MarkMonitor™

A Clarivate Analytics company

Datasheet | Dark Web and Cyber Intelligence

Protect against cyberattacks with dark web intelligence

Overview

Cyberattacks targeting corporate infrastructures are surging, and a growing number of these threats are propagated by entities lurking in the most hidden regions of the Internet.

MarkMonitor™ Dark Web and Cyber Intelligence provides near real-time monitoring of cyberattacks across the dark web, the deep web, fraudster-to-fraudster social media conversations and other digital channels, providing actionable intelligence and alerts to help organizations take the right steps to protect their financial assets, brands and customer reputations.

Challenge

Protect your infrastructure and customers from advanced threats in the dark web

Public and private sector organizations focus a tremendous amount of resources on IT security to defend their corporate networks from cyberattacks. A majority of these investments are made to protect infrastructure and data inside the organization's firewall, but they don't protect their customers from threats that take place outside the firewall. This can tarnish brand equity and customer trust. In the dark web, cybercriminals can operate anonymously, easily exchanging large volumes of stolen credit card numbers and insurance information.

Organizations might even attempt to infiltrate these cybercriminal networks themselves, but the process requires "building trust" with hackers and fraudsters, which is time consuming, labor intensive and not scalable as a reliable security strategy.

$1.1M+

Estimated cost of a cyber attack to a single enterprise[1]

Compromised data that ends up in the dark web can cause organizations and their customers significant financial loss – and damage brand equity and reputation. Companies must gain real-time visibility into dark web attacks so they can act decisively to protect their assets and customers.

Solution

Visibility, intelligence and smart infiltration technology to protect against dark web threats
MarkMonitor Dark Web and Cyber Intelligence provides near real-time threat intelligence before, during, and after cyberattacks that are propagated via the dark web, the deep web, chat rooms, Pastebin sites and threat actor groups in social networks. The solution offers deep visibility into the most obscure and dangerous layers of the Internet, automatically monitoring and identifying threats and enabling you to take necessary action to limit the damage.

Deep visibility and threat monitoring
Monitoring 24/7 across multiple cybercrime zones – including the dark web, the deep web, social networks, IRC and chat sites, Pastebin, forums and other sites – gives you deep visibility into imminent threats to your organization. Customized search keywords in over 150 languages provide insight into specific threat activity across multiple channels.

Actionable intelligence
Near real-time alerts before, during and after an attack enable your organization to quickly identify, analyze and take necessary action to minimize damage and ensure appropriate security measures are put in place. If an attack has already occurred, alerts can enable you to understand the extent of your breach and take steps to mitigate its impact.

24/7
Monitoring across multiple cybercrime zones

Smart technology to infiltrate criminal networks
Conventional threat analysis requires security analysts to scour the deep web and the dark web manually to identify threats. MarkMonitor leverages leading-edge robot technology that mimics human behavior to interact with cybercriminals and infiltrate their networks. The smart automated technology minimizes false positives and is a scalable alternative to manual analysis.

Ongoing personalized service
Customers receive 24x7x365 access to our Security Operations Center (SOC). An assigned Client Services Manager ensures that customer needs are continuously met and helps implement best practices for the most effective results.

Key features

Extensive dark web threat monitoring
Our threat monitoring penetrates more cybercrime zones than other solutions, including the deep web, the dark web, threat actor groups in social networks, IRC and chat sites, Pastebin, forums and other digital channels.

Customizable search keywords and websites
We target websites known to be active in cybercrime and can add additional sites at your request. We allow customized search keywords in over 150 languages to gain visibility into specific threat activity across multiple channels.

Near real-time alerts
Near instantaneous alerts provide proactive protection from threats that normally wouldn't be detected until after the attack has occurred. This gives you the ability to plan the appropriate response to reduce damage.

Smart search robots
We create a scalable alternative to manual searches for criminal behavior in the dark web using smart robot technology. Smart robots mimic human behavior to infiltrate criminal networks automatically and are targeted to each monitored source.

Deep visibility. Actionable intelligence. Efficient infiltration technology.

MarkMonitor Dark Web and Cyber Intelligence is a comprehensive solution that provides deep visibility into cyberattacks, actionable intelligence and near real-time alerts to defend against data breaches. Highly customizable smart robot technology infiltrates criminal networks so you can plan the most effective defense.

Why MarkMonitor

Advanced technology and strategic guidance
MarkMonitor protects the world's leading brands with the only solution that combines cutting-edge technology and consultative services. More than 200 brand protection veterans – in more than 30 languages – are on call to defend brand investments and preserve customer trust.

Superior service and expertise
We've built our reputation on dedicated, corporate-focused service with unparalleled industry expertise. MarkMonitor manages the domain portfolios of the ten most trafficked companies in the world, and executes more than 43,000 enforcements every day.

Extensive industry relationships
A comprehensive brand protection strategy requires a strong network of strategic allies. MarkMonitor experts are connected to an unparalleled ecosystem of partnerships and relationships with search engines, social media networks, online marketplaces, industry advocacy groups, registries and law enforcement agencies.

9/10

Nearly 9 out of 10 large organizations surveyed have suffered some form of security breach.[2]

[1] Cyberattacks now cost businesses an average of $1.1M. TechRepublic, January 15, 2019. https://www.techrepublic.com/article/cyberattacks-now-cost-businesses-an-average-of-1-1m/

[2] PwC 2015 Information Security Breaches Survey of UK Corporations. https://www.cybersecurityintelligence.com/blog/pwc-2015-information-security-breaches-survey-381.html

Contact our experts today:

+1 800 745 9229 (U.S.)
+44 (0) 1978 528 370 (Europe)

markmonitor.com