Timeline of a Malvertising Attack

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

1. **Bad actor creates malicious code and sets up a programmatic campaign**
2. **Pre-scanning blocklist tools check for malicious activity in creative, but malvertiser's tactics evade detection**
3. **Bad actor submits their campaign for creative review**
4. **Bad actor’s campaign wins auction bid**
5. **Blocklists try to catch known bad actors**
6. **Creative renders**
7. **Code executes malicious activity**
8. **Malicious activity affects publisher site and damages platform's reputation**

Without HUMAN

- **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
- **Easy to Evade**
  - Blocklists are reactive and only as good as the entries within them.
- **Put Revenue at risk**
  - Blocking ads and requesting new creative can risk revenue or diminish user experience

Where Blocklist Solutions Fall Short

Protected by HUMAN Malvertising Defense

- **Malvertising Defense scans a sample of creatives and monitors for malicious behavior in creative and on landing page in real-time**
- **Platform alerted of any malicious behavior to block**
- **Threat API is updated in real-time**
- **Publisher clients never receive malicious ads, platform reputation and revenue are protected**

Malvertising Defense Advantage

- Preserve Revenue
- Protect Brand Reputation
- Optimize Performance and Overhead

Take Control of Your Digital Ad Inventory

Find out how HUMAN uses modern defense strategies to help platforms safeguard their publisher partners and revenue from malicious ads. Visit HUMAN to request a demo.