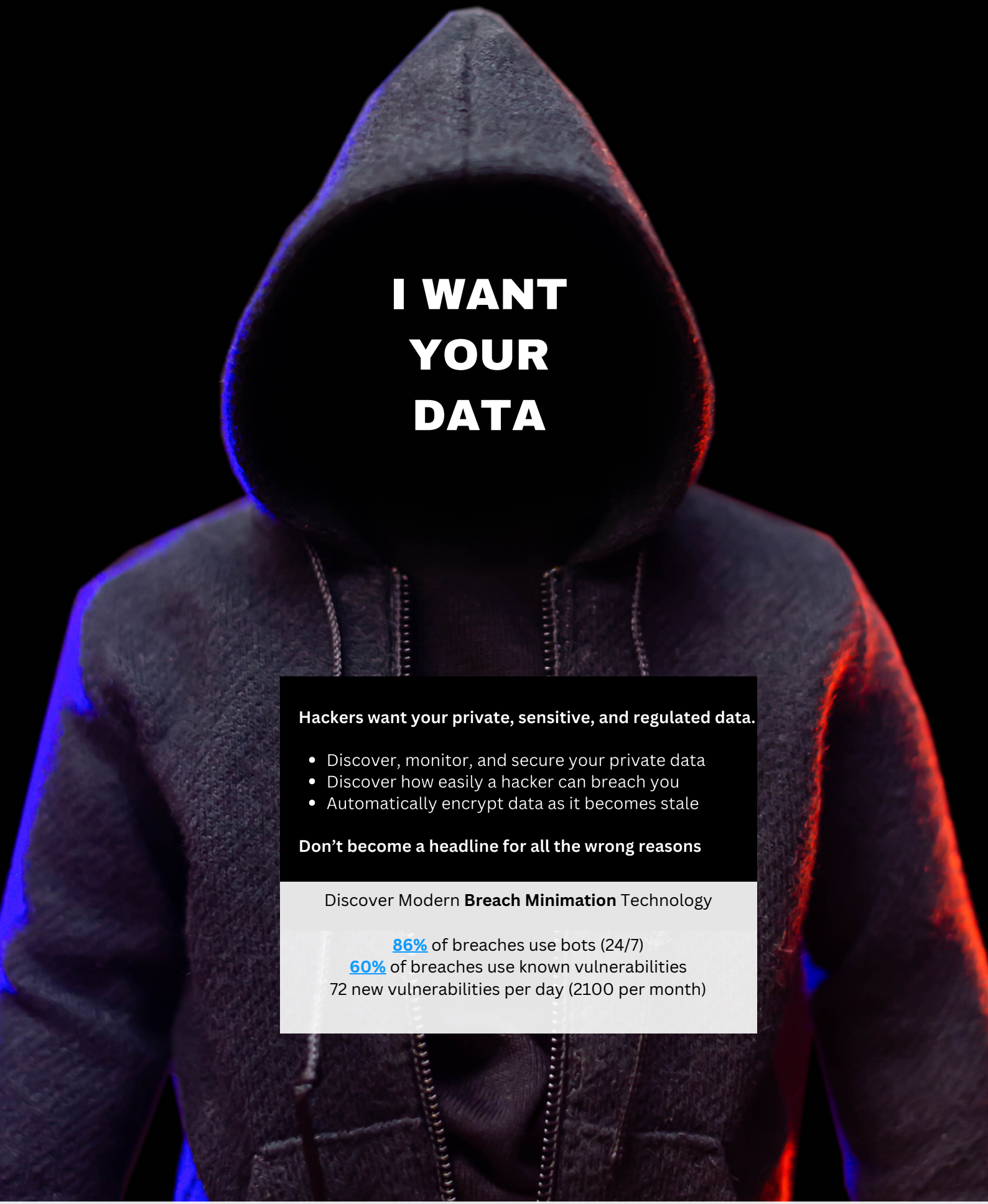
BREACH MINIMISATION TECHNOLOGY



Hackers want your private, sensitive, and regulated data.

- Discover, monitor, and secure your private data
- Discover how easily a hacker can breach you
- Automatically encrypt data as it becomes stale

Don't become a headline for all the wrong reasons

Discover Modern **Breach Minimation** Technology

86% of breaches use bots (24/7)
60% of breaches use known vulnerabilities
72 new vulnerabilities per day (2100 per month)

BREACH MINIMISATION TECHNOLOGY

YES	NO	DO YOU HAVE THESE CAPABILITIES THAT ARE DESIGNED TO HELP REDUCE CYBER ATTACKS AND BREACHES. AVAILABLE AS MONTHLY SUBSCRIPTION
How many vulnerabilities do you have in your network right now, today that a hacker can and will use to breach you and steal your data?		
		Perform daily external vulnerability scans to identify exploitable holes in your perimeter.
		Perform continuous or near continuous internal vulnerability scans to identify new vulnerabilities across Windows, Mac's, IOT, Active Directory, Firewalls and applications.
		Discover newly added devices to the network and determine their vulnerabilities.
		Determine patch status of operating systems and applications daily, weekly and monthly.
		Build remediation plans for your IT team or service provider to remediate as quickly as possible. Leverage the Enhanced Product Security Standard (EPSS) Model that predicts the likelihood of a vulnerability being exploited within a short time frame of 3, 15 or 30 days.
What is the value of your regulated data, who is at biggest risk, and what is your Data Risk Value?		
		Discover old and newly created private, sensitive, and regulated data across your PC's and servers, often the most exposed portion of a network are your PC's and laptops.
		Automatically **encrypt data** as it becomes stale at the **FILE LEVEL** making it useless to a hacker if it is stolen. This is not hard disk encryption. Users decrypt with a 'double click'.
		Breakdown data by classification (eg PII, PHI, PCI, Passport, Drivers Licenses, Medicare, TFN, etc) and by user and calculate the **DATA RISK VALUE** of that data/user/organisation.
		Monitor and track inbound and outbound flow of regulated data.
		Easily create rules to automatically encrypt/decrypt data as it flows to applications, locations, etc without intervention or disruption.
If a hacker successfully breaches you at 1am tonight, how much data can they steal by 8am?		
		Only allow **KNOWN SAFE** executables and scripts (eg Python, PowerShell, etc) to write to the Disk, COM Interface, and Registry on Windows systems All unknowns are examined in real-time, 24 / 7 using AI, ML and HUMANS and contained until proven to be safe. **ZERO TRUST**
		Ability to expand to include 24/7 threat hunting across endpoints/servers (MDR) and networks (MXDR) with experienced security experts from a global SOC.

It's difficult to know exactly how much cybersecurity is enough. You don't want to be the next victim in the news, but you don't want to spend money unnecessarily either.

Our Data Privacy and Risk Assessment helps you to evaluate your network's security posture to determine how much regulated data you have and the likelihood of a cybersecurity breach.

The good news is that a full **Breach Minimisation Platform** is typically between 1% to 3% of your data risk value - but let's first see the value of your data and if you are wide open and exposed to hackers and automated bots breaching you.

DigiCloud