PRODUCT BRIEF

Arkose Phishing Protection

Defending against MFA compromise and AI-powered phishing

The Threat Has Evolved—Your Defense Must Too

Multifactor authentication used to be the gold standard for enhancing enterprise security. But cybercriminals have evolved their tactics, launching sophisticated account takeover (ATO) attacks that compromise even 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.

Now, with AI agents capable of automated phishing campaigns at unprecedented scale, the threat landscape has reached a critical inflection point. The question isn't "is this a bot?" anymore—it's "is this agent authorized?"

This raises a critical question: How can you stop adversaries using advanced tactics that undermine conventional protocols?

Arkose Phishing Protection addresses this challenge head-on. As an integrated component of the Arkose Titan platform, the solution delivers comprehensive defense against AITM phishing attacks while providing unified protection against human and AI-powered fraud, scraping and bot attacks—from traditional bots to sophisticated AI agents using tools like Computer Use.

Understanding Adversary-in-the-Middle (AITM) Phishing

In AITM attacks, 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 in real-time, enabling complete account takeover.

The Attack Chain:

1. **User Deception:** The user is tricked and clicks on a malicious URL/link that appears legitimate.
2. **Proxy Interception:** The phishing site loads while the reverse proxy intercepts all traffic between the user and the target site.
3. **Credential Capture:** User enters username, password and MFA code—all captured in real-time by the attacker.
4. **MFA Bypass:** The proxy forwards credentials to the legitimate site, bypassing MFA and establishing an authenticated session.
5. **Session Hijacking:** Attacker steals the session cookie with full account access, enabling fraud while bypassing future MFA checks.

The AI Amplification Factor

AI agents using tools like large language models and browser automation can now conduct phishing campaigns at massive scale with human-like adaptability.

Why AI Makes Phishing More Dangerous

Automated Reconnaissance: AI agents can autonomously discover targets, craft personalized phishing content and identify high-value accounts to compromise.

Scale Without Limits: What once required human operators can now be automated across thousands of simultaneous phishing campaigns with minimal cost.

Adaptive Evasion: AI agents learn from failed attempts, automatically adjusting tactics to bypass detection systems and security controls.

Toolkit Proliferation: Pre-packaged phishing kits combined with AI agents make sophisticated attacks accessible to low-skill adversaries.

How Arkose Phishing Protection Works

Arkose Phishing Protection is designed specifically to counter MFA compromise and AI-powered phishing through a unique integration model that combines pioneering AITM defense with comprehensive fraud prevention capabilities.

Part of the Arkose Titan Platform

Unlike point solutions that only detect phishing, Arkose Phishing protection, part of Arkose Bot Manager, is integrated into the Arkose Titan platform—providing unified protection against human and AI-powered fraud, scraping and bot attacks across your entire user journey.

Core Arkose Titan Capabilities

- Detects automated bot attacks
- Stops AI agents & agentic attacks
- Device & behavioral anomaly detection
- 225+ risk signals across 7 detection vectors
- Real-time adaptive defenses
- Attack economics disruption

Phishing Protection Signals

- AITM reverse proxy detection
- Token-based authentication
- Suspicious hostname identification
- Real-time domain intelligence
- SSL/TLS certificate validation
- Client and server-side signatures
- Network fraud history analysis

The Power of Integration

Arkose Phishing Protection feeds risk data directly into Arkose Bot Manager's decision engine, correlating phishing indicators with device fingerprinting, IP reputation, behavioral signals and AI agent detection for a complete threat picture with automated enforcement.

Bottom Line: You're not just validating authentication—you're stopping automated bot attacks AND sophisticated human fraud actors using risky credentials. Arkose Titan stops the attack method across the entire user journey; Phishing Protection identifies and blocks the fraudulent session at sign-in.

The Phishing Protection Kill Chain

Here's how Arkose Phishing Protection stops attacks in action:

STEP 1
User Clicks Malicious Link

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

STEP 2
Phishing Site Loads

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

STEP 3
Advanced Detection

Arkose Phishing Protection identifies phishing traffic using numerous signals including token validation, domain analysis and behavioral signatures.

STEP 4
Mitigation Choice

Depending on the configured mode:

Active Mode:
- Alerts the user with a warning message
- Blocks the phishing attempt
- Prevents token validation
- Stops attack at point of authentication

Monitoring Mode:
- Detects the phishing attempt without user notification
- Tracks and reports potentially malicious activity
- Allows enterprise to leverage downstream mechanisms

STEP 5
Attack Fails

The phishing attempt fails as the Arkose Labs session token cannot be validated, stopping the attack before any credentials are compromised.

Enriched Phishing Intelligence

Arkose Phishing Protection delivers comprehensive phishing data through our real-time layer (RTL) for each session identified as phishing, providing immediate insights into targeted users and malicious domains.

Intelligence Use Cases:

Automated Takedown
Use domain intelligence to automate takedown requests for malicious domains with detailed evidence.

Threat Notifications
Implement real-time alerts to internal security teams with actionable domain and session data.

Account Protection
Trigger automated user account locking and password resets for compromised sessions.

Incident Response
Feed comprehensive phishing data into your SIEM for investigation and pattern analysis.

Why Arkose Phishing Protection Outperforms

Traditional Detection Falls Short

Traditional phishing detection tools often fail because they rely on static indicators like domain reputation, blacklists or predictable patterns in email content—ineffective against dynamic tactics like reverse-proxy phishing that operate in real time. Arkose Phishing Protection is built for modern threats, with superior technology that stops these attacks as they happen.

The Proof: Detection Effectiveness

Analysis of Requests Across Three Login Endpoints:
Traditional Phishing Detection: 10 out of 250 total suspicious domains detected (4%)

Arkose Phishing Protection:
- 49 domains less than 60 days old detected (indicating recent creation for attack)
- 191 short-lived URLs identified (indicating they served attack purpose then disappeared)
- 240 out of 250 suspicious domains caught (96%)

Conclusion: 96% of phishing attempts would have bypassed traditional protection mechanisms.

Arkose Phishing Protection in Action

Real-World Results: Major Gaming Company

The Challenge

A leading gaming company was grappling with mass creation of fake accounts and sophisticated AITM phishing attacks targeting player accounts, with attackers successfully bypassing MFA protections.

The Solution

Deployed Arkose Phishing Protection in active mode across authentication endpoints as part of comprehensive Arkose Titan platform implementation.

The Results

- **8M+ Phishing Attempts:** Fake account registration attempts and phishing sessions detected and mitigated annually
- **24% Lift:** Increase in fake account detection beyond existing bot traffic management capabilities
- **100% Coverage:** Stopped high volumes of attacks across major email domains including Gmail, Outlook and Hotmail
- **Zero Friction:** Legitimate users experienced seamless authentication with no false positives or added friction

About the Arkose Titan Platform

Arkose Titan is Arkose Labs' comprehensive platform that delivers end-to-end protection across every touchpoint of the user journey. The platform makes attacks unprofitable while keeping legitimate users moving seamlessly through:

- **Unified Intelligence:** Shared threat data across all touchpoints creates compounding protection where each interaction strengthens the entire system
- **Attack Economics Disruption:** Increases attacker costs exponentially while defender costs remain flat
- **Adaptive Enforcement:** Real-time response that evolves with sophisticated threats including AI-powered attacks
- **Zero-Friction for Legitimate Users:** 98%+ customer satisfaction with invisible protection for real customers

Arkose Titan secures every stage—from first account sign-up through ongoing platform activities—protecting registration, authentication, payments and in-platform interactions with one unified solution.

Schedule a Call with an Expert

See how Arkose Phishing Protection can safeguard your organization against MFA compromise and advanced phishing tactics while delivering seamless experiences for legitimate users.

Contact us today to schedule your personalized consultation and proof of value.

BOOK A DEMO

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.