Arkose Labs

# Arkose Phishing Protection

*Defending against MFA compromise and other advanced phishing tactics*

Multifactor authentication used to be the gold standard for enhancing enterprise security. But cybercriminals have upped their game, finding ways to launch account takeover (ATO) attacks even on MFA-protected accounts. They conduct adversary-in-the-middle (AITM) reverse proxy phishing attacks to intercept not just usernames and passwords, but also the crucial one-time passcodes generated by MFA. This raises a critical question: How can you stop adversaries using advanced tactics that undermine conventional protocols? Arkose Phishing Protection addresses this challenge. The solution integrates pioneering adversary-in-the-middle protection with our real-time digital risk intelligence capabilities to stop MFA compromise cold, delivering additional impact from the top of your user flow.

## How Arkose Phishing Protection Works

Arkose Phishing Protection, an add-on feature of the Arkose Labs solution, is designed specifically to counter MFA compromise. In this type of attack, a malicious actor sets up a reverse-proxy server that masquerades as the legitimate company website, phishing users to believe they are logging in directly. When users enter their credentials and the MFA one-time passcode, attackers capture the credentials and the OTP, enabling the bad actors to take control of the account.

Arkose Phishing Protection detects these phishing attempts by leveraging a unique integration model to combat MFA compromise and other advanced phishing attacks effectively. As part of the deployment strategy, the solution inspects every login request and requires a valid Arkose Labs token for authentication. This requirement extends to reverse proxy phishing attacks, which are required to still generate valid Arkose Labs tokens for every session to gain access.

This integration supports the real-time detection and blocking of phishing sites and can aid in formal takedown requests for identified phishing domains.

## Here's how the kill chain works:

**1**

The user is tricked and clicks on a malicious URL/link.

**2**

The phishing site loads while the reverse proxy intercepts traffic to the target site.

**3**

Arkose Phishing Protection identifies phishing traffic using numerous signals.

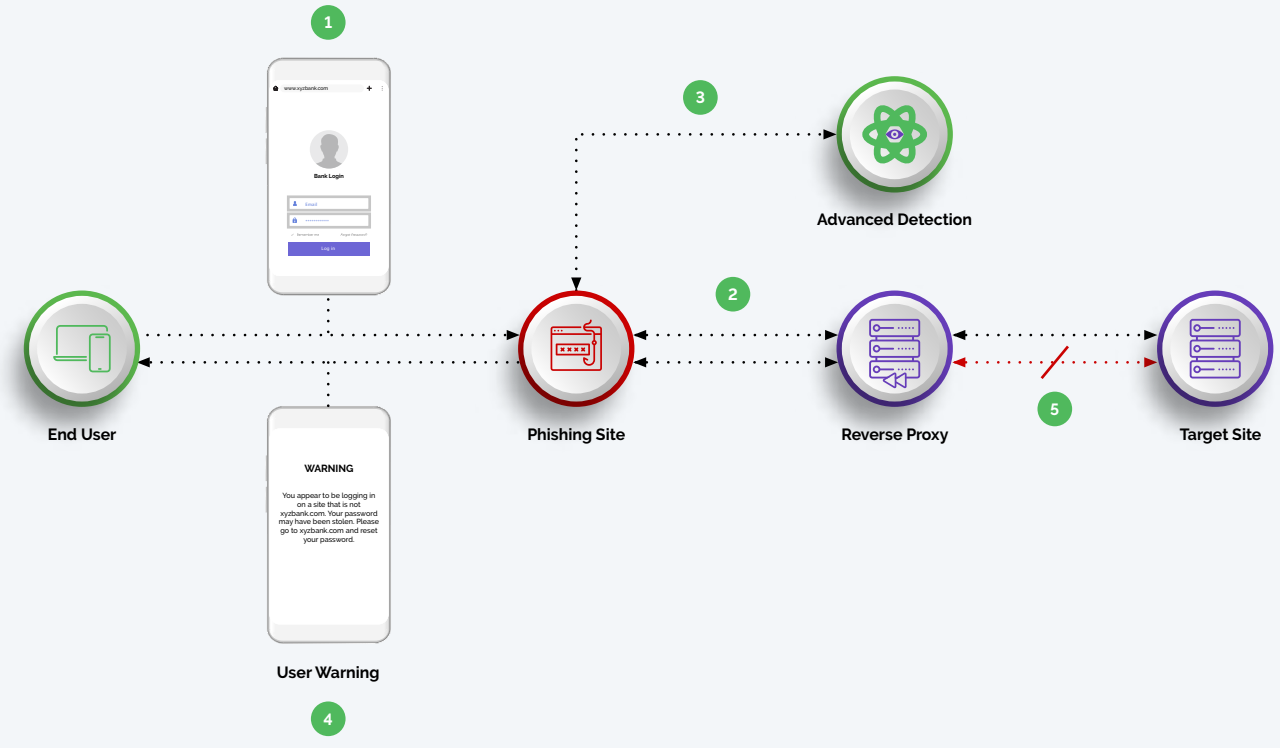
**4**

Mitigation Choice. Depending on the configured mode:

- Active Mode: Alerts the user and blocks the phishing attempt.
- Monitoring Mode: Detects the phishing attempt without user notification, allowing the enterprise to act later.

**5**

The phishing attempt fails as the Arkose Labs session token cannot be validated, stopping the attack.



### Why Arkose Phishing Protection Outperforms

- Verifying an Arkose Labs token is mandatory for completing the transaction.
- AITM proxies must deploy or transmit the Arkose Labs code.
- This process allows both client- and server-side capabilities to detect fraudulent attempts effectively.

## Why Add Arkose Phishing Protection To Your Deployment

### Superior Technology

Traditional solutions rely on static indicators and known phishing URLs. Arkose Phishing Protection builds on the unmatched real-time fraud detection technology of the Arkose Labs solution to stop reverse-proxy attacks and prevent the theft of login and MFA credentials.

### Real-Time Detection

Catch phishers in the act. Our solution includes live detection of reverse-proxy phishing attacks (using client- and server-side signatures), the option to display in-the-moment end user warning messages, the ability to block phishing sites, and immediate visibility of phishing sessions in the portal.

### Flexible Mitigation Options

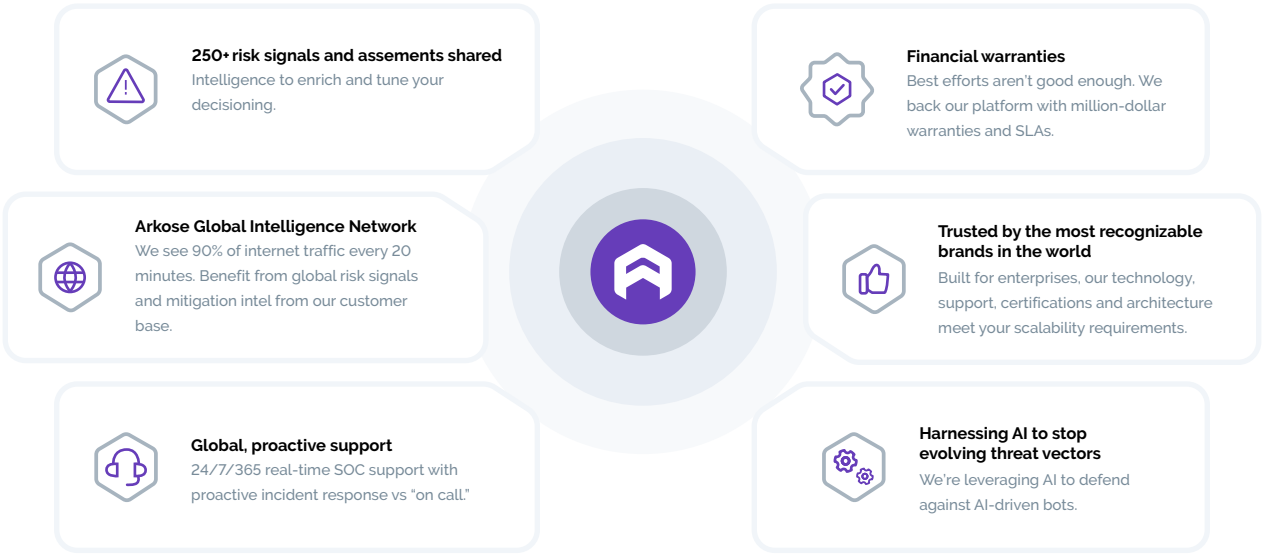
In “active” mode, suspicious hostnames are captured and anti-phishing pressure activates, displaying a warning message to the end user and blocking the phishing verification. Alternatively, businesses can opt for "monitor" mode, which tracks and reports potentially malicious activity without immediate intervention. This allows your enterprise to leverage your preferred downstream mechanisms, such as alerting users to change their passwords or lock their accounts.

### Seamless Integration: No Engineering Delays

We understand the challenges of securing engineering time, which is why Arkose Labs is designed for effortless integration. If you’re using a CDN like Cloudflare or Akamai, our pre-built CDN workers allow you to deploy our solution without any code changes to your application. This low-code implementation ensures you can get up and running quickly, without needing to pull your engineers away from their critical projects.

If you’re already a customer, the integration of the Arkose Phishing Protection add-on feature is ready to go, requiring minimal effort on your part. This means you can deploy robust protection without the usual delays, keeping your business secure without waiting months for engineering resources.

## The Arkose Labs Advantage




## ACTIR and the Arkose Labs SOC: Proactive Defense

Arkose Labs operates as an extension of your team, rapidly countering attacks and providing actionable insights without overburdening your internal resources. The Arkose Cyber Threat Intelligence Research (ACTIR) unit conducts proactive threat hunting, risk intelligence gathering and other counterintelligence methods to provide vital, fresh intelligence. Meanwhile, the 24/7/365 Security Operations Center (SOC) team focuses on identifying ann immediately stopping sophisticated low-and-slow attacks as well as large-scale attacks.

The SOC continuously monitors for new threats and collaborates with ACTIR. This feedback loop ensures a seamless collaboration between the SOC and ACTIR, enhancing the overall accuracy, timeliness and effectiveness of your cybersecurity defense.

## Arkose Labs Proof of Value

The Arkose Labs proof of value (POV) process offers your business a hands-on opportunity to experience the platform's capabilities. During the POV with production traffic, Arkose Labs provides expert guidance and consultation tailored to your specific needs, ensuring you can test the platform's effectiveness in real-world scenarios. This process allows your business to define and track its own success metrics, such as fraud reduction, improved user experience or cost savings, giving you a clear view of the value Arkose Phishing Protection can deliver.

## Arkose Phishing Protection in Action

Phishing attack methods have evolved to using pre-packaged reverse proxy based phishing kits. These kits, which are affordable and widely accessible, provide everything needed for a phishing campaign: scripts, templates for fake emails and websites, a web server and storage to collect stolen credentials. By leveraging this technology and registering dozens of domains to evade detection, attackers can now easily bypass traditional protection methods such as MFA, WAF deny lists and spam filters, enabling them to carry out MFA compromise and other advanced phishing attacks.

Traditional phishing detection tools often fall short because they rely on static indicators like domain reputation, blacklists or predictable patterns in email content, which are ineffective against dynamic tactics like reverse-proxy phishing. Reverse-proxy phishing operates in real time, relaying traffic between the victim and the legitimate site to intercept credentials and MFA tokens.

But unlike these traditional methods, Arkose Phishing Protection is specifically designed to detect and mitigate these types of attacks. The evidence speaks for itself: In our analysis of requests across three login endpoints, 96% of suspicious domains would have bypassed traditional protection mechanisms. Arkose Phishing Protection, however, provides the advanced defenses necessary to stop MFA compromise and other reverse proxy phishing attacks.


Comparison of phishing detection methods

Arkose Phishing Protection is the ultimate solution for staying ahead of advanced phishing tactics and safeguarding your enterprise against MFA compromise. Ready to see how it can protect your organization and enhance your security posture? Schedule a call with an expert today.

SCHEDULE CALL WITH AN EXPERT

Arkoselabs.com