



# Fastly Threat Report it-sa 2023

Jay Coley

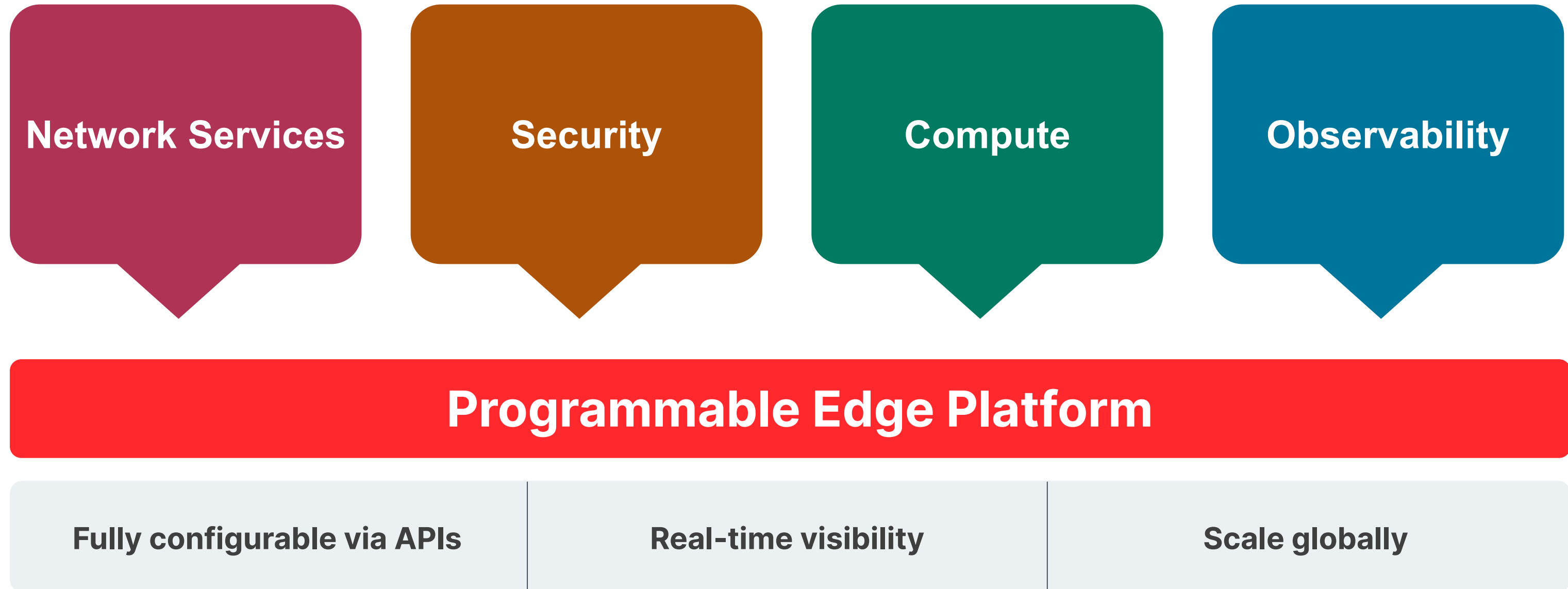
October 2023



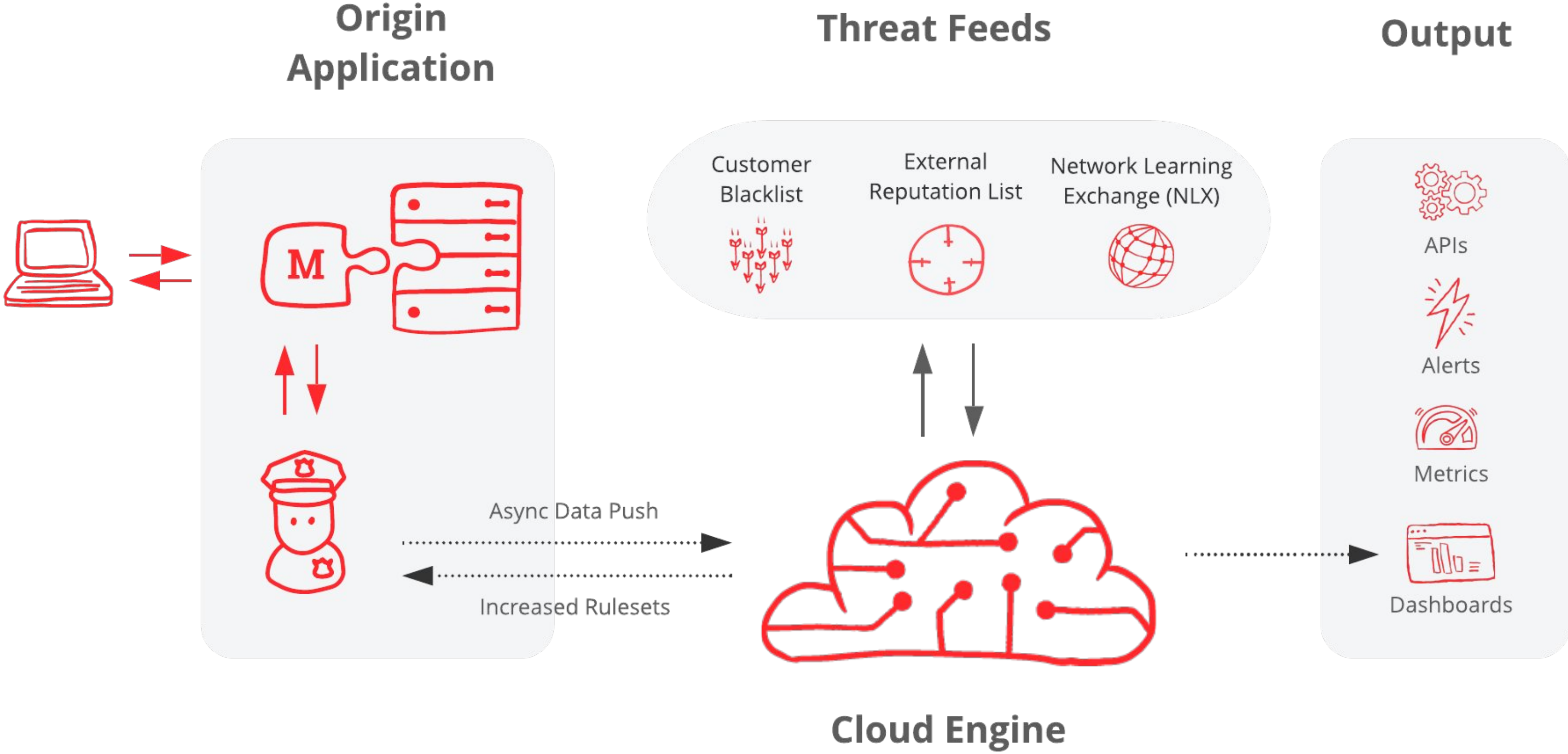


Making the internet a better place, where all  
experiences are  
**fast, safe and engaging**

# Snapshot of our portfolio



# Network Learning Exchange Threat Visibility



# Meet the Network Learning Exchange (NLX)

Fastly's proprietary IP reputation intelligence

## How NLX works

NLX flags validated malicious IPs as they visit your apps for decisioning

## Why it matters

54% of attack traffic is preemptively flagged by NLX

## What it enables

Stop attackers before they strike.

## Preemptive

Stop attacks before damage is done with Fastly's proprietary IP reputation intelligence

## Actionable

Block, rate limit, monitor, or generate rules to automatically engage flagged IPs

## Timely

Uncover real threats flagged within minutes and visible for 24 hours



## Trusted

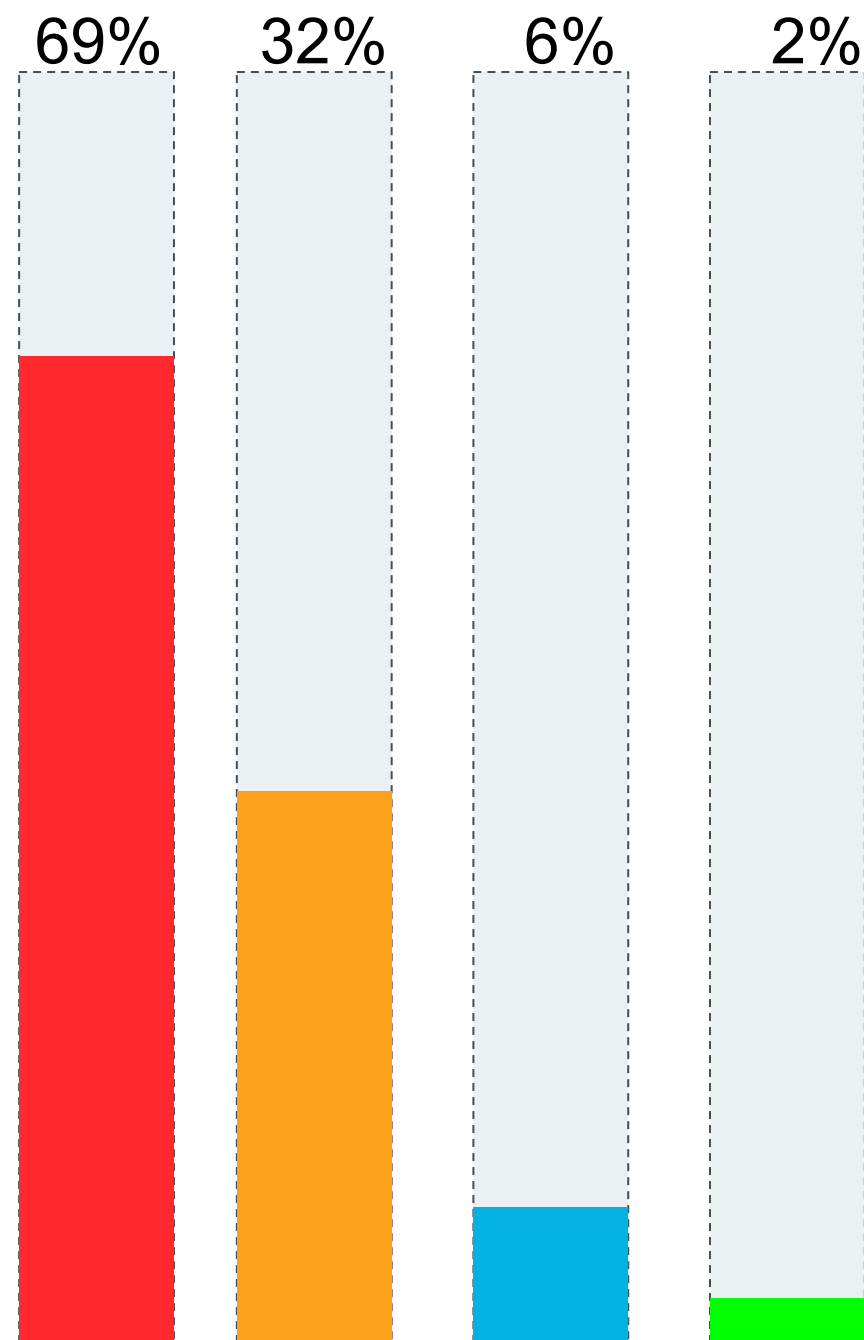
Leverage insights continuously fed by over 90,000 global customer apps and APIs

## Accurate

Root decisions in validated threat intelligence from patented contextual detection



# Network Effect Threat Report - Observations

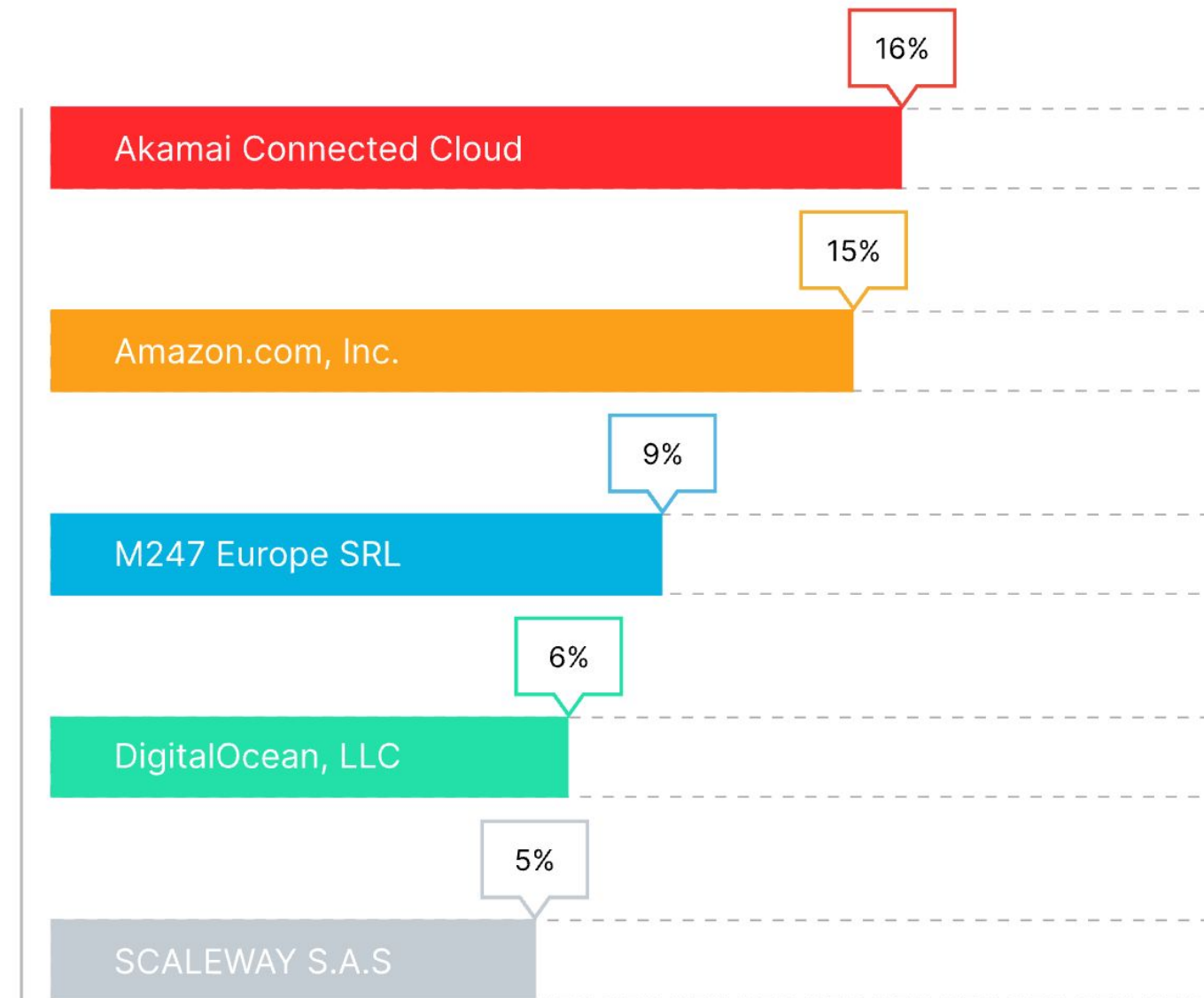
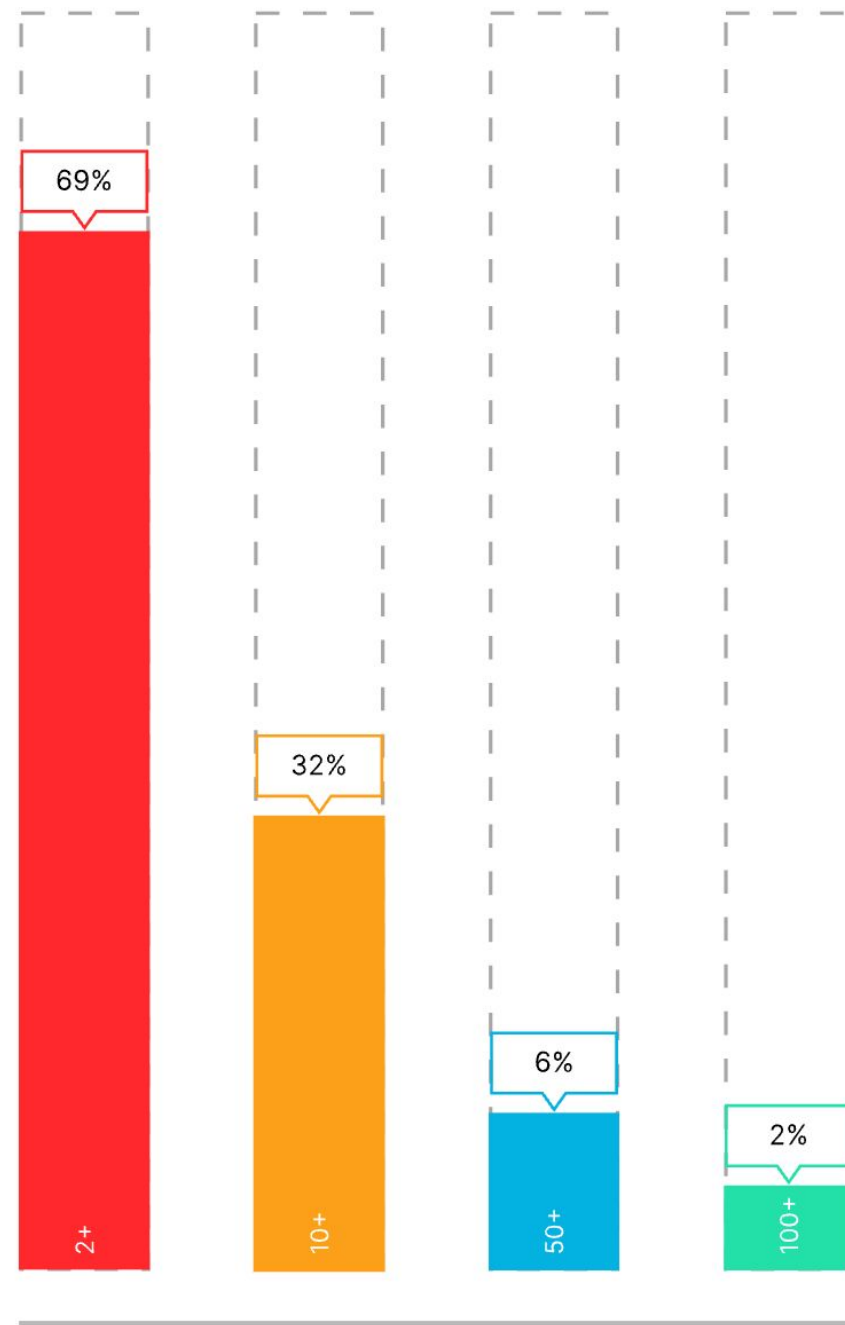


- Malicious IPs targeting multiple organisations
- 69% targeted multiple organisations / customers
- 64% targeted multiple industries / verticals
- *It's critical to have this visibility in securing applications.*



# Attackers are focused on multiple customers

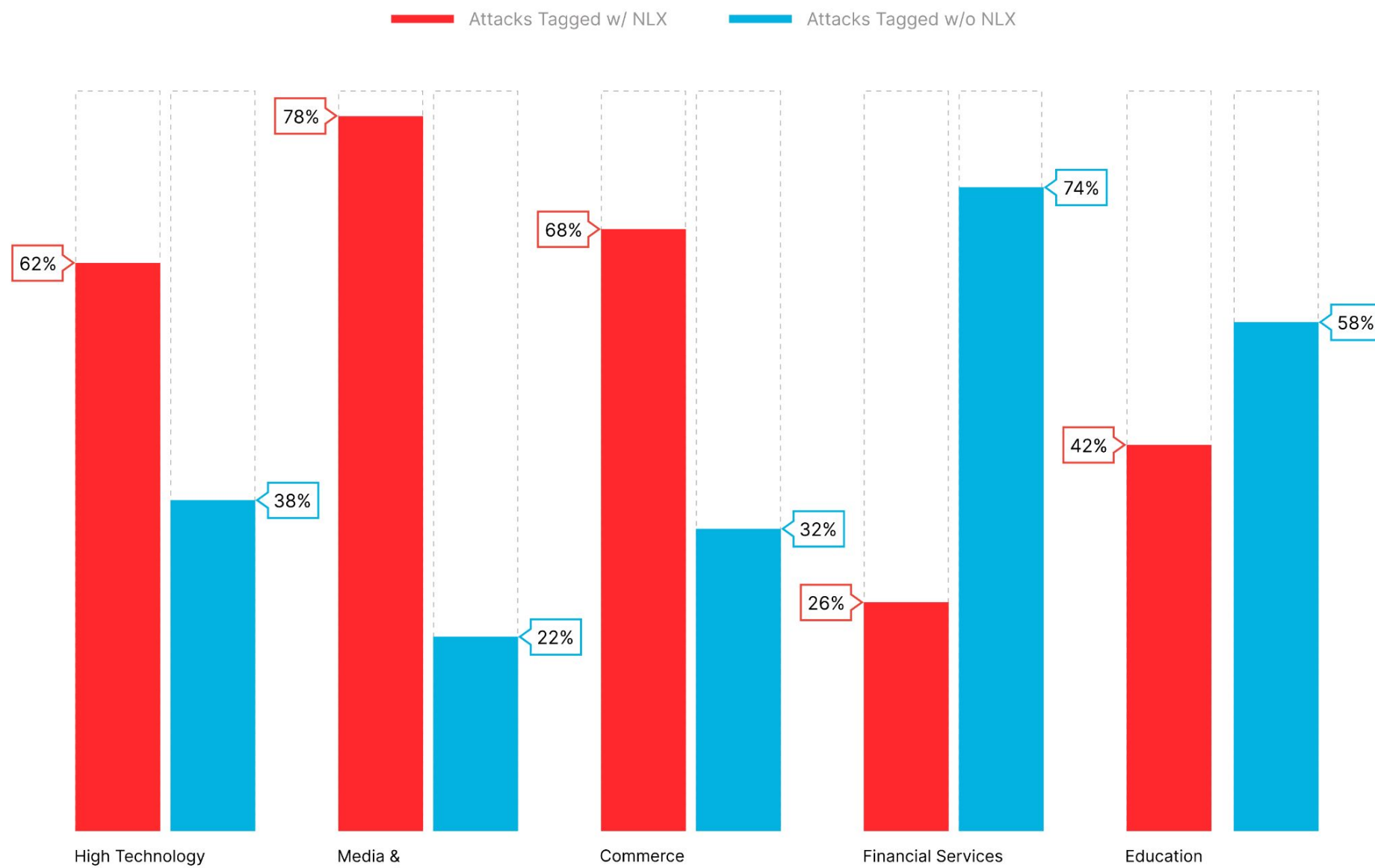
*Most of the attack traffic coming from Akamai (Linode) and Amazon*



- 69% of IP addresses targeted multiple customers
- 64% of IP addresses targeted multiple industries

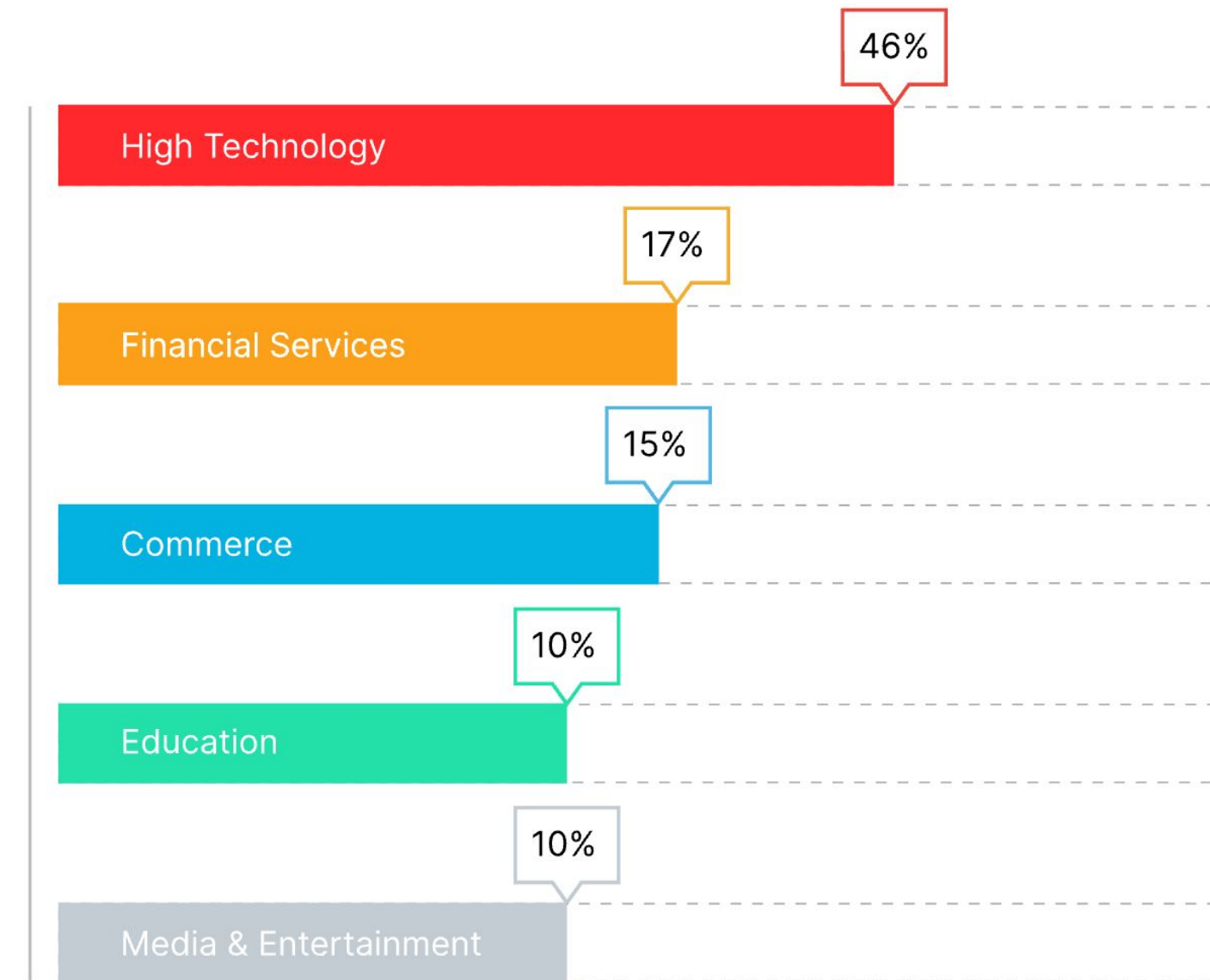


# NLX Attack data by industry



Attack traffic with and without NLX by industry

- The **Media & Entertainment sector** experienced 56% more attacks tagged with NLX
- The **Commerce industry** experienced 36% more attacks tagged with NLX
- The **High Tech industry** experienced 24% more attacks tagged with NLX.



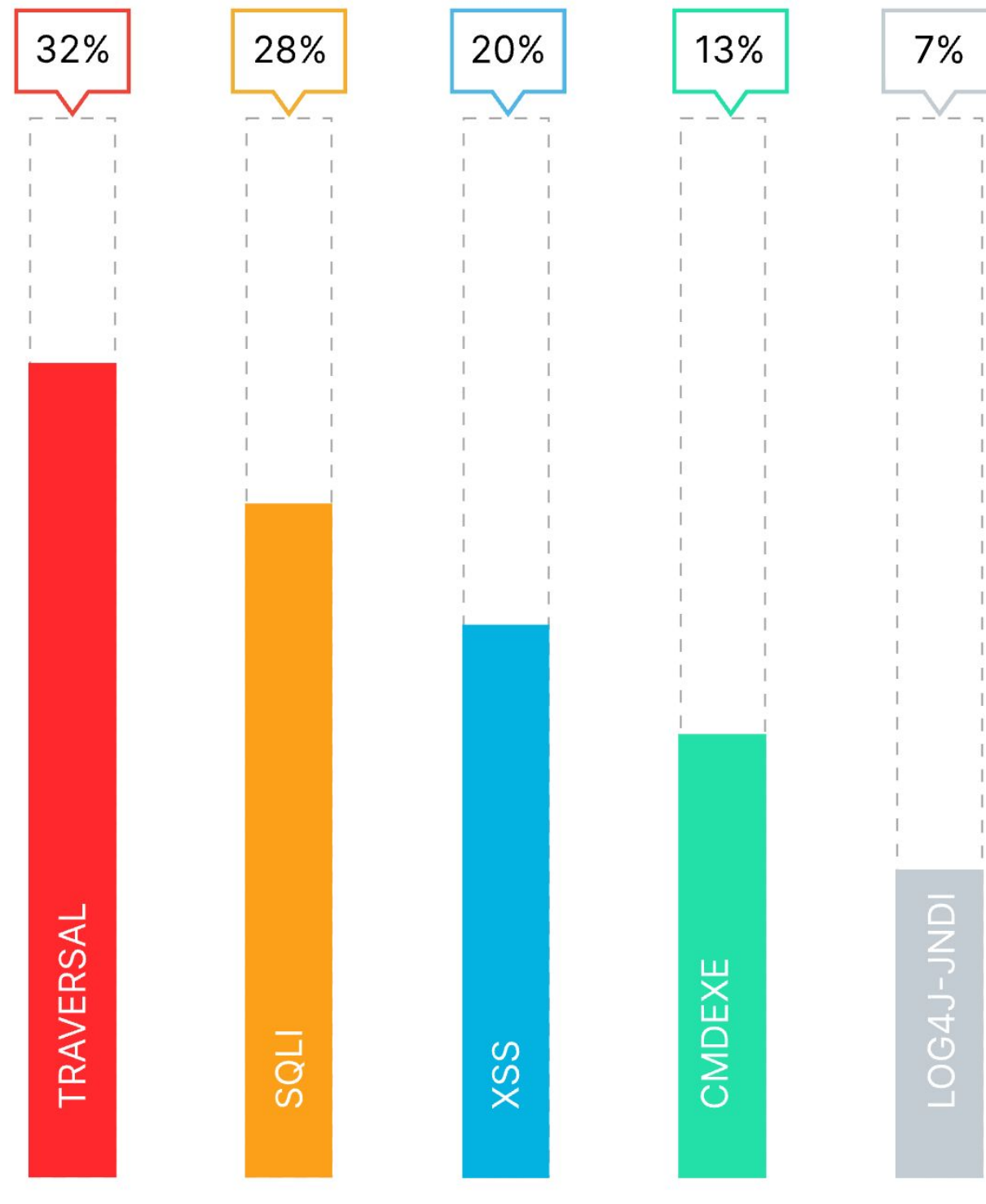
NLX attack traffic by industry

- The **High Tech industry** was targeted the most with 46% of NLX Traffic
- The **Commerce industry** experienced 36% more attacks tagged with NLX
- The **High Tech industry** experienced 24% more attacks tagged with NLX.

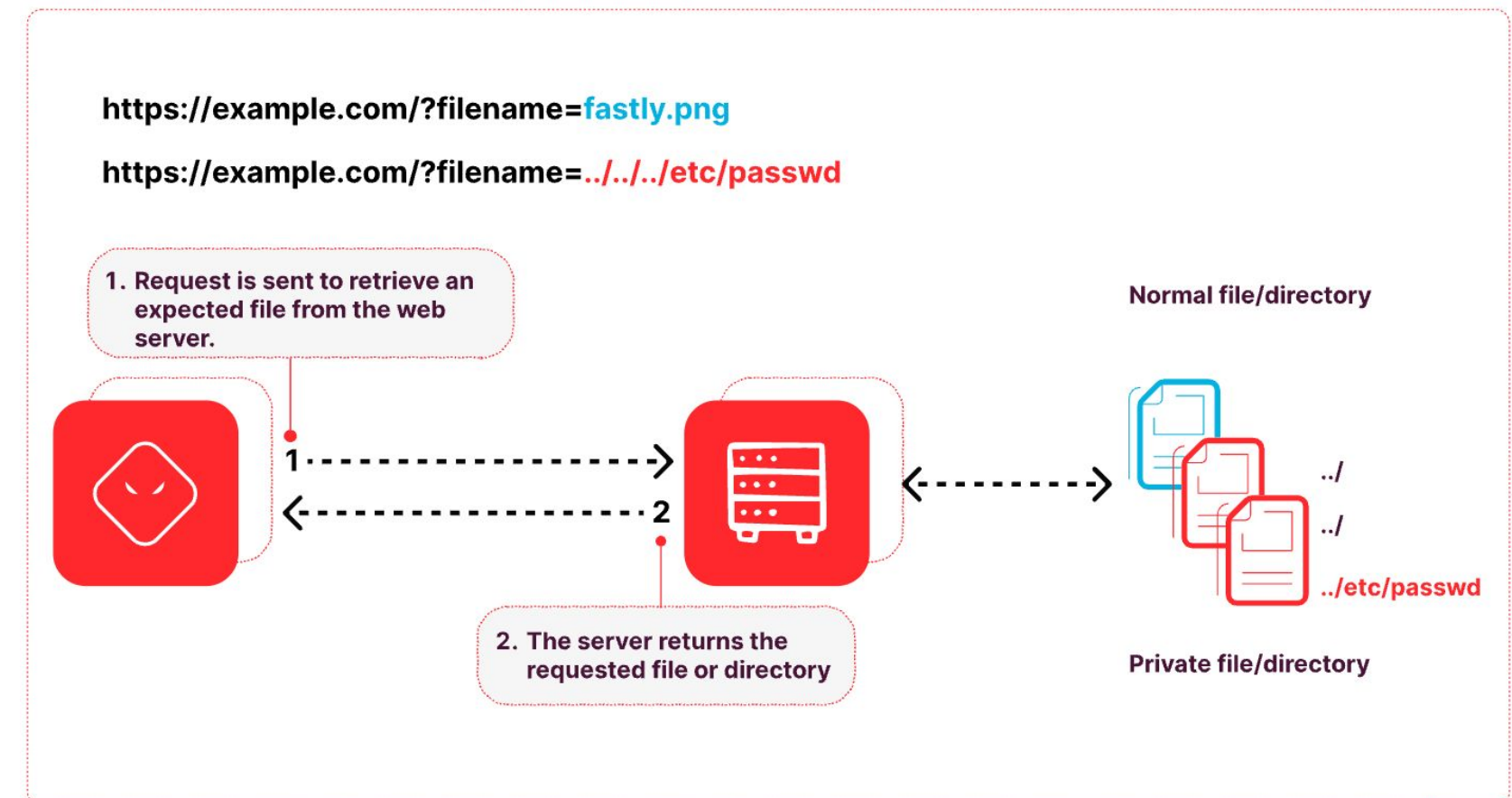
\*\* The **Media and Entertainment industry** benefited the most from the NLX's network effect \*\*



# Top Web and API Attacks



Top web and api attacks tagged by NLX

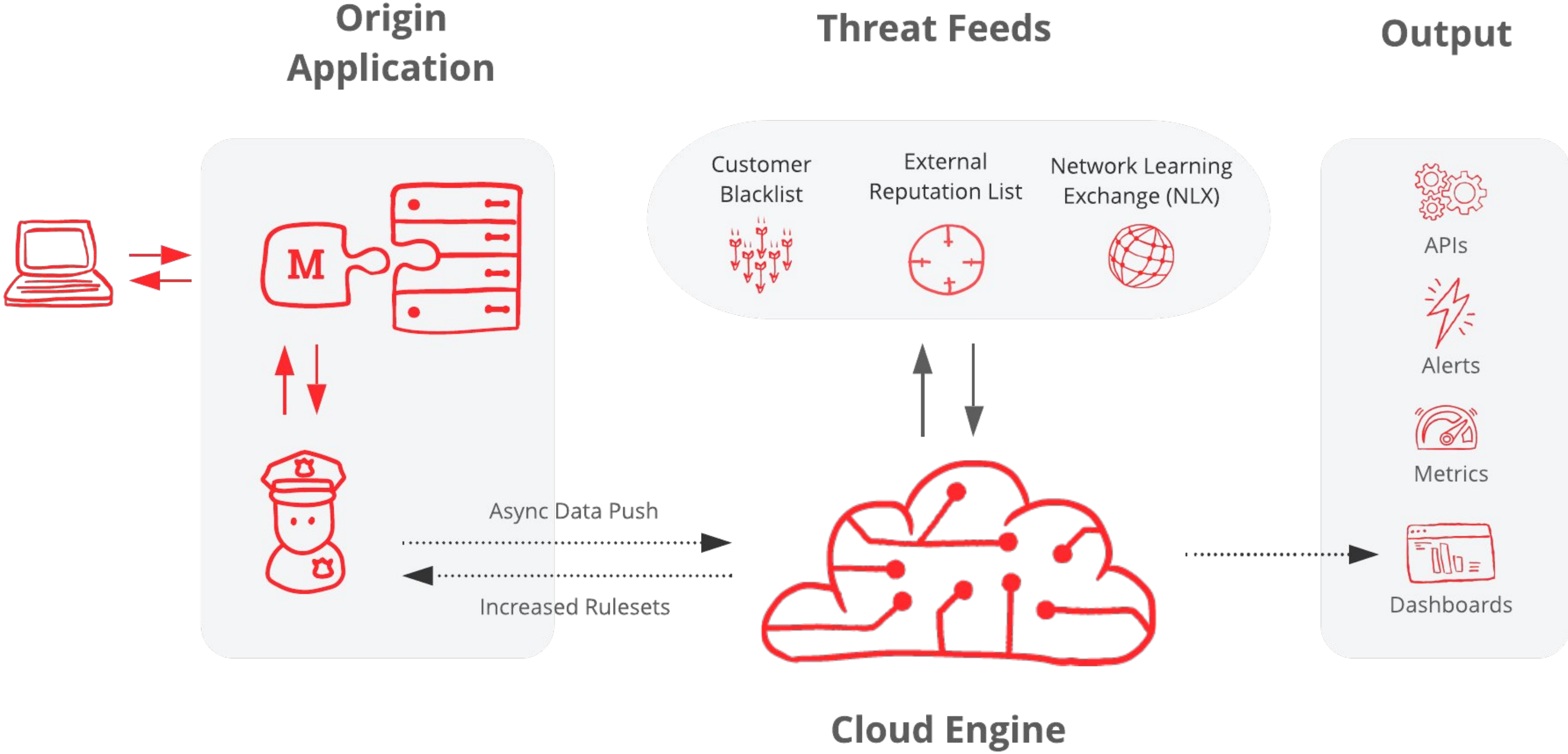


**Traversal vulnerabilities** enables attackers to read or write unwanted files, allowing them to reveal sensitive information, modify application data, and are commonly used to chain attacks together which can lead to remote code execution (RCE).

The preference for traversal could suggest that attackers are primarily focused on finding ways to execute arbitrary commands that can be used to **install malware, launch ransomware, and exfiltrate data.**



# Network Learning Exchange Threat Visibility



# Summary - See what's important and act

Type	Request rule
Conditions	<p>all of</p> <p>Signal exists where</p> <p>any of</p> <ul style="list-style-type: none"><li>Signal Type equals Tor Traffic</li><li>Signal Type equals SigSci IP</li><li>Signal Type equals Malicious IP</li></ul> <p>Signal exists where</p> <p>any of</p> <ul style="list-style-type: none"><li>Signal Type equals Attack Tooling</li><li>Signal Type equals Backdoor</li><li>Signal Type equals CMDEXE</li><li>Signal Type equals SQLI</li><li>Signal Type equals Traversal</li><li>Signal Type equals XSS</li></ul>
Actions	<p>Block</p> <p>Add signal</p> <ul style="list-style-type: none"><li>Known Attacker (corp)</li></ul>

- Unlocks visibility into your web traffic.
- Actions and automation based on near real time intelligence.
- Reduction in log mining and correlation services.
- Expedite legitimate traffic and block attackers at the door.

