

ONLINE BRAND PROTECTION FROM **ALLURE SECURITY**

Strengthen your proactive cybersecurity, fraud prevention and threat visibility strategy using a layered, full cycle approach with DefenseStorm and Allure Security.

DefenseStorm helps financial institutions achieve cyber risk readiness, to ensure you apply the same level of scrutiny to cyber risk as you do your financial risks. With Allure Security, you can extend your cyber risk readiness by eliminating online brand impersonation, phishing, and scams before anyone falls victim.

FIND & STOP MORE ONLINE BRAND IMPERSONATIONS FASTER

Allure Security online brand protection-as-a-service protects businesses and their customers against fraud and scams originating from websites, social media platforms, and mobile app stores. Allure Security's unique, automated approach to detection (combining computer vision and natural language processing) and multi-pronged response results in finding and disrupting more online brand impersonation attacks earlier than competing alternatives.

Fraudsters imitate brands online using spoof websites, fake social media accounts, and rogue mobile apps. These imitations exploit brands' trusted relationships with their customers, fans, and business partners to defraud consumers and steal credentials and other sensitive information.

Research shows that the majority of consumers blame the impersonated brand for brand impersonation fraud – resulting in damage to the brand and loss of revenue. Many businesses struggle to keep up with the deluge of online content published or updated each day whether that's new websites, social media accounts and posts, or mobile apps.

Traditional manual approaches to the problem of online brand abuse cost too much and miss most threats. In addition, businesses can't count on registrars, hosting providers, social media platforms or app store administrators to differentiate between authorized and unauthorized use of their brand assets.

Allure Security analyzes more than 70 million online artifacts every day and reduces takedown times from days to hours. As a result, Allure Security can find and mitigate online scams before a single person falls victim.

"We weren't as efficient because we don't have people whose whole job is to do this. They have other responsibilities equally important to protecting the cybersecurity of the credit union. Hiring Allure Security allowed us to operationalize that with procedures, reporting, and peace of mind that it's handled by professionals whose whole job is to detect and eliminate these threats."

VP Risk | Credit Union \$1.7B AUM

ONLINE BRAND PROTECTION FROM **ALLURE SECURITY**

Strengthen your proactive cybersecurity, fraud prevention and threat visibility strategy using a layered, full cycle approach with DefenseStorm and Allure Security.

HOW ALLURE SECURITY ONLINE BRAND PROTECTION-AS-A-SERVICE WORKS

Each day Allure Security's AI-powered detection engine automates the analysis of 70+ million online artifacts whether websites, social media profiles, or mobile app store product pages. Applying computer vision and natural language processing, Allure Security's engine renders content in a browser and examines it as a human analyst would, but at scale:

VISUAL COMPARISON

Learn the distinguishing features of a logo, product images, colors, fonts and more to identify clones and alterations no matter how nuanced

MESSAGING COMPARISON

Learn a brand's messaging, copyrighted material, slogans, keywords, and more to identify impersonations and variations

CODE STRUCTURE

Learn the structure of genuine pages including HTML, CSS, registration and hosting information, and associated digital certificates

WEBSITES

Allure Security collects URLs from newly registered and previously dormant domains and subdomains, partners, proprietary web beacons, third-party threat feeds, and permutations.

Allure Security's approach allows the identification of problematic domains during configuration and setup and before a single victim visits the site. Long-standing, trusted relationships built with registrars and hosting providers around the world also ensure accelerated takedowns of malicious sites.

SOCIAL MEDIA

Continuous scouring of various social media platforms allows Allure Security to find more new, or previously unknown, malicious profiles pedaling counterfeit goods or impersonating brands, their executives, spokespeople, fans, or influencer partners. In addition, Allure Security's constant vigilance over legitimate and authorized accounts ensures immediate detection of signals of social media account compromise such as suspicious posts or changes to the profile. Due to stringent evidence collection practices, Allure Security's threat response team has built significant credibility with social platform fraud and abuse teams resulting in reduced response times.

MOBILE APP STORES

Allure Security continuously monitors more than 25 official and unofficial mobile app stores for out-of-date, repackaged, newly published, and cloned apps, or related product information. Customers receive immediate notification of suspicious product pages and apps. Allure Security's expert team has collaborated with numerous app stores to remove known violations quickly.