
black hat
EUROPE 2017
DECEMBER 4-7, 2017
EXCEL / LONDON, UK
source
DEFENSE
#BHEU / @BLACK HAT EVENTS

Agenda - GDPR and third party JS - can it be done?

- Third party scripts – what are they? Why do we use them?
- Where is the problem?
- Third party security and privacy (OR) a bad inheritance
- GDPR – which part pf the beast are we talking about?
- What can we do about it?
- Why are we still exposed?
- Suggested solution

What are third party scripts?

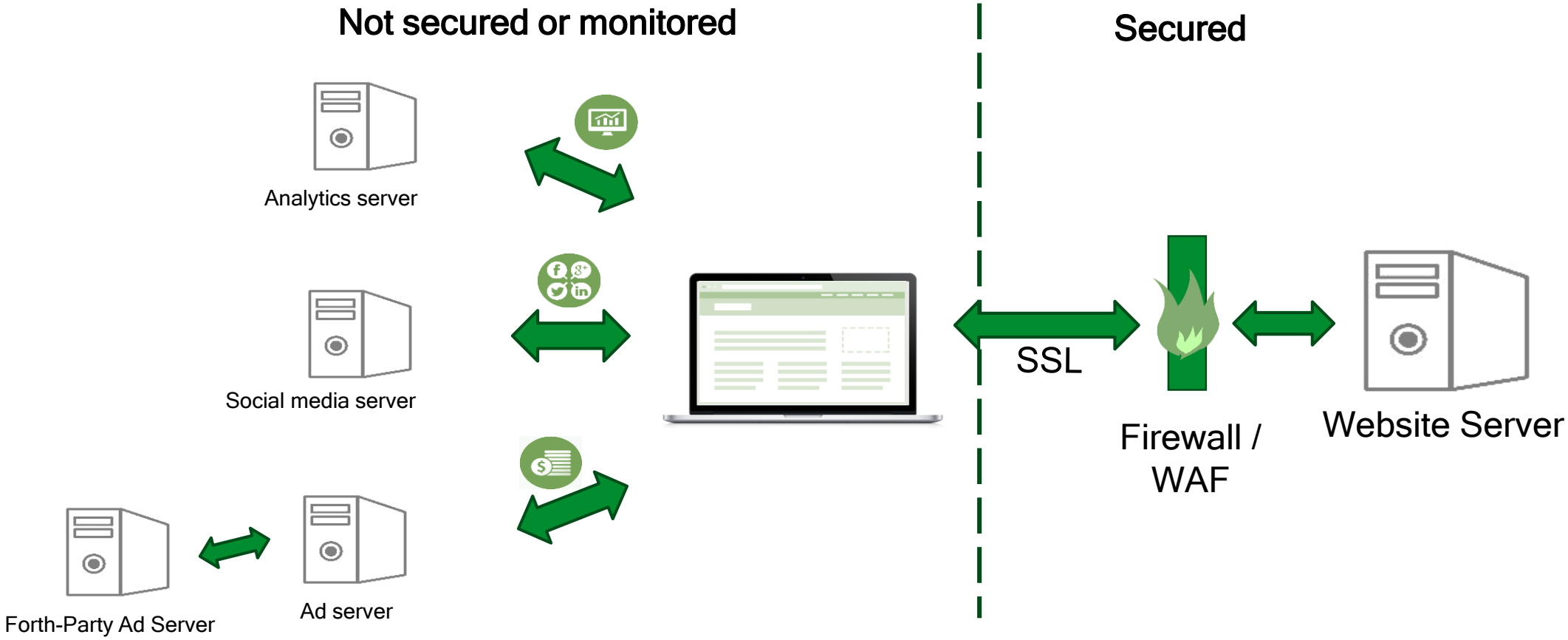
Third-party scripts

What are they and why do we use them?

Where is the problem?

Third-party scripts

Where is the problem?



Third-party scripts

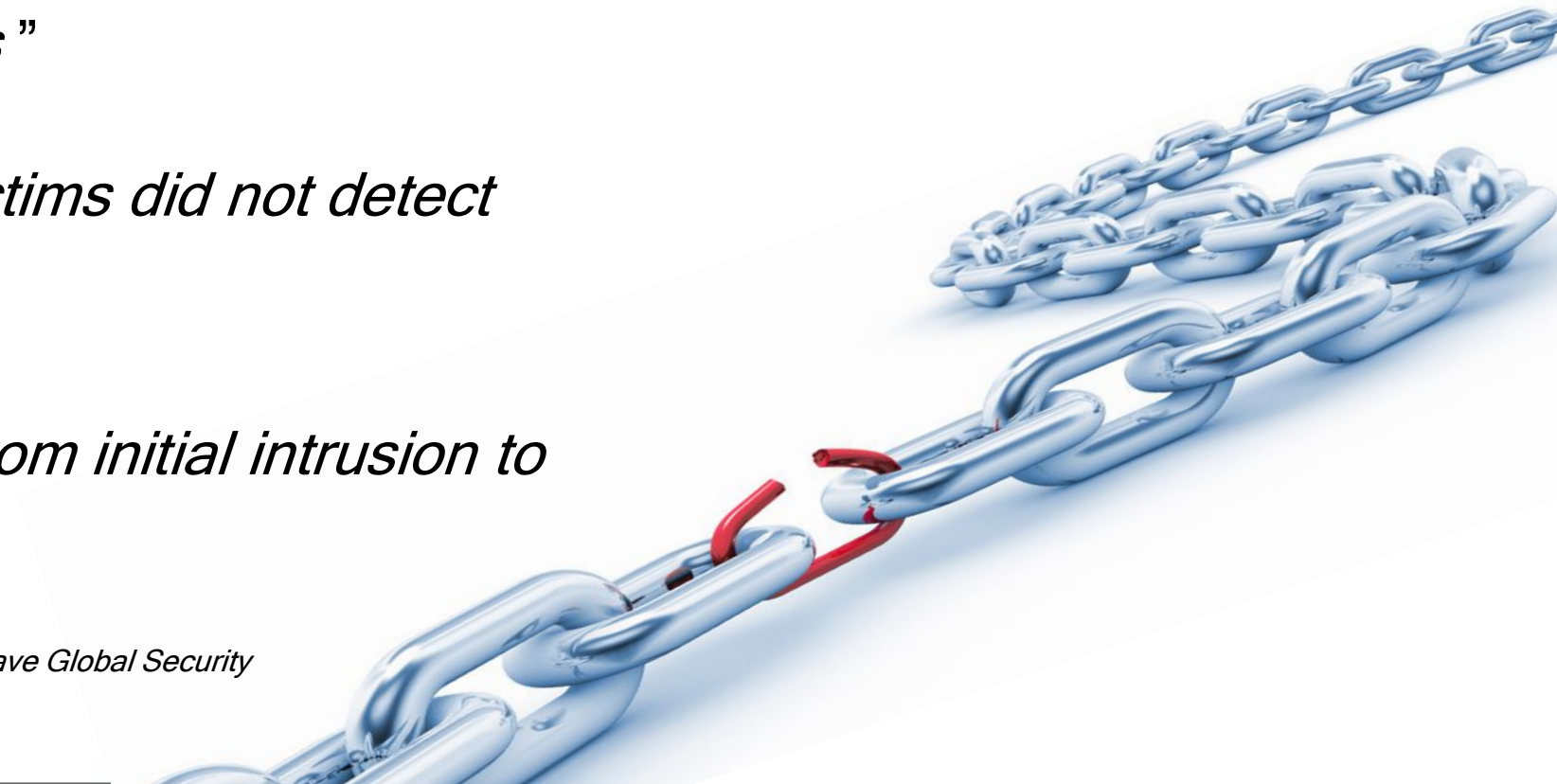
Third party security and privacy (OR) A bad inheritance

*"**85%** of the exploits detected at in recent years were of third-party plug-ins"*

*"**71%** of compromise victims did not detect breaches themselves"*

*"Median number of days from initial intrusion to detection **87** days"*

~Trustedwave Global Security



engadget | 3 related articles | Login

Latest in Gear

Australia may offer facial recognition data to telecoms and banks

4h ago

The big stores that track your every online move

Holiday shopping with Big Brother is always a bummer.

Violet Blue, @violetblue
11.24.17 in Security

785
Shares

BUSINESS INSIDER RETAIL

The "temporary security intrusion" lasted for about 28 hours, the notice said, and it's believed that names, billing ZIP codes, delivery addresses, email addresses and payment card information — meaning account number, expiration date and CVV number — were compromised.

Pizza Hut emailed thousands of customers this weekend to tell them they may have been impacted by a security breach.

Roughly 60,000 people were

How does it relate to the GDPR?

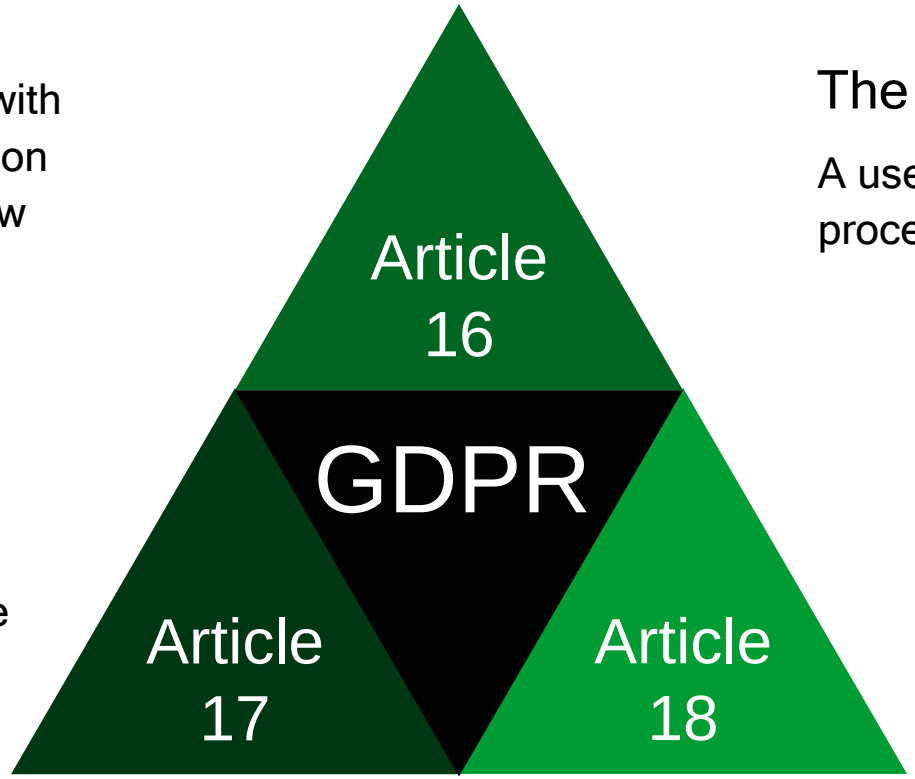
Which part of the beast are we talking about?

The right to rectification

A website must provide the user with the option to correct any information stored on him/her or provide a new statement

The right to be forgotten

A user has the right to request the immediate deletion of all information stored on him/her



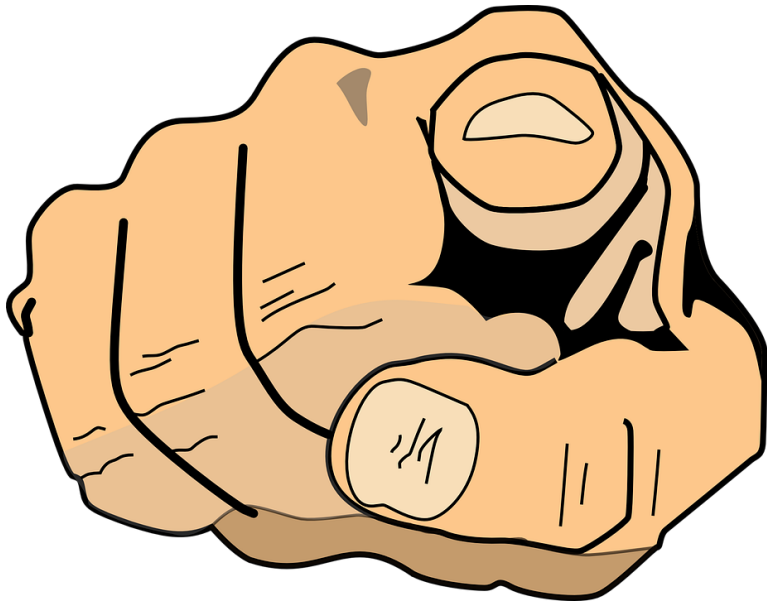
The right to restriction of processing

A user has the right to object to the processing of his/hers personal information

GDPR

The blame game (OR) is it my reasonability?

The controller(*) shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient (**) to whom the personal data have been disclosed



* **The controller -** the website
** **Recipient –** a third party vendor

What we can do about it ?

What we can do about it

iFrames and the HTML 5 iFrame sandbox

Pros:

- Isolation from the page
- Some measure of privacy
- Latency protection

Cons:

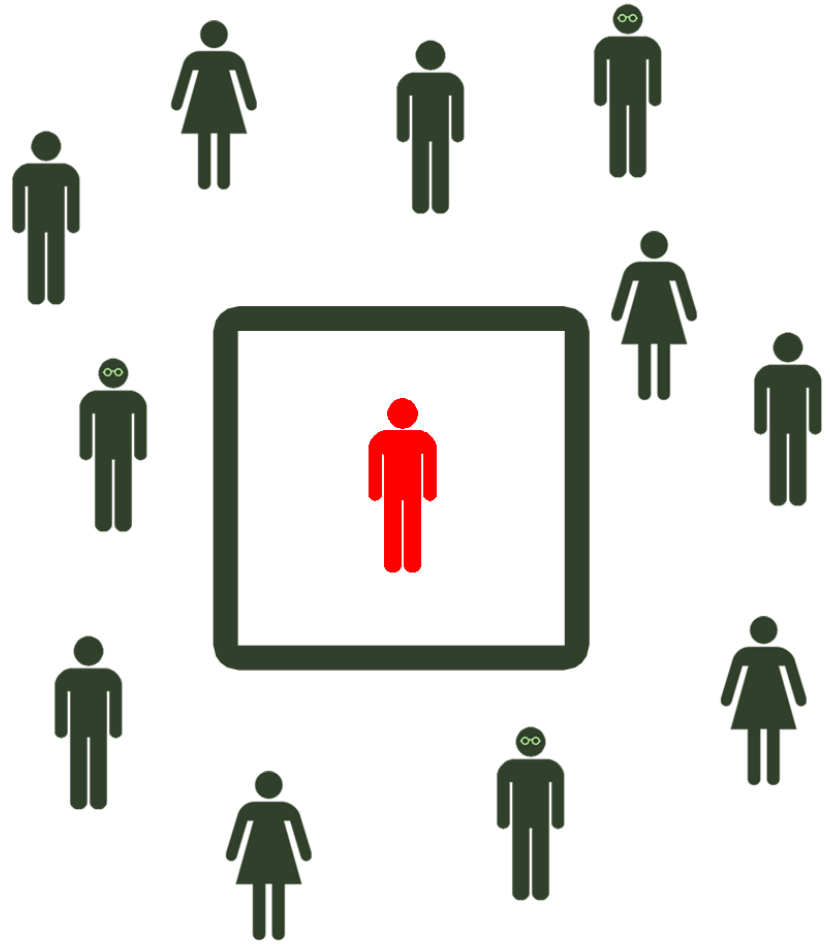
- Isolation from the page
- Some third-parties will not run in it

Prevent top-level navigation

Block script execution

Block form submission

Disable APIs



What we can do about it

HTTP headers

Pros:

- Content source control
- Secure content only

Cons:

- Might block third party operation
- Affects the entire page, not only the third party

CSP

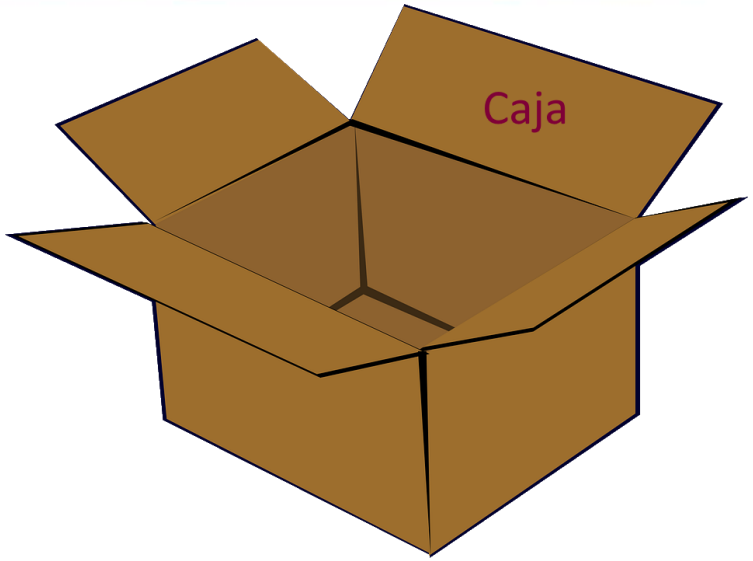
x-frame-options

HSTS

Set-Cookie

What we can do about it

JS libraries



Pros:

- High level of control
- Completely block harmful operations

Cons:

- High cost of deployment and maintenance
- Requires tailor made code by either the site or third party

AD safe™

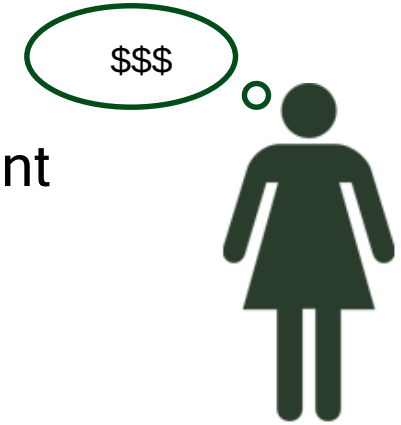
Why are we still exposed?

What we can do about it

Why the low adoption rate?

R&D

Implementation and management



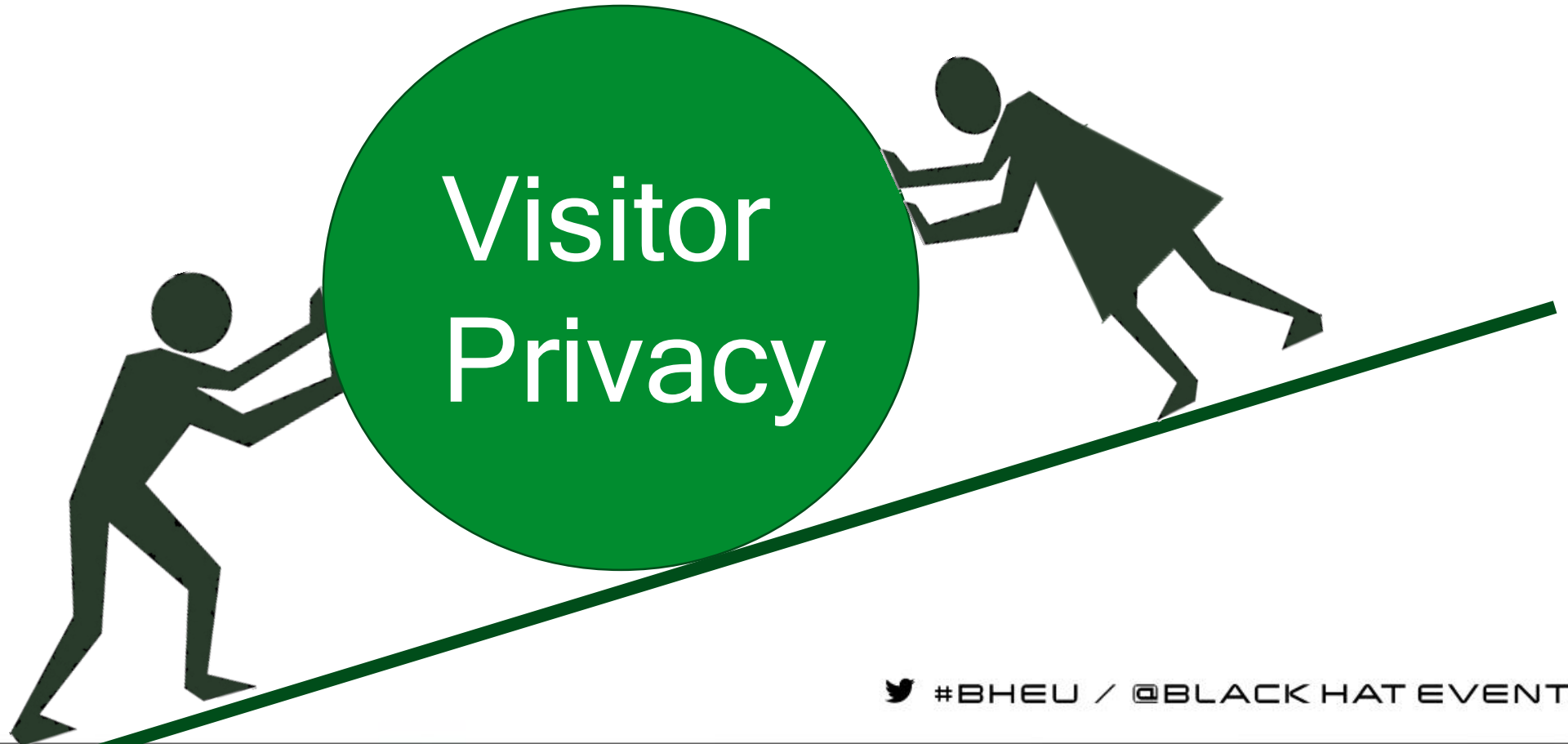
Marketing

Need for speed and flexibility

Security team

Need for security and privacy

Friction!!!



Suggested solution

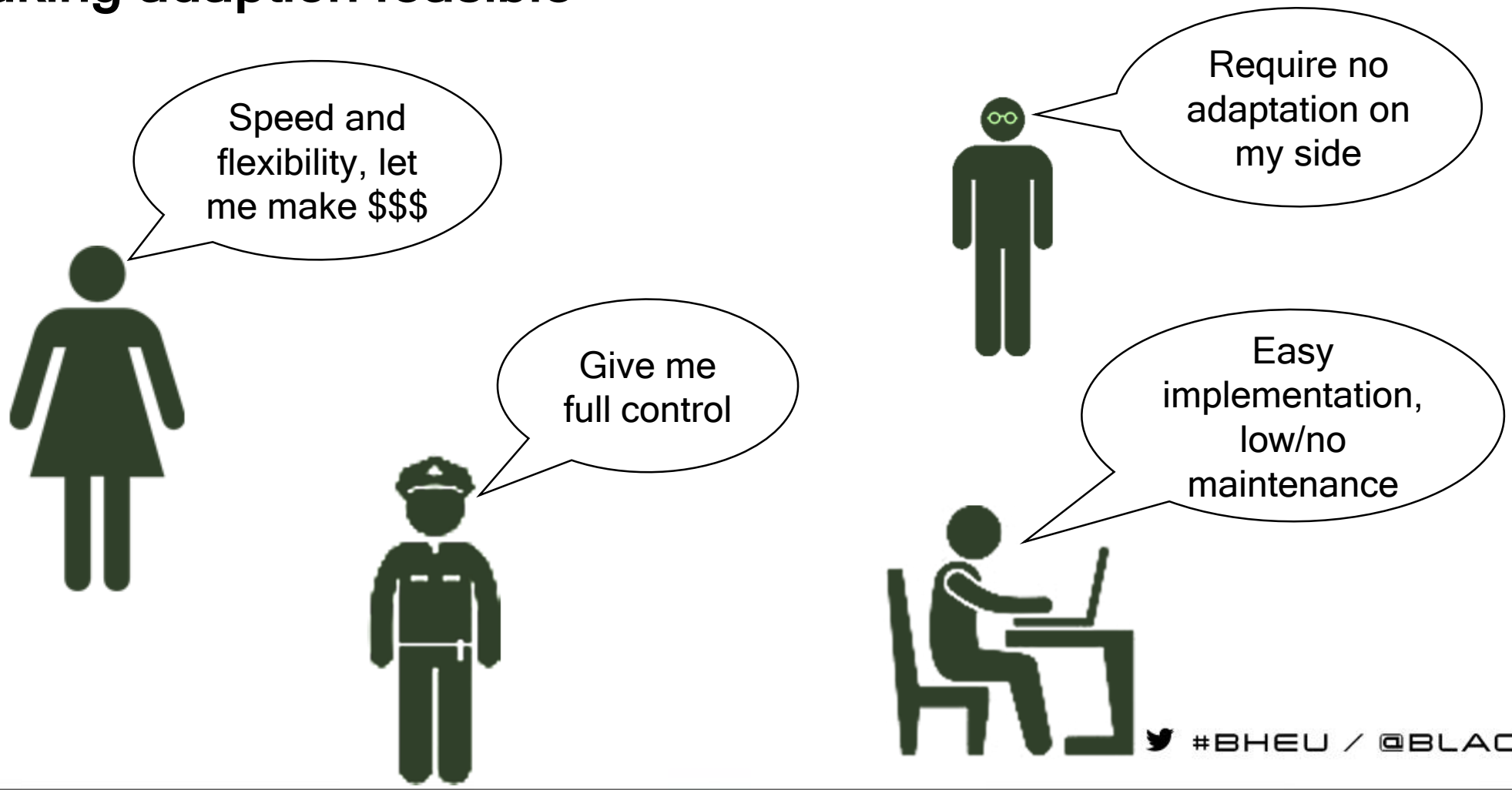
Suggested solution

Making adaption feasible

A policy based system that will easily identify third party scripts and allow the security team complete control over their read/write access, while staying transparent to the third parties and marketing team

Suggested solution

Making adaption feasible



source DEFENSE

Avital Grushcovski
+972-54-222-8380
avital@sourcedefense.com