The Xari Xecure® Suite

XARI Dark Web Monitoring

We go deep into the Dark Web to keep you out of it.

What is the Dark Web?

The Dark Web is made up of digital communities that sit on top of the Internet, and while there are legitimate purposes to the Dark Web, it is estimated that over 50% of all sites on the Dark Web are used for criminal activities, including the disclosure and sale of digital credentials. Far too often, companies that have had their credentials compromised and sold on the Dark Web don't know it until they have been informed by law enforcement — but by then, it's too late.

How does it happen?

When your employees use their work email on third party websites, like the types listed below, it makes your business vulnerable to a breach. With our Dark Web Monitoring, we can detect if your company is at risk due to exposed credentials on those websites.

HR & Payroll	Email Services
CRM	Travel Sites
Banking	Social Media

76% of people use the same password for most, if not all websites.[1]

What can you do to protect your business?

By signing up to Xari Dark Web Monitoring, a combination of human and sophisticated Dark Web intelligence with search capabilities, we are able to identify, analyse and proactively monitor for your organization's compromised or stolen employee and customer data.

81%
of hacking-related breaches leverage either a stolen and/or weak password.[2]

60%
of SMBs will go out of business within 6 months of a cyber incident.[3]

59%
of cyber attacks target SMBs.[4]

xarigroup

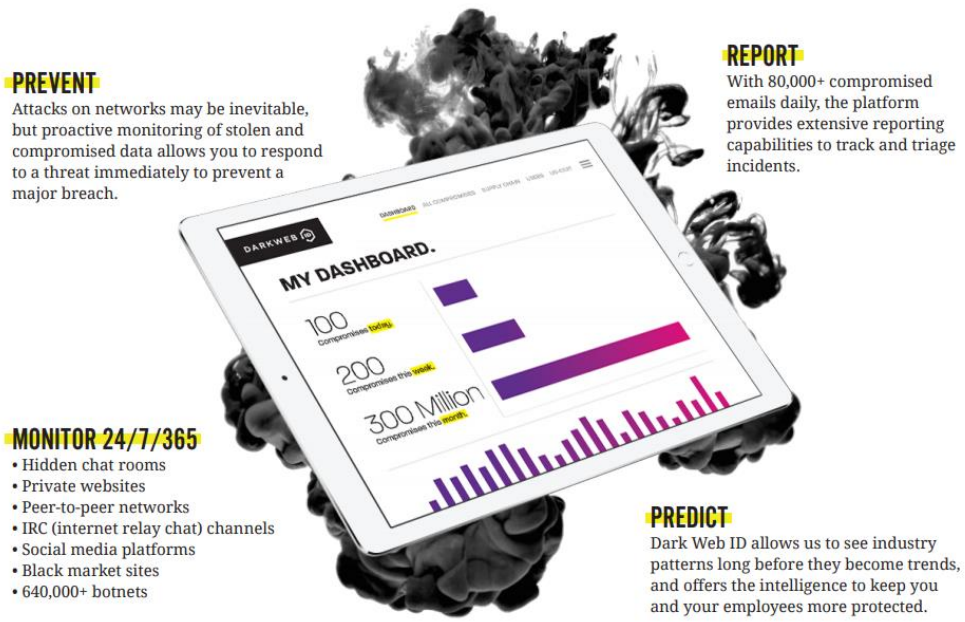
Xari Group Pty Ltd is a security-first MSP (Managed Services provider) based in Brisbane, with over 10 years of experience and expertise in IT and now cyber security, working with SMBs of varied size from diverse industries.

[1] *IDAgent Statistics*
[2] *IDAgent Statistics*
[3] *IBM Security, Cost of Data Breach Report 2019*
[4] *Data compiled by www.score.org, a group of mentors to America's small businesses*

The Xari Xecure® Suite

XARI DARK WEB MONITORING

Xari Dark Web Monitoring provides 24/7/365 monitoring of the Dark Web for signs of a company's exposed and compromised email credentials. We scour millions of sources including: botnets, criminal chat rooms, peer-to-peer networks, malicious websites and blogs, bulletin boards, illegal black market sites, and other private and public forums – all to ensure that we know as soon as compromise occurs. We persistently shine a spotlight on the darkest corners of the Dark Web, and know when any email with your domain extension ends up with credentials available, from email addresses, passwords, birth dates, social security numbers, home addresses, and driver's license numbers. A report is immediately sent to you.



Why is it important to keep you out of the Dark Web?

- Compromised credentials are used to conduct further criminal activity.
- Employees often use the same password for multiple services, such as network log-in, social media, and SaaS business applications, exponentially increasing the potential damage from a single compromised credential.
- Limited visibility when credentials are stolen; over 75% of compromised credentials are reported to the victim's organization by a third party, such as law enforcement.