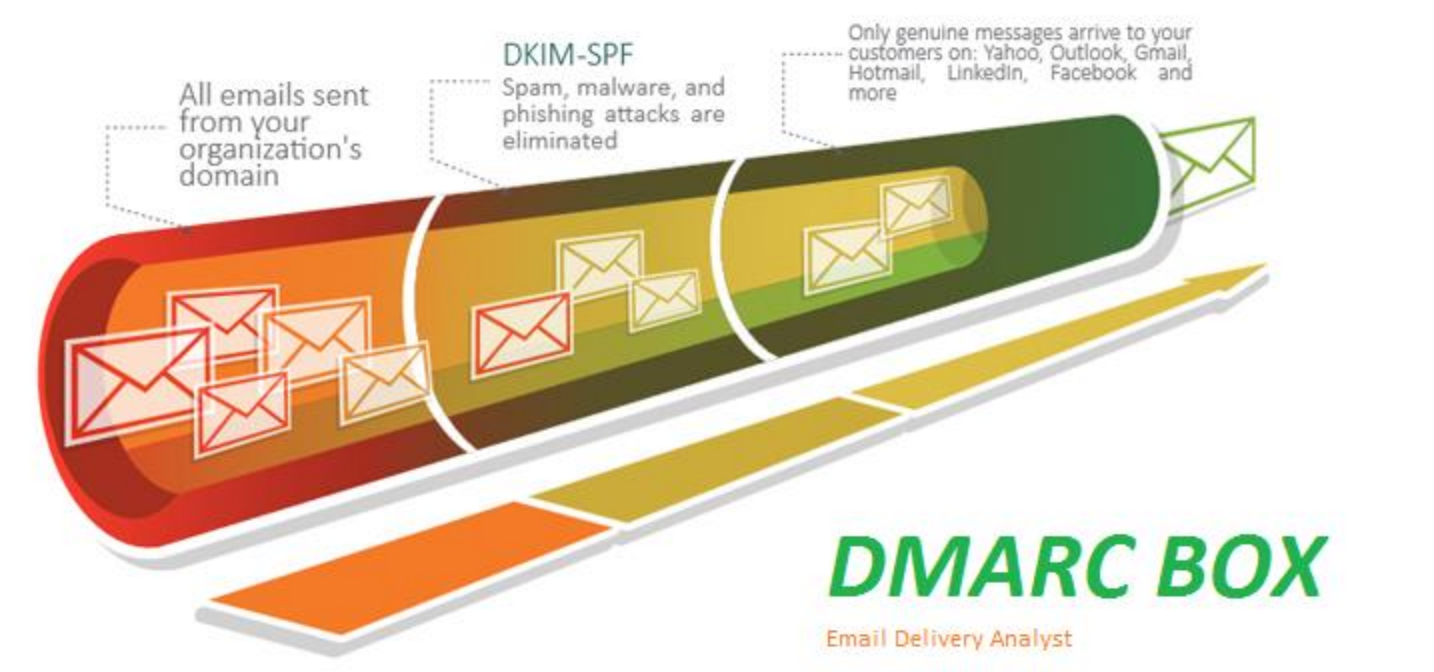
DMARC BOX Journey


All emails sent from your organization's domain
DKIM-SPF
Spam, malware, and phishing attacks are eliminated
Only genuine messages arrive to your customers on: Yahoo, Outlook, Gmail, Hotmail, LinkedIn, Facebook and more
DMARC BOX
Email Delivery Analyst

Date : 14 Feb 2018
Owner :SSIS India

Why DMARC?

Phishin

Financial Loss

Reputation loss?

DMARC is effective to Combat

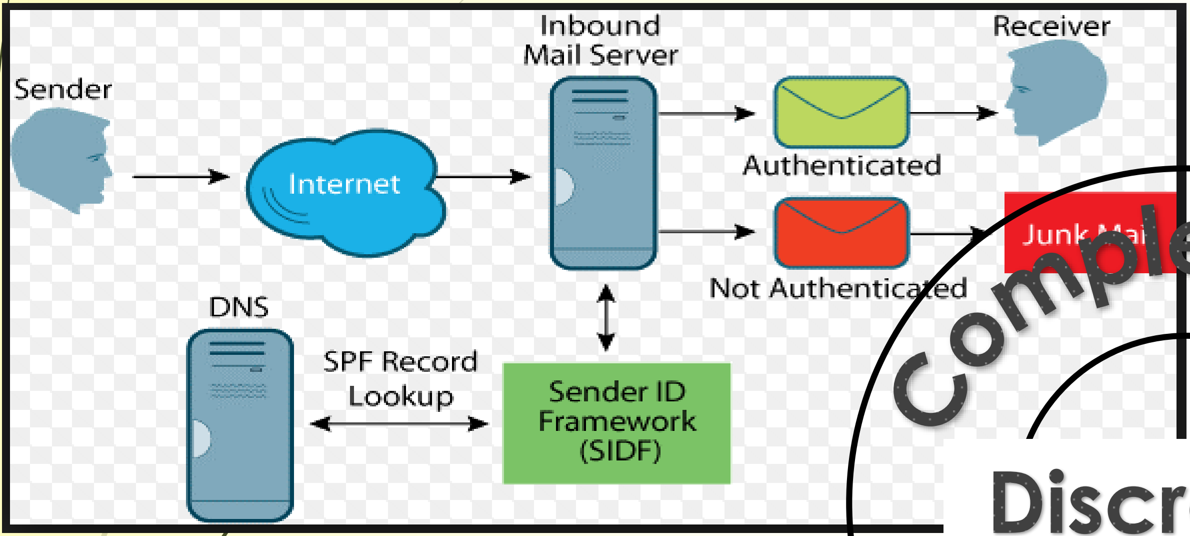
How Email Scam Starts?

Makes it simple for intruder

Anybody can Spoof your email domain name to phish target

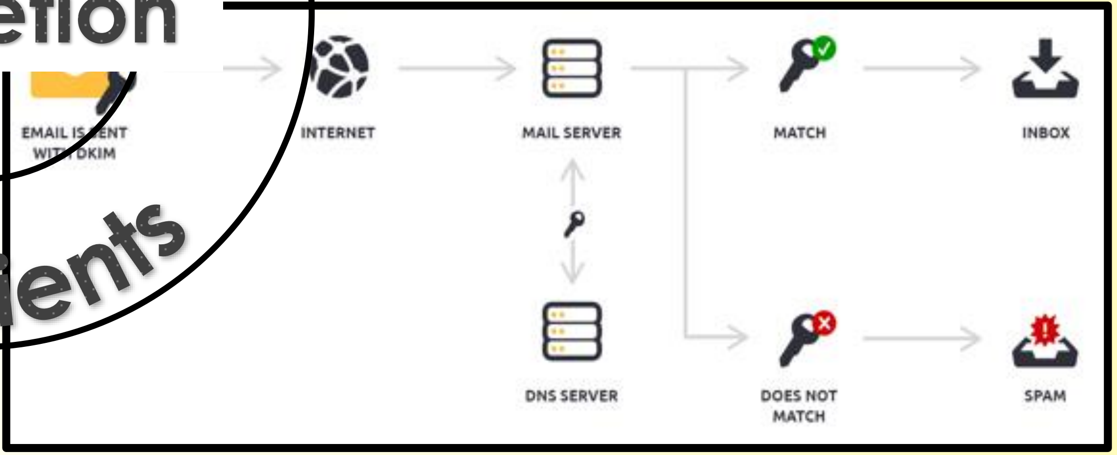
Why legacy Spoofing Controls are not sufficient?

Control 1: SPF



Completely At Discretion Recipients

Control 2: DKIM

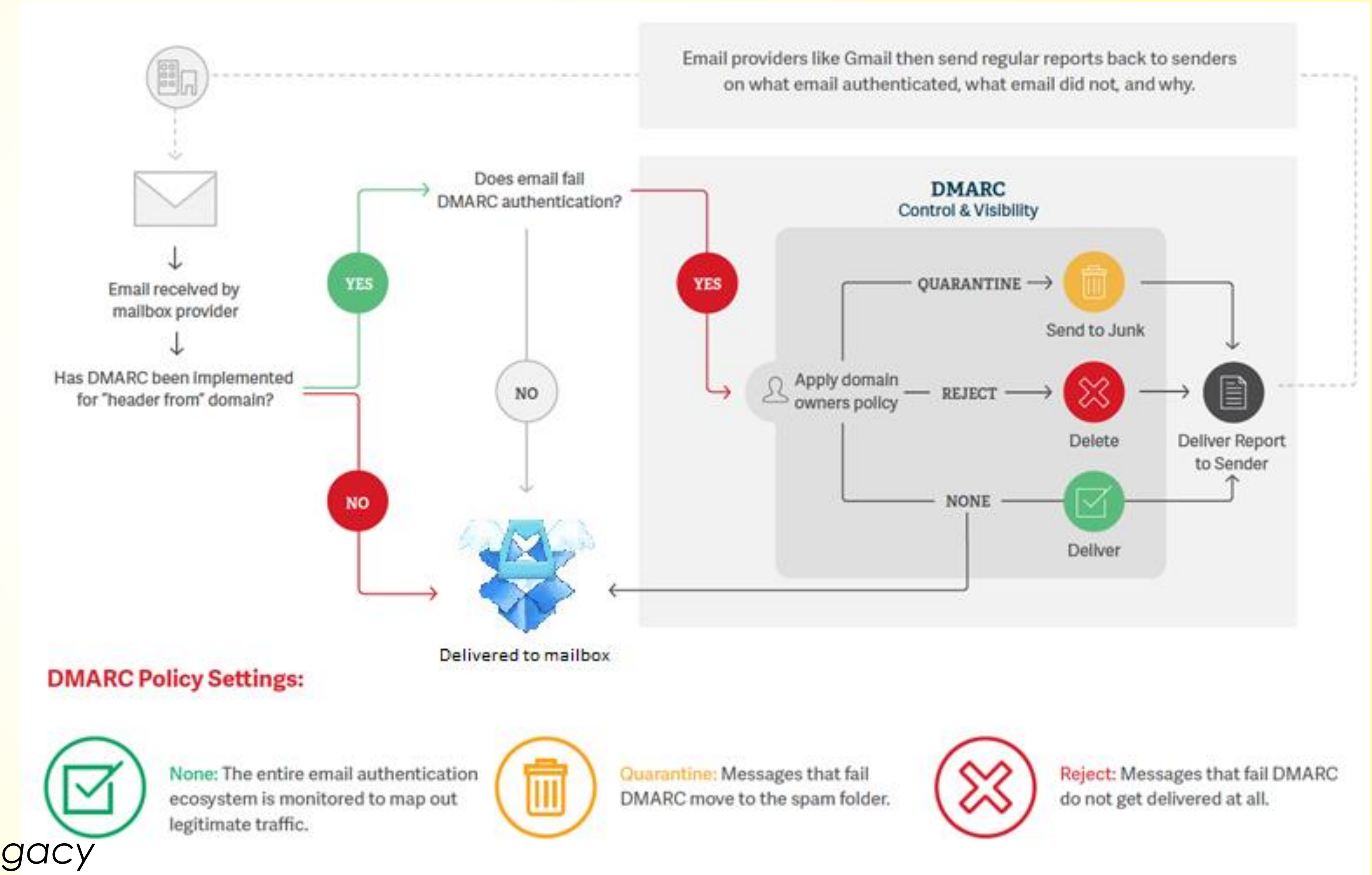


Both of these configurations were Completely controlled at Recipient's Email Gateway. Recipient can choose to ignore both records published by sender & allow email to land in recipients inbox

How DMARC is a effective Solution?

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email-validation system designed to detect and prevent email spoofing. It is intended to combat certain techniques often used in phishing and email spam, such as emails with forged sender addresses that appear to originate from legitimate organizations.

DMARC counters the illegitimate usage of the exact domain name in the From: field of email message headers.


Email providers like Gmail then send regular reports back to senders on what email authenticated, what email did not, and why.
Email received by mailbox provider
Has DMARC been implemented for "header from" domain?
YES
NO
Does email fail DMARC authentication?
YES
NO
Delivered to mailbox
DMARC
Control & Visibility
Apply domain owners policy
QUARANTINE
Send to Junk
REJECT
Delete
NONE
Deliver
Deliver Report to Sender
DMARC Policy Settings:

None: The entire email authentication ecosystem is monitored to map out legitimate traffic.

Quarantine: Messages that fail DMARC move to the spam folder.

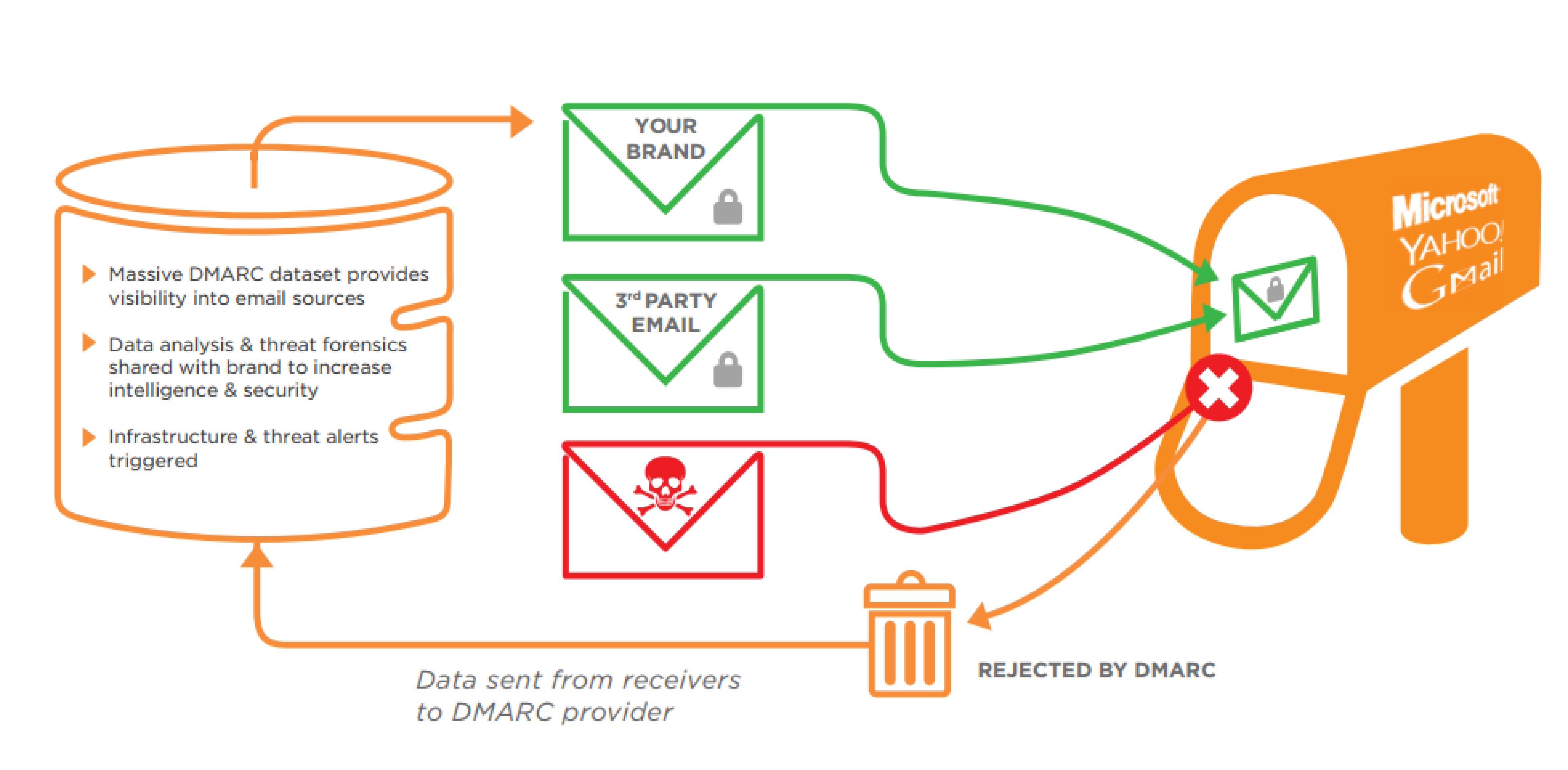
Reject: Messages that fail DMARC do not get delivered at all.

Major Points:

Which make this different then Legacy

- ***RUA & RUF reports Back to sender***
- ***Policy Control with Sender***

Report Classification

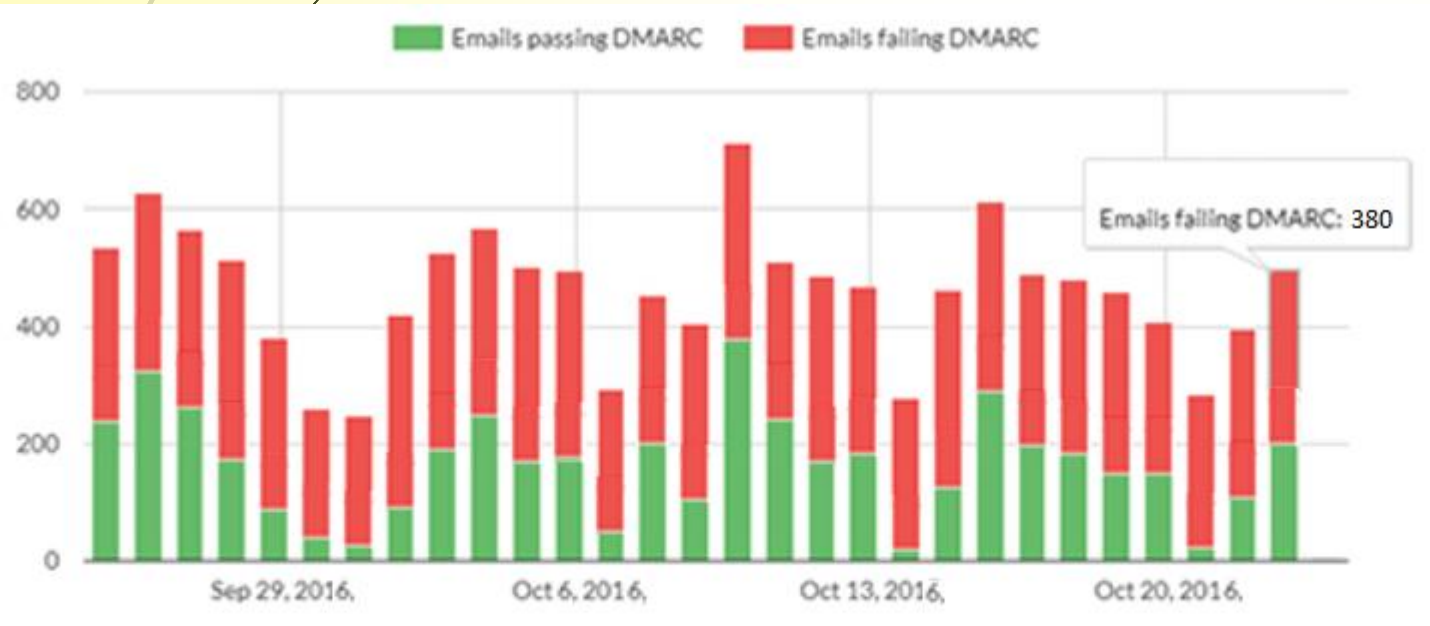


- Massive DMARC dataset provides visibility into email sources
- Data analysis & threat forensics shared with brand to increase intelligence & security
- Infrastructure & threat alerts triggered

Data sent from receivers to DMARC provider

Reports Analysis

Step 1- Set DMARC in Monitoring Mode



Actions:

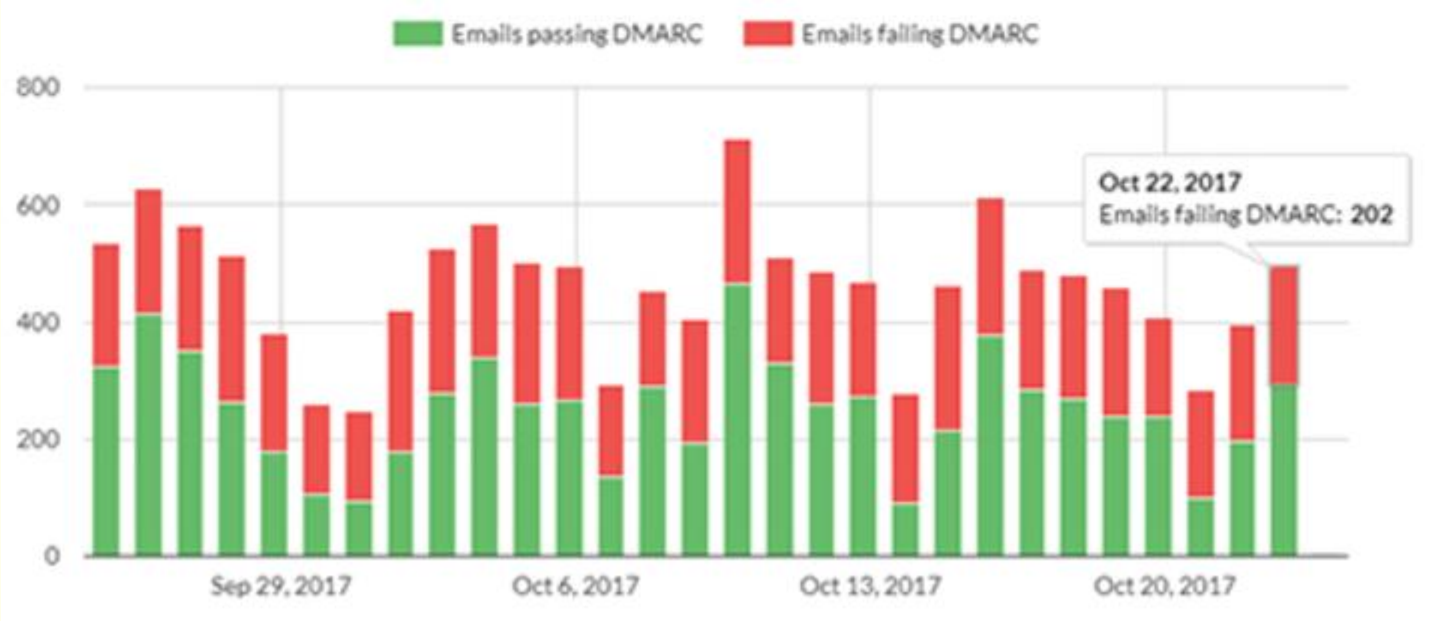
1) Set SPF, DKIM for Known Email outbound
2) Set DMARC
3) Setup DMARC report Analyzer
4) Monitor Reports of unknown IPs/ Providers
5) Collect information from Business teams
6) List out Known Marketing complainers
7) Add legitimate Ips in records

Reports Analysis

Step 2- Set DMARC in Quarantine Mode

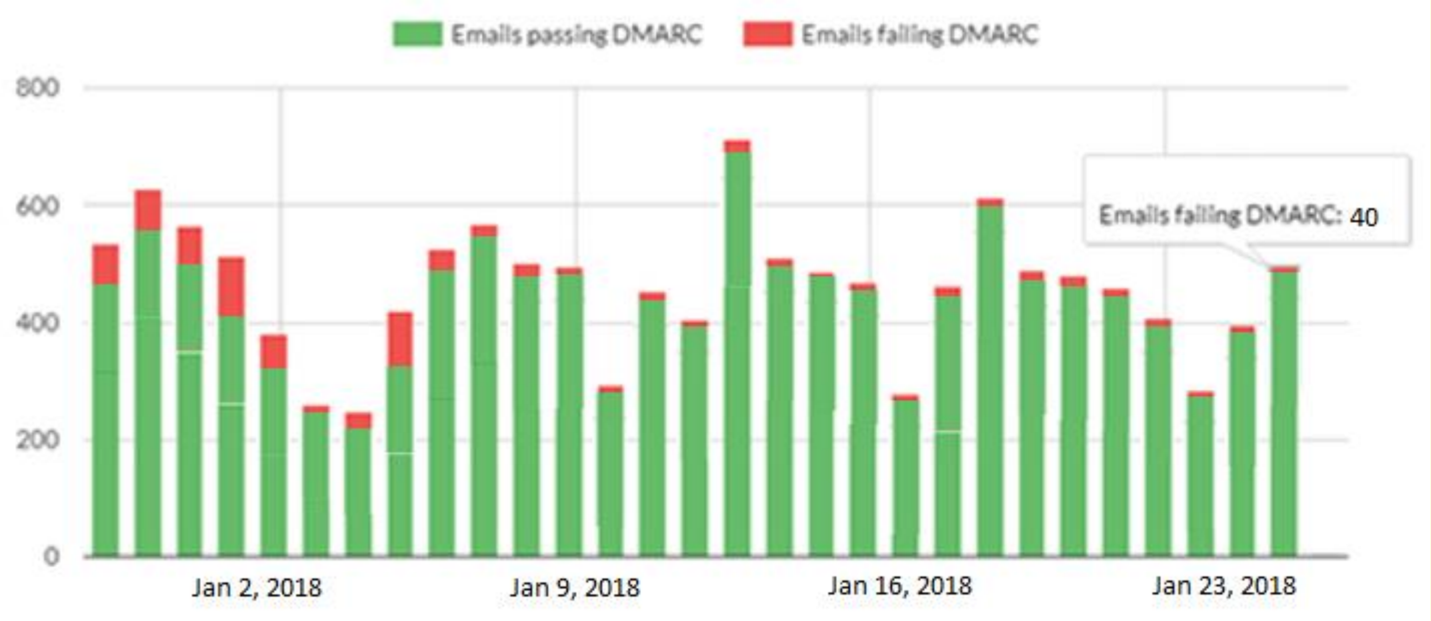
Actions:

1) Set DMARC to Quarantine
2) Finetune SPF, DKIM for legitimate outbound
3) Monitor Reports of unknown IPs/ Providers
4) Collect information from partners teams
5) Add legitimate Ips in records



Reports Analysis

Step 3- Set DMARC in Reject Mode

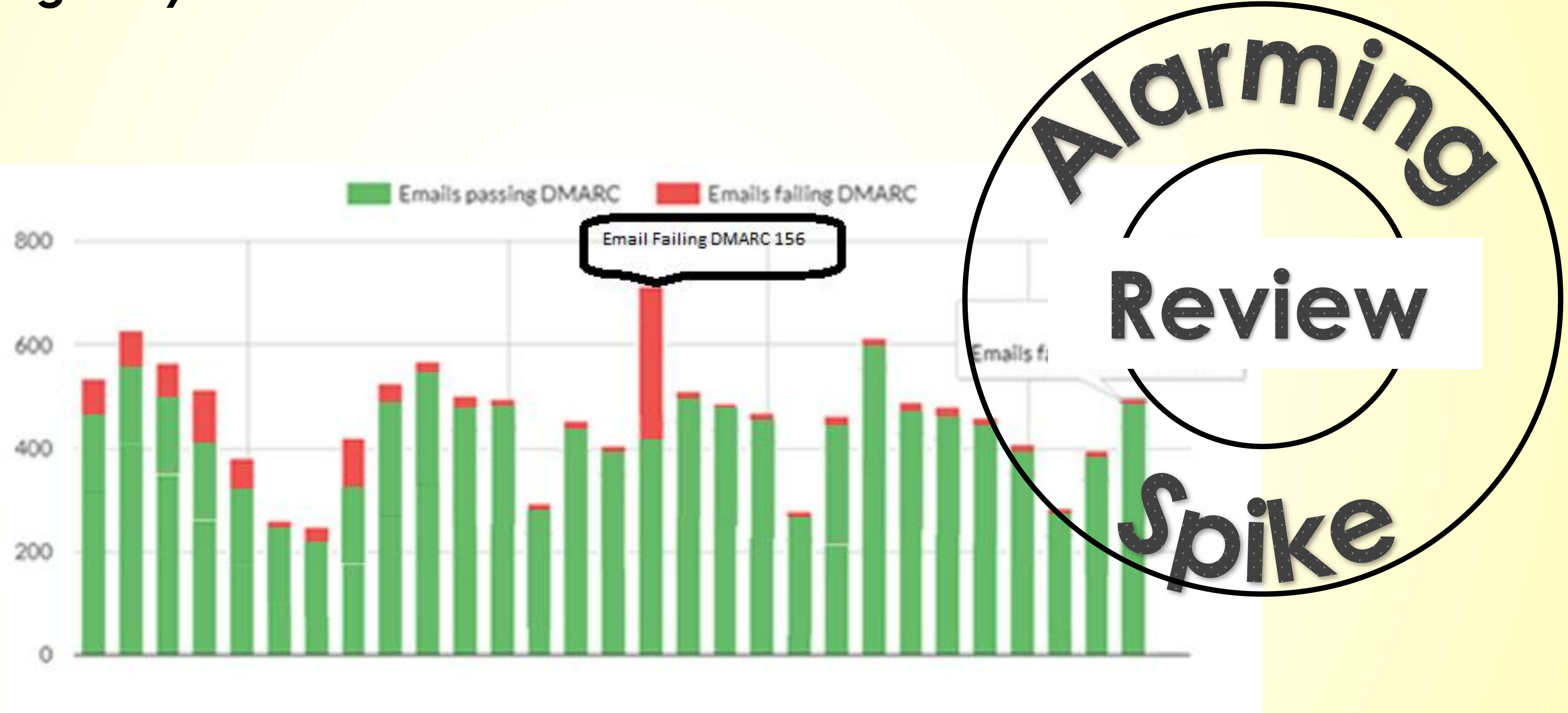


Actions:

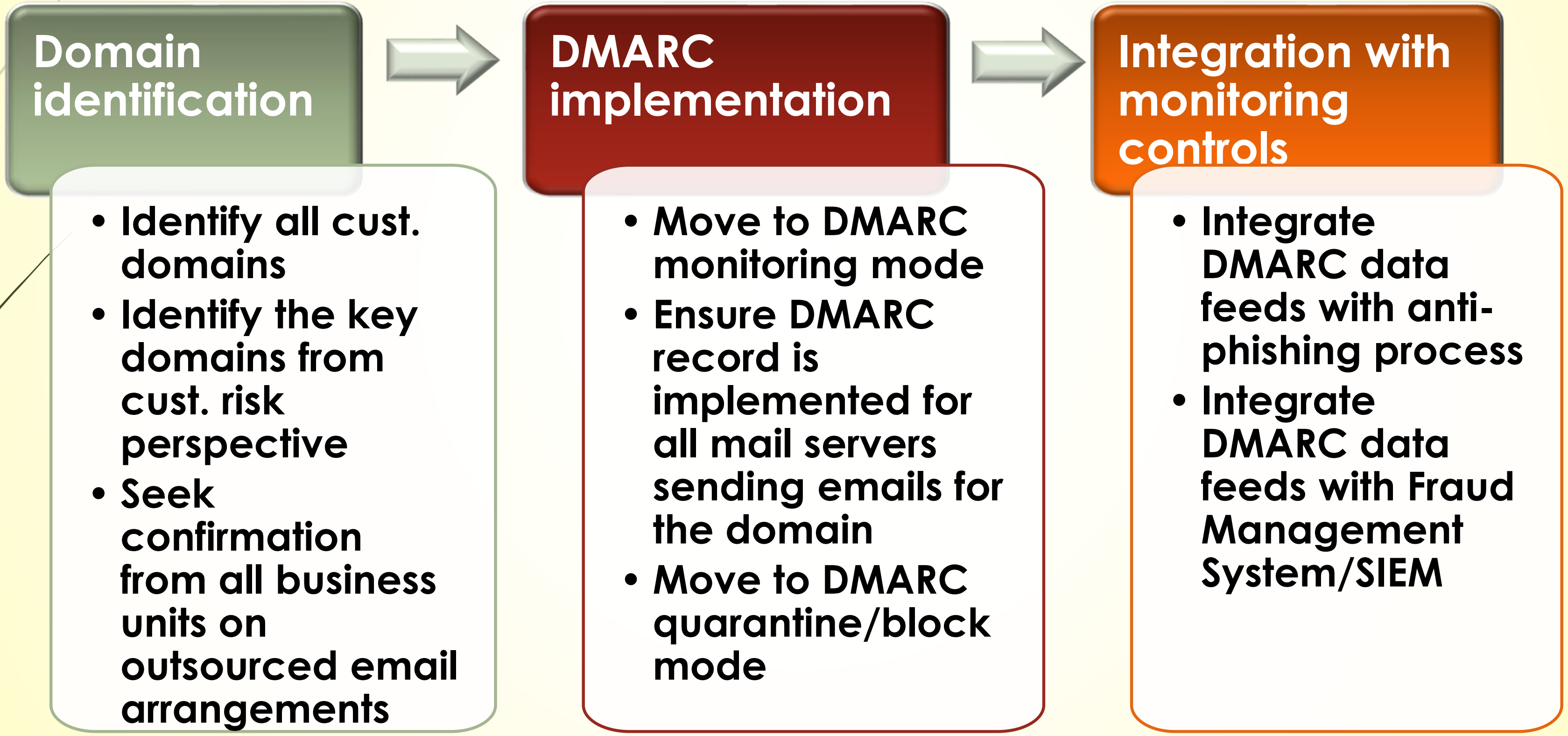
1) Set DMARC to Reject
2) Finetune SPF, DKIM for legitimate outbound
3) Monitor Reports of unknown IPs/ Providers
4) Collect information from partners teams
5) Add legitimate Ips in records

Reports Analysis

Step 4- Review Regularly



Implementation Approach



Domain identification

- Identify all cust. domains
- Identify the key domains from cust. risk perspective
- Seek confirmation from all business units on outsourced email arrangements

DMARC implementation

- Move to DMARC monitoring mode
- Ensure DMARC record is implemented for all mail servers sending emails for the domain
- Move to DMARC quarantine/block mode

Integration with monitoring controls

- Integrate DMARC data feeds with anti-phishing process
- Integrate DMARC data feeds with Fraud Management System/SIEM

THANK YOU