are fully equipped to curtail threats in each of the common danger scenarios discussed above. In the event that a device is lost or stolen, RiskResponder can automatically time-out sessions, and block data access after excess login attempts or if the device travels too far from where it’s supposed to be. Employees who neglect smart security practices or click the wrong links are nevertheless protected from their own actions with RiskResponder looking over their shoulder. And, insider threats who attempt to circumvent security will receive clear warnings via dialogue alerts, have their actions logged, and have their data access removed if their actions present a recognized risk.

While ransomware captures the lion’s share of security headlines and dominates conversations around security tooling, businesses are best served by a comprehensive security stack. Organizations must be protected by a breadth of safeguards that ensure data safety in the face of any threat scenario – from device loss to poor employee security hygiene, to nefarious insider threats, to compliance audits. Leveraging a balanced and holistic approach to security provides tremendous business value by ensuring the prevention of data breaches and regulatory repercussion.

Businesses that value effective and comprehensive security will achieve it, while those that angle for bargains only invite danger. As one Beachhead customer puts it: “Insufficient security is like asking where you want the hole in your house. In the ceiling? The wall? The floor? No matter where that hole is, it’s going to cause problems sooner or later.” The most effective security stacks are carefully assembled out of complementary technologies, which cannot be removed or replaced without creating dangerous vulnerabilities.

As a business with systems and data that demand 24/7/365 protection, so much is inherently out of your control (how your employees behave, the newest zero day threat attack vectors from bad actors, etc.) that you need to be in a position of full command over thwarting whatever lies ahead. With BeachheadSecure and its Compliancy Report and Beachhead RiskResponder® as part of your security stack, you have a best-in-class solution to securely and confidently protect your business.

BEACHHEAD

Beachhead Solutions Inc.
1150 S. Bascom Avenue
San Jose, CA 95128

Question, comments?
408.496.6936 sales@beachheadsolutions.com