



DATA SHEET

DIGITAL THREAT PROTECTION

Protect your business from phishing and external threats

Online attacks impersonating companies, brands and employees are on the rise. Those attacks threaten customers' sensitive information as well as their trust and loyalty towards an organization. A business with an unsavory reputation suffers financial loss.

Appgate helps companies develop a proactive strategy to protect against digital external threats. Our unique approach discovers and eliminates threats at scale, drastically reducing criminal gains while deterring future attacks—enabling companies to focus on the future, not fear of fraud.

DIGITAL THREAT PROTECTION DISRUPTS AND DETERS ATTACKS

We continuously analyze and monitor a wide range of digital channels across emails, web and social media channels, with custom and dataset integration such as DMARC reports, abuse box, referrer weblogs, and others.

UNIQUE DETECTION AND INTELLIGENCE

Quickly finds and confirms evidence of phishing and other attacks at scale by using different proprietary machine learning classification algorithms.

EXPEDITED ATTACK TAKEDOWN

Eliminates identified threats before customers or employees become aware of them.

CONVENIENT ADOPTION

A turnkey service means simple setup, no integration required and minimal resource investment.

UNDERSTAND THE IMPACT OF FRAUD ATTACKS

Unique detection and reporting to alert organizations about which users were compromised by an attack.



BENEFITS:

Unique detection and reporting to alert organizations about which users were compromised by an attack.

Quickly finds and confirms evidence of phishing and other attacks at scale using proprietary machine learning classifications.

Eliminates identified threats before customers or employees become aware of them.

A turnkey service means simple setup, no integration required and minimal resource investment.

THE FACTS

97%

of people globally cannot accurately identify phishing emails.¹

Businesses lose

\$5.3 billion

from compromised emails.²

Most Fortune 500 companies take

\$5.3 billion

to detect cyberattacks.³



EARLY PHISHING DETECTION

Wide coverage of web, social media and email sources to detect newly configured phishing attacks—often before they are fully launched.



ROGUE MOBILE APPLICATION PROTECTION

Detect and remove unauthorized applications imitating your official app from third-party app stores. This reduces the risk of customers inadvertently downloading imposter apps.



DOMAIN AND SOCIAL MEDIA FOR IMPERSONATION MONITORING

Analysis of social networks and domain registrations to find fake social profiles, malicious mentions and similar domains that impersonate legitimate companies and compromise customer information.



VICTIM INSIGHTS

See which users clicked on phishing sites and what information they entered using an encrypted key. Armed with information about which users have fallen victim to phishing attacks, organizations can now mitigate their effects against those users almost immediately.



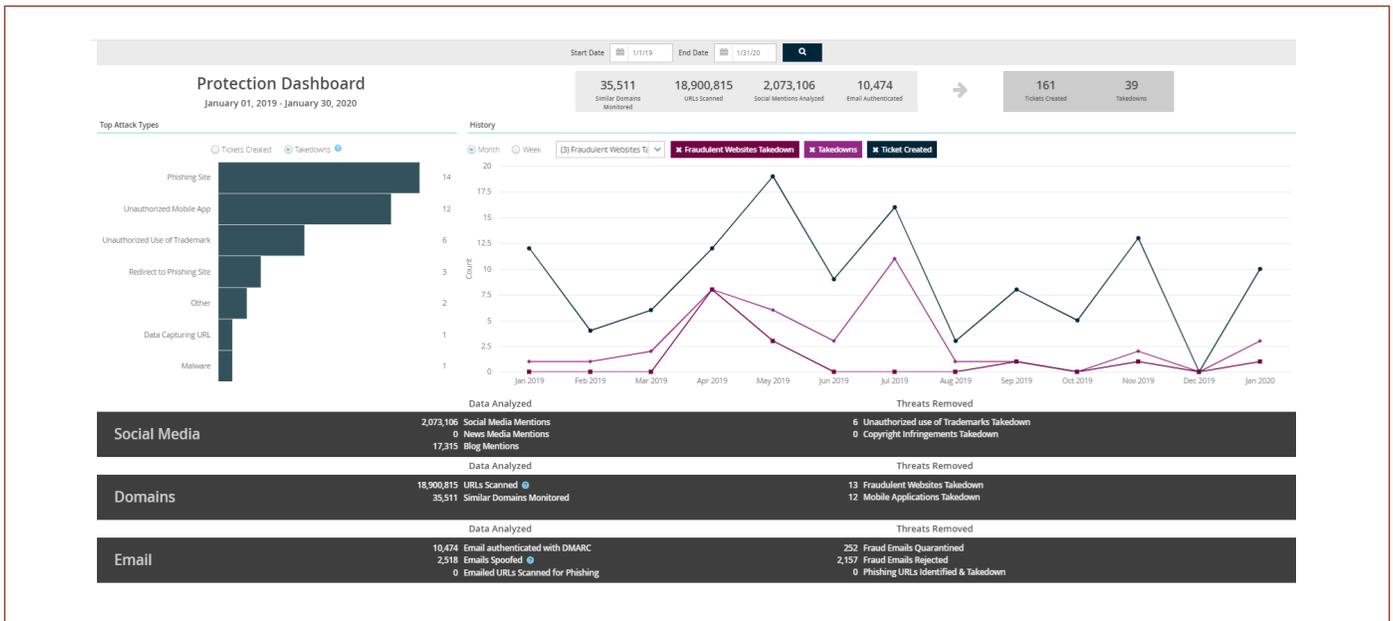
DARK WEB SCANNING FOR STOLEN/COMPROMISED CARDS

Our unique threat monitoring solution penetrates the restricted cybercrime zone known as the Dark Web looking for compromised credit/debit card data to proactively mitigate impact after breaches.



COMPREHENSIVE REPORTING

Our cloud portal delivers a real-time view of all the components of an organization's digital threat protection strategy. An all-encompassing dashboard illustrates threat data, including volume by source and category, and takedown status. Users can also set up email alerts, create a wide range of customized online or printed reports, request takedowns—plus data is readily integrated with other systems with REST APIs.



1 <http://securityaffairs.co/wordpress/36922/cyber-crime/study-phishing-emails-response.html>
 2 <https://www.ic3.gov/media/2017/170504.aspx>
 3 <http://www.securityweek.com/breach-detection-time-improves-destructive-attacks-rise-fireeye>