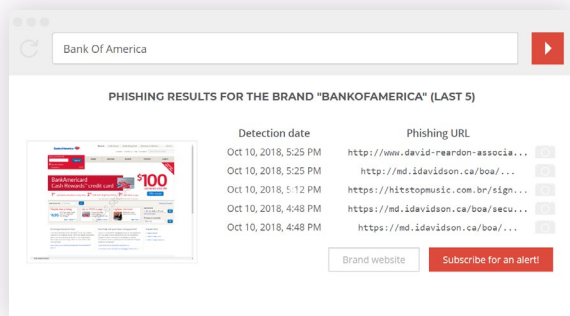


# IsItPhishing Threat Detection

Real-time phishing protection  
powered by artificial intelligence

**WHY** – Every day, your SOC has to process a growing number of alerts, analyze them, and launch corrective actions. Containing and stopping compromise attempts that threaten your business is an ongoing challenge.

**SOLUTION** – Vade's IsItPhishing Threat Detection detects phishing pages in real time to protect your employees and your IT system.



## Real-time analysis of phishing urls and web pages

IsItPhishing Threat Detection uses artificial intelligence and smart patterns to provide advanced protection against phishing, even in short-wave, highly targeted attacks. Thanks to the combination of these technologies, Vade can ensure that no false positives are detected.

To make a decision, IsItPhishing performs a real-time analysis of the web page (URL sandboxing):

- The service first compares the URL against Vade's real-time threat intelligence to immediately weed out known threats. On average, 10,000 new URLs are detected daily by Vade and its technology partners.
- Then, IsItPhishing Threat Detection performs a real-time analysis of the URL and page content, following all redirections to reach the final page and determine if it is malicious.

**IsItPhishing Threat Detection does not stop at content, but analyzes the global context of the URL and page using various technologies:**



**Smart patterns** – This is a set of predictive heuristic rules developed by Vade and updated daily. These models analyze key features of URLs and pages (e.g. redirections, file paths, scripts, etc.) to identify malicious content.



**Machine learning** – To provide maximum responsiveness to small-scale, unknown attacks, IsItPhishing Threat Detection uses artificial intelligence to make automatic decisions under the supervision of a team based around the world. Supervised machine learning algorithms analyze more than 40 characteristics of URLs and web pages (for example, how the page and form are created, use of URL redirects and shortcuts, the use of obfuscation techniques, etc.) to detect phishing.

## Intercept the most complex attacks

IsItPhishing Threat Detection thwarts the most complex attacks and integrates advanced counter-measure features, such as:



**Anonymization of parameters** – The tokens contained in URLs are replaced randomly so that the content of the page can be safely explored on behalf of the user, without triggering any action or tracking. This function is essential for analysis at the time of click, which blocks attacks based on dynamic links and dormant pages.



**Mobile rendering** – Pages are browsed with more than 30 device and browser combinations (e.g. Safari on iPhone, Chrome on Android, etc.) to block attacks designed to display only on mobile devices.



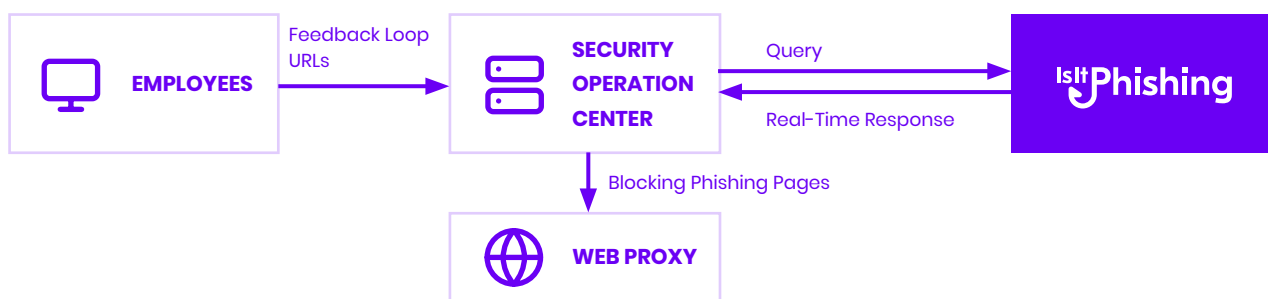
**Browsing regional pages** – We can browse pages from four regions (North America, South America, Europe, and Asia) to combat phishing pages that only appear when the user is located in the target region.

## Integrate data into your orchestration tools

IsItPhishing Threat Detection is available as a REST API for real-time analysis of web pages. It integrates into your orchestration scenarios and determines whether or not the web pages behind suspicious URLs are legitimate. IsItPhishing Threat Detection easily integrates with leading SIEM and SOAR solutions, allowing you to enhance your organization's security without disrupting your existing architecture.



Example of IsItPhishing integration:



IsItPhishing is based on patented technologies developed by Vade, the leader in predictive email defense. You can test it by accessing [www.isitphishing.ai](http://www.isitphishing.ai)

### About Vade

- 1 billion mailboxes protected
- 100 billion emails analyzed / day
- 1,400+ partners
- 95% renewal rate
- 15 active international patents

### Learn more

[www.vadecure.com](http://www.vadecure.com)



@vadecure

### Contact

Sales US / EMEA

[sales@vadecure.com](mailto:sales@vadecure.com)