

# Obsidian Security vs Abnormal



IDENTITY THREAT PREVENTION

Identity-based attacks, especially spear phishing, are a popular tactic for adversaries. To combat these threats, email security vendor Abnormal Security deploys behavioral AI technology to identify anomalies in email communication.

While Abnormal's API-based approach of running threat detection models post-delivery to analyze emails already in the inbox works well to spot fraudulent activity like executive impersonation, it's not successful in stopping the latest attack trend: adversary-in-the-middle (AiTM) phishing kits.

AiTM attacks have grown in popularity due to their ability to bypass email scanning and other defenses like multi-factor authentication (MFA). One popular AiTM kit called [Mamba 2FA](#) involves a CAPTCHA challenge to fool automated scanners from detecting the phishing page. Other kits may use reverse proxy techniques; all AiTM tactics are geared towards circumventing traditional security and authentication measures to steal credentials.

## AiTM Phishing Attacks Are Growing

**77%**

of phishing sites use turnstiles  
to prevent automated scanning<sup>1</sup>

## Email Filters Don't Stop Every Threat

**93%**

of phishing compromises  
bypassed email security<sup>1</sup>

## MFA Is Not A Silver Bullet

**84%**

of compromised accounts  
had MFA enabled<sup>1</sup>

Plus, if your employees ever use their personal email on a business device, your existing solutions have no visibility or protections to stop credential theft.

# Kill Attacks Directly in the Browser

To defeat modern phishing attacks, security teams need to harden their defenses where identity compromise actually occurs—the browser. Obsidian Security offers an in-browser AiTM phishing prevention solution that **stops 100% of popular AiTM kits** like Evilginx and Tycoon.












Sitting in the browser, Obsidian Security deeply inspects web content using advanced visual and content analysis plus applied threat intelligence to instantly block malicious webpages as soon as they render—even for never-before-seen AiTM phishing kits or threats to personal inboxes.

By seeing what the user sees, Obsidian is able to thwart AiTM evasion techniques that bypass Abnormal and other security solutions.

“A spear phishing email was sent to the inboxes of our sister company. It bypassed their email security completely undetected. But as soon as a user clicked on the link, we got an alert from Obsidian. Within minutes, the team was able to quarantine those emails and block the websites.”

Leading financial services company

## Head-to-Head Comparison: Obsidian vs. Abnormal

	 <b>OBSIDIAN</b>	<b>Abnormal</b>
<b>Phishing Delivery Method</b> Corporate email, viewed on a managed device		
Personal email, viewed on a managed device		
<b>Detection Efficacy &amp; Blocking</b> Detect Evilginx and other proxy-based AiTM toolkits		
False positive reduction through device/browser attestation		
Stop zero day phishing attacks		

Abnormal Security primarily operates after emails have been delivered. While this is effective for catching advanced threats, it means that novel malicious emails might reach users' inboxes if their models have not seen these new attack patterns. Obsidian Security conducts deep visual and content inspection of webpages, meaning even if new techniques are used, threats are still able to be detected before credentials are stolen.

Combining Obsidian Security with Abnormal or other email security tools provides defense in depth to better protect your business from a wide range of popular and sophisticated identity-targeted attacks.

## Privacy-First Protection



### Local Analysis

Everything is done locally in your browser, guaranteeing privacy and fast performance



### Flexible Deployment

Deploy in minutes across major browsers to instantly stop identity threats



### Easy Management

Get automated protection from day one, no ongoing tooling or extra work needed



### Trusted Protection

Leading enterprises trust Obsidian, including 35+ from the Fortune 1000 and Global 2000

## The Obsidian Advantage

Detected threats continuously inform and refine security rules through Obsidian's AI-powered dynamic feedback loop, delivering automated defenses that adapt as your organization grows. This ensures full visibility and proactive protection across SaaS.

[Get Started for Free](#)

