Warding Against the Dark Arts

Crafting a Defense Strategy against DDoS attacks

Shirleen Sharma & Aaron Heady

Roadmap

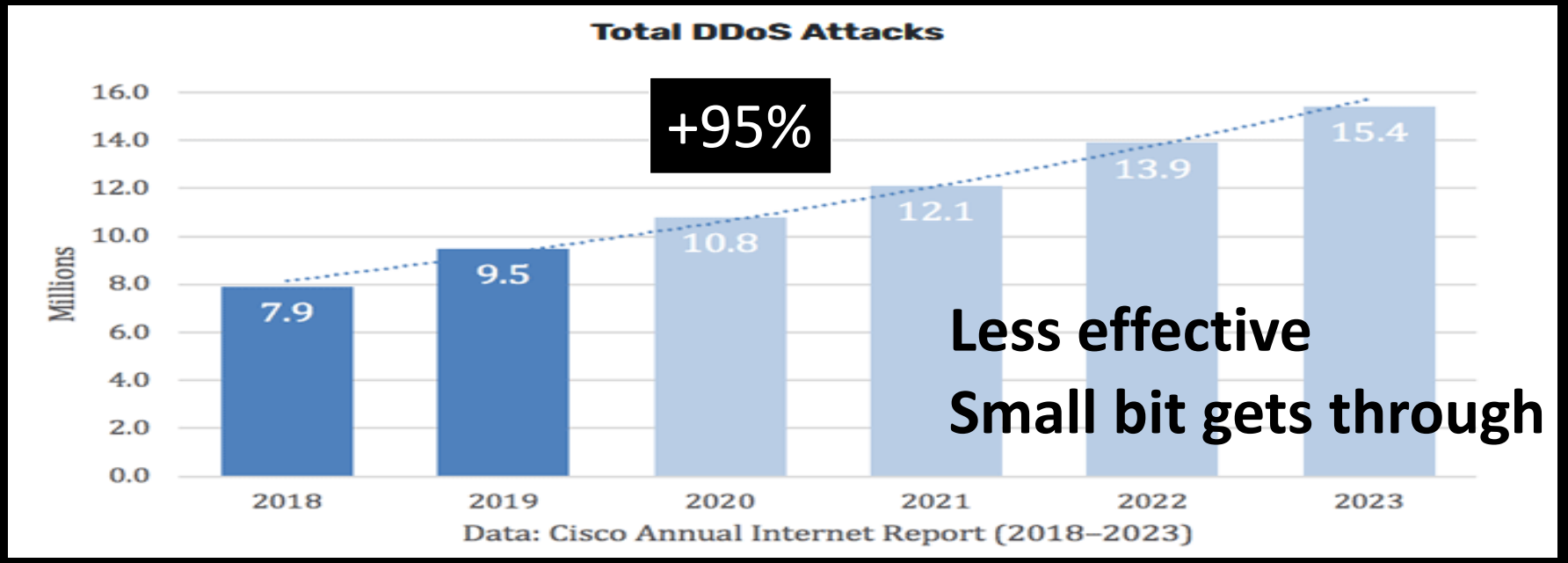
Why should you care?

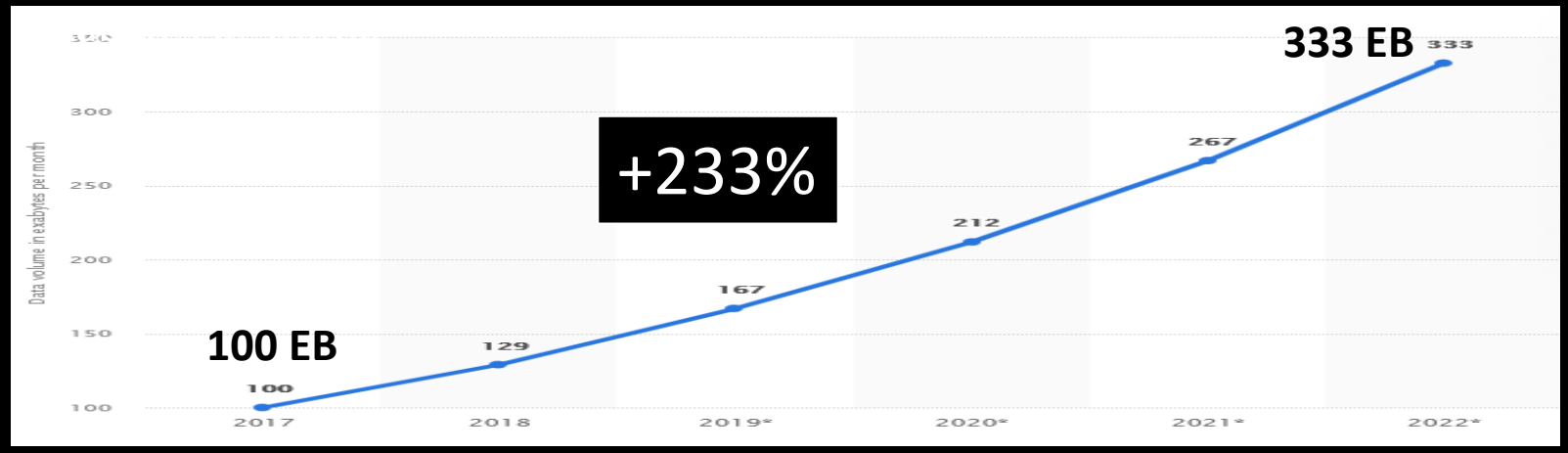
What other benefits does this work have?

How to get started?

What else?

Attacks are increasing with the growth of the Internet





2017 2020 2022

You can be down for as long as an attacker has more resources than your response strategy can absorb.

- ***DDoS-as-a-Goal***
- ***DDoS-as-an-Extortion***
- ***DDoS-as-a-Distraction or Opportunity***
- **Best Strategy**
- ***FBI** Report DDoS Extortion at https://www.ic3.gov/*

But how do customers feel about DDoS?

Yet again I find myself feeling that there just isn't a harsh enough punishment for the scum who do stuff like this. (ransomware, DDOS etc.) Strapped down naked in desert sun? ... Put into an iron maiden while the door is closed ever so slowly?

As a customer of <<company>>, I am extra irritated by this.

If <<company>> pays the ransom, I will be looking for a new <<service>> provider.

If the extortion is a Molotov cocktail, paying the ransom is picking it up off the floor of your house and tossing it into your neighbor's house. And it simply guarantees that they will be hit again in the future, because they're known to pay.

I do think we should start calling these attacks what they are, though: cyber terrorism...

https://arstechnica.com/gadgets/2021/09/canadian-voip-provider-hit-by-ddos-attack-phone-calls-disrupted/?comments=1&comments-page=1

Audience Survey

Who has been attacked by a DDoS?

Of those, who took actions that mitigated it, versus it just stopping on its own?

Who thinks they are adequately investing in DOS preparedness?

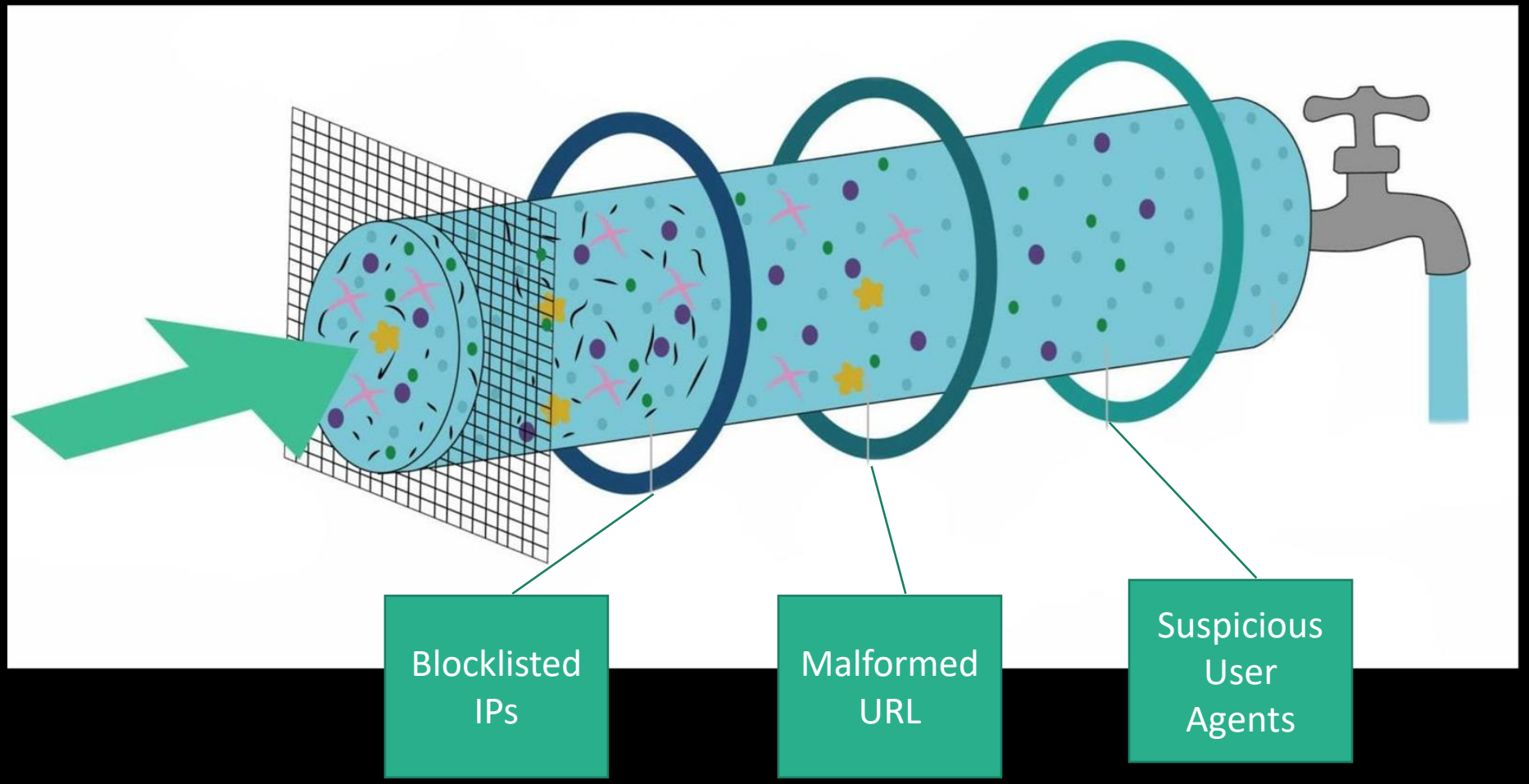
The capacity test you never asked for.

Service-wide *Graceful Degradation* is the most comprehensive strategy.

How do you know you're under attack?

- Increase in Failure Rates
- Increase in Latency
- Unresponsive Services
- Unexplained Traffic Shifts
- Simultaneous Incidents across Stack

What does a good request even look like?



Demo

Load Demo

Start

Total Traffic 303
Errors: 93
Degraded: 115

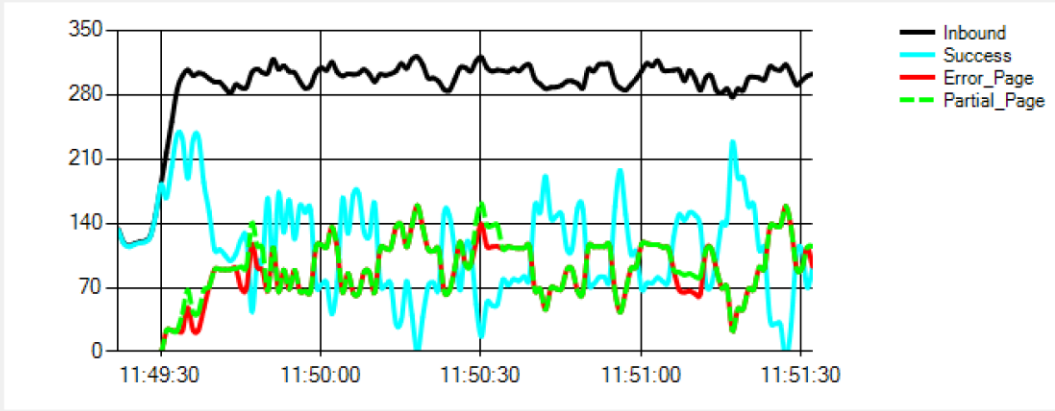
Current Load: 75

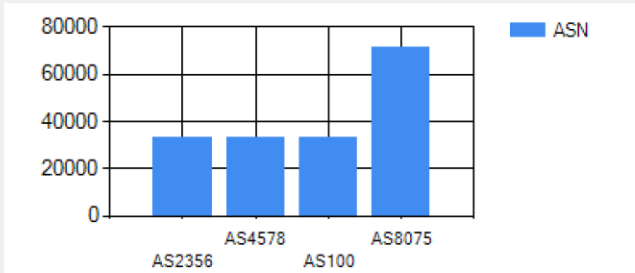
DC West
110

DC Central
121

DC East
106

- [ ] Blockade
- [x] Graceful Degradation
- [x] Expensive Content
- [x] Reduce Algo Count
- [x] Disable Low Engageme
- [ ] Lazy Load





Generate

HttpHeaderUrlPath
^\/search$
match
X-FD-RevIP
,asn=AS8075,

Graceful Degradation

Definitely Not a Search Engine

Search Suggestions

Image Answer

Entity Details

Search Results

Algo Result 1
Algo Result 2
Algo Result ...
Algo Result ...
Algo Result 11
Algo Result 12

Related Topics

Map Answer

Below The Fold

49°F
Mostly cloudy

Search

ENG

11:49 AM
3/23/2023

Blocking requests

```
######################
# ICM xxxxx queries from <ASN>
# triggering 404 or overloading backend services
######################
rule
match
HttpHeaderUrlPath
^\/search$
match
X-FD-RevIP
,asn=<ASN>,
```

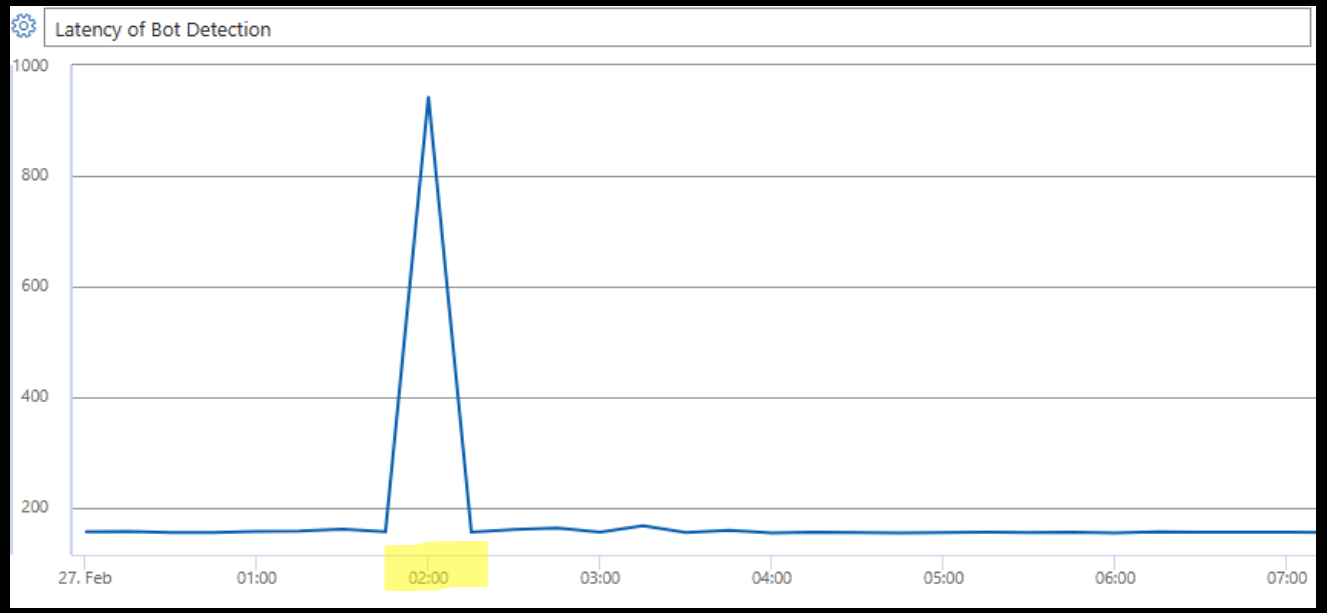
Where to block the request

On a normal Tuesday

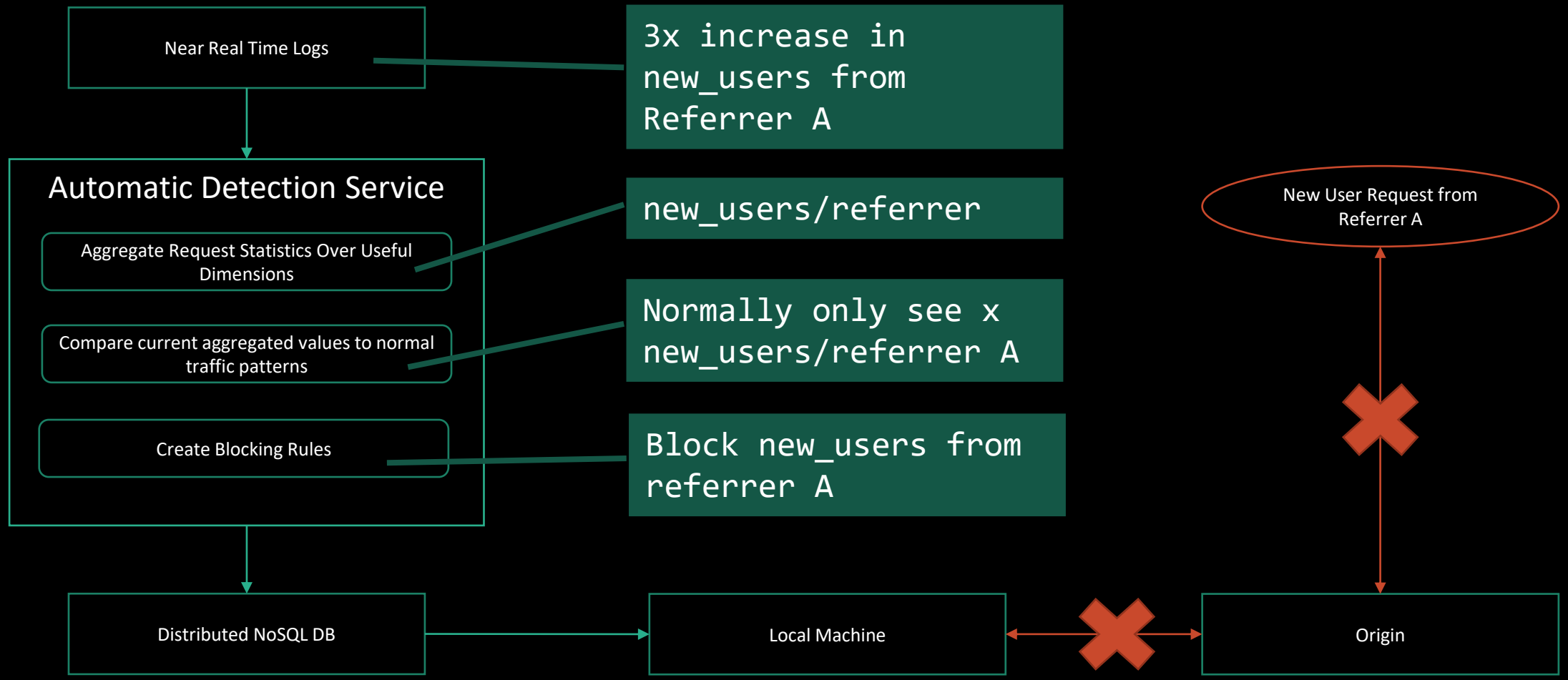
- Identify and protect real users
- Filtering happens further down the request pipeline to minimize collateral damage

During a DDoS Attack

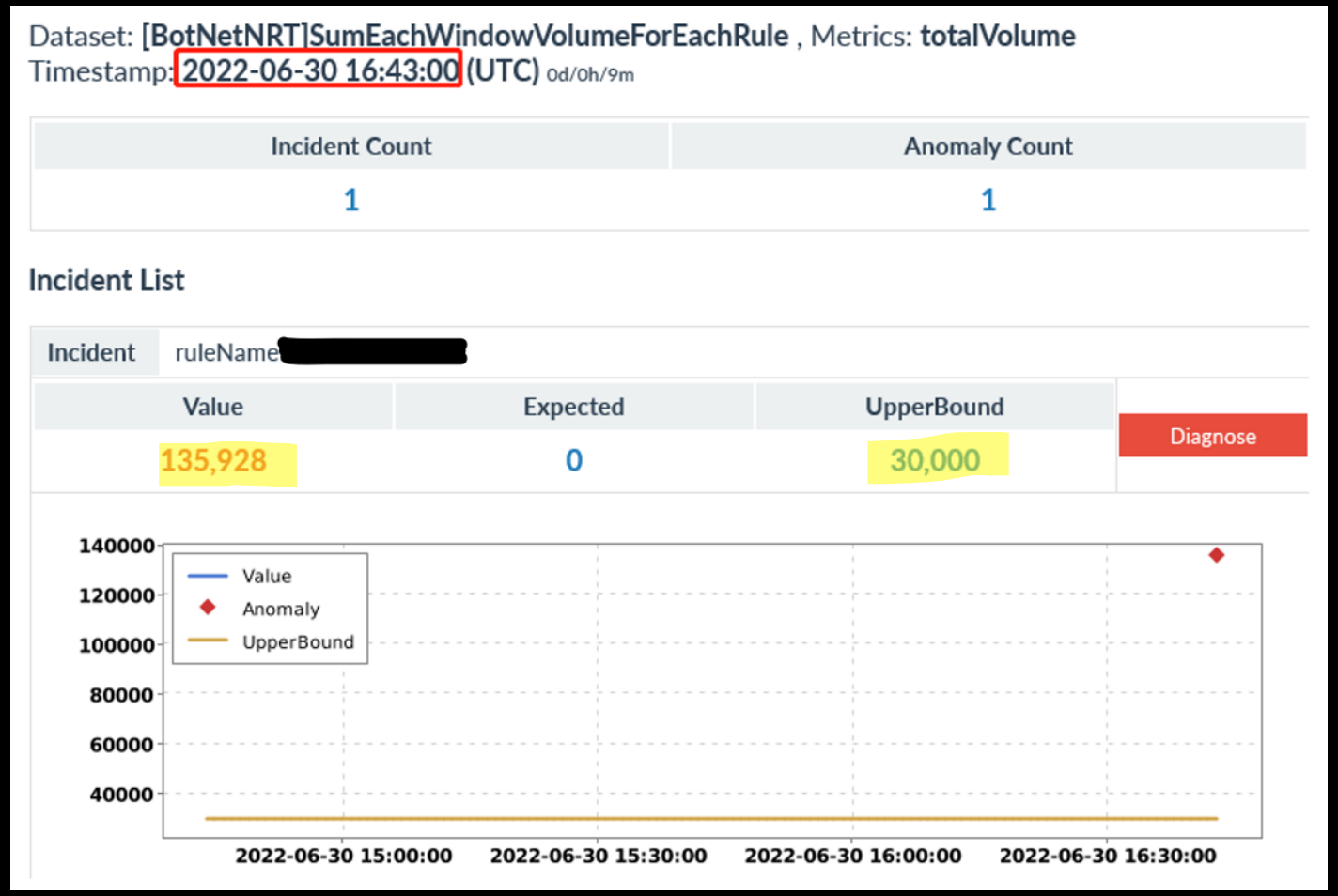
- Protect the service
- Filtering is done right at the start of the request pipeline



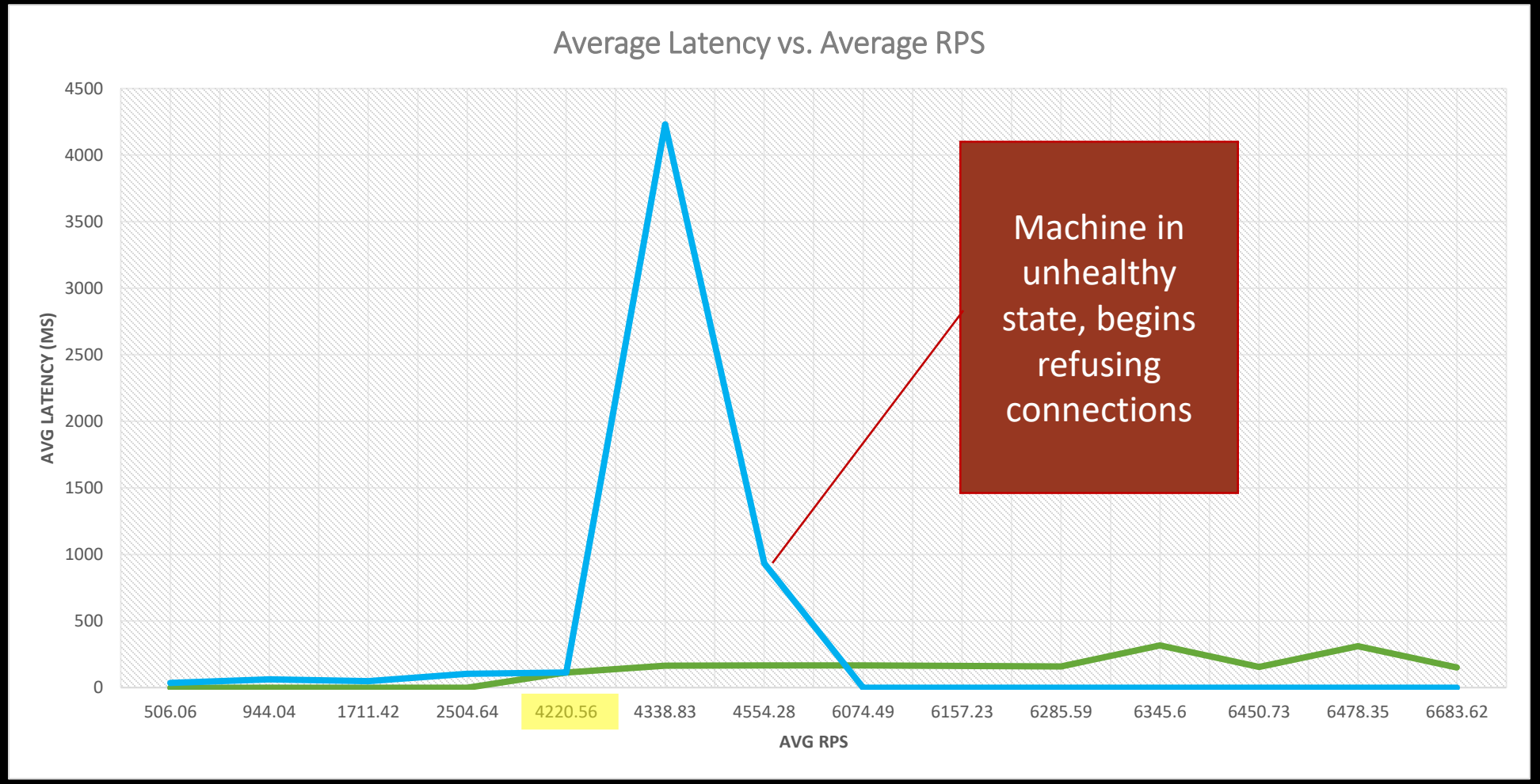
Moving to Automatic Detection



Moving to Automatic Detection



Designing for Failure



Recap

Detect attacks reliably

Block traffic based on important request parameters

Automatic detection and rule creation

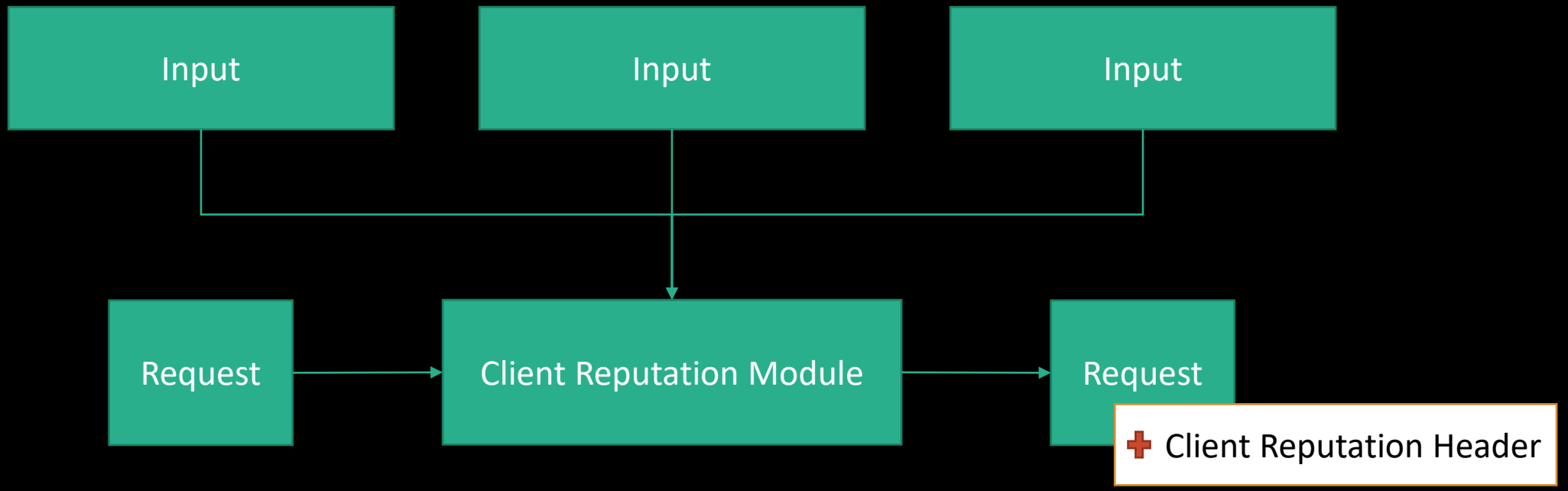
Local Rules as final layer of protection

Minimizing Collateral Damage

- Throttle
- Deprioritize
- Return a lighter experience
- Redirect
- Captcha

Client Reputation

Determining how “reputable” a request is, and the risk it may pose to your service


Input
Input
Input
Request
Client Reputation Module
Request
Client Reputation Header

Summary

MVP	Nice to Have
• Robust near real-time logging and metrics • Inexpensive blocking	• Automatic Detection • Client Reputation • Graceful degradation

Questions