

# Timeline of a Malvertising Attack

How malicious ads go from idea to threat and how Malvertising Defense helps ad tech platforms protect their publisher clients from this ever-evolving threat.

#### Malvertising threats for Platforms



Redirects away from publisher sites



Ad cloaking to execute clickbait scams



Redirects to malicious landing pages



Distribution of malware



Client-side injections to steal user info



Pixel/Video Stuffing



Bad actor creates malicious code and sets up a programmatic campaign



Bad actor submits their campaign for creative review



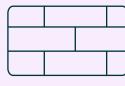
Pre-scanning blocklist tools check for malicious activity in creative, but malvertiser's tactics evade detection



Bad actor's campaign wins auction bid

### **Without HUMAN**

Blocklists try to catch known bad actors



Where Other

**Solutions Fall Short** 

High False positive and negative rates

Non-malicious ads can get blocked, causing unwanted revenue loss

**Add Latency** 

Size of the blocklist can cause latency on pages due to list load

# **Protected by HUMAN Malvertising Defense**



Patented behavioral engine scans a sample of creatives and monitors for malicious behavior in creative and on landing page in real-time



Platform alerted to any malicious behavior to block



Threat API is updated in real-time



Site visitors don't see malicious action, platform reputation and



revenue are protected

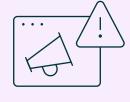


Code executes malicious

activity

Creative renders

Malicious activity affects publisher site and damages platform's reputation



**Easy to Evade** 

Blocklists are reactive and only as good as the entries within them.

# Malvertising Defense Advantage



**Protect Revenue** with More Precision



Preserve Brand Reputation



**Optimize Performance** and Overhead



**Prevent Visitor** Harm

## Take Control of Your Digital Ad Inventory