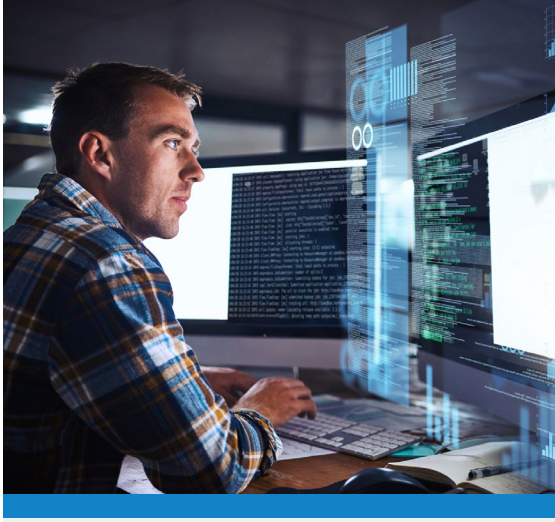

Dark Web Monitoring

Advanced warning about potential attacks or data leaks

Cybercriminals are known to craft targeted attacks at organizations and their employees, and these events are often proceeded by suspicious domain registrations or a build-up in activity on forums and darknet sites. In addition, many data breaches are first discovered when stolen data is made available for sale on the dark web.

Thrive Dark Web Monitoring service combines domain and email threat detection with dark web monitoring to provide proactive intelligence about potential attacks against your systems, brand, and key employees. The service gives visibility into the potential for cybercrime and reputation damage by monitoring new domain registrations and searching for activity over several communication channels including darknet sites, forums and chat rooms.

Domain Threat Detection

- Detects new domain registrations that could be spoofing the Client's legitimate domain name, including transposed letters, letters replaced by numbers, or different extensions.
- Provides a risk rating that indicates whether the new domain is benign or a potential launch pad for phishing and other cyber-attacks.

Data Breach Intelligence

- Identifies users that have compromised email addresses or credentials on the dark web.
- Includes information about the affected account along with the type of data that was compromised.

Dark Web Monitoring

- Daily search for surveillance keywords such as company domain name, IP address, or VIP email addresses in the Dark Web Monitoring platform.
- Provides a proprietary negativity score for each result, in addition to the threat date, threat content, and source.

Thrive Dark Web Monitoring is integrated with the Thrive platform so clients can easily review new domain threats and access monthly reports on the dark web surveillance terms. Intelligence results include risk ratings to help you understand and prioritize potential threats.

According to Gartner®:

"Subscribe to dark-web-monitoring services to **protect against "lookalike" domains, credential dumps and sale of access regarding your digital assets."***

"The cost of recovery and resulting downtime in the aftermath of a ransomware attack, and the cost of the reputational damage, can amount to **10 times the amount of the ransom itself."***

*Source – Gartner: How to Prepare for Ransomware Attacks, by Paul Furtado, 16 April 2024.