

# Phishing Protection Datasheet

Argos provides comprehensive and proactive protection from phishing attacks. From domain protection and the detection of cloned websites to identification of brand abuse and managed takedown services, Cyberint mitigates phishing risks from end to end.

## Challenge

Phishing continues to be a top attack vector in corporate breaches. A staggering 41% of security incidents involve phishing for initial access, according to recent research from IBM. Threat actors use a variety of phishing techniques, including brand impersonation and social engineering, to fool their victims into opening a malicious file, downloading a malicious app, or simply giving up their credentials.

## Solution

The Cyberint Argos platform provides proactive, end-to-end defense against phishing risks. Domain protection quickly alerts you to lookalike domains and misuse of brand names. Argos also detects unauthorized use of your brands and logos. The Phishing Beacon, a proprietary technology developed by Cyberint, immediately detects clones of your organization's websites. The Cyberint team provides takedown services, ensuring that phishing sites are taken offline as quickly as possible.

### Key Benefits:

- Identify lookalike domains, subdomains, and subdirectories
- Detect misuse of brand trademarks and logos on third-party websites
- Receive immediate notifications if a clone of your site is published online
- Monitor the dark web for phishing kits and other signs of an impending attack
- Take down phishing sites as quickly as possible with support from Cyberint

## Quickly Detect Lookalike Domains

Registration of a lookalike domain that resembles your organization's brand name is a clear indication that a phishing attack is imminent. Detect lookalike domains to take action before the attack develops.

### Continuous Open Web Monitoring

Cyberint continuously scans 2.5 billion IP addresses as well as DNS records to immediately detect suspicious domains.

### Detect All Potential Threats

Uncover all typosquatting and lookalikes across domains, subdomains, and subdirectories.

### Act Fast To Avoid Damages

Get immediate notifications when suspicious domains are created to take action before an attack is launched.

## Identify Clones Of Your Website & Misuse Of Logos

Cyberint uses a number of techniques to proactively detect phishing sites that mimic your organization's legitimate website, impersonate your brand, and misuse your logos.

### Get Immediate Visibility On Clones

Cyberint's Phishing Beacon sends a signal within seconds of a clone of your website being published online.

### Uncover Misuse Of Logos

Cyberint uses machine learning to detect unauthorized usage of your organization's trademarked logos on phishing sites.

### Protect Your Brands' Reputation

Ensure that threat actors don't damage your reputation or hurt customer trust in your brand with phishing attacks.

## Fast & Effective Takedown Services

After a phishing site is detected, Cyberint customers can choose to take action themselves or request a takedown that will be quickly managed by the Cyberint team.

### 200+ Takedowns Each Month

The Cyberint team average more than 200 takedowns per month, many within 24 hours of receiving the request.

### 95% Takedown Success Rate

Cyberint's team of cyber experts have has a 95% success rate in taking down phishing sites.

### Simple & Fast Requests Process

Customers can request a takedown with the click of a single button in the Cyberint Argos platform.

## About Cyberint

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure. Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.