SOFTWARE-DEFINED WEB & CLOUD CONTROLS

Securing Application Infrastructure in Multi-Cloud Environments

Jay Smith, Founder and CTO
WEBSCALE

QUICK INTRO

WEBSCALE

- **The E-Commerce Cloud Company**
- **Cloud management and control for critical web applications.**
  More than $3 Billion processed through platform in 2017
- **Black Friday 2017**
  - **~1 Billion page views**
  - More than **83 billion HTTP request decisions** made, a significant portion of which were security-related
  - **10,000+ application scaling events**
- We work with web application frameworks, across multiple clouds, that are widely popular (Wordpress, PHP, Ruby), and carry a high profit motive for hackers

APPLICATION FRAMEWORKS – THE GOOD/BAD

WEBSCALE

THE GOOD

- Speed up development
- Large supportive community, lots of developers to work with
- Open source, easy access to all of the code to tailor and customize the user experience

THE BAD

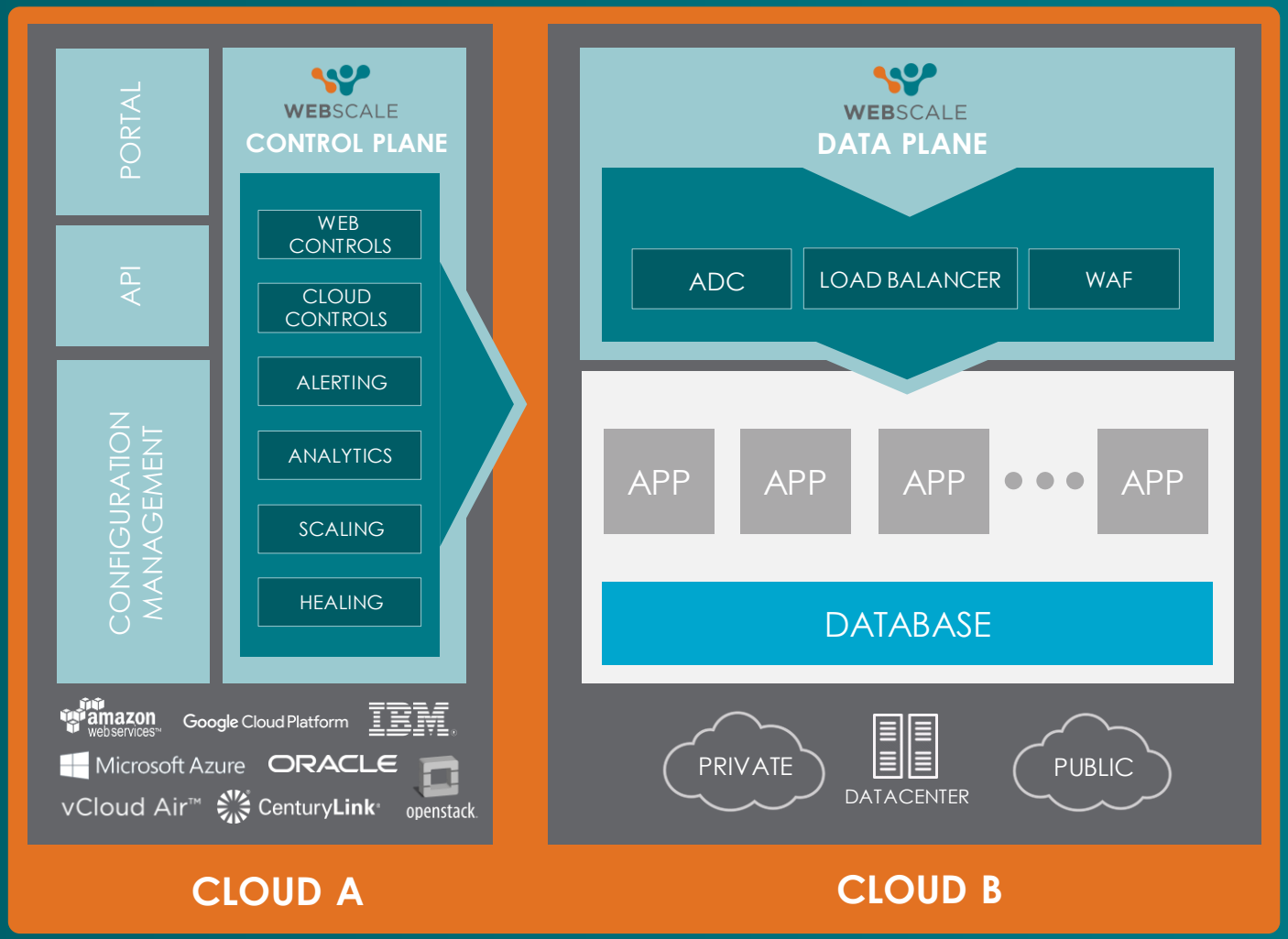
- E-commerce sites handle credit cards, either directly or indirectly, making them high value targets for attackers
- 100,000s of sites running the same framework increases the value of new exploits
- New attacks can be very profitable for bad guys

WHAT APPLICATION CONTROL MEANS TO US

WEBSCALE

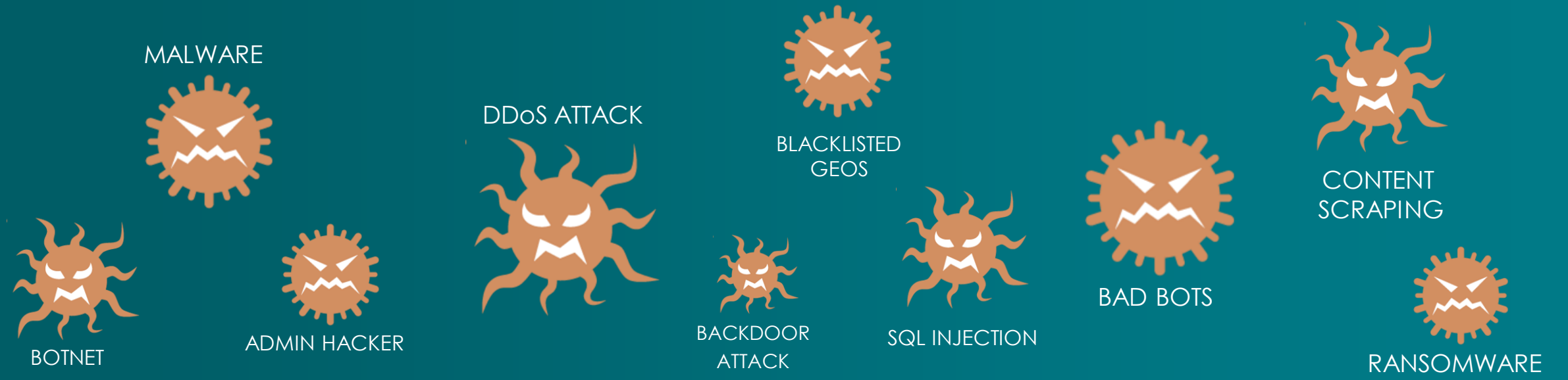
- Separate control & data planes
- Strong data plane security model
- Everything monitored and tracked
- Customizable rules engine
- Triggered automated actions

WEBSCALE MULTI-CLOUD ARCHITECTURE

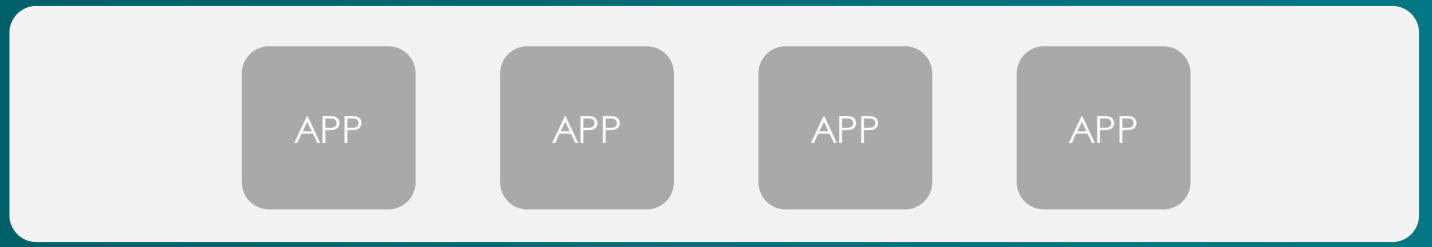


KNOWN ATTACKS

WEBSCALE

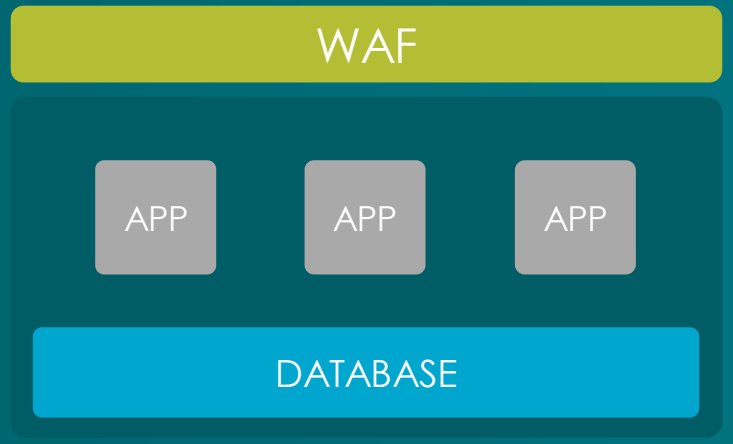


WEB APPLICATION FIREWALL



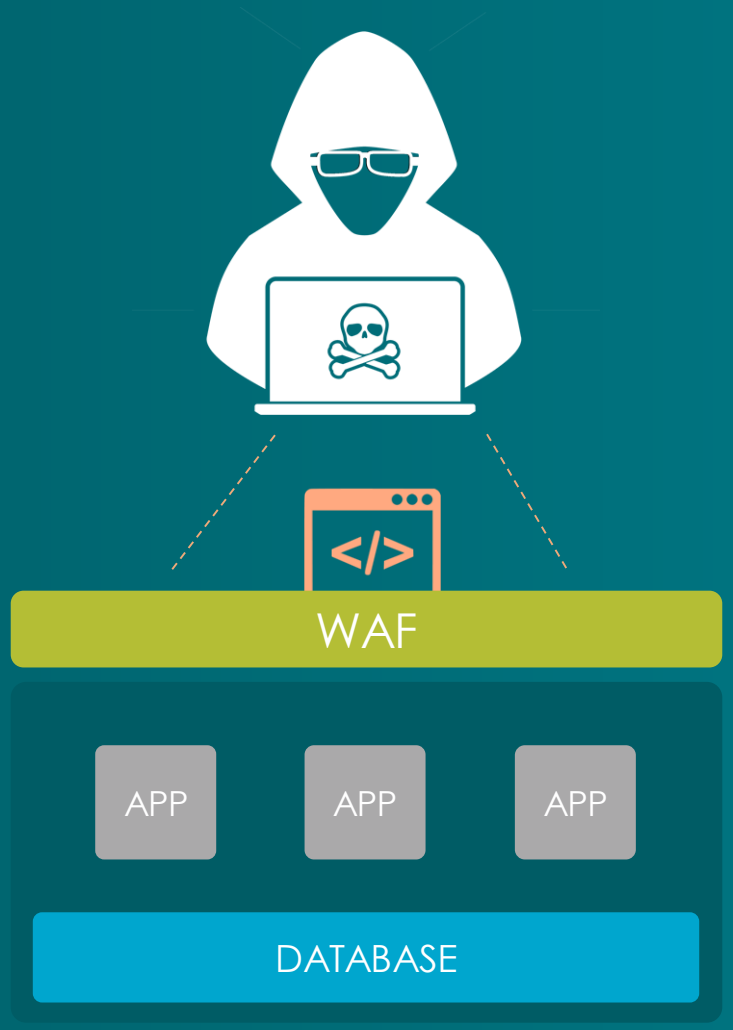
EXPLOITS STILL HAPPEN

WEBSCALE



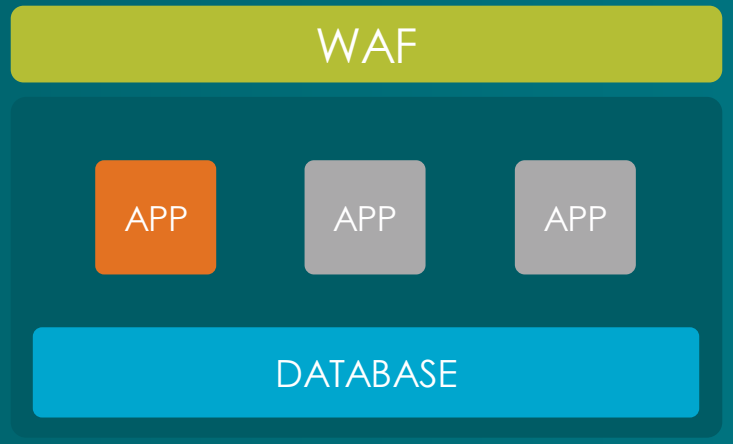
EXPLOITS STILL HAPPEN

WEBSCALE



EXPLOITS STILL HAPPEN

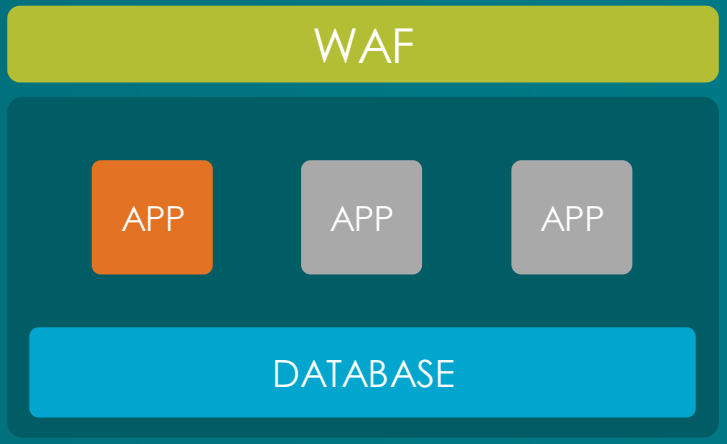
WEBSCALE



EXPLOITS STILL HAPPEN

WEBSCALE

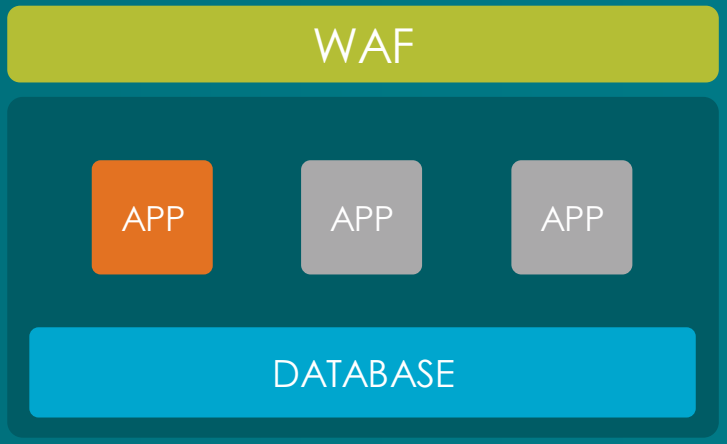
- Unexpected file change



EXPLOITS STILL HAPPEN

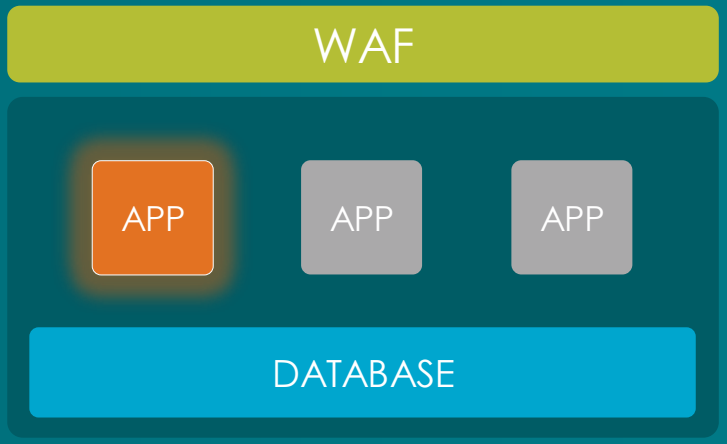
WEBSCALE

- Unexpected file change
- Alert on file modification event



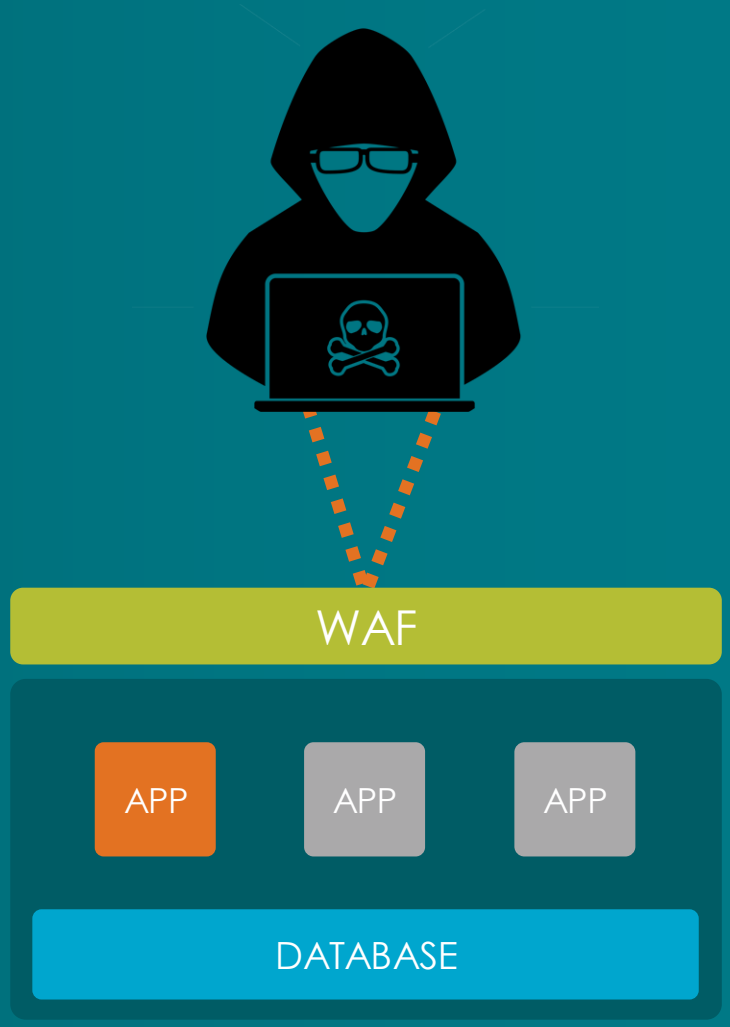
EXPLOITS STILL HAPPEN

- Unexpected file change
- Alert on file modification event
- Automatically ID server affected



EXPLOITS STILL HAPPEN

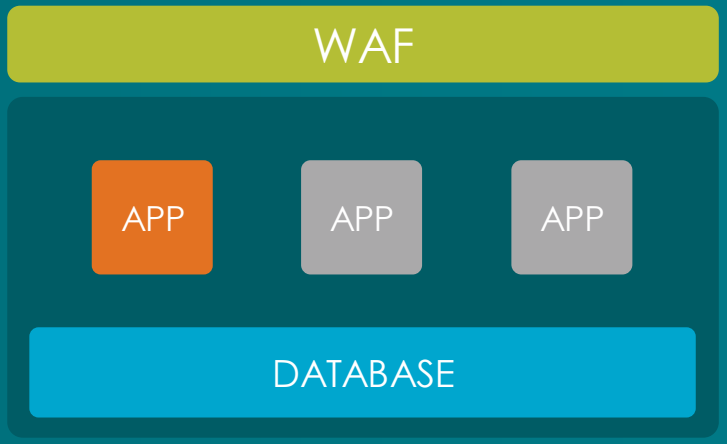
- Unexpected file change
- Alert on file modification event
- Automatically ID server affected
- Automatically blacklist access to file



EXPLOITS STILL HAPPEN

WEBSCALE

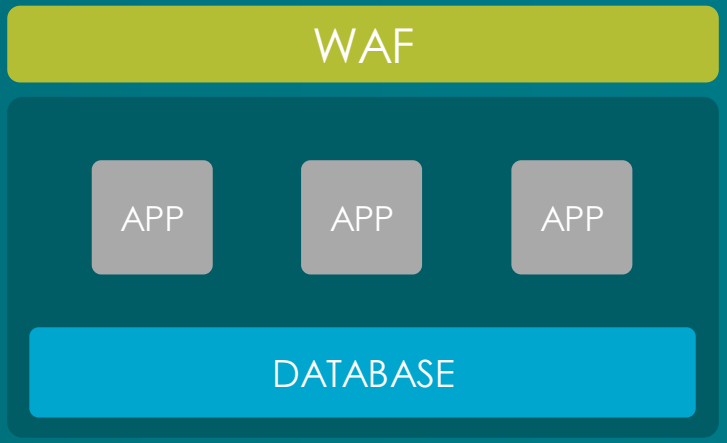
- Unexpected file change
- Alert on file modification event
- Automatically ID server affected
- Automatically blacklist access to file



EXPLOITS STILL HAPPEN

WEBSCALE

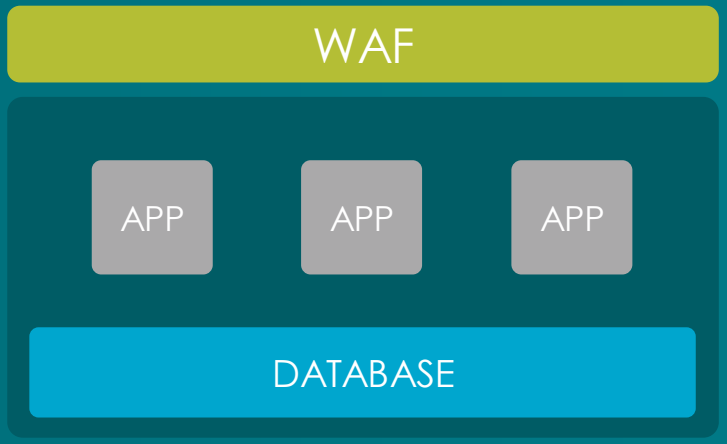
- Unexpected file change
- Alert on file modification event
- Automatically ID server affected
- Automatically blacklist access to file
- Auto-quarantine & replace server



EXPLOITS STILL HAPPEN

WEBSCALE

- Unexpected file change
- Alert on file modification event
- Automatically ID server affected
- Automatically blacklist access to file
- Auto-quarantine & replace server
- Create incident and alert SecOps



AFTERMATH

WEBSCALE

Admins use portal to analyze traffic and events, identify attack patterns and prevent further security violations, across entire customer network

ATTACK ANALYSIS

- Identify attack vector
- Location of attack
- Details of file change

ACTIONS

- Blacklist/Whitelist IP
- Install new WAF rule
- Block traffic
- Blacklist requestor
- Whitelist acceptable access

AFTERMATH – IDENTIFICATION & ANALYSIS

WEBSCALE

Dashboard / Application / Traffic Viewer

www.webscale.com

Webscale hostname NFDFNQXM.lagrangesystems.net

Actions

7d 19h 49m
since last outage
Online since January 20, 2016

Status running
CDN enabled

Traffic

Urls | Time

Start: 3/7/2018, 15:06 UTC
End: 3/7/2018, 18:06 UTC

Summary

Url	Requests
https://www.webscale.com/category/media-coverage/feed/	4,239
https://www.webscale.com/	456
http://www.webscale.com/	204
https://www.webscale.com/feed/	35
https://www.webscale.com/wp-content/themes/Divi/js/custom.min.js	23
https://www.webscale.com/wp-content/themes/Divi-child/style.css	22
https://www.webscale.com/wp-content/uploads/2017/08/products-n...	22
https://www.webscale.com/wp-content/uploads/2017/08/why-websc...	22
https://www.webscale.com/wp-includes/js/wp-emoji-release.min.js	21
https://www.webscale.com/wp-content/themes/Divi/style.css	19
https://www.webscale.com/robots.txt	18
https://www.webscale.com/wp-content/themes/Divi-child/smooth-m...	18
https://www.webscale.com/wp-content/uploads/2017/08/customers...	18
https://www.webscale.com/wp-content/uploads/2017/08/solutions-n...	18
https://www.webscale.com/wp-content/themes/Divi/core/admin/fon...	17
https://www.webscale.com/wp-content/uploads/2017/12/linkedin-lo...	15
https://www.webscale.com/wp-content/uploads/2017/12/twitter-log...	15

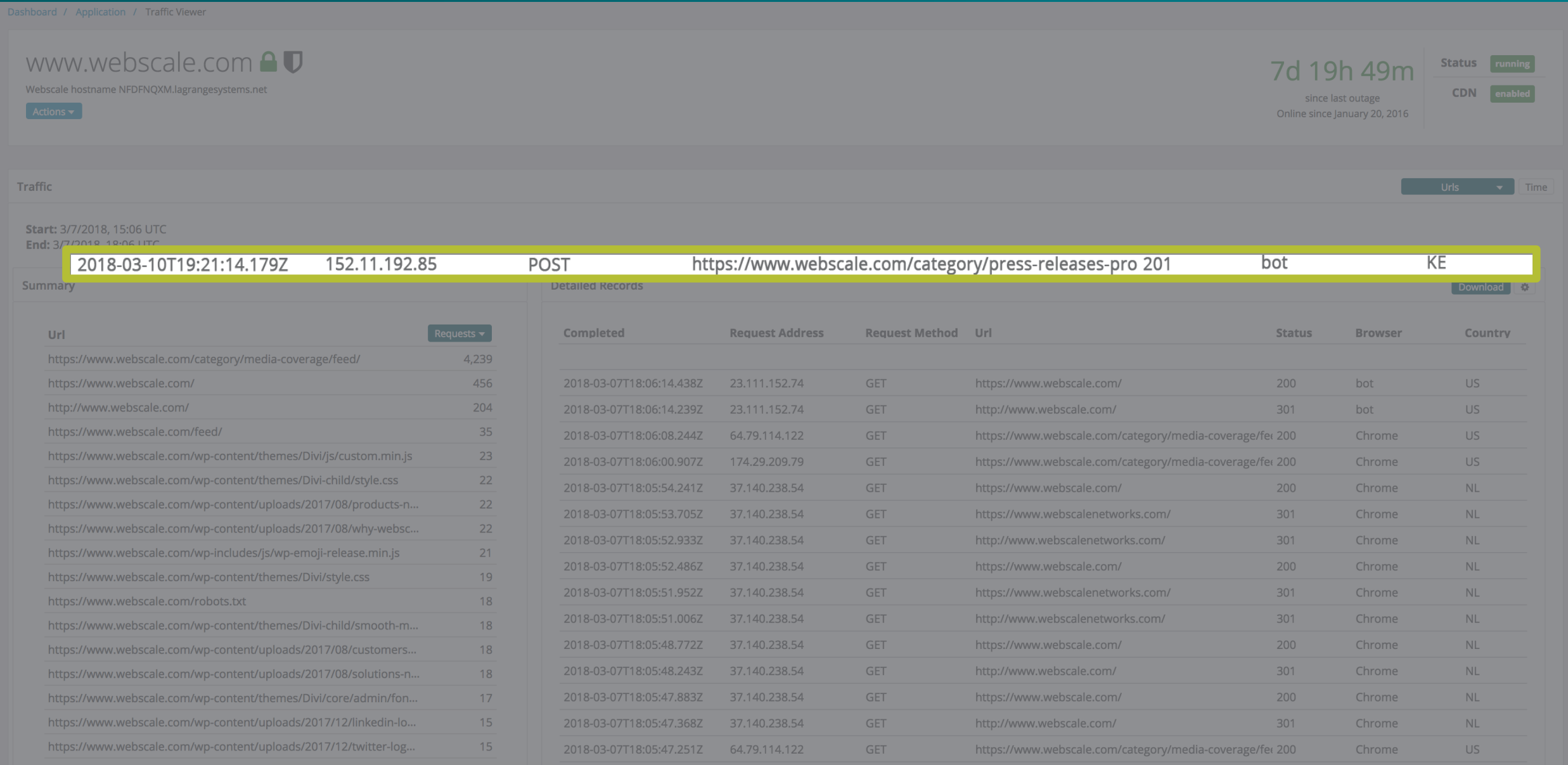
Detailed Records

Download

Completed	Request Address	Request Method	Url	Status	Browser	Country
2018-03-10T19:21:14.179Z	152.11.192.85	POST	https://www.webscale.com/category/press-releases-pro	201	bot	KE
2018-03-07T18:06:14.438Z	23.111.152.74	GET	https://www.webscale.com/	200	bot	US
2018-03-07T18:06:14.239Z	23.111.152.74	GET	http://www.webscale.com/	301	bot	US
2018-03-07T18:06:08.244Z	64.79.114.122	GET	https://www.webscale.com/category/media-coverage/fe	200	Chrome	US
2018-03-07T18:06:00.907Z	174.29.209.79	GET	https://www.webscale.com/category/media-coverage/fe	200	Chrome	US
2018-03-07T18:05:54.241Z	37.140.238.54	GET	https://www.webscale.com/	200	Chrome	NL
2018-03-07T18:05:53.705Z	37.140.238.54	GET	https://www.webscalenetworks.com/	301	Chrome	NL
2018-03-07T18:05:52.933Z	37.140.238.54	GET	http://www.webscalenetworks.com/	301	Chrome	NL
2018-03-07T18:05:52.486Z	37.140.238.54	GET	https://www.webscale.com/	200	Chrome	NL
2018-03-07T18:05:51.952Z	37.140.238.54	GET	https://www.webscalenetworks.com/	301	Chrome	NL
2018-03-07T18:05:51.006Z	37.140.238.54	GET	http://www.webscalenetworks.com/	301	Chrome	NL
2018-03-07T18:05:48.772Z	37.140.238.54	GET	https://www.webscale.com/	200	Chrome	NL
2018-03-07T18:05:48.243Z	37.140.238.54	GET	http://www.webscale.com/	301	Chrome	NL
2018-03-07T18:05:47.883Z	37.140.238.54	GET	https://www.webscale.com/	200	Chrome	NL
2018-03-07T18:05:47.368Z	37.140.238.54	GET	http://www.webscale.com/	301	Chrome	NL
2018-03-07T18:05:47.251Z	64.79.114.122	GET	https://www.webscale.com/category/media-coverage/fe	200	Chrome	US

AFTERMATH – IDENTIFICATION & ANALYSIS

WEBSCALE



Dashboard / Application / Traffic Viewer

www.webscale.com

Webscale hostname NFDFNQXM.lagrangesystems.net

Actions

7d 19h 49m
since last outage
Online since January 20, 2016

Status running
CDN enabled

Traffic

Urls Time

Start: 3/7/2018, 15:06 UTC
End: 3/7/2018, 18:06 UTC

2018-03-10T19:21:14.179Z 152.11.192.85 POST https://www.webscale.com/category/press-releases-pro 201 bot KE

Summary

Url	Requests
https://www.webscale.com/category/media-coverage/feed/	4,239
https://www.webscale.com/	456
http://www.webscale.com/	204
https://www.webscale.com/feed/	35
https://www.webscale.com/wp-content/themes/Divi/js/custom.min.js	23
https://www.webscale.com/wp-content/themes/Divi-child/style.css	22
https://www.webscale.com/wp-content/uploads/2017/08/products-n...	22
https://www.webscale.com/wp-content/uploads/2017/08/why-websc...	22
https://www.webscale.com/wp-includes/js/wp-emoji-release.min.js	21
https://www.webscale.com/wp-content/themes/Divi/style.css	19
https://www.webscale.com/robots.txt	18
https://www.webscale.com/wp-content/themes/Divi-child/smooth-m...	18
https://www.webscale.com/wp-content/uploads/2017/08/customers...	18
https://www.webscale.com/wp-content/uploads/2017/08/solutions-n...	18
https://www.webscale.com/wp-content/themes/Divi/core/admin/fon...	17
https://www.webscale.com/wp-content/uploads/2017/12/linkedin-lo...	15
https://www.webscale.com/wp-content/uploads/2017/12/twitter-log...	15

Detailed Records

Download

Completed	Request Address	Request Method	Url	Status	Browser	Country
2018-03-07T18:06:14.438Z	23.111.152.74	GET	https://www.webscale.com/	200	bot	US
2018-03-07T18:06:14.239Z	23.111.152.74	GET	http://www.webscale.com/	301	bot	US
2018-03-07T18:06:08.244Z	64.79.114.122	GET	https://www.webscale.com/category/media-coverage/fe	200	Chrome	US
2018-03-07T18:06:00.907Z	174.29.209.79	GET	https://www.webscale.com/category/media-coverage/fe	200	Chrome	US
2018-03-07T18:05:54.241Z	37.140.238.54	GET	https://www.webscale.com/	200	Chrome	NL
2018-03-07T18:05:53.705Z	37.140.238.54	GET	https://www.webscalenetworks.com/	301	Chrome	NL
2018-03-07T18:05:52.933Z	37.140.238.54	GET	http://www.webscalenetworks.com/	301	Chrome	NL
2018-03-07T18:05:52.486Z	37.140.238.54	GET	https://www.webscale.com/	200	Chrome	NL
2018-03-07T18:05:51.952Z	37.140.238.54	GET	https://www.webscalenetworks.com/	301	Chrome	NL
2018-03-07T18:05:51.006Z	37.140.238.54	GET	http://www.webscalenetworks.com/	301	Chrome	NL
2018-03-07T18:05:48.772Z	37.140.238.54	GET	https://www.webscale.com/	200	Chrome	NL
2018-03-07T18:05:48.243Z	37.140.238.54	GET	http://www.webscale.com/	301	Chrome	NL
2018-03-07T18:05:47.883Z	37.140.238.54	GET	https://www.webscale.com/	200	Chrome	NL
2018-03-07T18:05:47.368Z	37.140.238.54	GET	http://www.webscale.com/	301	Chrome	NL
2018-03-07T18:05:47.251Z	64.79.114.122	GET	https://www.webscale.com/category/media-coverage/fe	200	Chrome	US

AFTERMATH

WEBSCALE

Admins use portal to analyze traffic and events, identify attack patterns and prevent further security violations, across entire customer network

ATTACK ANALYSIS

- Identify attack vector
- Location of attack
- Details of file change

ACTIONS

- Blacklist/Whitelist IP
- Install new WAF rule
- Block traffic
- Blacklist requestor
- Whitelist acceptable access

BRINGING IT ALL TOGETHER

WEBSCALE

THANK YOU

Questions?

WEBSCALE