***Breach Response helps you understand the full scope of a data breach by identifying credentials that were previously compromised elsewhere as well as identifying when, and which, credentials are actively being used by bad actors.***

## BREACH RESPONSE & REMEDIATION

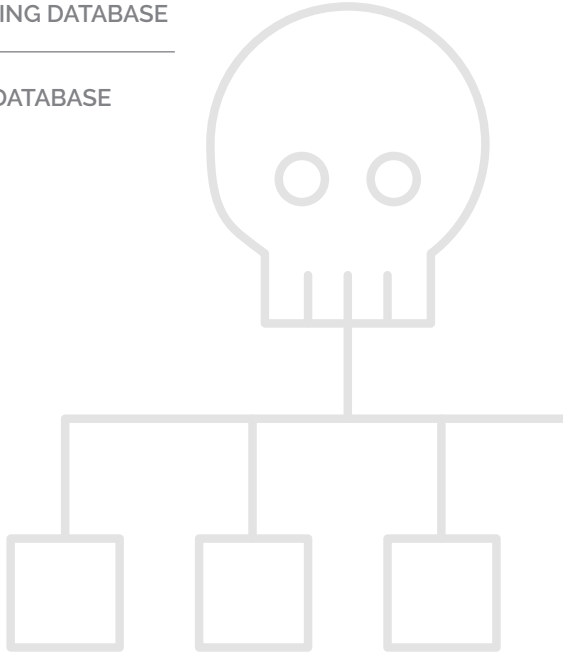
*Breach Response & Remediation* leverages myNetWatchman's massive and ever-expanding repository of compromised credential pairs and payment card data to provide you with immediate intelligence as well as long-term security after a breach. *Breach Response & Remediation* helps your organization understand the short term scope of liability and fallout related to a data breach or credential leak, while also providing one year of continuous monitoring following the attack so you can identify and assist compromised users if their breached credentials or payment card information is detected in the future.

**1.5 MILLION**
domains are tracked by us each month to uncover attacks fueled by breaches and the credentials used in those attacks

| | |
|---|---|
| 2+ | MILLION DISTINCT COMPROMISED PAYMENT CARDS + 100K NEW CARDS ADDED DAILY |
| 35+ | BILLION UNIQUE, COMPROMISED CREDENTIAL PAIRS IN OUR EVER-EXPANDING DATABASE |
| 15 | MILLION NEWLY-COMPROMISED CREDENTIAL PAIRS ADDED DAILY TO OUR DATABASE |

You're alerted when a breached credential pair (username/email and password), payment card number, and other payment information such as expiration date, CVV and more, are presented or are attempted to be used externally.

- Limit the scope of liability with hard data showing that many user credentials implicated in a data breach were already being utilized by bad actors.



- Execute damage control by working with and notifying users impacted by a breach if you see their compromised credentials used externally.

- Build back brand trust by showing customers that you are taking measures to rectify a data breach that impacted them.

## BUSINESS USE CASES

*Quantify Risk and Reduce Liability*

The fallout following a data breach goes beyond breach notification requirements, representing significant brand and financial risk. The more efforts that your organization takes after a data breach to understand the true scope of the event, and the more actions you can show were taken to protect impacted users, the better off your organization will be in both a court of law and the court of public opinion. myNetWatchman's *Response & Remediation* provides an immediate assessment of the data compromised in a credential leak or data breach to identify how much of this data was already in the hands of fraud rings and bad actors. Whether it's the username/email and password credential pair, or payment card details, if it has been used by bad actors months, sometimes even years, before it was implicated in a recent breach, this greatly reduces the financial damages impacted users could seek.

*Response & Remediation* also enables your organization to reduce the scope of impact and liability as you are alerted when breached credentials are actively exploited by bad actors. If myNetWatchman only sees a small percentage of compromised credentials used in the months to a year following the data breach, this provides evidence that the impact of the breach is relatively minor. However, even if myNetWatchman detects recently breached credentials actively being used, this intelligence enables your organization to reduce fallout by notifying users impacted by the breach.

Documenting fraudster use of compromised credentials prior to your breach event reduces fallout and liability for your organization

If your organization is impacted by a data breach, you can require implicated users to change their passwords on your site. However, that requirement doesn't extend to external accounts your implicated users may have outside your organization. Being able to alert impacted users that their breached credentials are being exploited externally should encourage them to change credentials everywhere they are using them. If that consumer later suffers account takeover through use of the shared, compromised credentials, you can show that you notified users but they chose to ignore your warning.

> Protect your brand by protecting your users from potential long-term impacts of a breach

***Win Back the Trust of Impacted Customers***

Go beyond the minimum requirements—typically offering one year of credit report monitoring. Instead, reassure your impacted users that you are leveraging a service that is actively looking for the use of any password or payment credentials implicated in the data breach, and that you will alert them if that happens. Remind them that credit report monitoring doesn't notify them of account takeover or fraudulent payment card transactions and that only your organization—thanks to myNetWatchman's *Response & Remediation*—offers that level of vigilance. Chances are your users have been previously impacted by a data breach. They may be pleasantly surprised to see how much better you handle it with *Breach Response & Remediation* compared to others.

myNetWatchman

1 Diamond Causeway
Suite 21-246
Savannah, GA 31406
+1 678-624-0924

contactus@mynetwatchman.com
mynetwatchman.tech