RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: CCS-W05

Building a Cloud Security Solution in a Multi-Tenant Environment

David Andrews

Lead Engineer – Security Core
Verizon Digital Media Services
@daveisangry | @VerizonDigital

#RSAC

Why Should You {stay,go}?

But first...what can you expect from this talk?

1. Insight into our architecture
   - Skip scalability iterations
2. Lessons learned from multi-tenant ModSecurity
3. Practical tips for event log delivery (via rsyslog)

<structured_talk_is_structured>

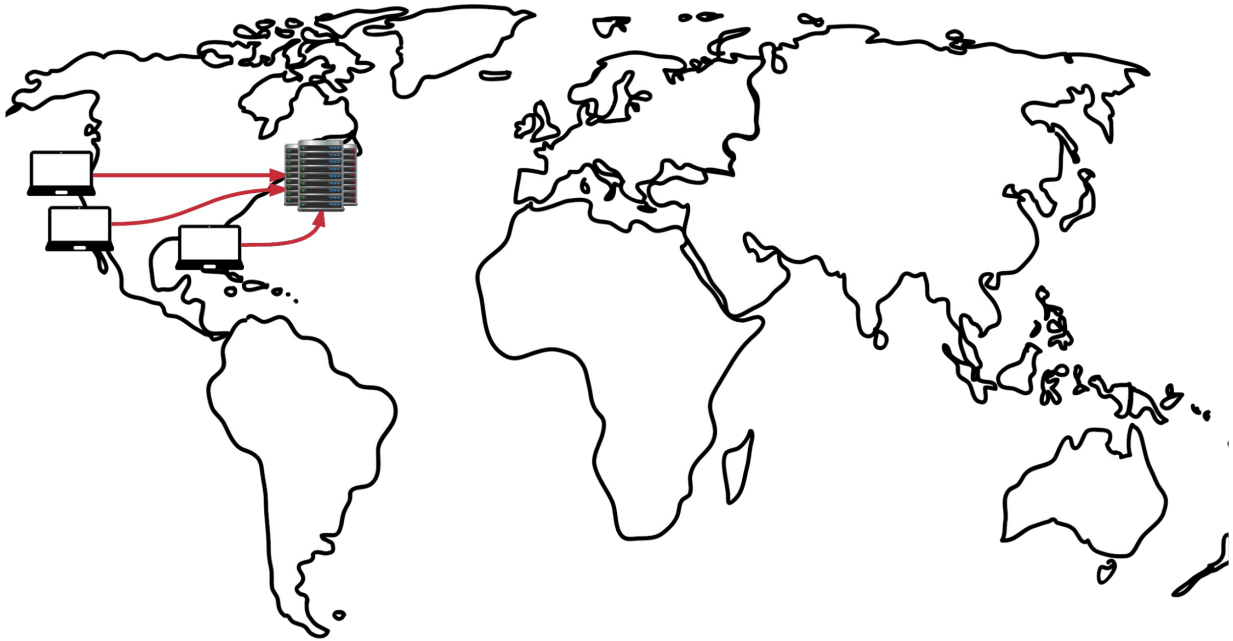
- Intro to Content Delivery Networks and WebSec | *3 minutes*
- EdgeCast Network WebSec | *20 minutes*
- Forging in the white-hot fires of Production | *20 minutes*
- Conclusion and Questions | *the rest of the time...*

Content Delivery Networks and WebSec

In the beginning
there were websites...

So simple

...



Content Delivery Networks and WebSec

In the beginning
there were websites...

So simple

...

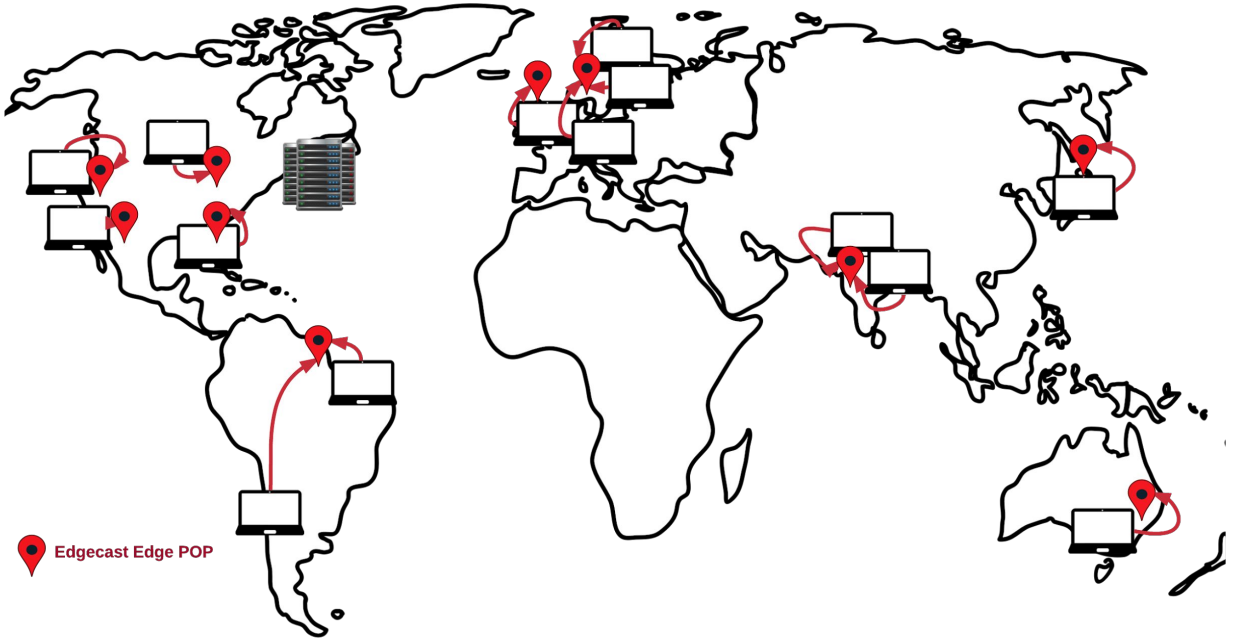
Uh oh, people want to use it from everywhere!

Content Delivery Networks and WebSec

Enter the Content Delivery Network (CDN)

Scalable

Global

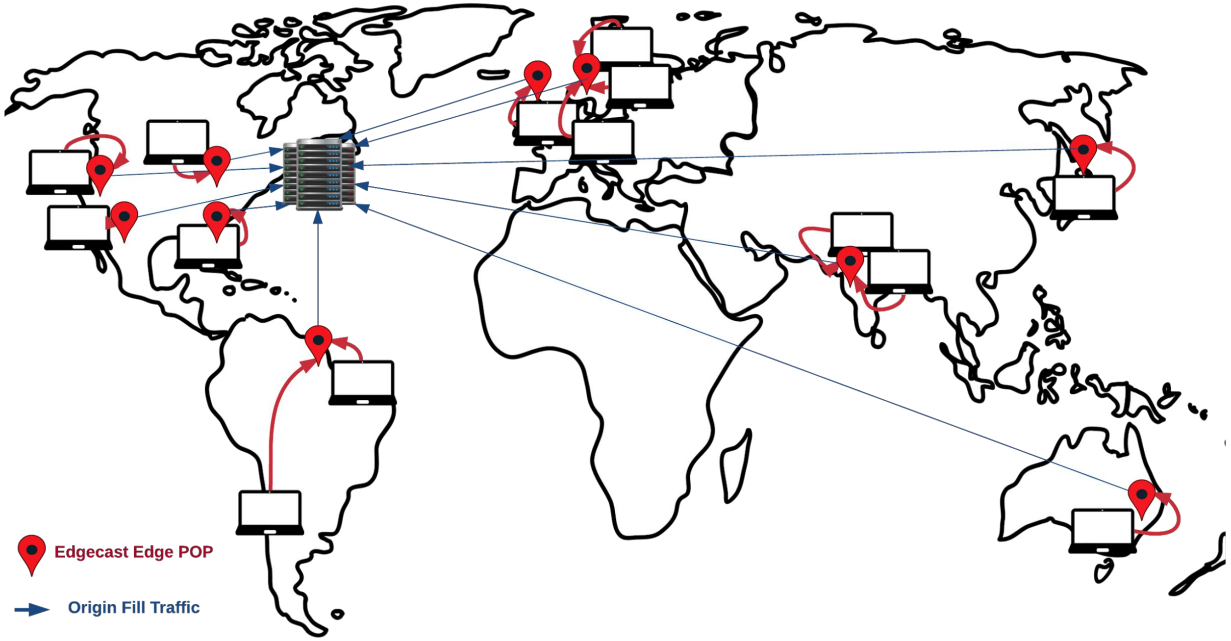


Content Delivery Networks and WebSec

Enter the Content Delivery Network (CDN)

Scalable

Global



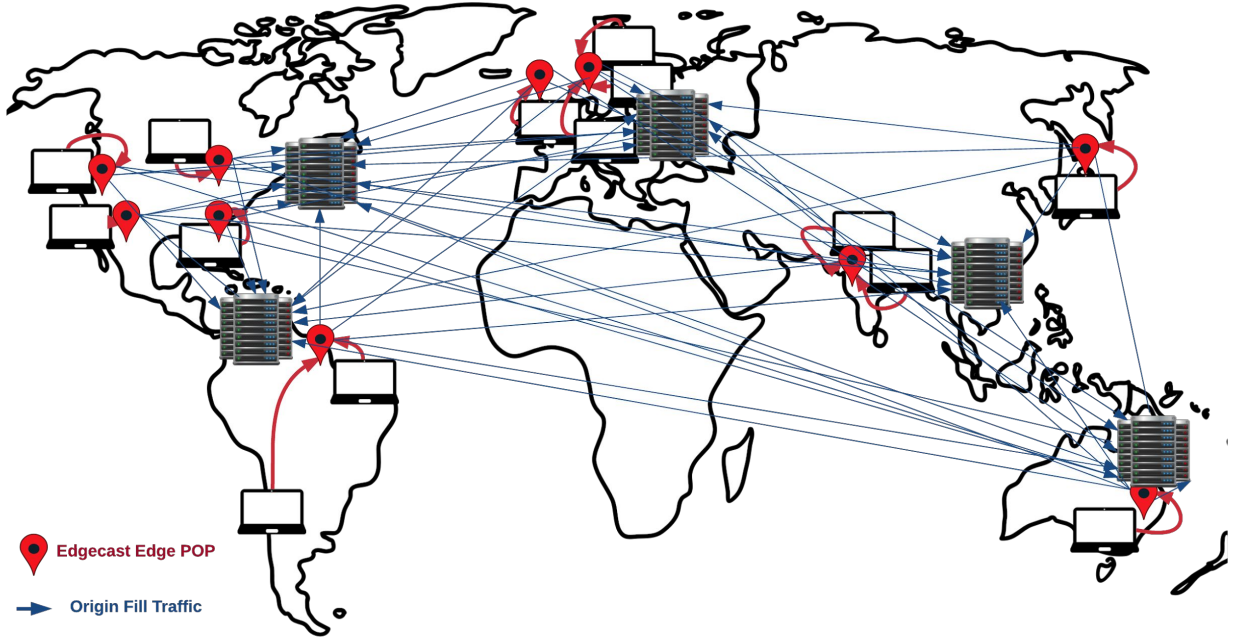
Content Delivery Networks and WebSec

Enter the Content Delivery Network (CDN)

Scalable

Global

Multi-tenant



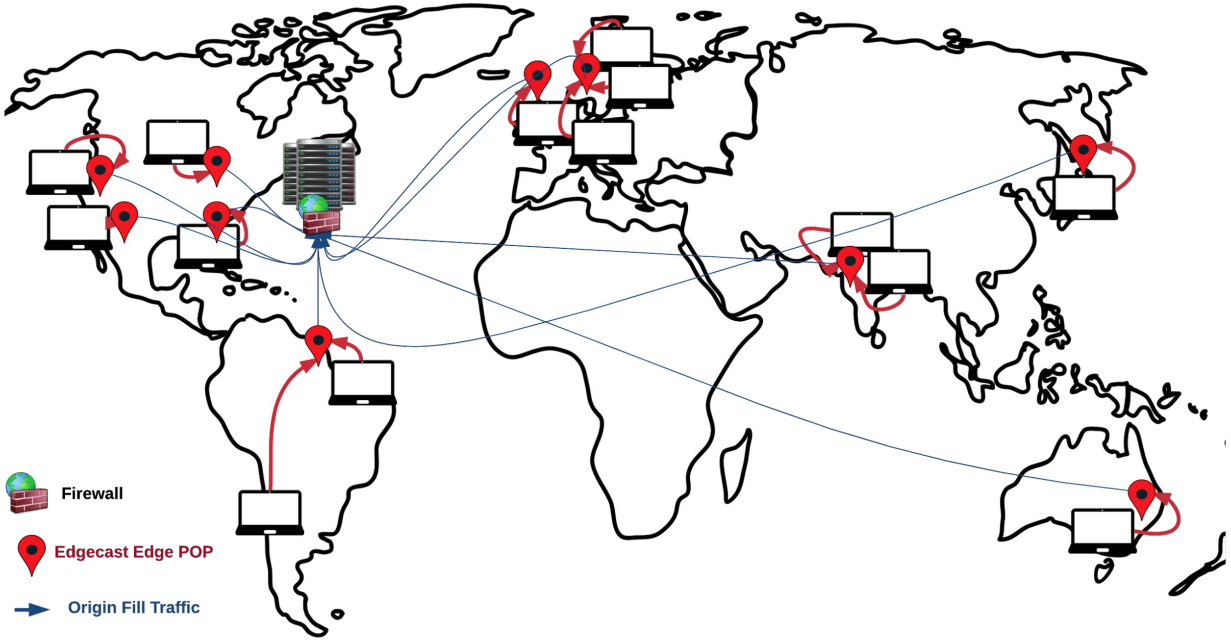
Content Delivery Networks and WebSec

Oh there is money on the Internet?!

Great!

...

And now we need a firewall...



Content Delivery Networks and WebSec

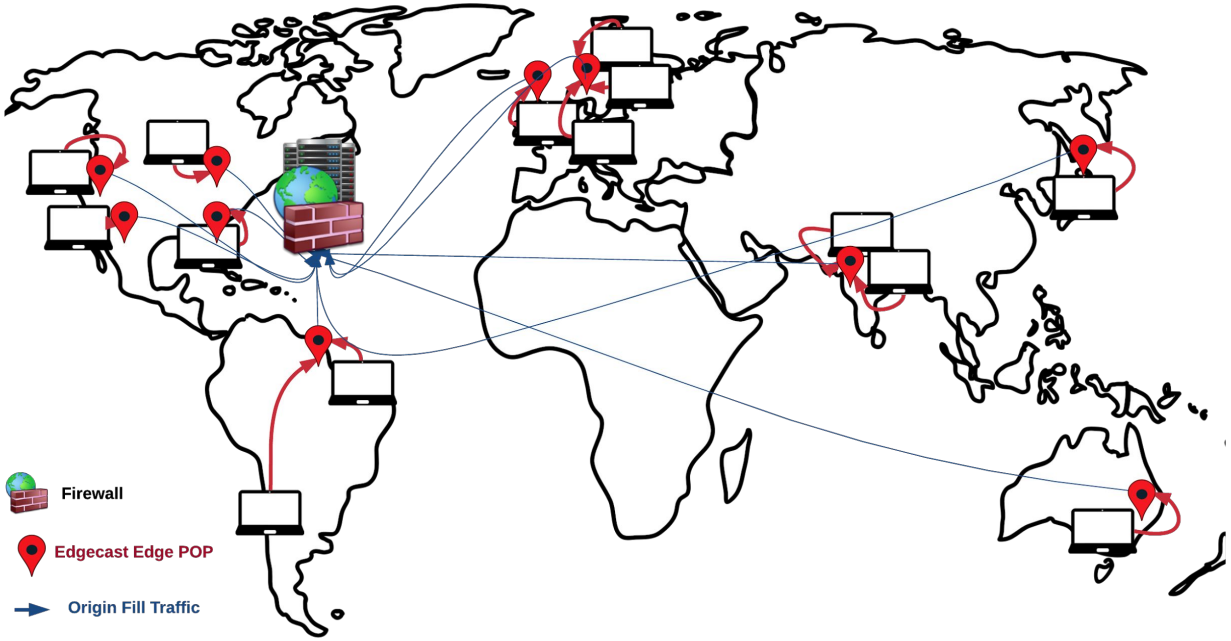
Oh there is money on the Internet?!

Great!

...

And now we need a firewall...

And now we need a bigger one!

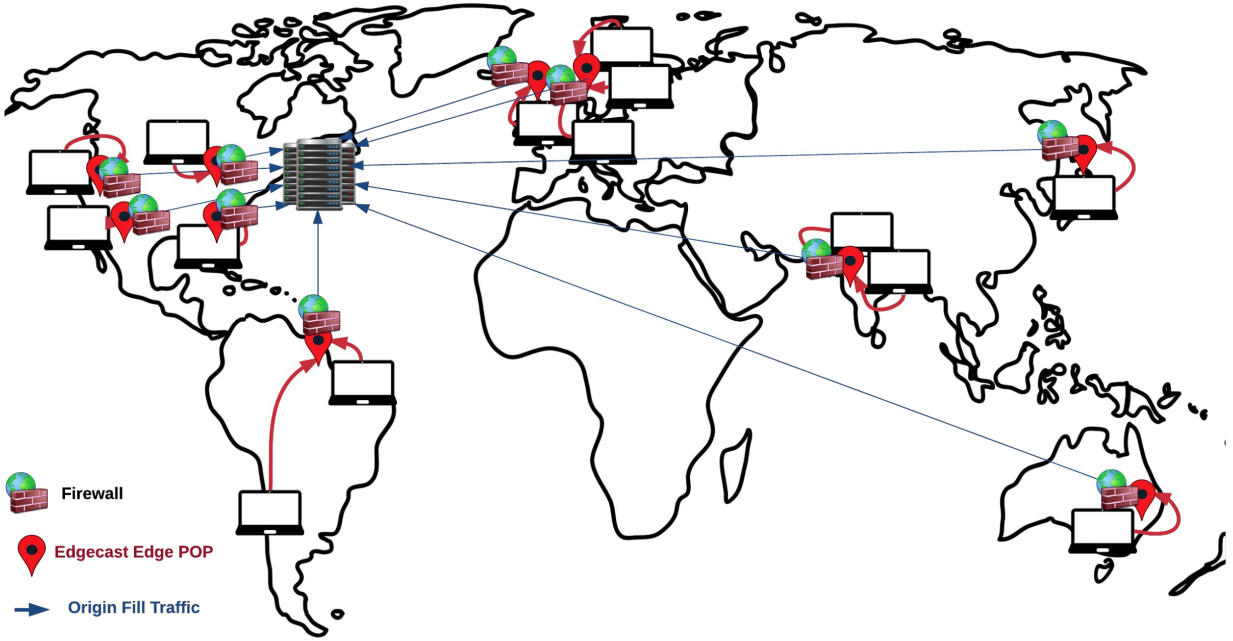


verizon

Content Delivery Networks and WebSec

We can just pay someone else to do this?

We're already paying that CDN thing...



The Task: WebSec on our CDN

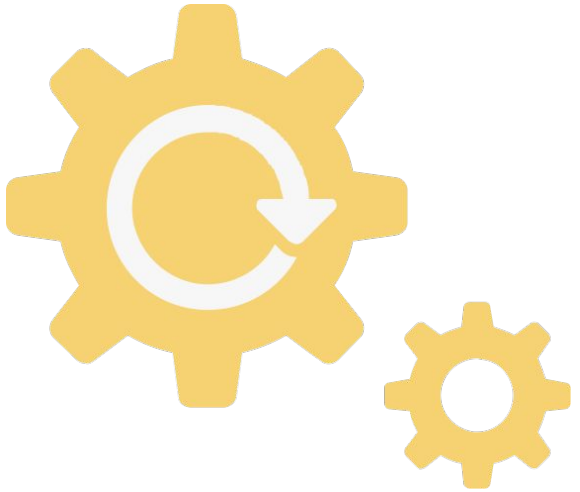
- WebSec for Verizon's Edgecast Content Delivery Network (Verizon CDN)
- Project 0: WAF
- Same features as on-premise solutions (of course)
  - Real-time configuration updates
  - Real-time dashboards
  - Highly customizable
- Nevermind that it's somewhat more complicated...

Edgecast Network WebSec - Early Decisions

- ModSecurity WAF
  - Open source, active community
  - Excellent rulesets available (OWASP, Trustwave)
  - Allows for encapsulated instances
- Runs as a module in Sailfish
  - Our HTTP server
  - For the performs

Edgecast Network WebSec - Config Updates

- Real-time requirements
  - Need to balance risk vs. flexibility
- Update between requests
  - Load new instance, replace old
  - Immediate code changes required to support this with no leaks
- Customers have two instances: Audit and Production
  - Allows seamless staging and promoting to prod



Edgecast Network WebSec - Config Updates

Atomic JSON Configs

- Verifiable
- Extensible
- All the good JavaScript things

```
    "name": "WAF Demo Instance 1",
    "enabled_date": "7/19/2016 10:07 PM",
    "id": "254",
    "prod_profile": {
        "access_settings": {
            "ip": {
                "blacklist": [],
                "whitelist": [
                    "127.0.0.1"
                ]
            },
...
        },
        "name": "trustwave test",
        "ruleset_version": "Latest",
...
            "allowed_request_content_types": [
                "application/x-www-form-urlencoded"
            ],
            "max_num_args": 512,
            "total_arg_length": 64000,
            "allowed_http_methods": [
                "GET",
                "POST",
            ],
            "arg_length": 8000,
            "arg_name_length": 10,
```

Edgecast Network WebSec - Config Updates

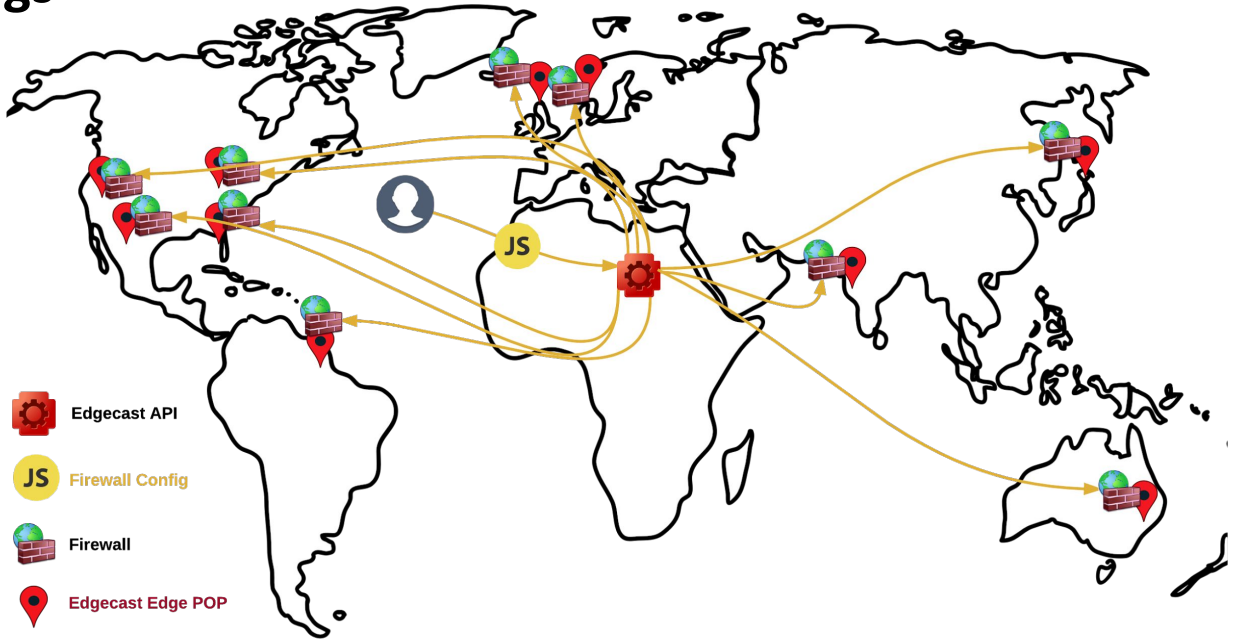
Atomic JSON Configs

Compiled down to native ModSecurity rules format by Sailfish right before loading

Edgecast Network WebSec - Config Updates

Atomic JSON Configs

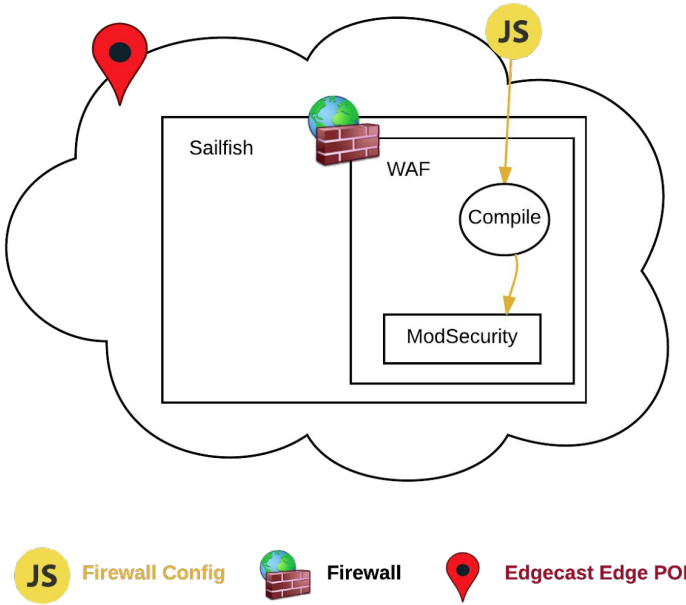
Compiled down to native ModSecurity rules format by Sailfish right before loading



Edgecast Network WebSec - Config Updates

Atomic JavaScript Configs

Compiled down to native ModSecurity rules format by Sailfish right before loading



Edgecast Network WebSec - Config updates

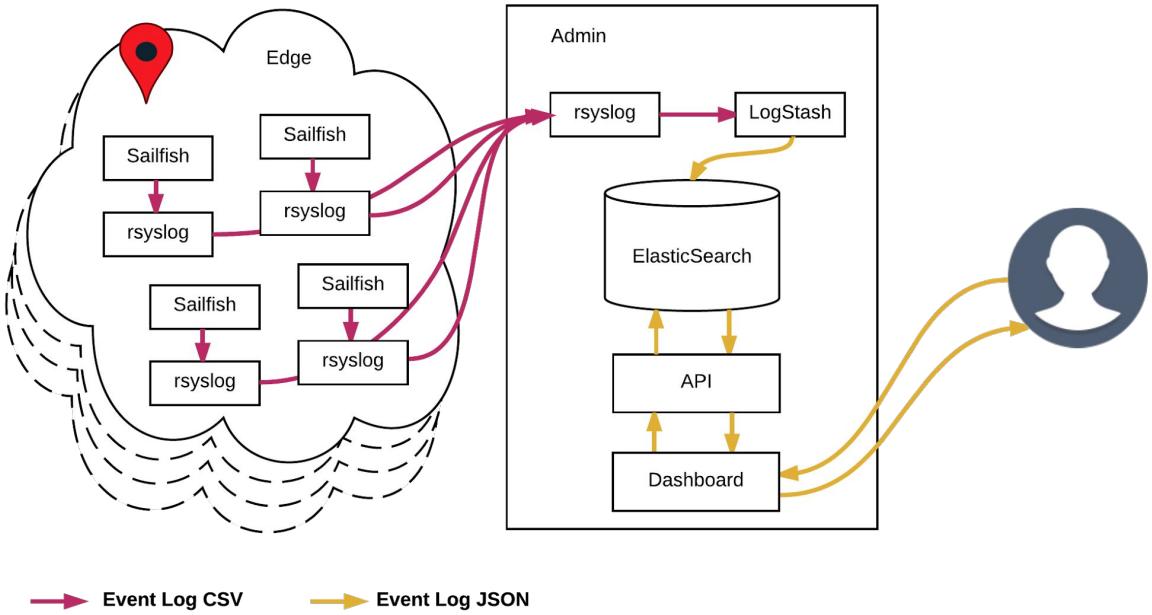
```
Include "/EdgeCast/waf/ruleset/Trustwave-OWASPIntegration-Application/modsecurity_crs_20_protocol_violations.conf"
Include "/EdgeCast/waf/ruleset/Trustwave-OWASPIntegration-Application/modsecurity_crs_21_protocol_anomalies.conf"
Include "/EdgeCast/waf/ruleset/Trustwave-OWASPIntegration-Application/modsecurity_crs_22_custom_ec_rules.conf"
Include "/EdgeCast/waf/ruleset/Trustwave-OWASPIntegration-Application/modsecurity_crs_23_request_limits.conf"
Include "/EdgeCast/waf/ruleset/Trustwave-OWASPIntegration-Application/modsecurity_crs_30_http_policy.conf"
Include "/EdgeCast/waf/ruleset/Trustwave-OWASPIntegration-Application/modsecurity_crs_35_bad_robots.conf"
Include "/EdgeCast/waf/ruleset/Trustwave-OWASPIntegration-Application/modsecurity_crs_40_generic_attacks.conf"
...
```

Rulesets re-used by many compiled configs

Edgecast Network WebSec - Dashboard

Event logging stack

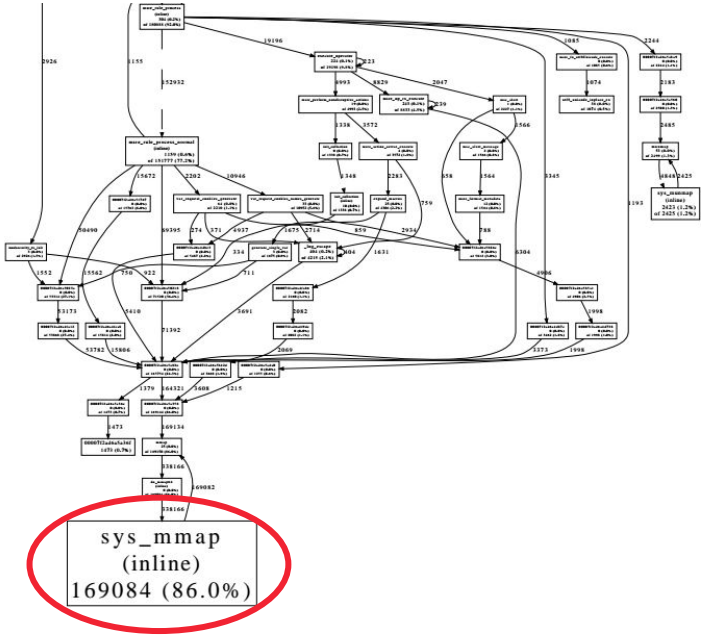
First version



Forging in the White-hot Fires of Production

CPU utilization issues...

Forging in the White-hot Fires of Production



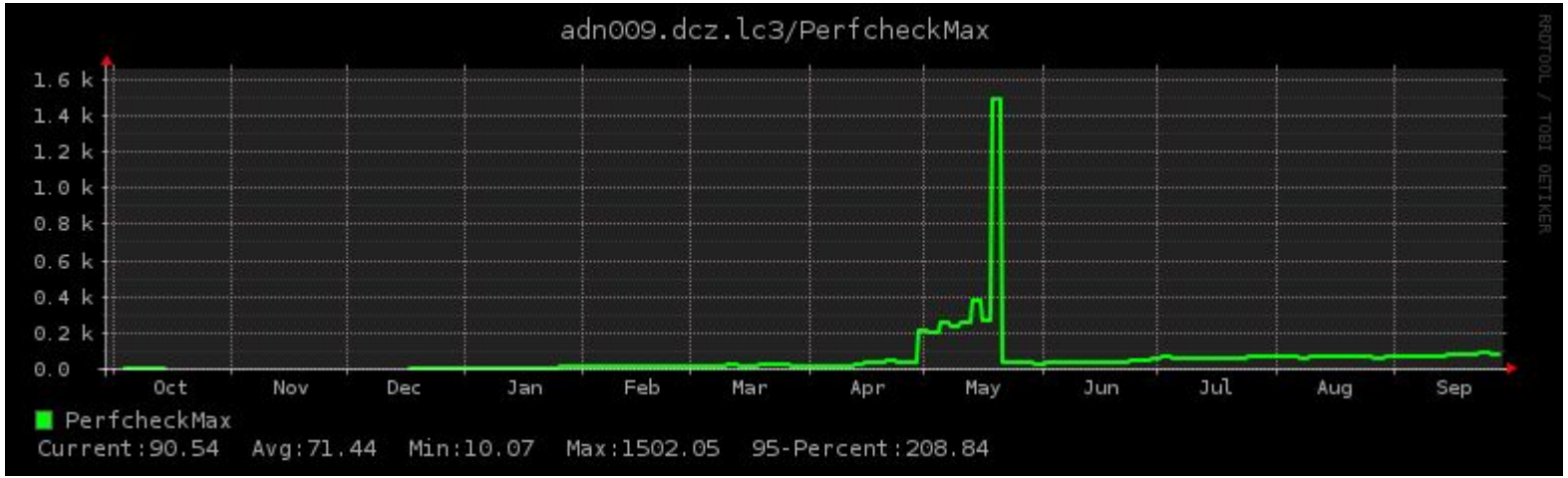
CPU utilization issues...

Forging in the White-hot Fires of Production

```
Tue May 19 20:28:29 dandrews@dandrews:~/Work/dev/git/play/apr$ grep
configure apr-1.4.6/debian/rules
./configure --host=$(DEB_HOST_GNU_TYPE)
   --build=$(DEB_BUILD_GNU_TYPE)
   --enable-layout=Debian --includedir=\$${prefix}/usr/include/apr-1.0
   --with-installbuilddir=\$${prefix}/usr/share/apr-1.0/build
   --enable-nonportable-atomics
   --enable-allocator-uses-mmap
```

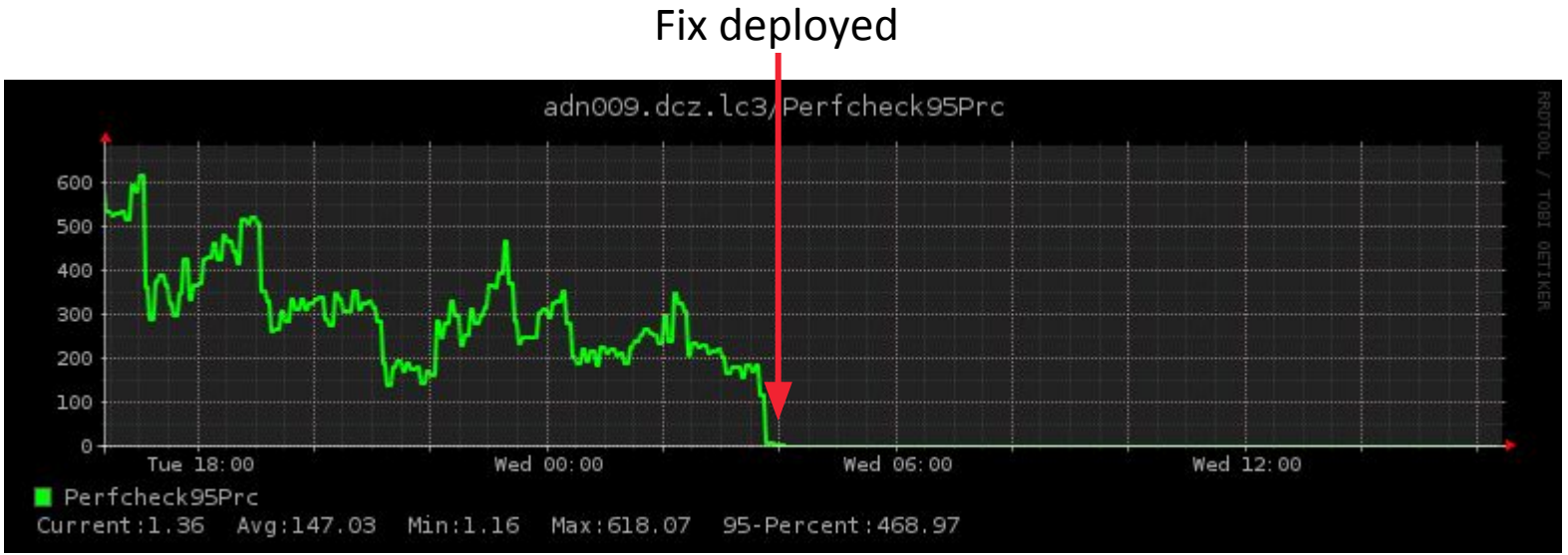
CPU utilization issues...

Forging in the White-hot Fires of Production



CPU utilization issues...

Forging in the White-hot Fires of Production

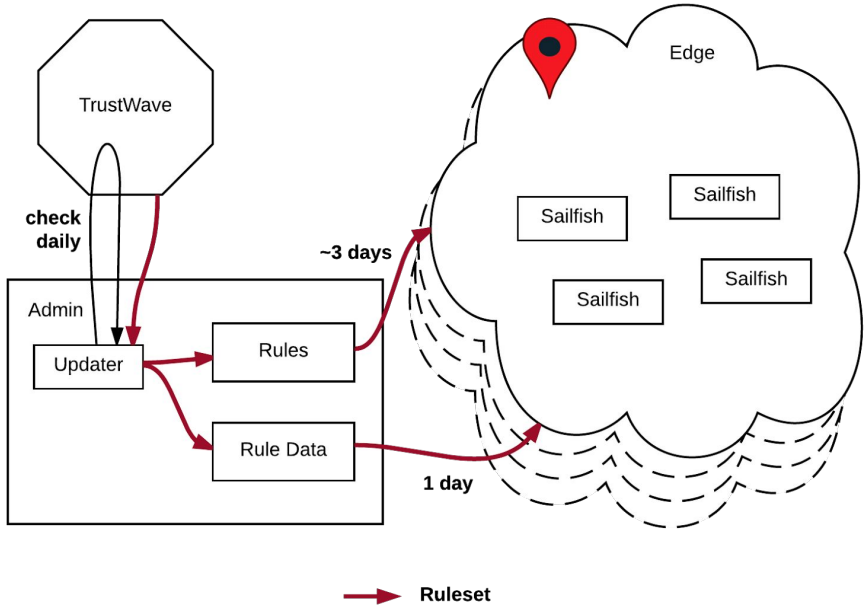


CPU utilization issues...

Forging in the White-hot Fires of Production

Managing Ruleset Updates

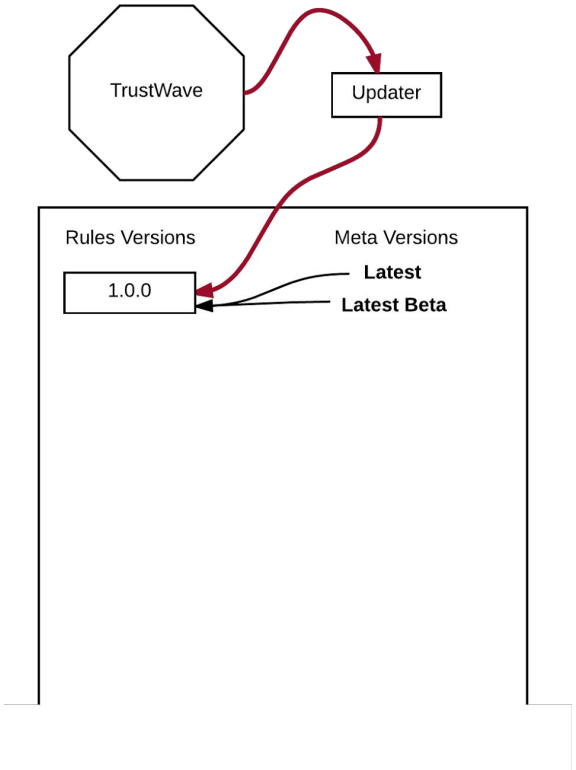
- Upstream updates regular **and** unpredictable
- Fast turnaround required
- Rules as code: ~3 day canary
- Data as config: daily push



Forging in the White-hot Fires of Production

Managing Ruleset Updates

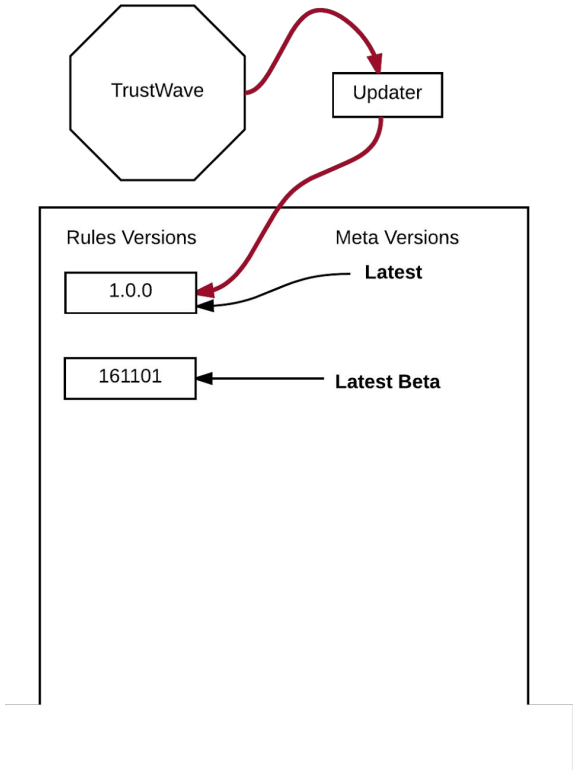
- Date-based versioning
  - 160111 -> 2016, Nov., first release
- Low maintenance options
  - Meta-versions
    - Latest, Latest-Beta



Forging in the White-hot Fires of Production

Managing Ruleset Updates

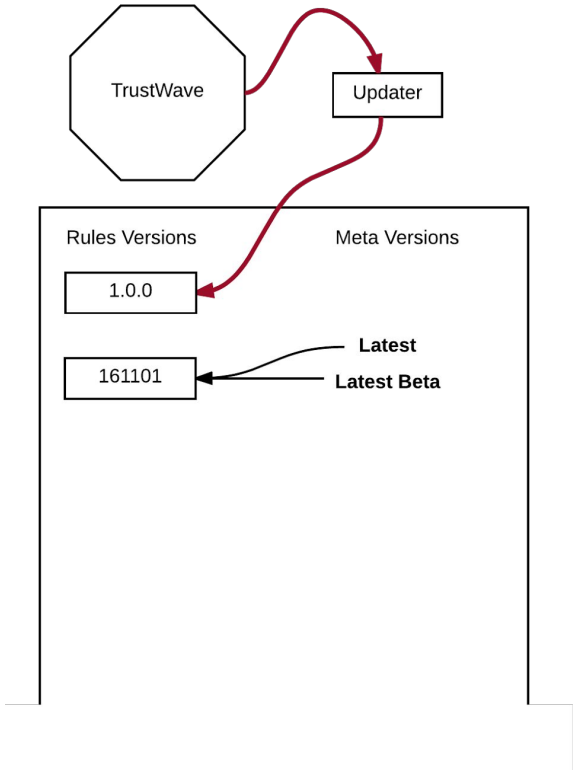
- Date-based versioning
  - 160111 -> 2016, Nov., first release
- Low maintenance options
  - Meta-versions
    - Latest, Latest-Beta



Forging in the White-hot Fires of Production

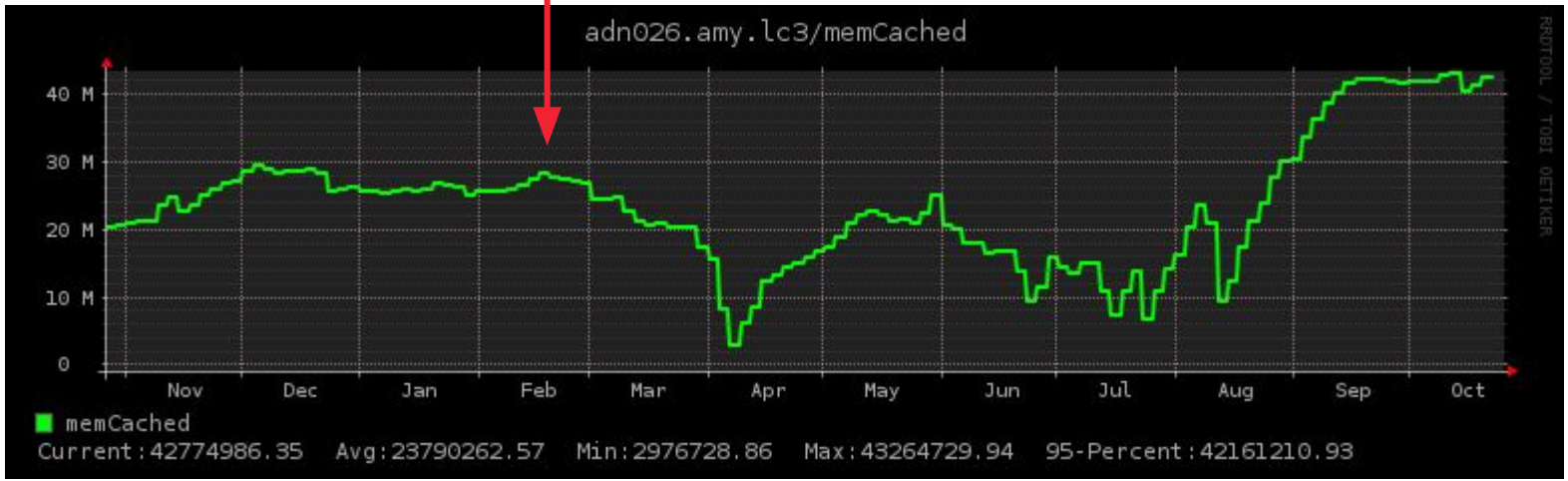
Managing Ruleset Updates

- Date-based versioning
  - 160111 -> 2016, Nov., first release
- Low maintenance options
  - Meta-versions
    - Latest, Latest-Beta



Forging in the White-hot Fires of Production

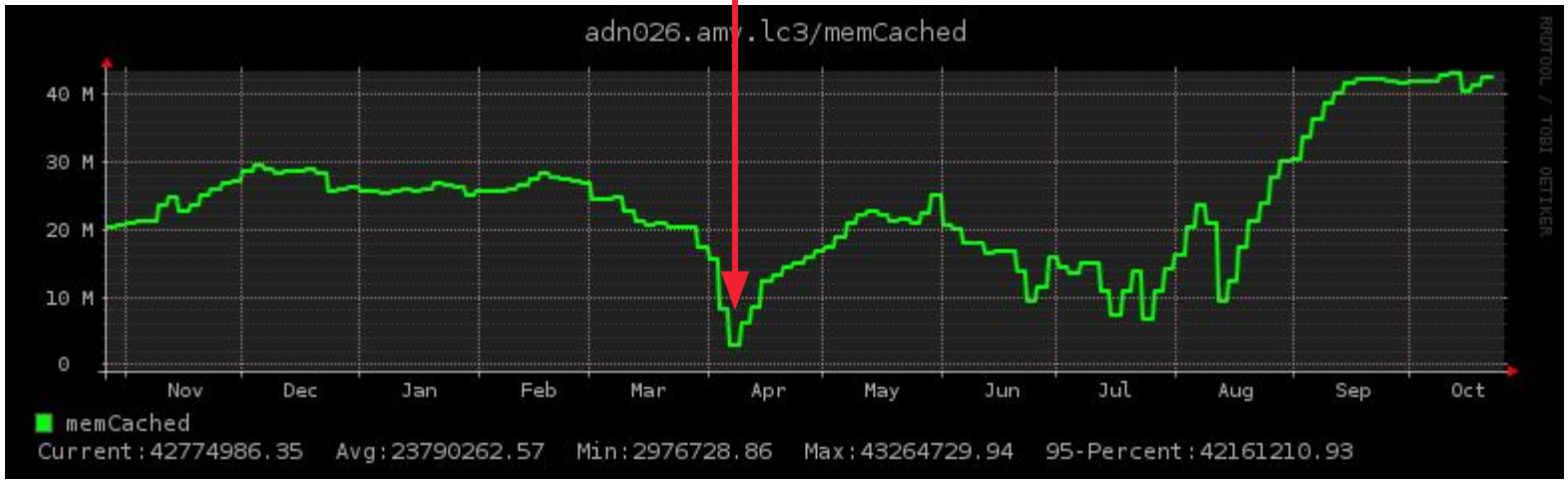
WAF uptake accelerates



Memory utilization issues...

Forging in the White-hot Fires of Production

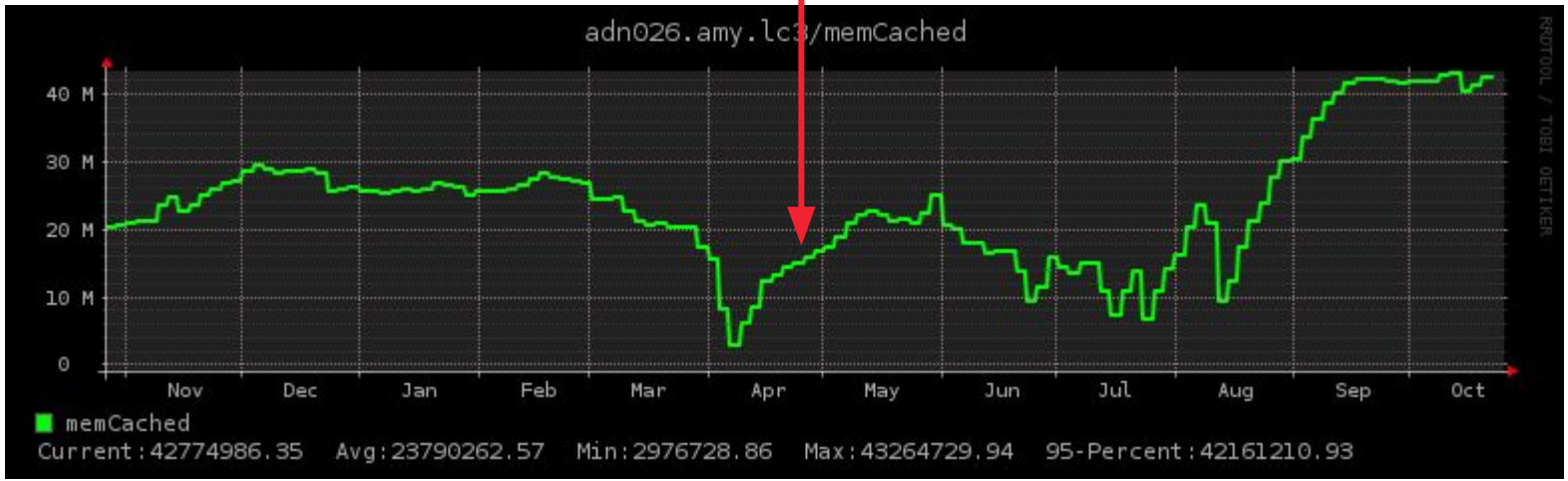
Many systems run out of memory entirely and crash



Memory utilization issues...

Forging in the White-hot Fires of Production

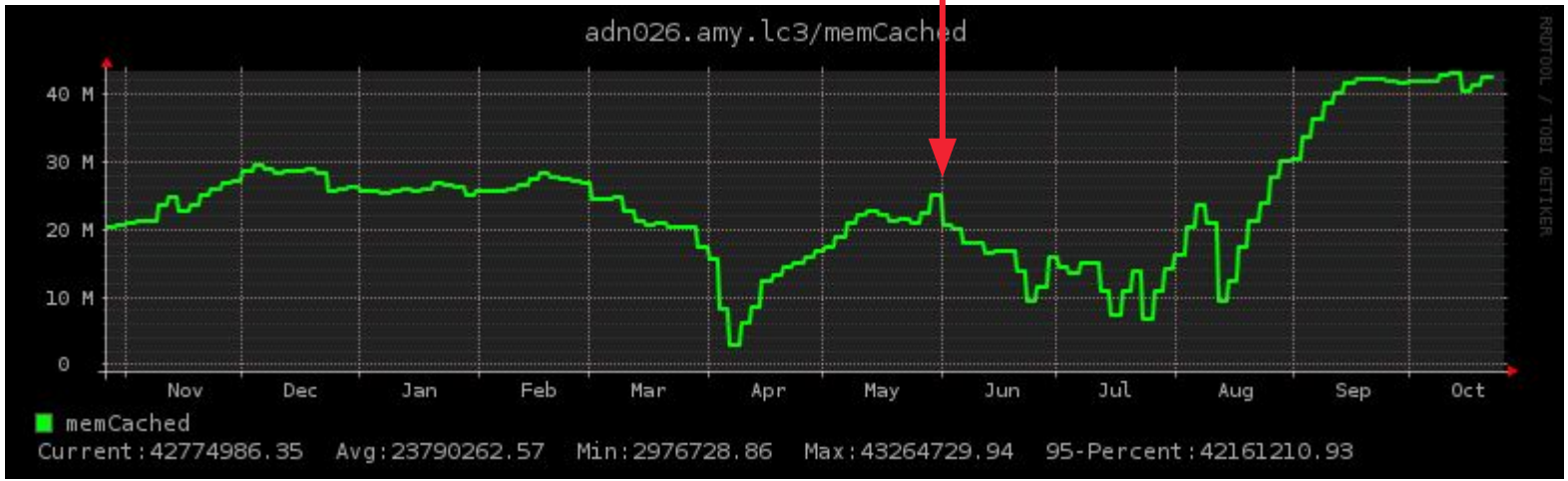
Test and trial WAFs cleaned up to recover



Memory utilization issues...

Forging in the White-hot Fires of Production

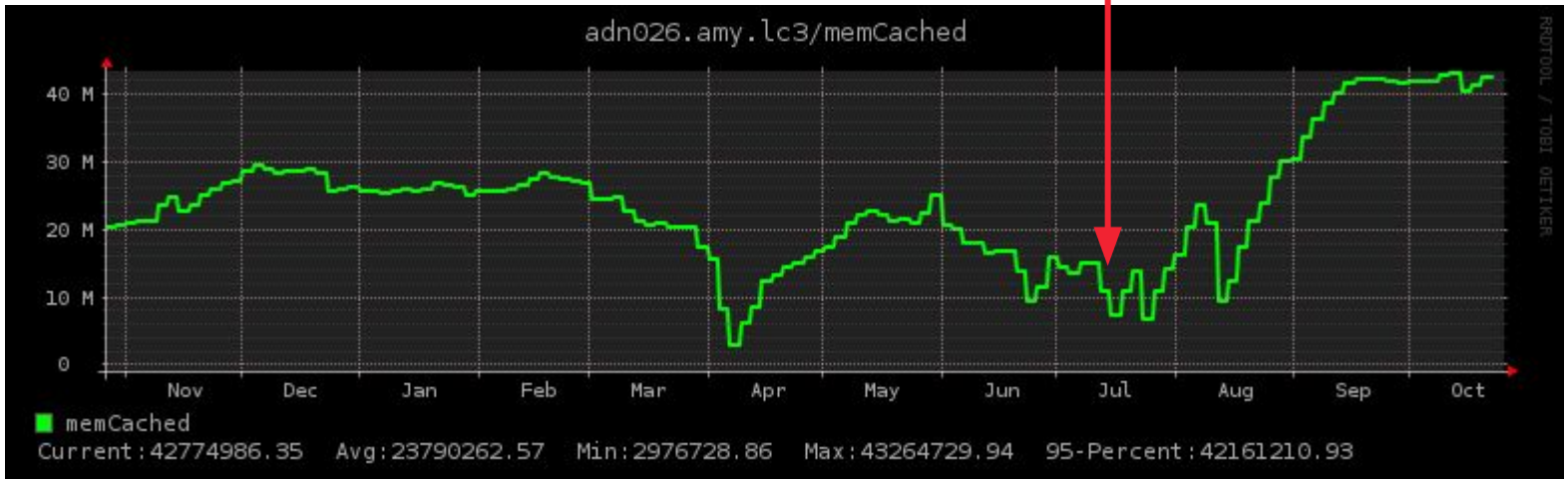
Development of solution finishes...



Memory utilization issues...

Forging in the White-hot Fires of Production

First canary of solution starts



Memory utilization issues...

Forging in the White-hot Fires of Production

Memory utilization issues...

Forging in the White-hot Fires of Production

Memory Utilization Issues

- Every (encapsulated) WAF allocated duplicate rules & associated structures
- Significant code changes required to fix

Diff Stats

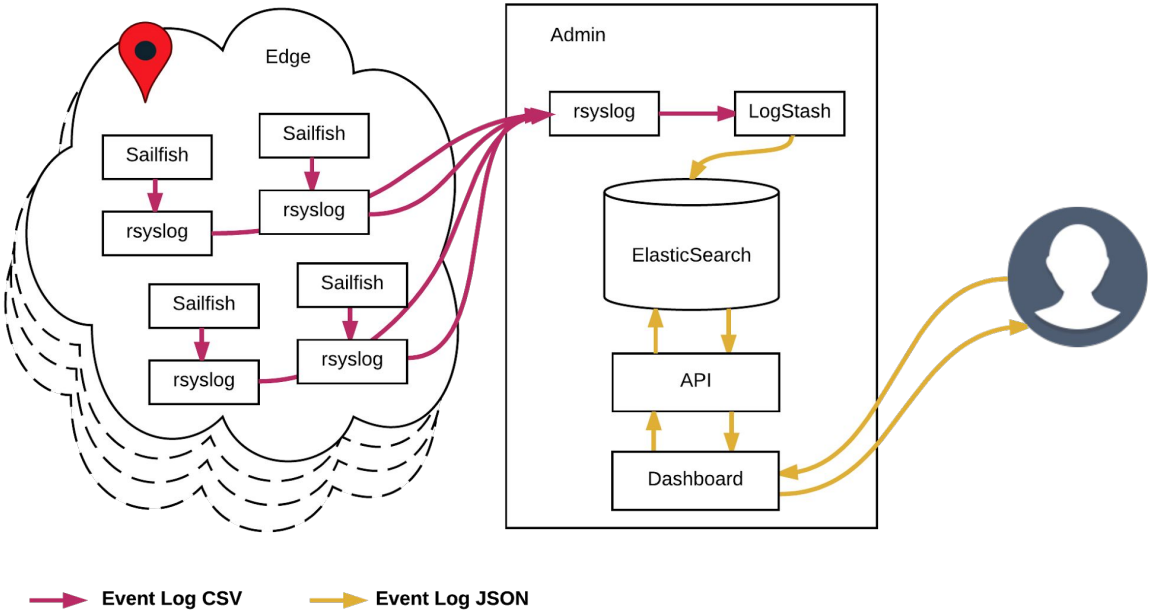
$ git diff --shortstat 6391962..c457ef3 -- modsecurity/

9 files changed

417 deletions (-)

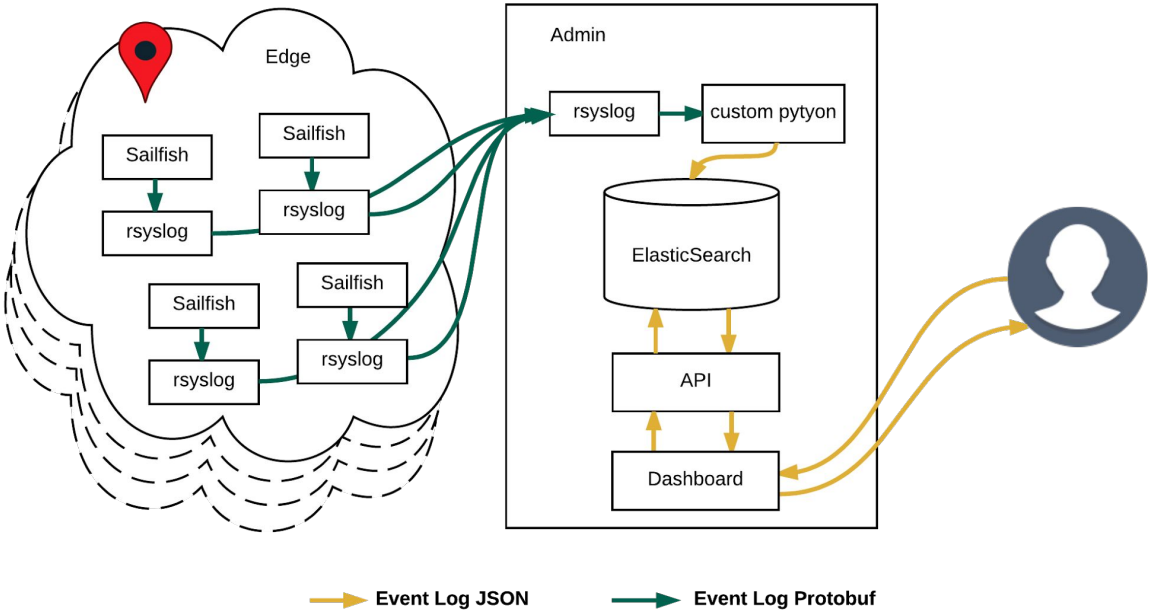
698 insertions (+)

Forging in the White-hot Fires of Production



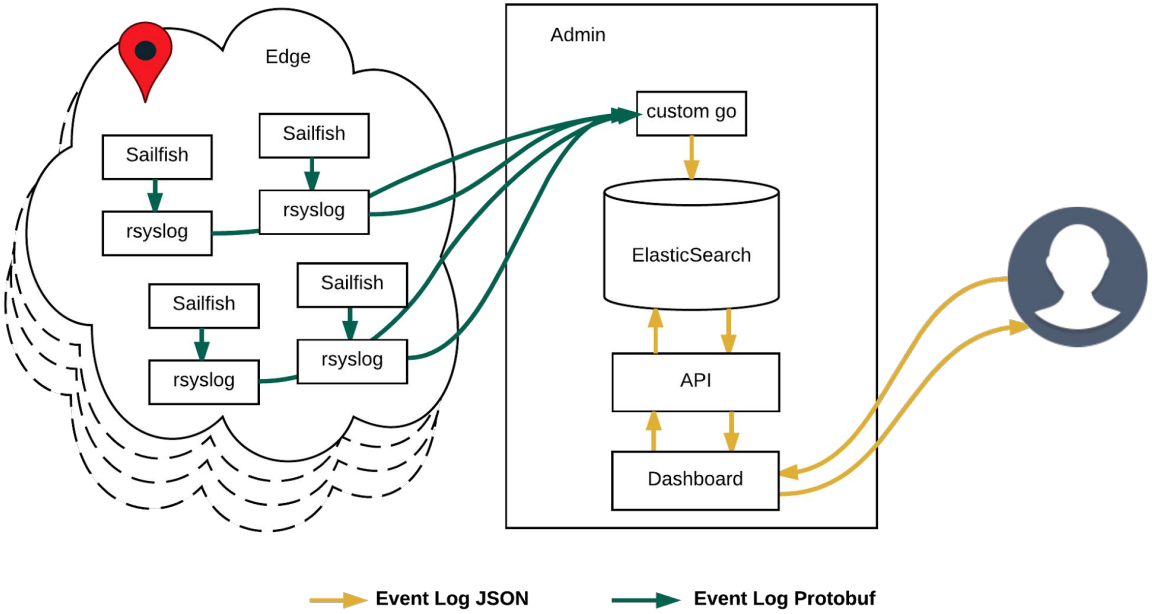
Event Logging Iterations

Forging in the White-hot Fires of Production



Event Logging Iterations

Forging in the White-hot Fires of Production



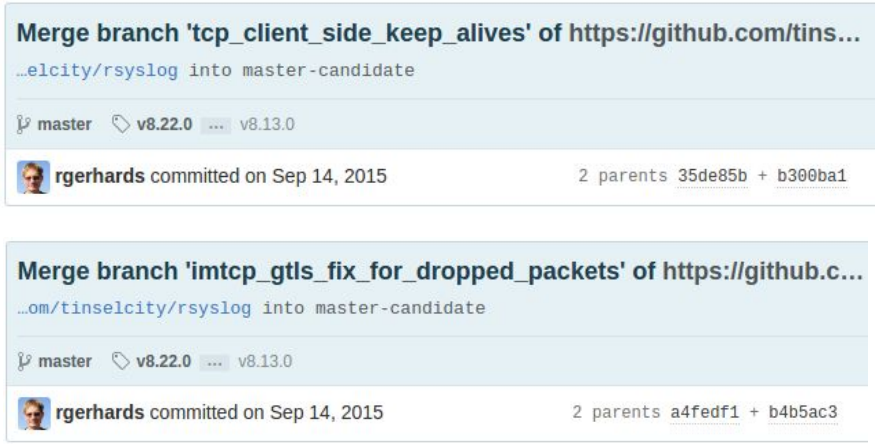
Event Logging Iterations

Forging in the White-hot Fires of Production

Event Logging Issues

- rsyslog bugs
  - busy loops, stuck states

Some fixes



Forging in the White-hot Fires of Production

Event Logging Issues

- rsyslog bugs
  - busy loops, stuck states
- Disk-assisted queues, yay
  - TLS without blocking system logging

Example

```
$MaxMessageSize 1000k
$WorkDirectory /var/EdgeCast/rsyslog/daq
$ActionQueueFileName wafir500log
$ActionQueueMaxDiskSpace 10g
$ActionQueueSaveOnShutdown on
```

Forging in the White-hot Fires of Production

Event Logging Issues

- rsyslog bugs
  - busy loops, stuck states
- Disk-assisted queues, yay
  - TLS without blocking system logging
  - … not perfect, they get {slow,corrupt} at times

Tools

https://github.com/rsyslog/rsyslog/blob/master/tools/recover_qi.pl

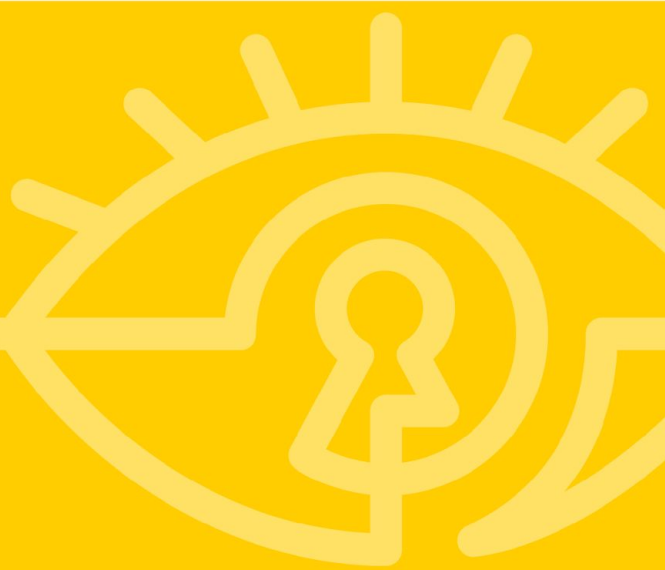
https://github.com/VerizonDigital/rsyslog/blob/master/tools/fix_daq_and_restart.sh

Conclusions

- ModSecurity allowed us to bootstrap quickly
- But repeated {identification,fixing} for multi-tenancy is expensive
  - Configuration layout, memory usage, CPU usage
- Due to {cruft,complexity} open source project waflz replacement
  - First release was July 2016
    - Parse ModSecurity config language
    - Product well-structured documents (json, protocol buffers)
  - Next major release planned for Q2 2017
    - Goal: replace ModSecurity on the edge

Applicable Tips

- Next week, you could...
  - Ensure you're at the latest stable in your logging infrastructure
  - Add disk assist for log delivery
  - Add event log timestamping (collection vs. ingest) to capture lag
- Next three months, you could...
  - Monitor more: CPU, memory, config reloads, event log traffic, etc.
  - Set limits on config reload rates to protect against unknown issues
- Next six months, you could...
  - Participate in waflz v1.0 development! https://github.com/VerizonDigital/waflz



Thank You