RepKnight

Protecting your customer data with BreachMarkers

> How would you find out if a supplier breached your data?

October 2018

Clients, customers, users, subscribers, contacts, prospects, leads…

Whatever your business calls them, all organizations hold data about customers and prospective customers – usually in dozens of different systems and places.

With data about customers increasingly being stored in the cloud, and outsourced to third parties who handle lead generation, payment, support, and order fulfilment, it's almost impossible to defend against hacking, breaches and data loss across your entire supply chain. And with GDPR now in force, the stakes just got a lot higher - punitive fines of up to 4% of global turnover can be levied on companies failing to take adequate precautions against data leaks.

> The average enterprise uses more than 1,100 cloud applications, and the vast majority are 'shadow IT'
>
> *Source: Netskope*

With many high-profile breaches originating from supply chain and technology partners, defending your own perimeter simply isn't a viable strategy any more.

This white paper explains how BreachMarkers can be used as digital watermarks in your customer data sets, providing real-time alerts if data is breached, leaked, or misused – buying you valuable time to remediate the breach, and providing traceability back to the source of the leak.

As an integral component of RepKnight's award-winning BreachAlert Dark Web monitoring platform, BreachMarkers can be deployed in minutes for proactive end-to-end protection of your customer data sets – a key part of your GDPR compliance strategy.

How many different places do you store and process client data?

From initial lead generation and prospecting, through the customer sales journey and beyond, you'll probably be surprised at how many different places you store your client data.

Lead Generation	Sales Cycle	Order Fulfilment	Customer Support
Marketing Automation platform Email campaigns Website registrations Prospecting database Webinar systems Event management Excel Spreadsheets	CRM Platform Sales forecasting Quote systems E-signature platform Outlook / Office365	Online ordering Payment processing Accounting system Shipping & Logistics Installation & Training User login details	E-learning platform Support portal Customer Helpdesk Ticketing System Maintenance Notifications Customer newsletters Event invitations

Depending on the size of your organization, you may outsource many of these functions to third parties, whether that's lead generation, order fulfilment, or customer support.

But how would you find out if one of those systems or partners lost your data? No matter where it's stored, or who's processing it on your behalf, it's your company reputation that suffers – and under GDPR it's also your legal responsibility.

It's all in the cloud

A February 2018 report from Netskope found that the average large enterprise is using 1,181 cloud services, with almost 93% of them judged as not "enterprise ready". Many of these systems are user-installed "shadow IT" apps, many of them free, which are often deployed without the knowledge of the IT security team.

HR and Marketing were the two largest categories, using an average of 139 and 121 different cloud systems respectively, with CRM adding another 62. And with many of these tools allowing users to install add-ons and connectors via an online marketplace, it's inevitable that users will sign up to (and deploy) multiple apps and connectors to make their jobs easier and more efficient.

But each and every one of these apps is vulnerable to hacking or misuse, whether by hackers, former members of staff, or through an employee using the same password across multiple systems.

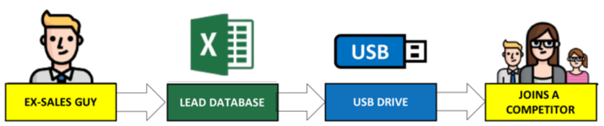
How do breaches happen? It's not just the hackers.

Although many high profile breaches are down to targeted hacking, it's often not the company itself that suffers the security problem.

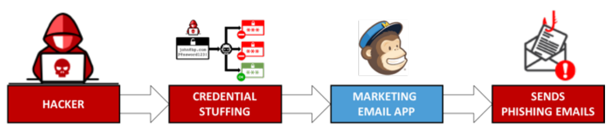
The recent breach at Ticketmaster was down to compromised JavaScript on a technology partner's platform. US Retail giant Target's 2013 breach started with credentials stolen from Fazio Mechanical Services, Target's air conditioning supplier.

But over 90% of breaches notified to the UK Information Commissioner's Office in 2017/18 were not even cybersecurity incidents at all – many were simple human error, such as sending an email to the wrong recipient.

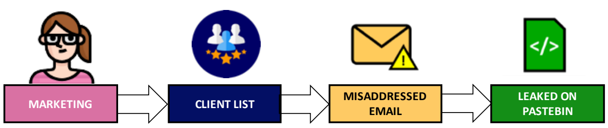
BreachAlert can detect multiple types of breach, no matter which organization the data leaked from.



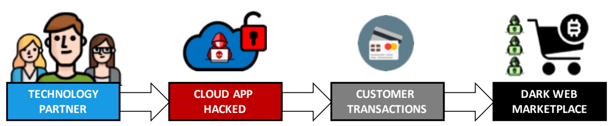
- Sales guy leaves, and joins one of your competitors, taking a copy of your lead database with him on a USB stick.
- BreachMarker email inbox receives email from competitor
- BreachAlert alerts you in real-time, allowing you to contact the competitor and take action



- Hacker finds plaintext passwords and corporate email addresses from previous breaches. Password re-use by one of your marketing staff gets him into your email marketing application.
- He downloads the client list, & starts sending phishing emails
- BreachAlert alerts you in real-time of the potential breach



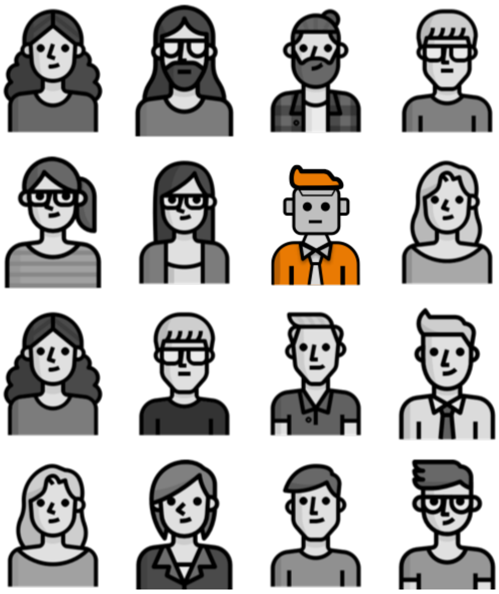
- Marketing has an "Outlook moment", and emails the client list to the wrong Joe – an ex-Employee who holds a grudge.
- Joe decides to post the data on Pastebin, and plans to share the link with the trade press.
- BreachAlert alerts you in real-time, allowing you to immediately make a takedown request to Pastebin.



- A technology partner's cloud application gets hacked, and all your customer transactions for the last month get siphoned off.
- The hacker starts selling the credentials on a Dark Web marketplace, and gives out a few free samples.
- BreachAlert alerts you in real-time, and the BreachMarker identifies the technology partner as the source of the leak.

What is a BreachMarker?

A BreachMarker is a simple concept – a synthetic (or 'fake') digital identity, added to your datasets to act as a marker in the event of a data breach.



Sometimes called 'watermarking' or 'seeding', the principle has been used for years by mailing list companies to detect misuse or breach of licensing conditions.

In our post-GDPR digital world, BreachMarkers provide a powerful mechanism to detect data being misused, leaked or sold online, and can often be deployed in minutes.

RepKnight's BreachAlert web application provides continuous 24/7 monitoring, alerting you in real-time if any of your BreachMarker's details are posted on the Dark Web, and hundreds of dump and paste sites used by cybercriminals to share hacked, leaked or stolen data.

Inbox monitoring also alerts you if one of your BreachMarkers starts receiving spam, or emails from a competitor – another clear indicator of compromise.

A unique identity – eliminating false positives

RepKnight's BreachAlert platform allows you to create unique BreachMarker identities, which are not used anywhere else on the internet. When you add them to one of your customer datasets, it's a unique identifier which unambiguously identifies it as yours.

Because those details aren't used anywhere else, any unauthorised usage or leaks of that data indicate a compromise. Unlike genuine customers or employees – who may have featured in hundreds of third party breaches over the past 10 or more years – BreachMarkers don't have any history, and so you don't have to figure out if this is "new data".

And because BreachMarkers aren't 'natural persons', GDPR rules don't apply. You can treat the alert as an IT security incident, and take your time to investigate it properly – without having to start the 72 hour GDPR notification timer.

Deployed in minutes – it's as easy as registering on your own website

Putting BreachMarkers into most of your customer datasets probably isn't that difficult – you can start by registering them on your own website, or signing them up to your own marketing newsletters. Just use the keyword exclude feature to ensure you don't get alerted every time your company sends out a newsletter.

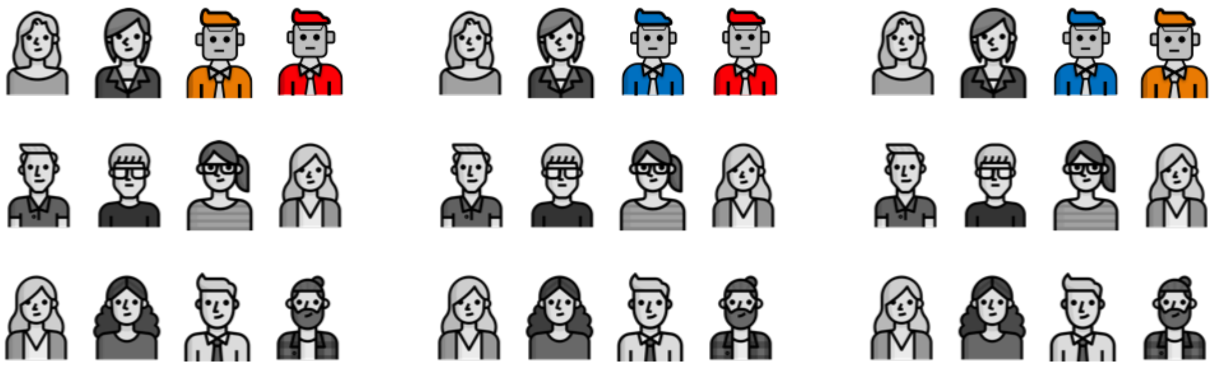
And if you're a pizza company, why not buy a pizza using the BreachMarker identity? You'll have watermarked your dataset against future breaches in less time than it takes the pizza to cook – let alone be delivered.

Dynamic BreachMarking – where did the leak come from?

By deploying BreachMarkers dynamically, organizations can also provide traceability back to the date, time, place & person from whom the leak originated.

For example, slightly different variants of the BreachMarkers can be inserted whenever a customer data set is shared with a different third party, or stored on a particular system.

In the diagram below, three different BreachMarker identities are added to the same data set when it is shared with different partners, on different days.



Supply chain partner A
System X
3 October 2018

Supply chain partner B
System Y
4 October 2018

Supply chain partner C
System Z
5 October 2018

Figure 1 : Example of dynamic BreachMarker combinations used to identify specific datasets

Name	Address	Email
Mrs Christine P Pengilly	19 Cocknage,Stoke-on-Trent,Staffordshire,ST3 4AE	christine_pengilly@icloud.com
Mr Peter M Brown	314 Lythalls Lane,Coventry,West Midlands,CV6 6GA	peterbrown@virgin.co.uk
Mr Lee J Owen	4 Kent Road,Doncaster,South Yorkshire,DN4 8JG	lee.owen81@googlemail.co.uk
Mr Jonathan Carter	**St John's Innovation Centre, Cowley Road, Cambridge CB4 0WS**	**jonathan.carter@rngdesigns.co.uk**
Mr Tristan J Watkins	2 Greenside Close,Kidsgrove,Stoke-on-Trent,Staffordshire,ST7 4TG	tristan.j.watkins@btopenworld.com
Mrs Emma P Whitla	247 Rowrah Crescent,Middleton,Manchester,Greater Manchester,M	emma.whitla@gmail.com
Mr Michael M Brown	64 Chalfont Road,London,Greater London,N9 9LY	michael.brown83@btinternet.com
Miss Gemma A Munro	40 Marne Street,Hull,North Humberside,HU5 3SU	gemma.munro@gmail.com
Ms Saffron S Paine	**14 Gray's Inn Road, London WC1X 8HN**	**saffron.paine@rngdesigns.co.uk**
Ms Karen S Hutton	110 Evenlode Road,Southampton,Hampshire,SO16 9EG	karen.hutton83@me.com
Mr Nayan A Rogers	Alder Lane Barn,Alder Lane,,Burtonwood,Warrington,Cheshire,WA5	nayan.rogers10@yahoo.co.uk
Mr Simon N Lynch	55 Cumberland Road,Castleford,West Yorkshire,WF10 2RA	simon.lynch83@btinternet.com
Mrs Chantelle P Checketts	20 Poplar Drive,Alsager,Stoke-on-Trent,Staffordshire,ST7 2RE	chantelle_checketts@hotmail.com
Mrs Shania P Derham	21 Hollyhock Drive,Mansfield,Nottinghamshire,NG19 7FG	shania_derham@outlook365.com
Mr Stephen J Foster	57 Argyle Street,Tamworth,Staffordshire,B77 3EQ	stephen.foster82@googlemail.co.uk

Figure 2 : Example of leaked dataset with unique BreachMarker combination

If a leaked dataset is subsequently detected containing both jonathan.carter@rngdesigns.co.uk (the orange BreachMarker) and saffron.paine@rngdesigns.co.uk (blue), e.g. Figure 2, the breach can be traced back to the dataset delivered to Partner C, on 5th October 2018.

API integration with BreachAlert allows dynamic BreachMarker datasets to be generated, deployed, and audited in a fully automated 'zero touch' model.

Detecting BreachMarker data misuse with BreachAlert

Your BreachMarker's contact details should only ever exist within your own systems. If they ever appear on the outside, there's a very high probability that your data has been compromised.

BreachAlert is a SaaS platform for Dark Web monitoring and Data Breach Detection, and provides a rich set of detection capabilities, alerting you in real-time if your data is breached, leaked, or misused.

BreachAlert can detect and alert you when:

- The BreachMarker's email address is posted on the Dark Web, or one of hundreds of paste and dump sites used by cybercriminals to market and share data which has been leaked or hacked;
- The BreachMarker's email address is included in a spam list, or large third party data breach;
- The BreachMarker starts receiving spam emails;
- The BreachMarker starts receiving emails from a competitor.

Alert notifications can be sent by Email, SMS, Slack, or via API integration to a wide variety of SIEM and IT Ticketing systems.

BreachAlert's built-in keyword filtering can be used to ensure you don't get alerted when your BreachMarker receives legitimate emails – for example, your own marketing newsletter.

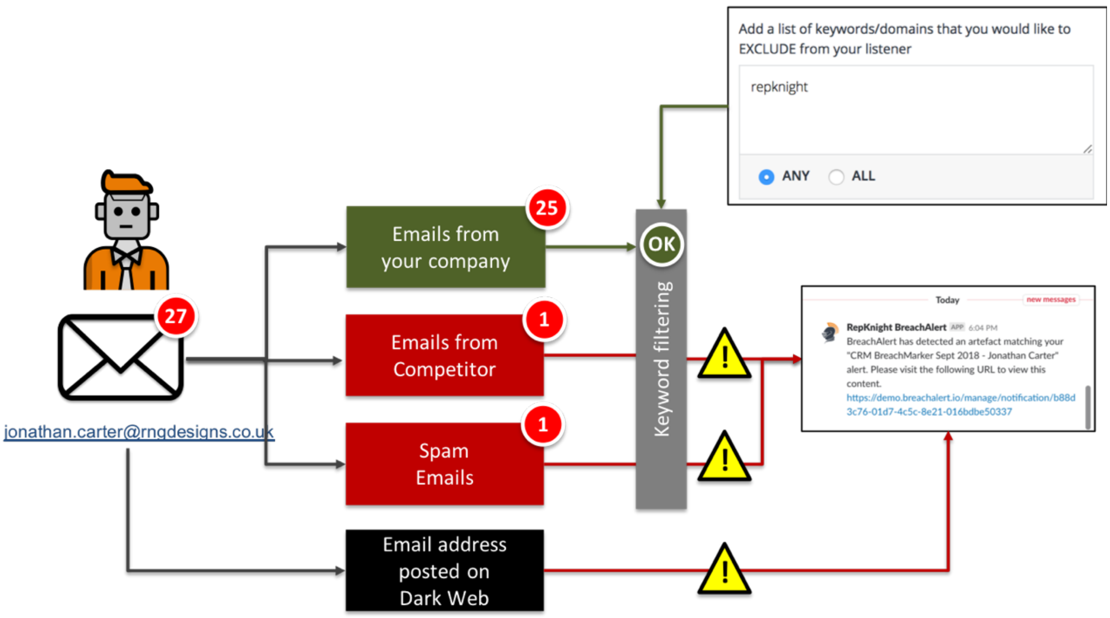


Figure 3 : Detecting BreachMarker misuse with BreachAlert

BreachAlert and BreachMarkers can be deployed in minutes, with nothing to install.

For more information, or to book an online demo, please contact info@repknight.com.

> **BreachAlert can be configured in minutes, with nothing to install – an essential component of GDPR compliance**