appgate

DIGITAL RISK PROTECTION

Uncover compromised information, prevent targeted attacks, improve your security posture

Cybercriminals are intent on compromising employee credentials and sensitive company data to gain access to a network of valuable information. This information is then used to carry out highly sophisticated attacks for profit.

Compromised credentials are the primary cause of most data breaches and targeted attacks. With the high volume of compromised information for sale across the Dark Web, Digital Risk Protection (DRP) provides peace of mind and reports risk exposure in detail. DRP reduces attacks through its wide range of visibility and proactive threat mitigation.

Gain control over compromised data before it impacts your organization with detailed visibility and reporting.

DIGITAL RISK PROTECTION DEFENDS AGAINST TARGETED THREATS BY:

- Pinpointing exactly which employee credentials have been breached and are circulating across the Dark Web.
- Mitigating the effects of targeted threats by reporting risk exposure to ensure quick action against exposed data.
- Proactively discovering how your organization's digital presence is being targeted by phishing, brand infringement, and much more.

FEATURES INCLUDE:

Compromised credential monitoring
Discover compromised employee credentials in databases across Dark Web with detailed reporting.

Threat detection & removal
Detect and remove phishing sites, fake social media accounts, and trademark infringement.

Squatted domain name reporting
Uncover cyber- and typo-squatted domain names involving your company name or brand.

Detection of exposed documentation & leaked source code
Find leaked or stolen documents related to your company on Dark Web marketplaces and hacking forums. Uncover accidentally or maliciously exposed source code on public code repositories such as Github.

Discovery of breached IT systems
Find mentions of your systems throughout Dark Web marketplaces and hacking forums, enhanced with monitoring of threat intelligence feeds and IoC lists.

BENEFITS

Reduces manual processes by continuously reporting newly discovered threats.

Mitigates the effects of a data breach.

Provides unparalleled visibility across the Dark Web.

Round-the-clock monitoring to quickly report compromised data.

Minimizes risk exposure, keeping organizations well informed.

There has been a 450% surge in breaches containing usernames and passwords globally in the last two years.[1]

About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Learn more at appgate.com

1 https://betanews.com/2021/06/07/username-password-breaches-increase/