RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **RMG-W09**

PCI DSS 4.0: Evolution, Revolution, or An Omen of Extinction?

John Elliott

Consultant and Pluralsight Author
Withoutfire

@withoutfire

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

I don’t have any inside knowledge of the plans of a card brand or the Payment Card Industry (PCI) Security Standards Council (SSC).
This presentation is my own opinion.

What is PCI DSS 4.0?

Evolution

Revolution

Heading for Extinction

Agenda

- A brief history of PCI DSS
- The DSS 4 development timeline
- New requirements in version 4.0
- The *Customized Approach* for validation
- Changes in the payment landscape
- Evolution, revolution or extinction?

PCI DSS 101

A written security standard

Developed by the Payment Card Industry (PCI) Security Standards Council (SSC)

Applies to entities that store, process or transmit cardholder data

Compliance is required by contract (not law*)

* Some countries / states have incorporated it into local/national regulation and laws

What problem was PCI DSS the answer to?

Criminals using stolen payment card data to commit fraud.

There were two possible fixes for this

Design the payment system so that stolen payment card data cannot be used to commit fraud

Make everyone that stores, processes or transmits payment card data protect it so it can’t be stolen

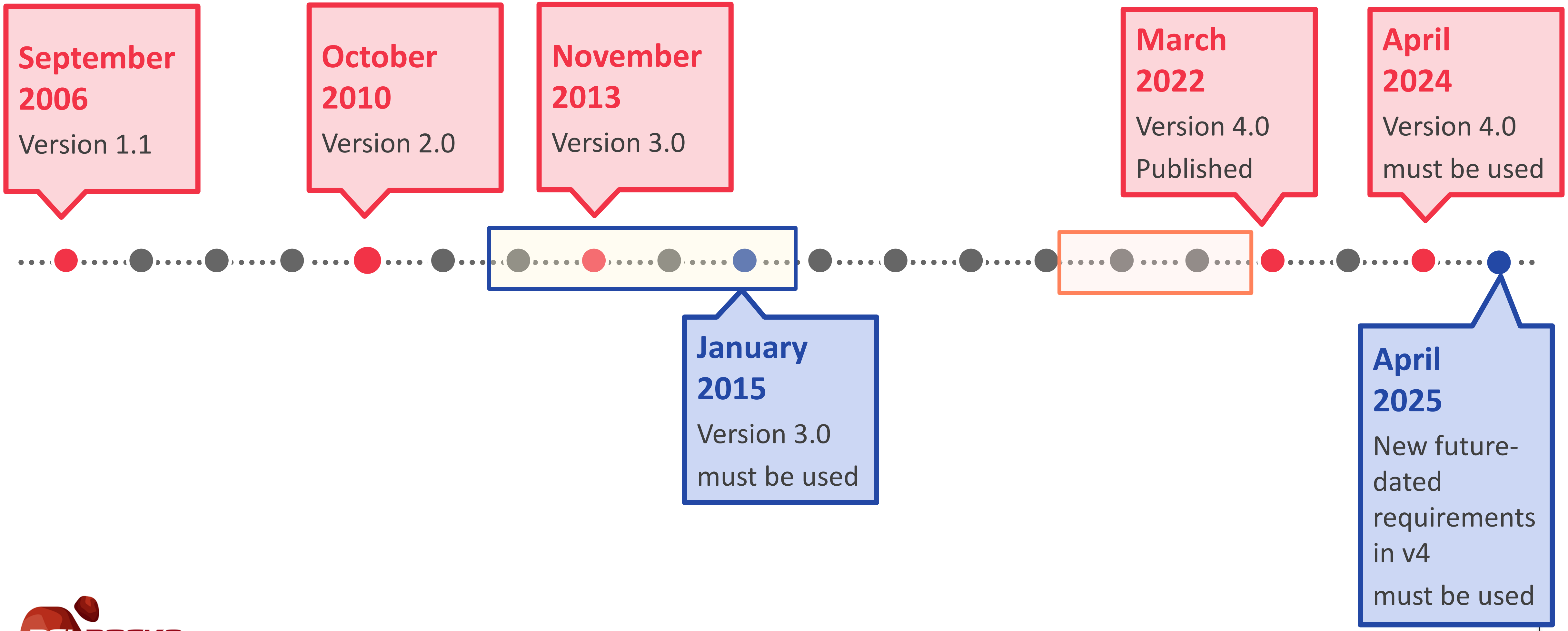
Why Does PCI DSS Exist?

To prevent Federal regulation of card data security

To pass liability for breaches to card-accepting merchants

To secure cardholder data

PCI DSS history



September 2006
Version 1.1

October 2010
Version 2.0

November 2013
Version 3.0

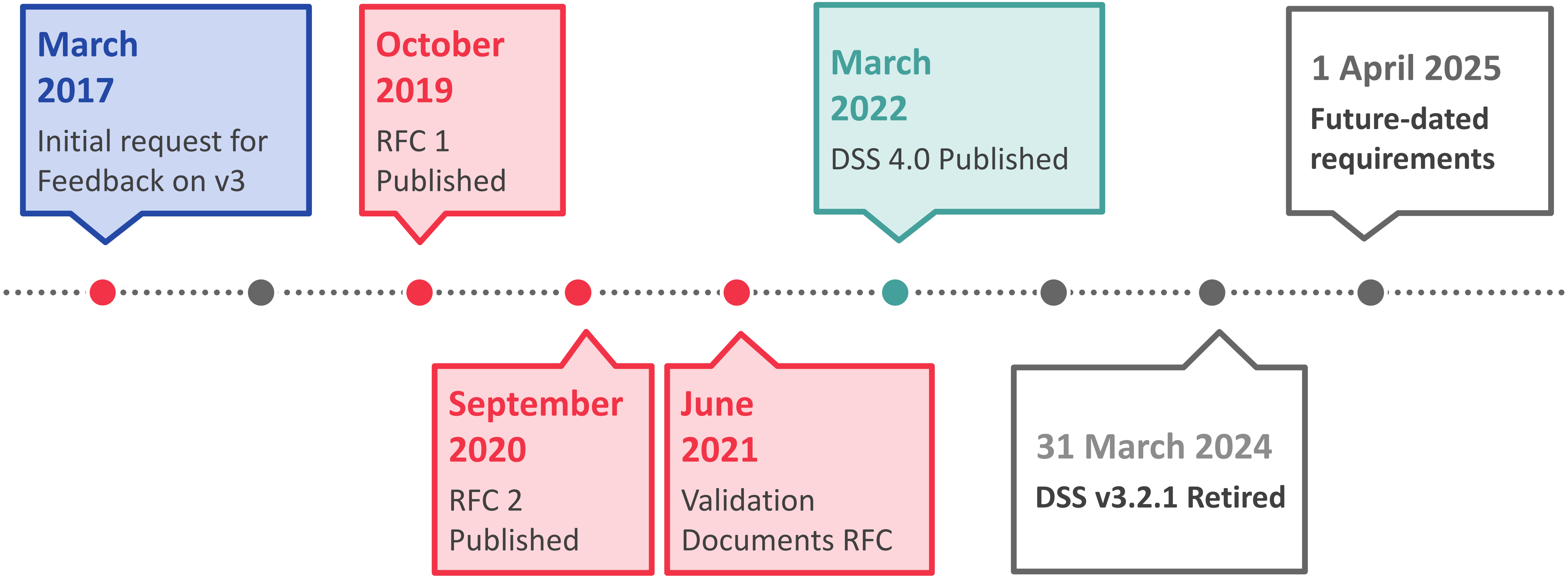
January 2015
Version 3.0
must be used

March 2022
Version 4.0
Published

April 2024
Version 4.0
must be used

April 2025
New future-dated requirements in v4
must be used

DSS 4 Development Timeline



March 2017
Initial request for Feedback on v3

October 2019
RFC 1 Published

September 2020
RFC 2 Published

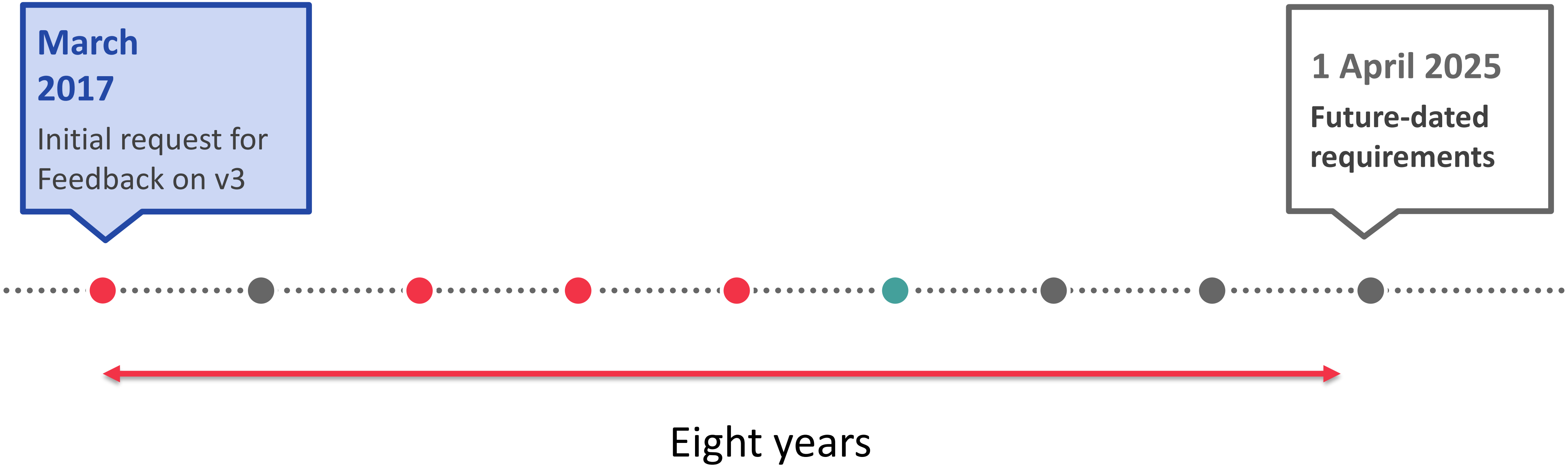
June 2021
Validation Documents RFC

March 2022
DSS 4.0 Published

31 March 2024
DSS v3.2.1 Retired

1 April 2025
Future-dated requirements

DSS 4 Development Timeline



March 2017

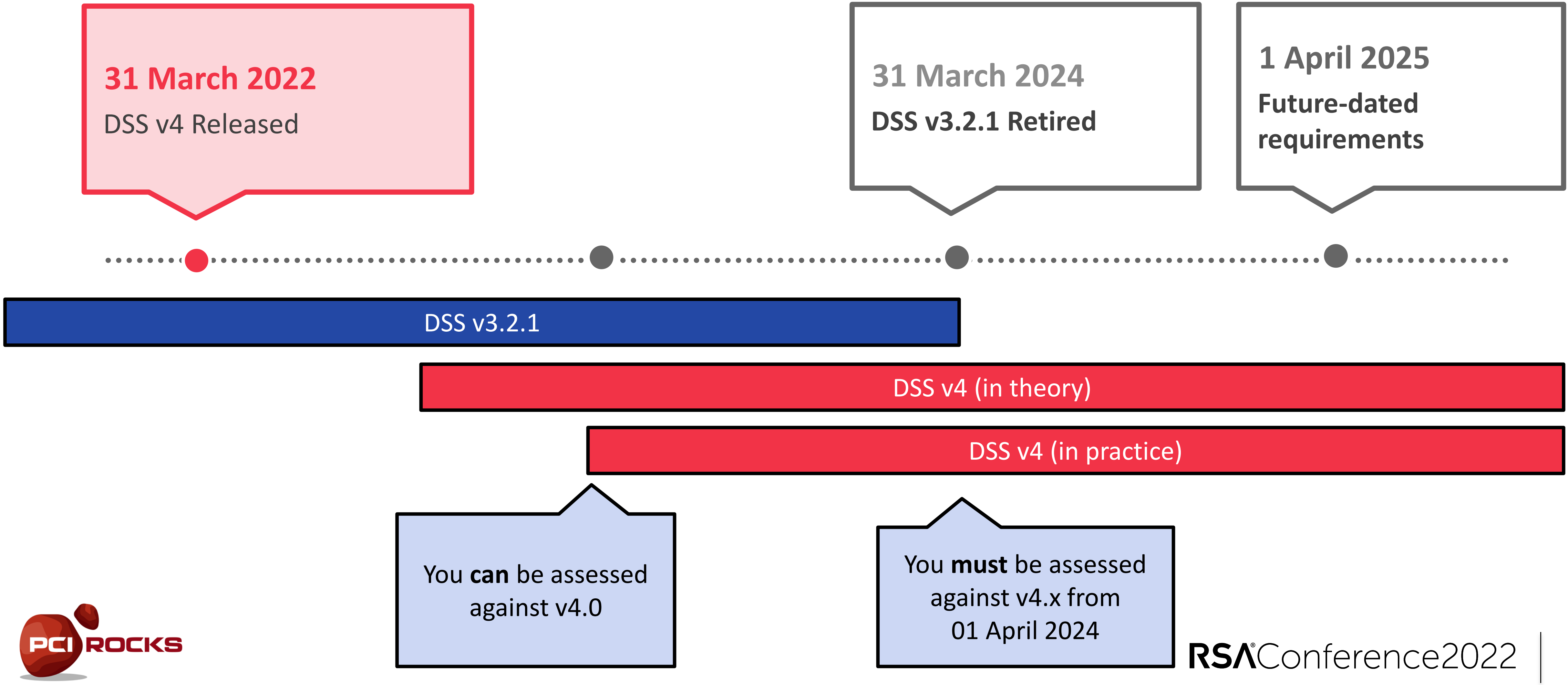
Initial request for Feedback on v3

1 April 2025

Future-dated requirements

Eight years

DSS 4 timeline



31 March 2022

DSS v4 Released

31 March 2024

DSS v3.2.1 Retired

1 April 2025

Future-dated requirements

DSS v3.2.1

DSS v4 (in theory)

DSS v4 (in practice)

You **can** be assessed against v4.0

You **must** be assessed against v4.x from 01 April 2024

What's New

4.0

- 13 policy or process new requirements
- 51 technology new requirements
  - All future-dated, applicable one year after the standard becomes effective
- Some allowance for risk
  - Mainly in determining the period over which things should be done
- Two ways of validating compliance with a requirement
  - **Defined Approach**: Prescriptive requirement and testing procedures
  - **Customized Approach**: Meet the security objective

Evolution

Some of the new requirements in PCI DSS 4.0

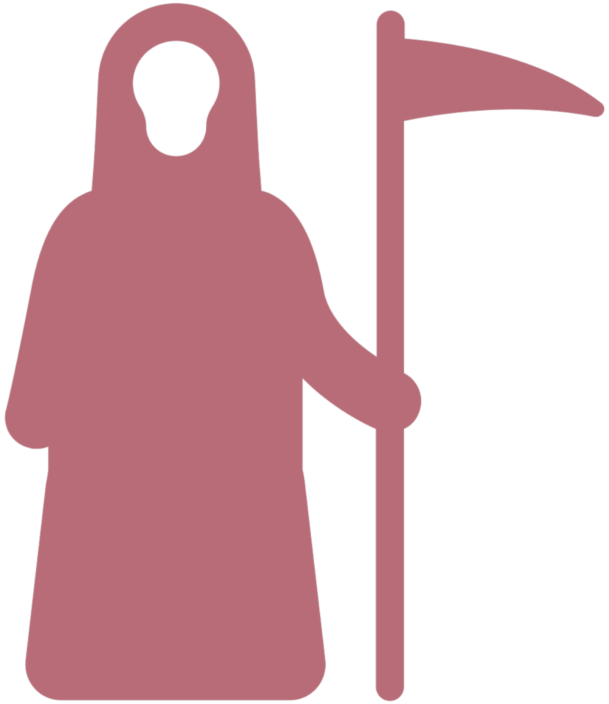
Major new requirements

- If hashing PANs, hash needs to be keyed
- Disk encryption no longer sufficient except on removable media
- Managed System and Application Accounts
  - Least privilege, password complexity & change, strong controls if used for interactive login (PAM)
- MFA for all access to the CDE
- Authenticated internal vulnerability scans
- Anti-phishing technology & training

Protecting e-commerce

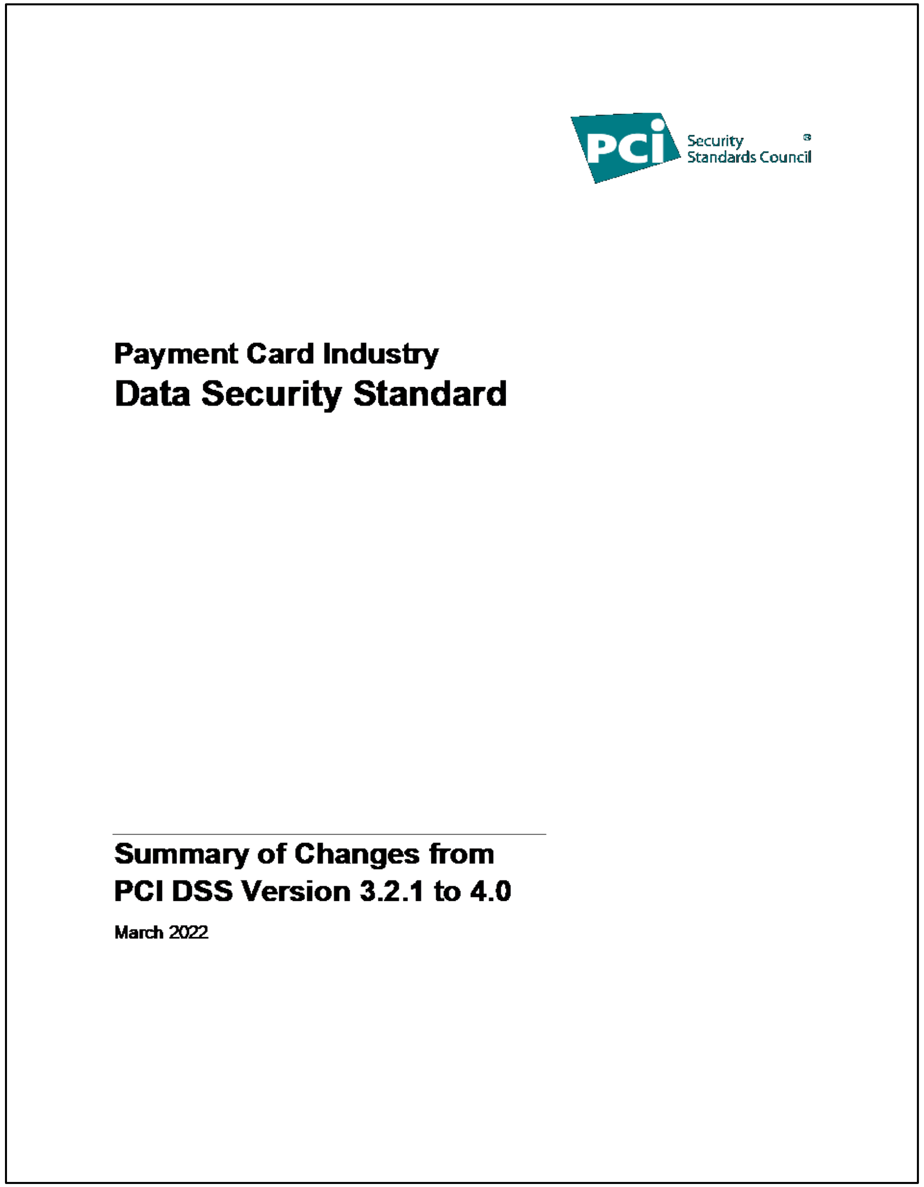
- Prevent skimming Requirement: 6.4.3
  - Only necessary scripts
  - Authorised by management
  - Integrity validated
    - Prevent malicious script execution
    - CSP and SRI
- Detect skimming Requirement: 11.6.1
  - Tamper detection / tamper prevention
  - CSP violation reporting
  - External monitor / checker

Inventories and End-of-life



- Bespoke and Custom Software 6.3.2
  - Vulnerability and patch management
  - An SBOM by any other name?
- (Hardware and Software 12.5.1
  - Not a new requirement)
- BUT: Review annually 12.3.4
  - Still supported by the vendor?
  - Plan to remediate end-of-life components
- Cryptography 12.3.3

Recommended Download



PCI Security Standards Council

Payment Card Industry
Data Security Standard

Summary of Changes from PCI DSS Version 3.2.1 to 4.0

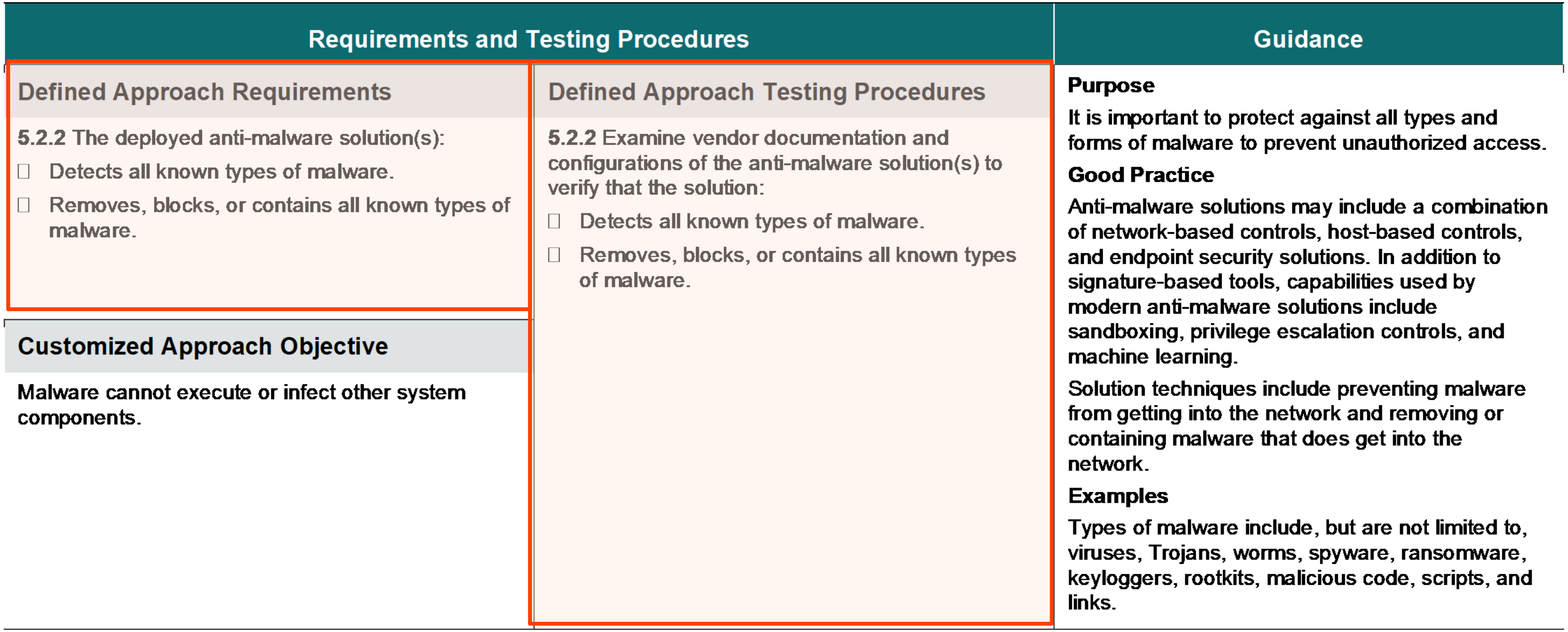
March 2022

64 new requirements

Revolution

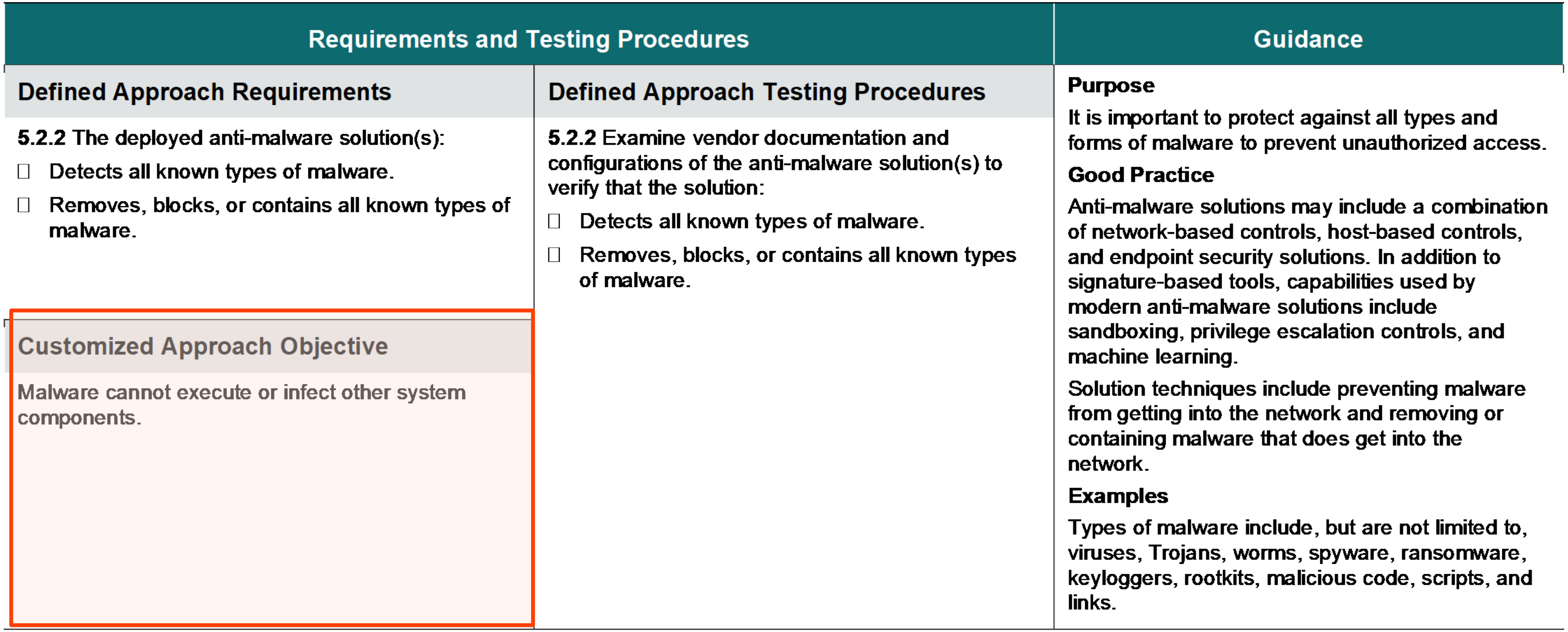
The Customized Approach

How the customized approach works



Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important to protect against all types and forms of malware to prevent unauthorized access. **Good Practice** Anti-malware solutions may include a combination of network-based controls, host-based controls, and endpoint security solutions. In addition to signature-based tools, capabilities used by modern anti-malware solutions include sandboxing, privilege escalation controls, and machine learning. Solution techniques include preventing malware from getting into the network and removing or containing malware that does get into the network. **Examples** Types of malware include, but are not limited to, viruses, Trojans, worms, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links.
5.2.2 The deployed anti-malware solution(s): □ Detects all known types of malware. □ Removes, blocks, or contains all known types of malware.	**5.2.2** Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution: □ Detects all known types of malware. □ Removes, blocks, or contains all known types of malware.	
Customized Approach Objective		
Malware cannot execute or infect other system components.		

How the customized approach works



Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** It is important to protect against all types and forms of malware to prevent unauthorized access. **Good Practice** Anti-malware solutions may include a combination of network-based controls, host-based controls, and endpoint security solutions. In addition to signature-based tools, capabilities used by modern anti-malware solutions include sandboxing, privilege escalation controls, and machine learning. Solution techniques include preventing malware from getting into the network and removing or containing malware that does get into the network. **Examples** Types of malware include, but are not limited to, viruses, Trojans, worms, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links.
5.2.2 The deployed anti-malware solution(s): □ Detects all known types of malware. □ Removes, blocks, or contains all known types of malware.	**5.2.2** Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution: □ Detects all known types of malware. □ Removes, blocks, or contains all known types of malware.	
Customized Approach Objective		
Malware cannot execute or infect other system components.		

How the customized approach works

Defined Approach

Requirement

5.2.2 The deployed anti-malware solution(s):

- Detects all known types of malware.
- Removes, blocks, or contains all known types of malware.

Testing Procedure

Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution:

- Detects all known types of malware.
- Removes, blocks, or contains all known types of malware.

Customized Approach

Objective

5.2.2 Malware cannot execute or infect other system components.

An organisation can select its own controls to meet the customized approach objective.

How the customized approach works

Defined Approach

Requirement

5.2.2 The deployed anti-malware solution(s):

- Detects all known types of malware.
- Removes, blocks, or contains all known types of malware.

Testing Procedure

Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution:

- Detects all known types of malware.
- Removes, blocks, or contains all known types of malware.

Customized Approach

Objective

5.2.2 Malware cannot execute or infect other system components.

Example:
An organisation deploys allow-listing to prevent all unknown software executing

How the customized approach works

Defined Approach

Requirement

5.2.2 The deployed anti-malware solution(s):

- Detects all known types of malware.
- Removes, blocks, or contains all known types of malware.

For each requirement you can do this

Testing Procedure

Examine vendor documentation and configurations of the anti-malware solution(s) to verify that the solution:

- Detects all known types of malware.
- Removes, blocks, or contains all known types of malware.

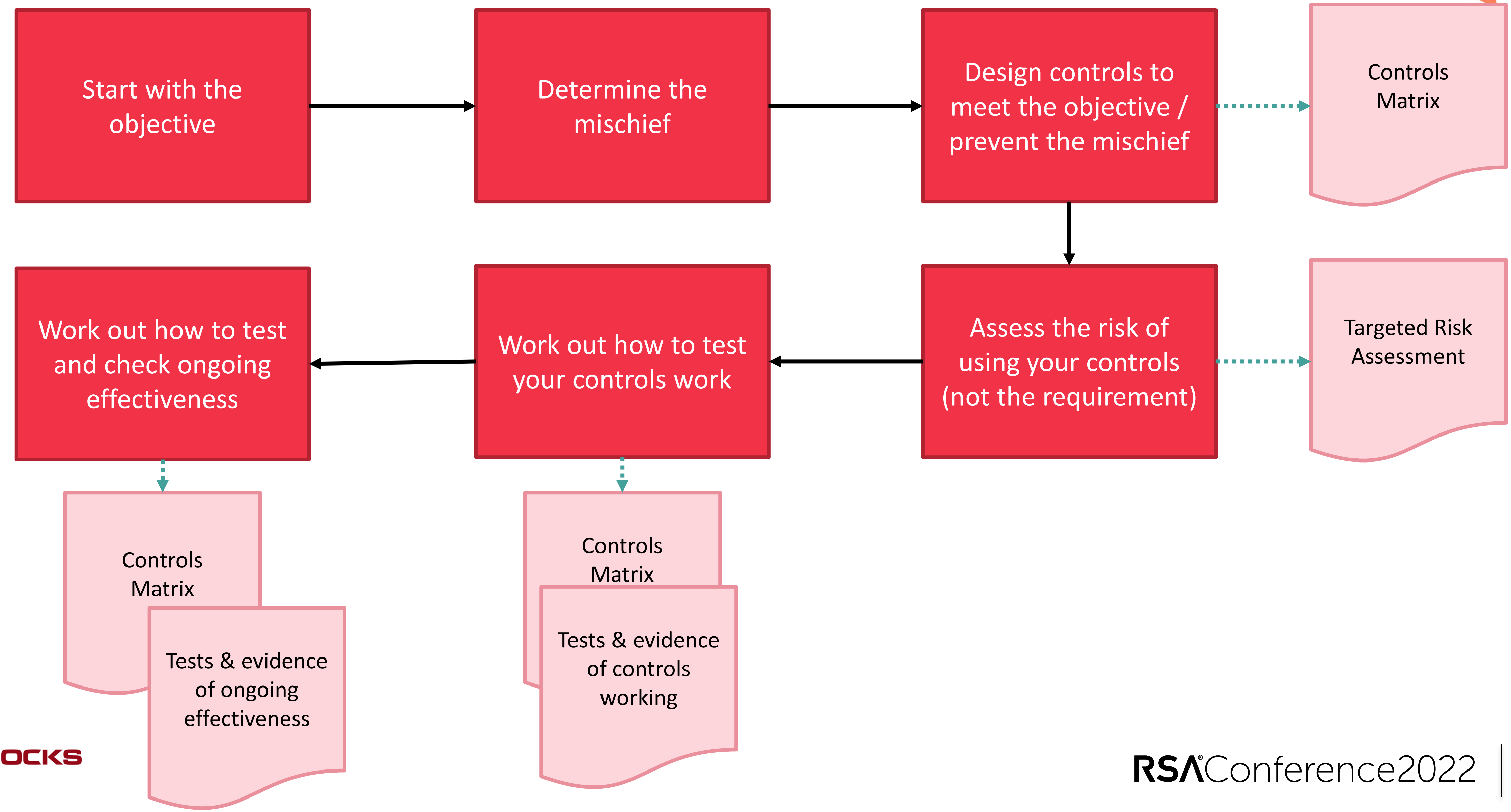
Customized Approach

Objective

5.2.2 Malware cannot execute or infect other system components.

or this

How to do the customized approach



Start with the objective

Determine the mischief

Design controls to meet the objective / prevent the mischief

Controls Matrix

Assess the risk of using your controls (not the requirement)

Targeted Risk Assessment

Work out how to test your controls work

Controls Matrix

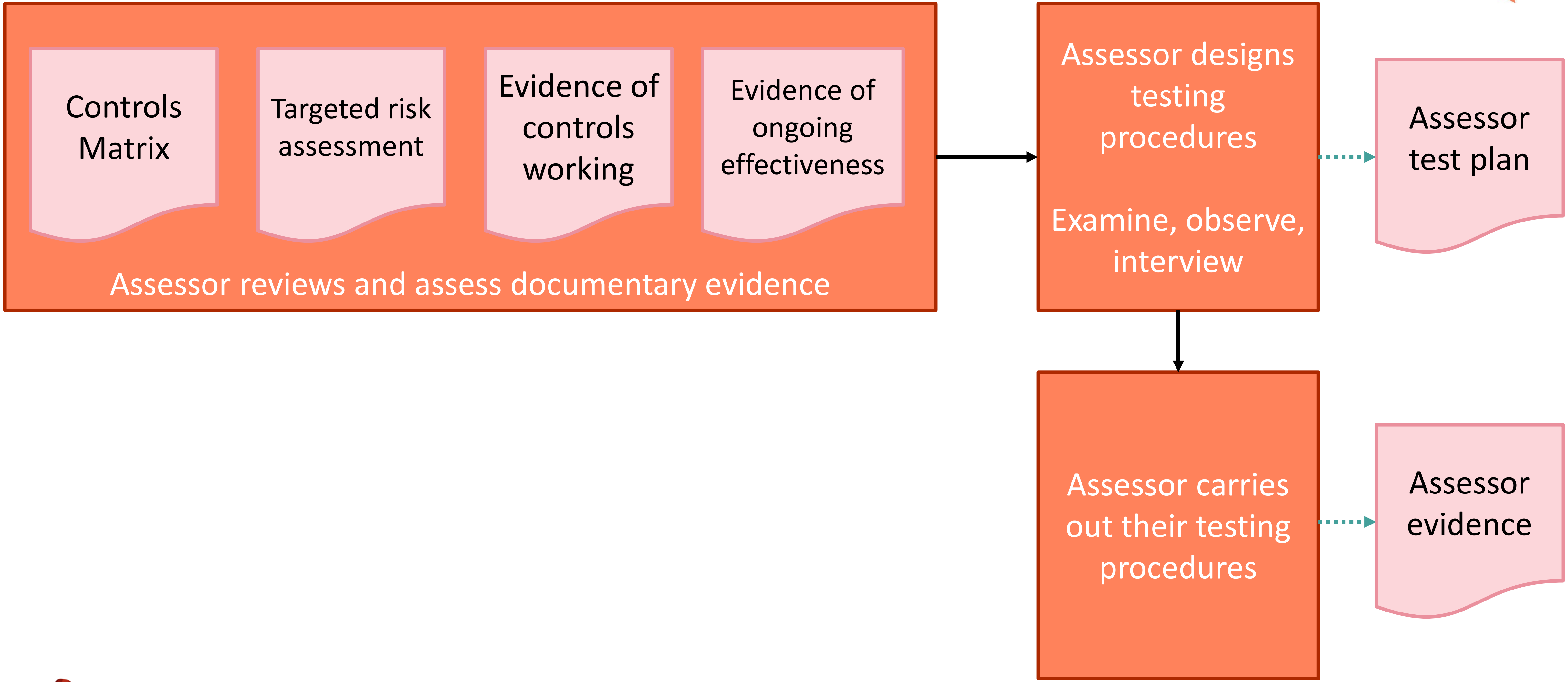
Tests & evidence of controls working

Work out how to test and check ongoing effectiveness

Controls Matrix

Tests & evidence of ongoing effectiveness

How it will be assessed

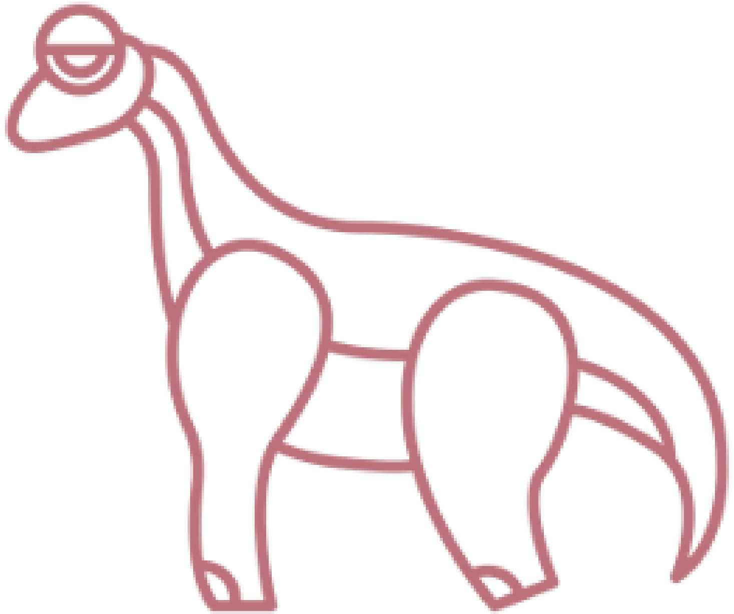

Controls Matrix
Targeted risk assessment
Evidence of controls working
Evidence of ongoing effectiveness
Assessor reviews and assess documentary evidence
Assessor designs testing procedures
Examine, observe, interview
Assessor test plan
Assessor carries out their testing procedures
Assessor evidence

RSA Conference2022

Extinction?

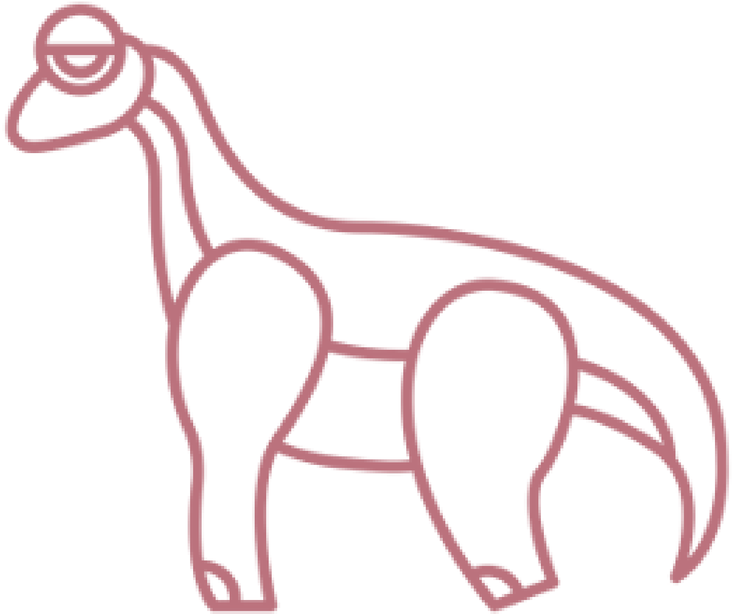
What’s wrong with PCI DSS 4.0

What’s wrong with PCI DSS 4.0



- Still very infrastructure-centric
  - Almost as if cloud doesn’t exist
  - Or agile doesn’t exist
- All 300+ controls have equal weight
- It’s too late. You should already be doing most of the new controls if they are appropriate for your environment

Do we need PCI DSS 4.0?



- In 2006 the world needed a prescriptive security standard

"When I got out of jail everyone had a firewall, and stealing card data got much harder"

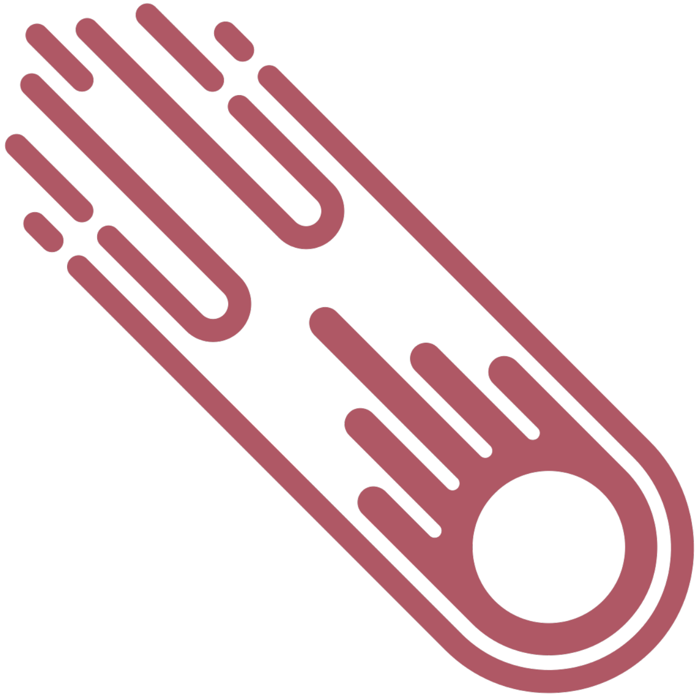
- Not threat-related
  - See Adam Shostack @ RSAC 2021
- Does the world need a prescriptive security standard in 2025?

RSA Conference2022

Extinction?

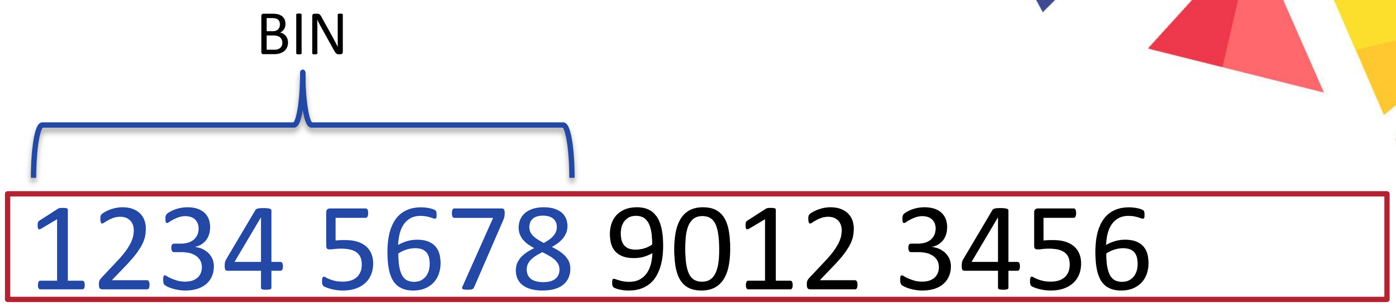
The Changing Payments World

Do we even need to protect cardholder data?



- Do truncated PANs need protecting?
  - Only 3 digits to guess

Truncation of PANs



BIN

This is a PAN 1234 5678 9012 3456

It is so sensitive and valuable to criminals that it needs to be protected by >300 information security controls

Truncation of PANs

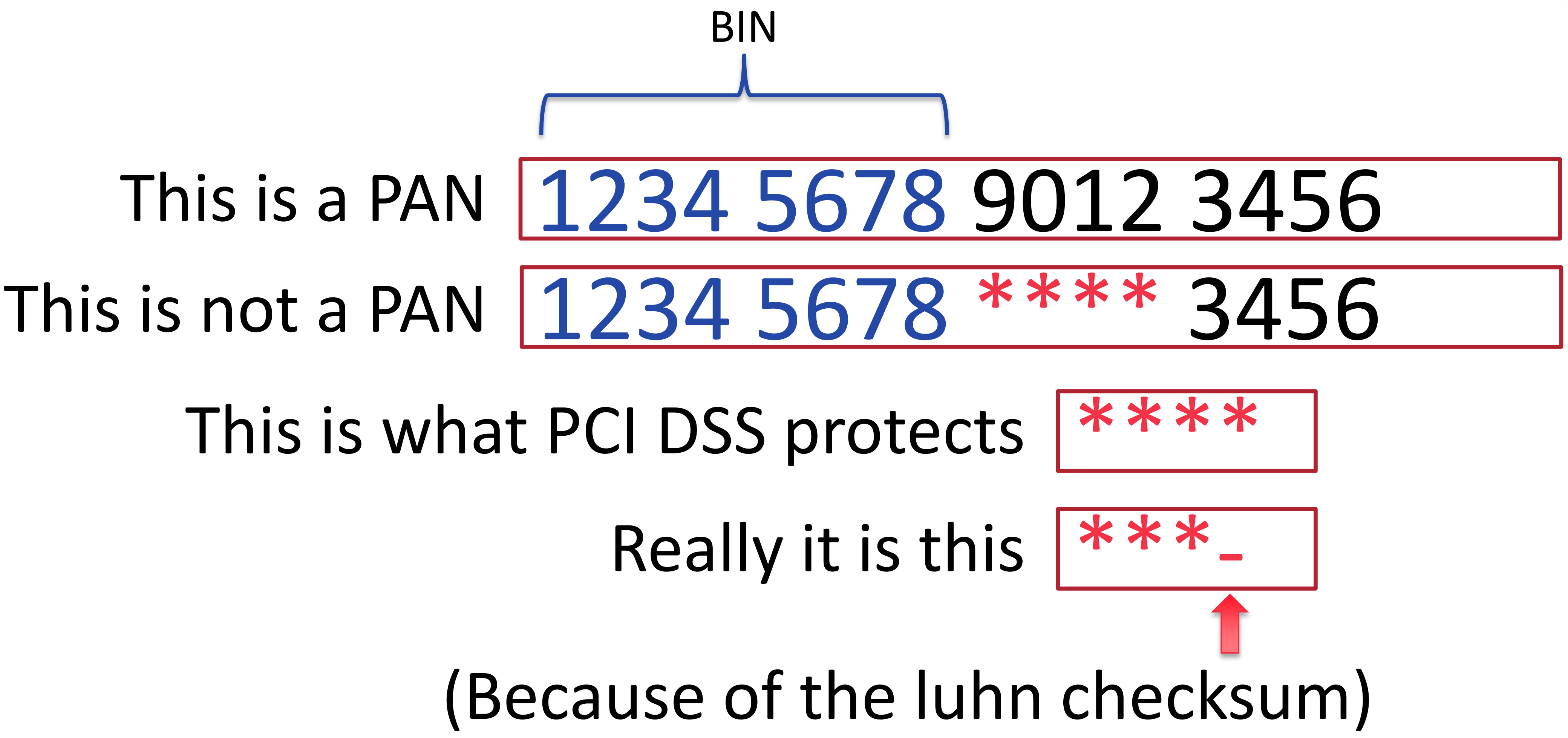
BIN

This is not a PAN 1234 5678 **** 3456

Supposedly it is not sensitive or valuable to criminals so it needs no protection.

FAQ 1117: “Systems that store, process, or transmit only truncated PANs (where a segment of PAN data has been permanently removed) may be considered out of scope for PCI DSS if those systems are adequately segmented from the cardholder data environment, and do not otherwise store, process, or transmit cardholder data or sensitive authentication data. This applies to any truncation that meets the acceptable PAN truncation formats specified in FAQ 1091.”

Truncation of PANs



BIN

This is a PAN 1234 5678 9012 3456

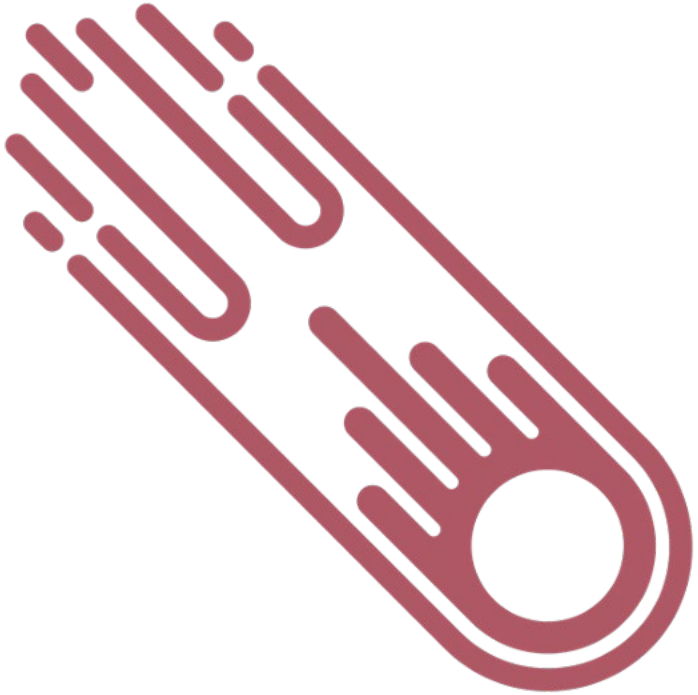
This is not a PAN 1234 5678 **** 3456

This is what PCI DSS protects ****

Really it is this ***_

(Because of the luhn checksum)

Do we even need to protect cardholder data?



- Do truncated PANs need protecting?
  - Only 3 digits to guess
- Card brands exempt EMV accepting merchants from PCI DSS *validation*
  - Stolen PAN from EMV data not a risk

Card Brand Rules

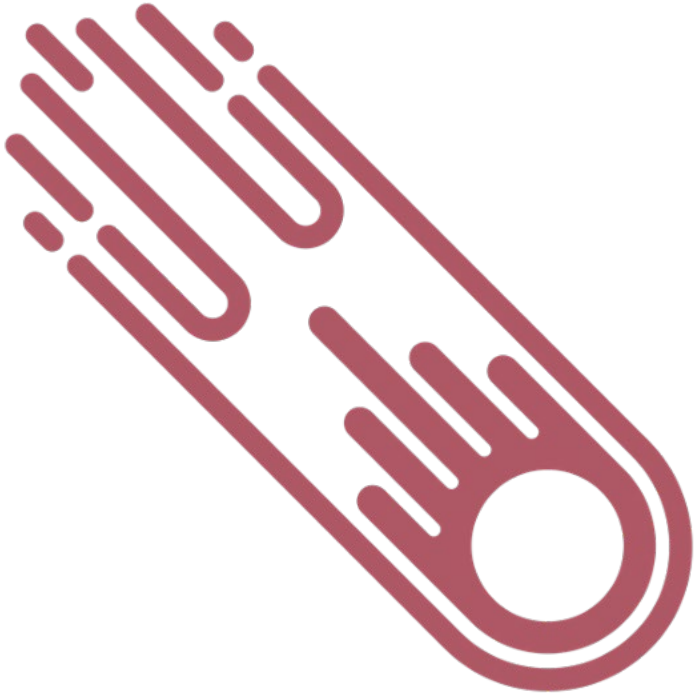
Mastercard

All qualifying Merchants may participate in the Mastercard PCI DSS Compliance Validation Exemption Program which exempts the Merchant
from annually validating its compliance with the PCI DSS. At least 75 percent of the Merchant’s annual total acquired Mastercard and Maestro Transaction count is processed through Hybrid POS Terminals.

Visa

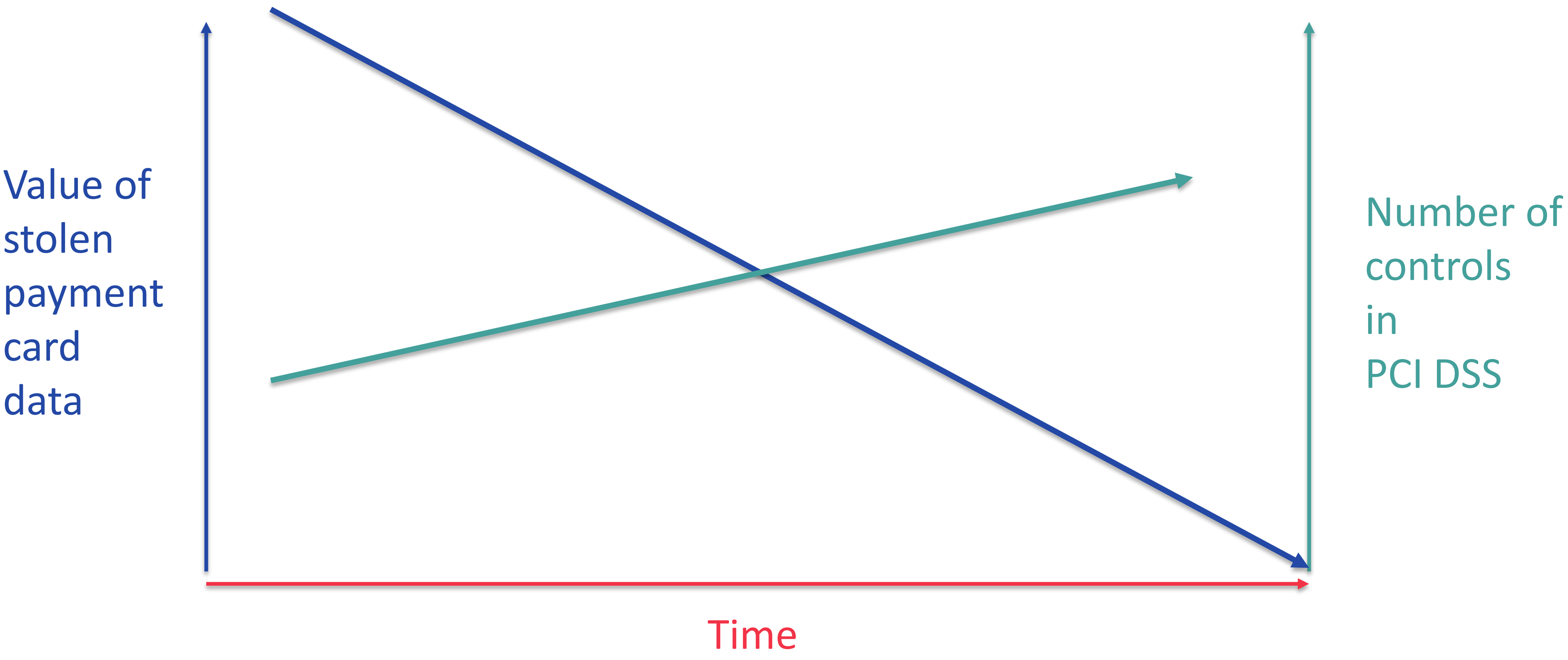
This program rewards eligible merchants by eliminating the requirement to verify compliance with the PCI DSS when at least 75 percent of yearly transactions originate through any combination of the dual-interface EMV chip-enabled terminals ...

Do we even need to protect cardholder data?

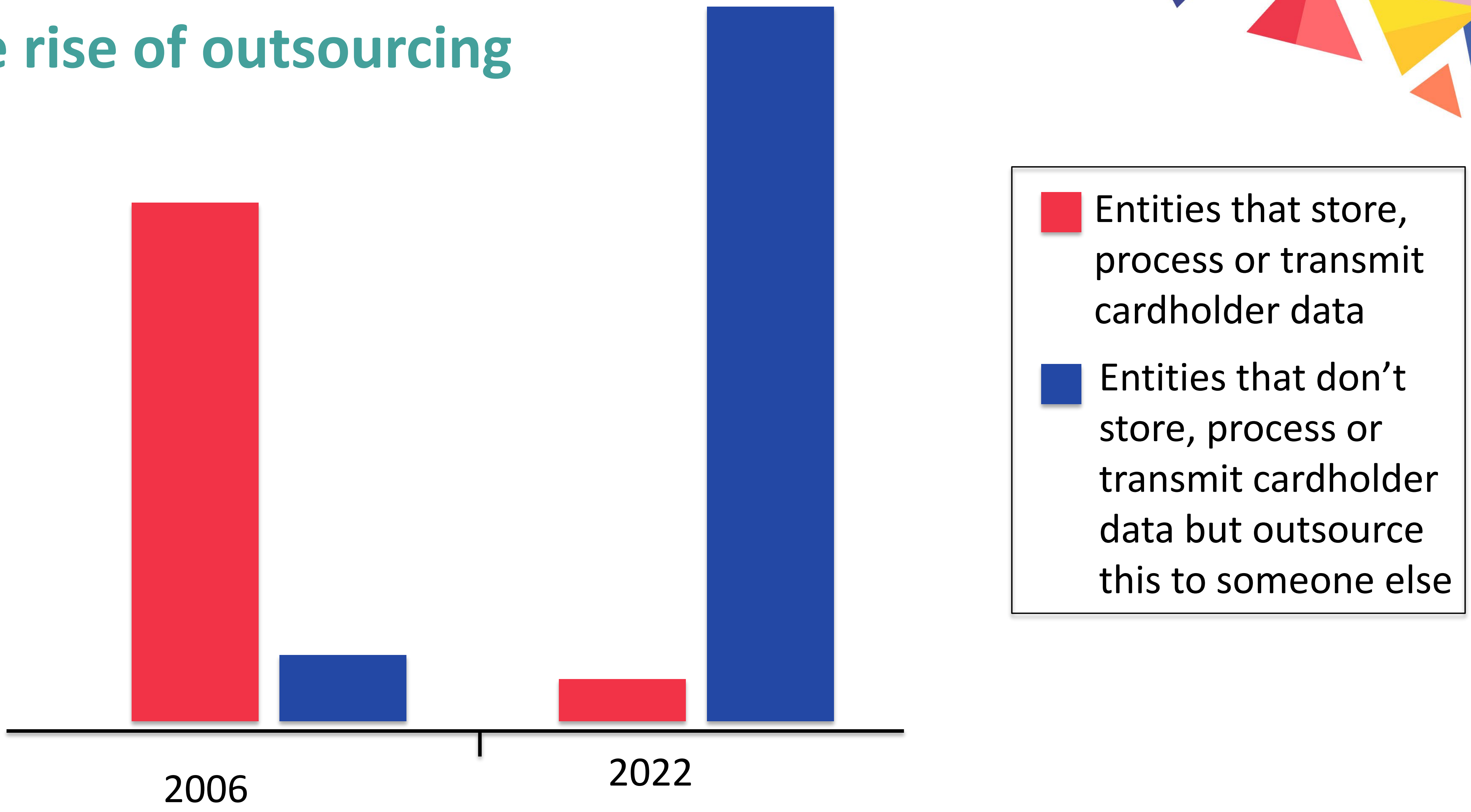


- Do truncated PANs need protecting?
  - Only 3 digits to guess
- Card brands exempt EMV accepting merchants from PCI DSS validation
- Secure Customer Authentication (SCA) mandatory in the EU and UK
  - 3D Secure that works (3DSv2)
  - Stolen PAN + CVV2 valueless
- EMV Payment tokens on devices

This Perhaps Doesn't Add Up



The rise of outsourcing



Why Does PCI DSS Exist?

To prevent Federal regulation of card data security

To pass liability for breaches to card-accepting merchants

To secure cardholder data

Why Does PCI DSS Exist?

Close to having global privacy laws

Regulation is now for technology.

EMV

SCA

To pass liability for breaches to card-accepting merchants

To secure cardholder data

Why Does PCI DSS Exist?

Close to having global privacy laws

Regulation is now for technology.

EMV

SCA

Other sources of risk for merchants

To secure cardholder data

Why Does PCI DSS Exist?

Close to having global privacy laws

Regulation is now for technology.

EMV

SCA

Other sources of risk for merchants

Soon stolen cardholder data will be valueless (from a payments perspective)

The Card Brands
(who make the compliance mandates)
have no reason for PCI DSS to exist

any more

The Card Brands
(who make the compliance mandates)
have no reason for PCI DSS to exist
(certainly in Europe)
any more

But …

How long will it take to roll out secure customer authentication (3DSv2) in all international markets?

Can it be attacked?

The Card Brands
(who make the compliance mandates)
have no reason for PCI DSS to exist
for the face-to-face environment any more

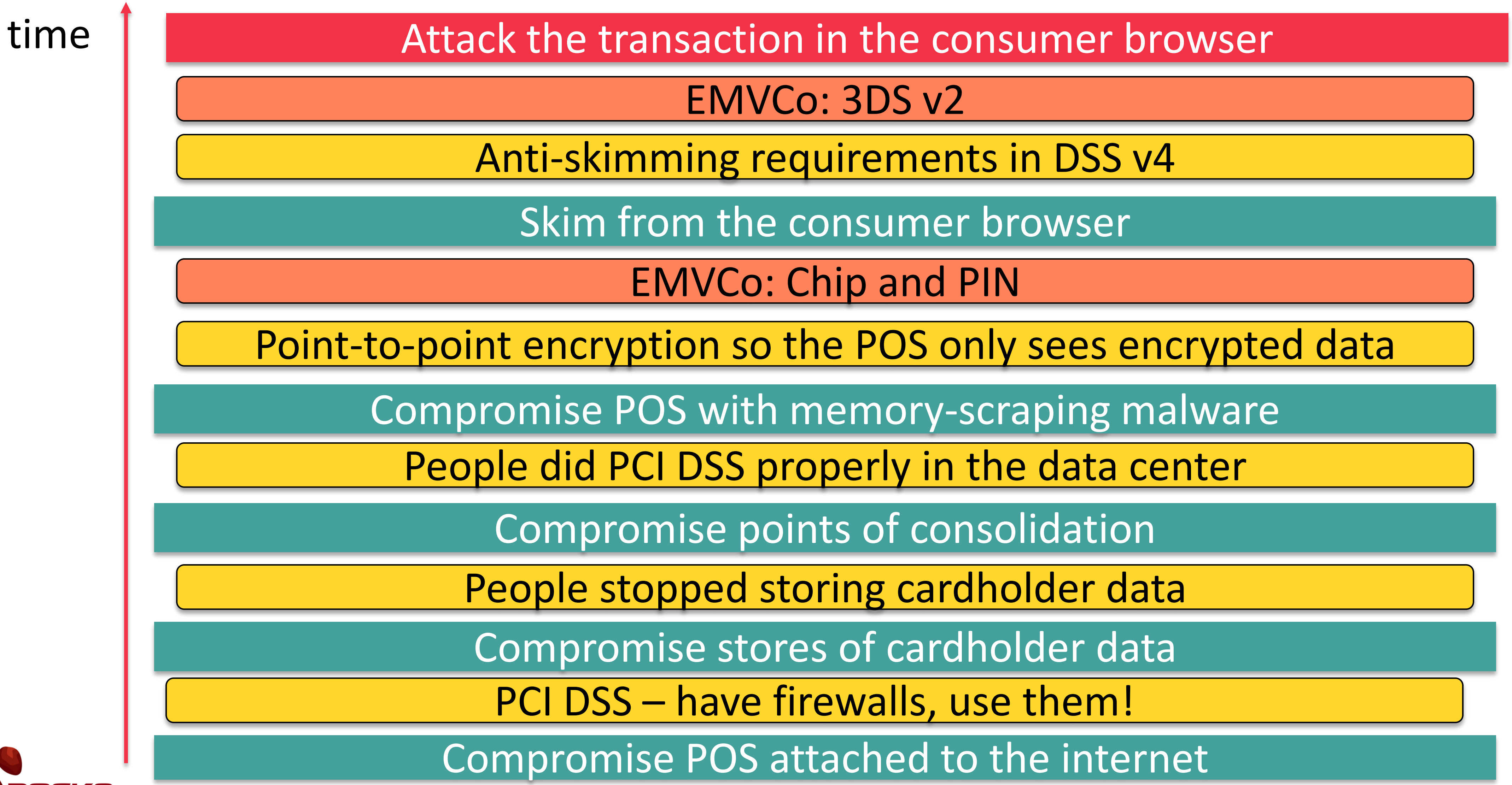
More Evolution?

The Changing Attack Surface

The SCA / 3DSv2 Problem

- Criminals are not going to stop being criminals
- There will be attacks against 3DSv2
  - Poor issuer implementations (e.g. not checking the cryptogram)
  - Tricking consumers
  - Relay attacks
  - Frame overlay
- Inside the brands, PCI DSS is regarded by everyone as the instant and magical answer to what appears to be any security problem

How the standard and criminals have evolved



time

Attack the transaction in the consumer browser

EMVCo: 3DS v2

Anti-skimming requirements in DSS v4

Skim from the consumer browser

EMVCo: Chip and PIN

Point-to-point encryption so the POS only sees encrypted data

Compromise POS with memory-scraping malware

People did PCI DSS properly in the data center

Compromise points of consolidation

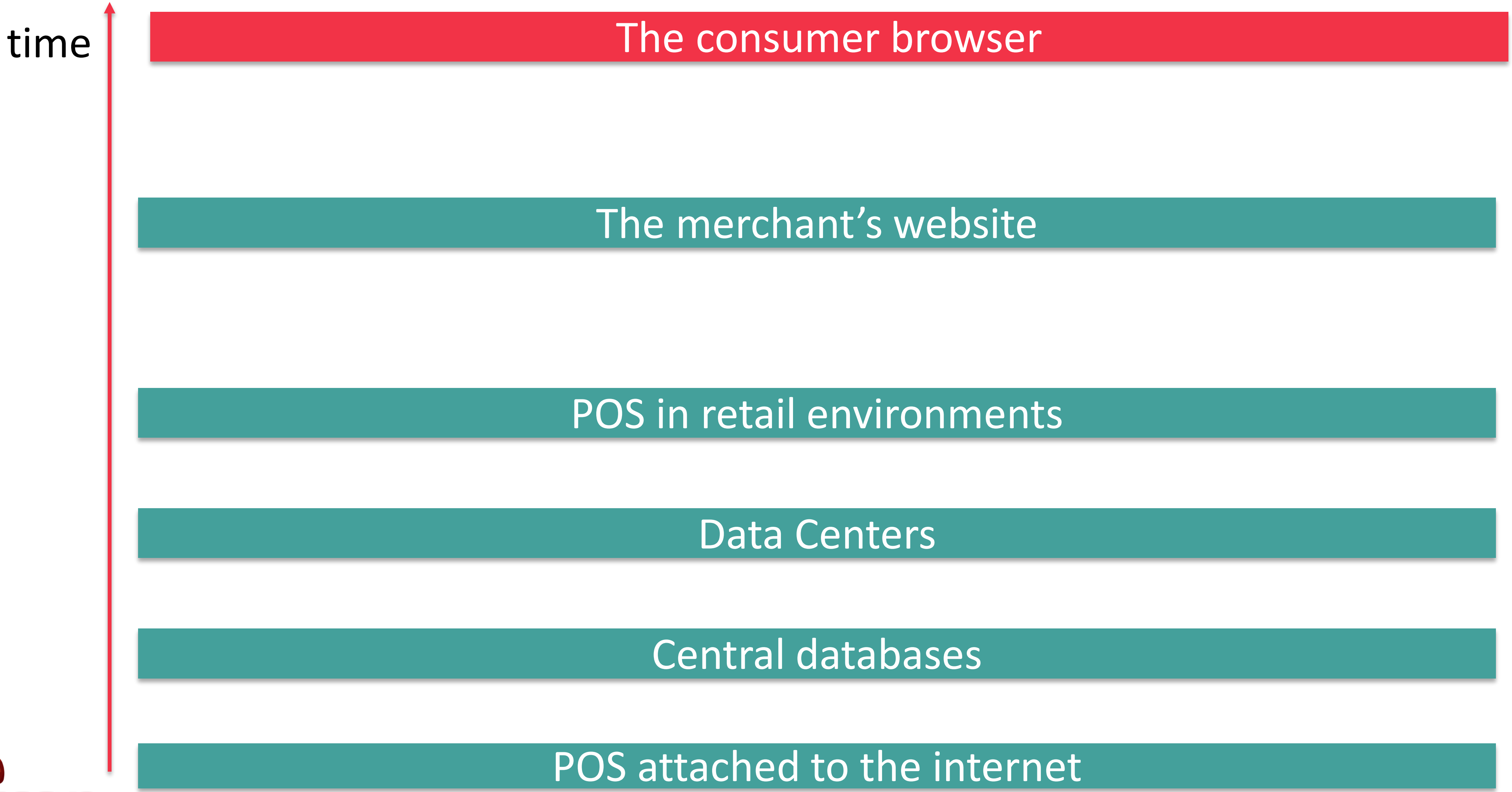
People stopped storing cardholder data

Compromise stores of cardholder data

PCI DSS – have firewalls, use them!

Compromise POS attached to the internet

The evolution of the attack surface



time

The consumer browser

The merchant’s website

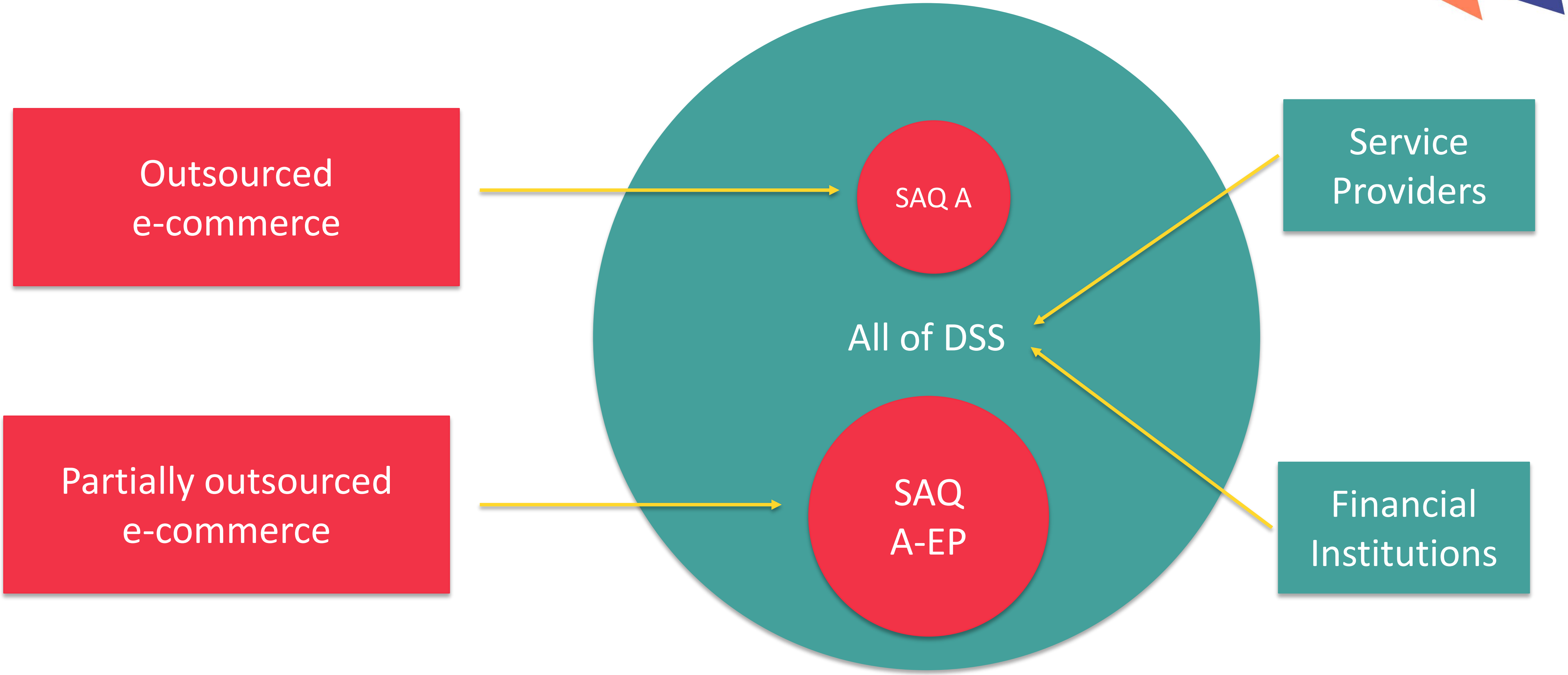
POS in retail environments

Data Centers

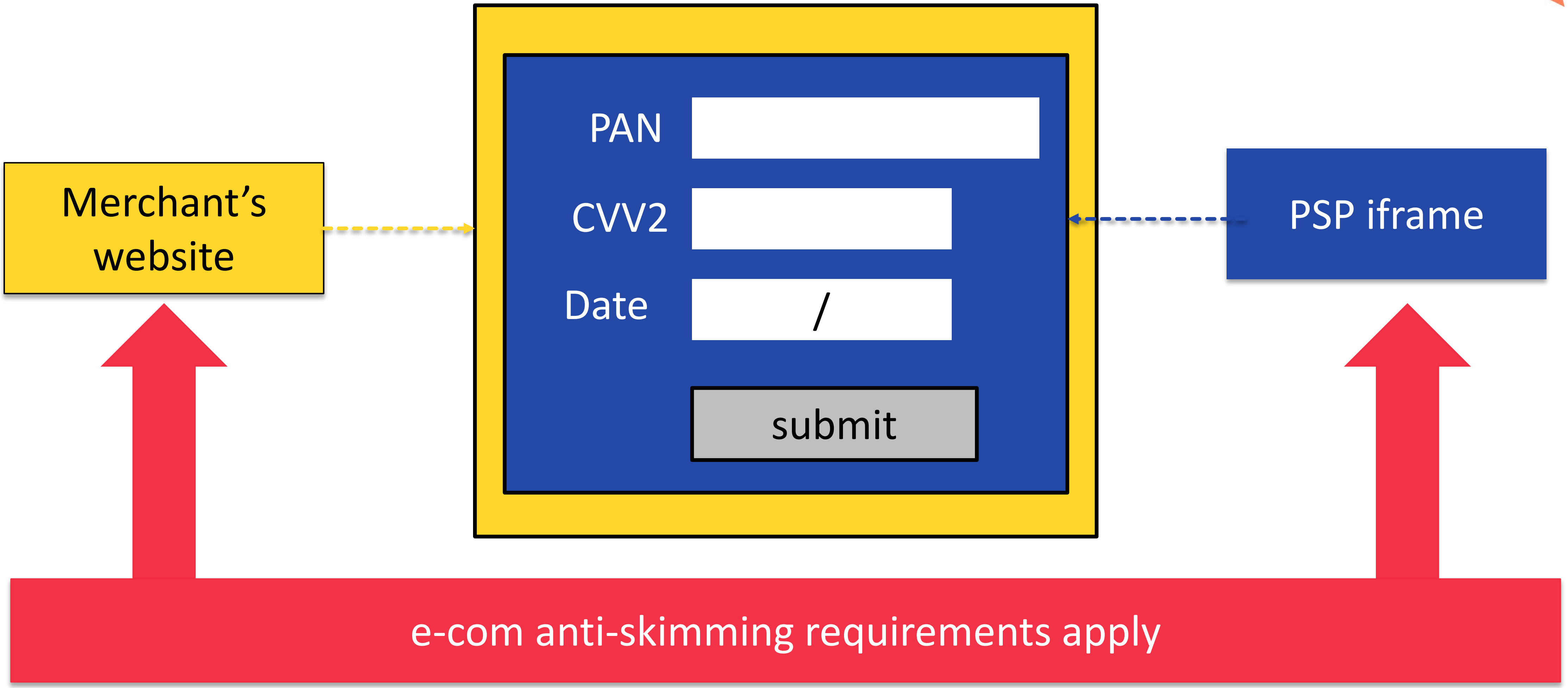
Central databases

POS attached to the internet

Prediction: More Limited and Targeted



Evolution: SAQ A

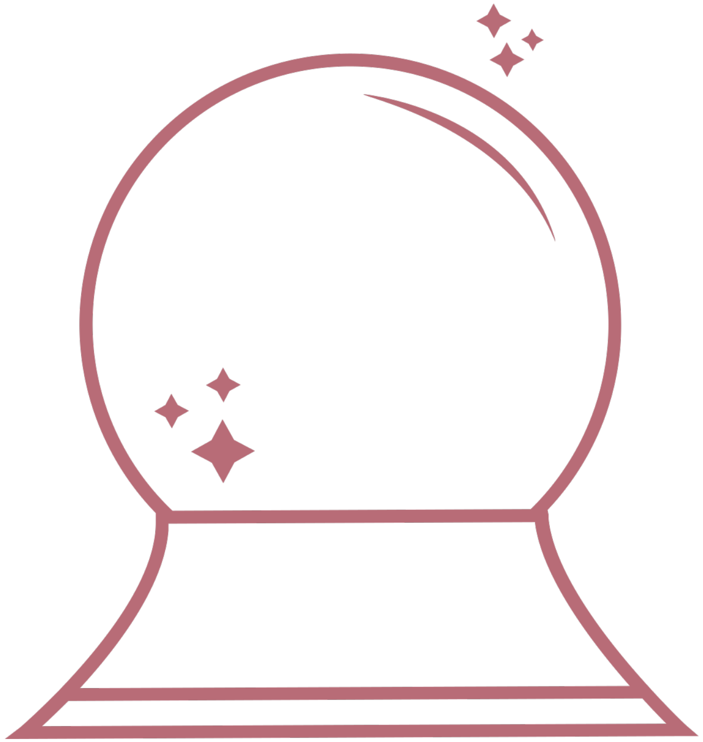


RSAConference2022

PCI DSS v4: Conclusions

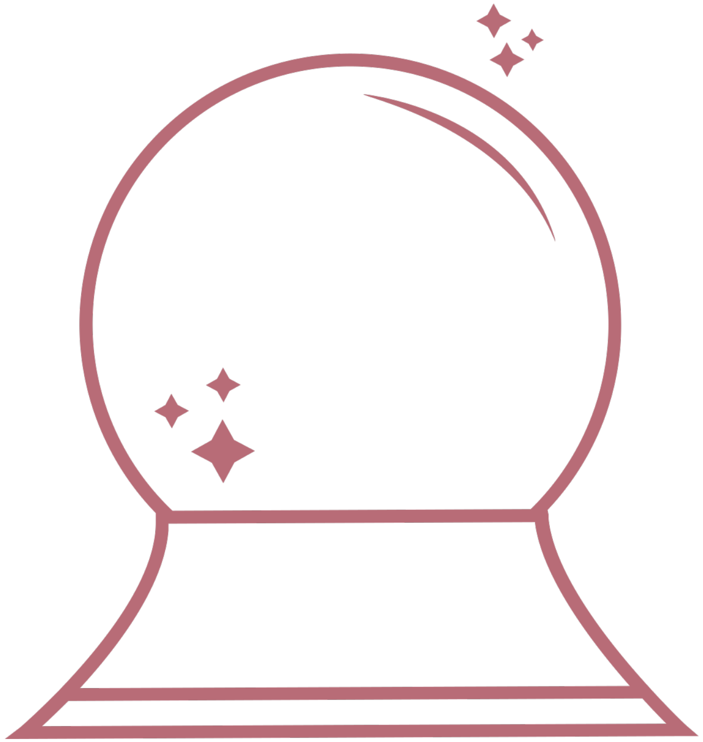
Evolution, revolution or soon-to-be extinction?

Conclusions – The Standard



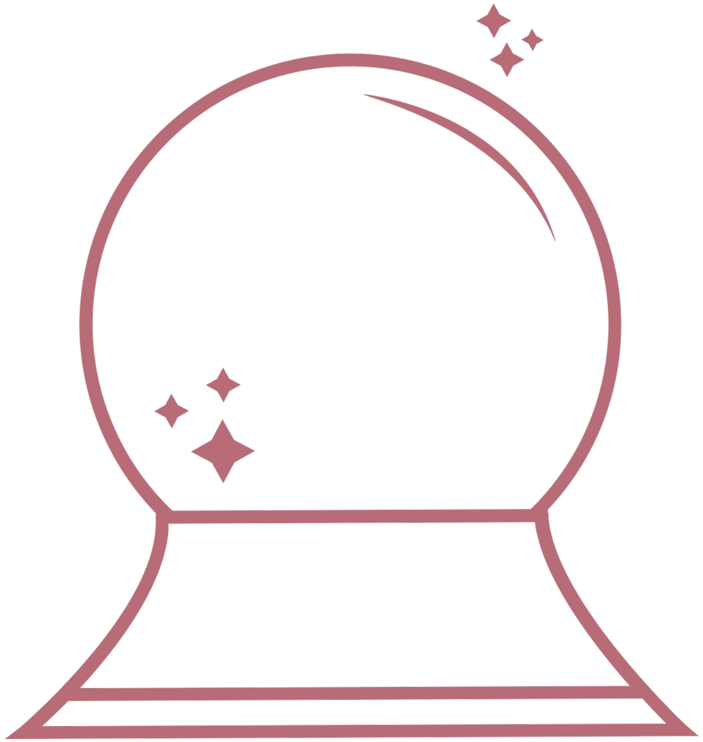
- DSS 4.0 is still a pretty good security standard
  - For infrastructure
  - For e-commerce – the consumer browser is the new attack surface
  - It’s late
  - It’s very comprehensive but shows its origins
- Where it falls short
  - Cloud and agile
- The customized approach is really good

Conclusions – The Environment



- Increasingly cardholder data doesn't need to be protected
- The application of DSS will shrink accordingly
- The card brands don't want or need to be the "enemy"
- Regulators are stepping into this area:
  - EMV chip in face-to-face
  - Secure Customer Authentication for e-commerce
  - Regulating technology, not security

Predictions – e-commerce



- Secure Customer Authentication / 3DSv2 will take some time
- It will be attacked
- There will be demands that transactions (rather than just cardholder data) will need to be protected
- A cut-down PCI DSS (now it has some e-com skimming requirements) will still be seen as the answer by the card brands
- Full PCI DSS still needed for service providers

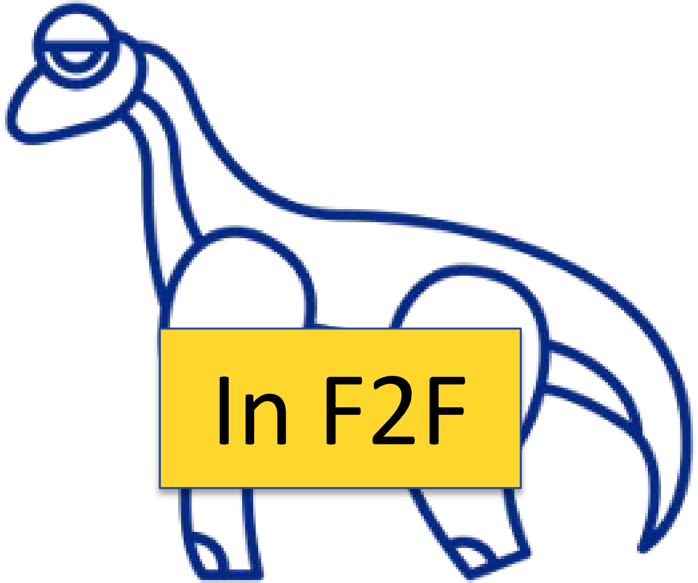
What is PCI DSS 4.0?

Evolution

YES

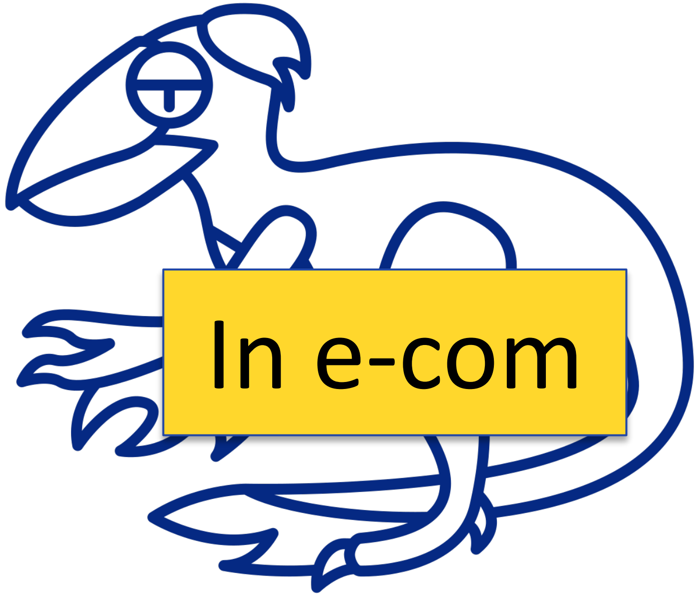
Revolution

YES



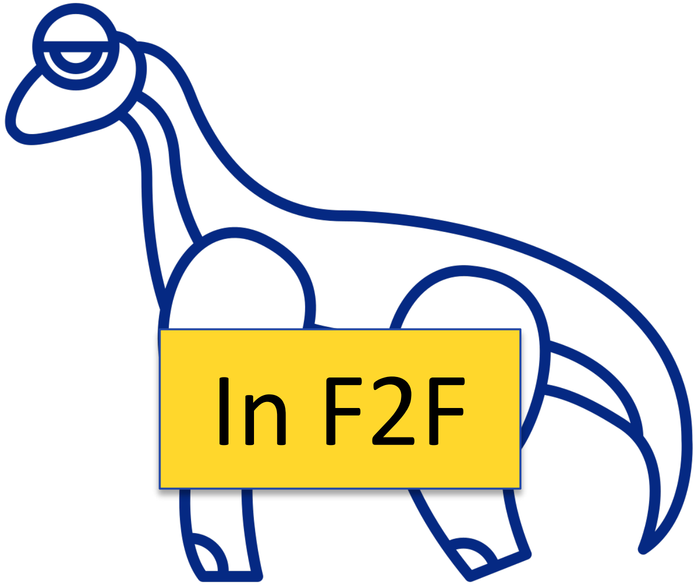
In F2F

What is PCI DSS 4.0?

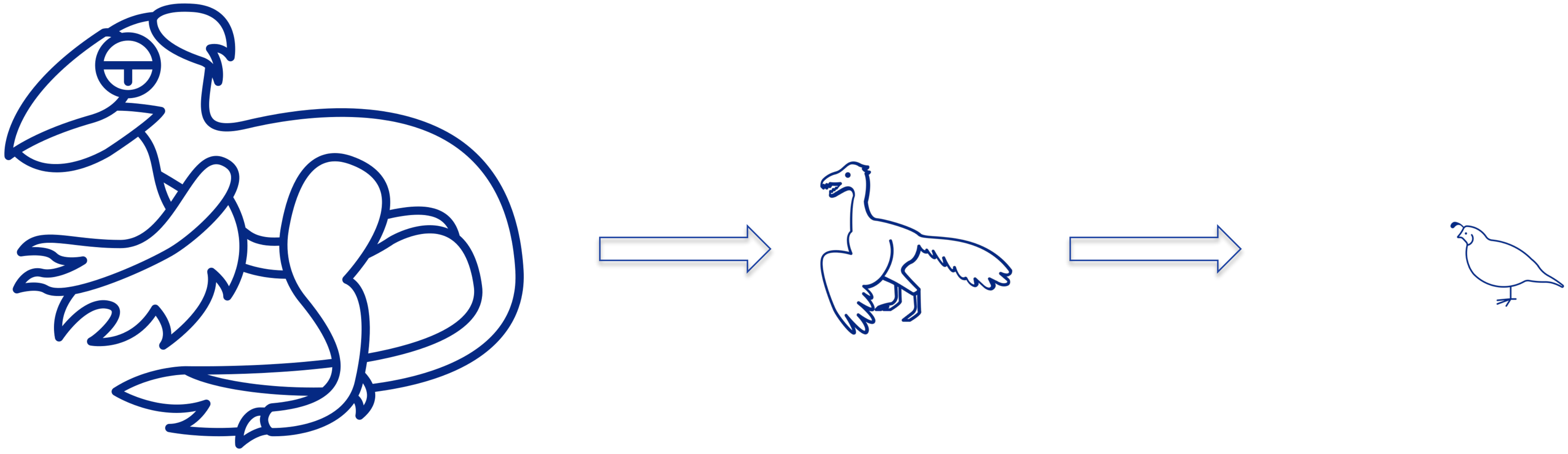


Revolution

YES



Evolution



Deinonychus

Archaeopteryx

Birds

What Now

This month

- Download the Summary of Changes
- Download the Standard
- Talk with your assessor
- Register for the PCI SSC Global Symposium
  - June 21, 2022
  - Participating organizations

What Now

Next quarter

- Impact assessment
  - Cryptographic inventories
  - No use of disk or partition encryption
  - Prevent phishing and train users
  - Prevent & detect e-com skimming
  - System and application account management
  - MFA for all
  - Authenticated internal vulnerability scans
- What should you do now for security?
  - E-com skimming
- Can you reduce scope?

What Now

This year

- Talk with senior management
- If you are a merchant, talk to your acquirer or who you report compliance to
- Understand the latest you need to start projects to have the new requirements in place to meet your first assessment after 01 April 2025
- Work out how long you can wait (F2F)
- How does this fit into your:
  - Budget cycle
  - Project/program cycle