



proofpoint[®]

+

 **CROWDSTRIKE**

Technical Overview of Threat Intel. Integrations

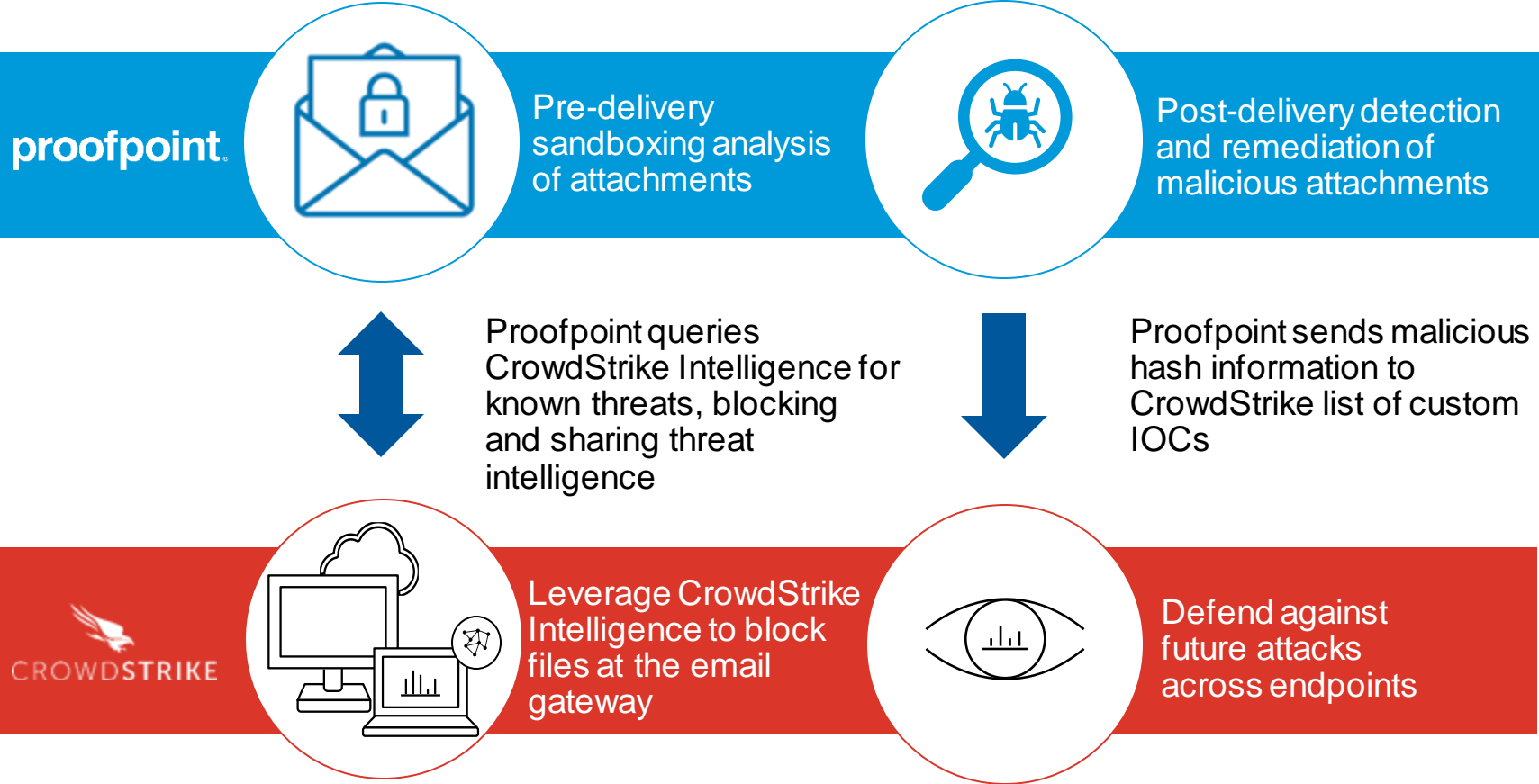
Aug 2021

Proofpoint and CrowdStrike Partnership At-A-Glance

Leveraging best-of-breed threat intelligence for enhanced protection

Integration 1

Integration 2



Solution Benefits

- Proofpoint and CrowdStrike combine their visibility and extensive threat detection capabilities to provide unparalleled protection for the user and their endpoint
- Proofpoint shares intelligence about previously unknown threats to CrowdStrike to generate alerts around future attacks on the endpoints
- Free and seamless implementation

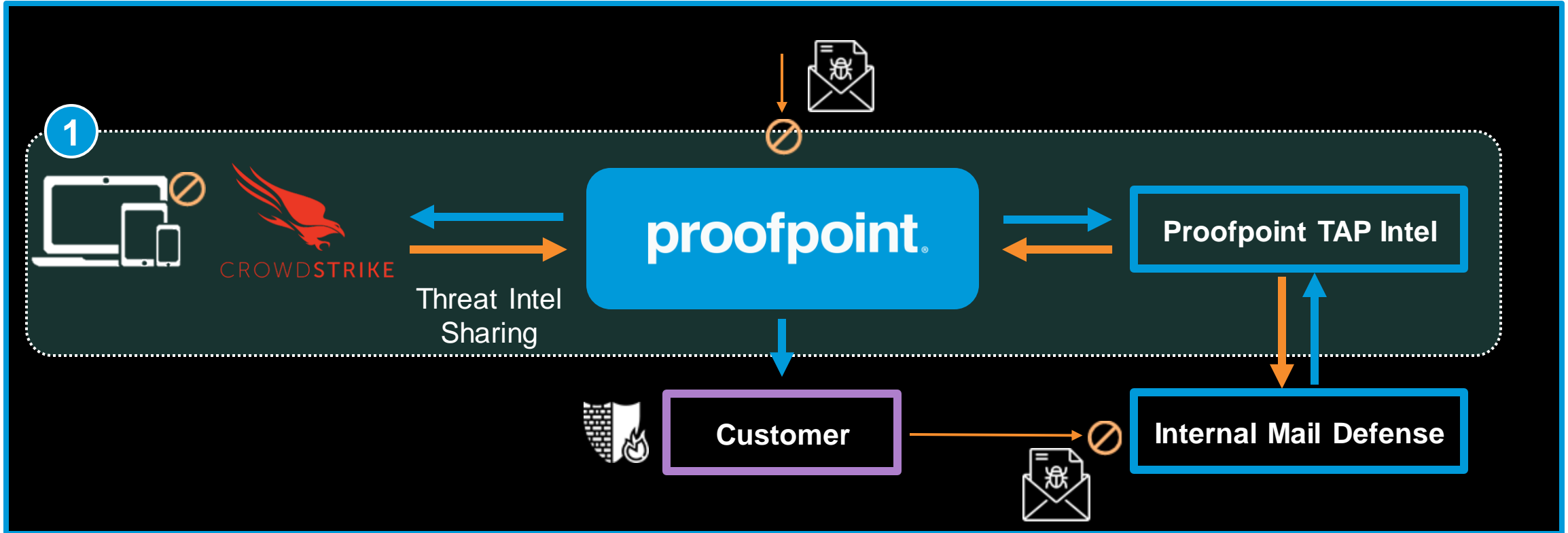
Proofpoint and CrowdStrike: Threat Intelligence Sharing

Pre-Delivery Attachment Defense

Pre-Delivery Attachment Defense: Internal and External Threats

1

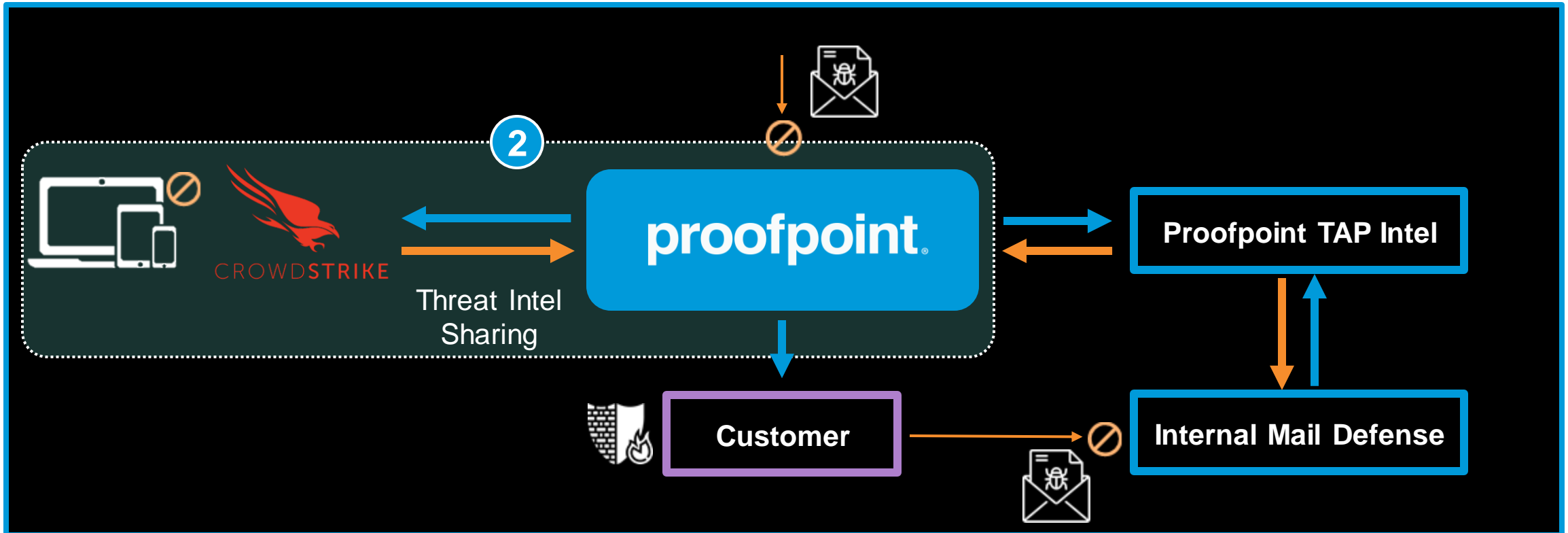
Proofpoint begins sandboxing file and will also query the CrowdStrike Intelligence API for file reputation.



Pre-Delivery Attachment Defense: Internal and External Threats

2

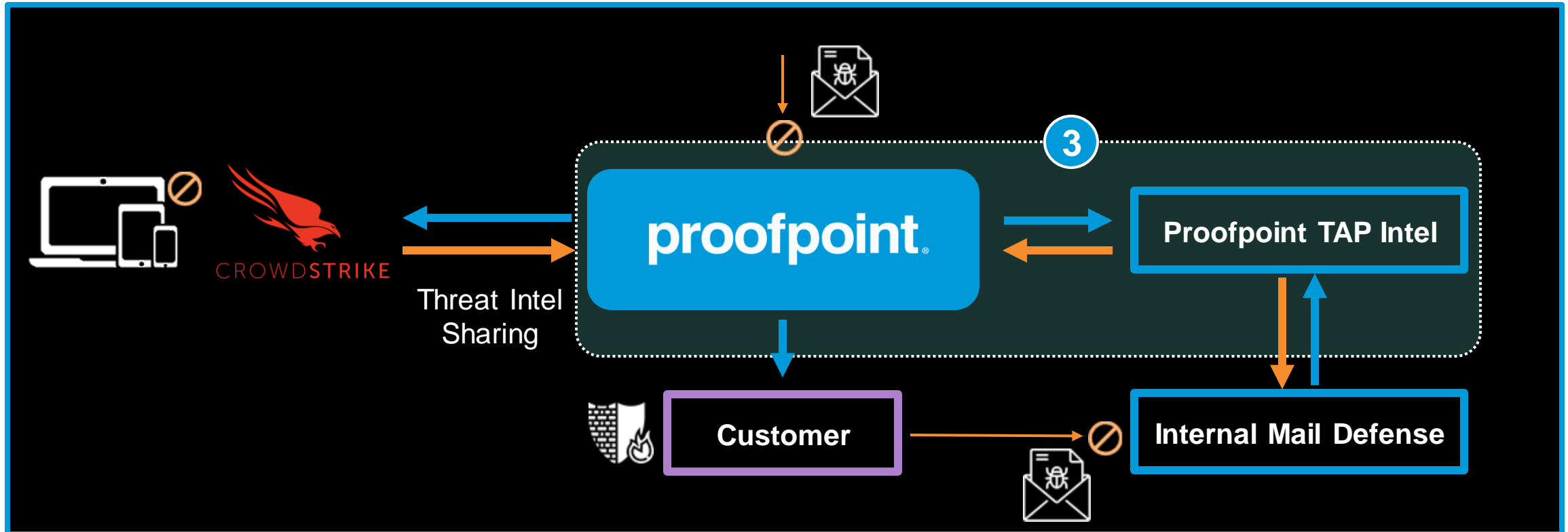
If CrowdStrike knows the file to be malicious, this threat intel will be shared with Proofpoint and file will be blocked within TAP. Never delivered to end-user.



Pre-Delivery Attachment Defense: Internal and External Threats

3

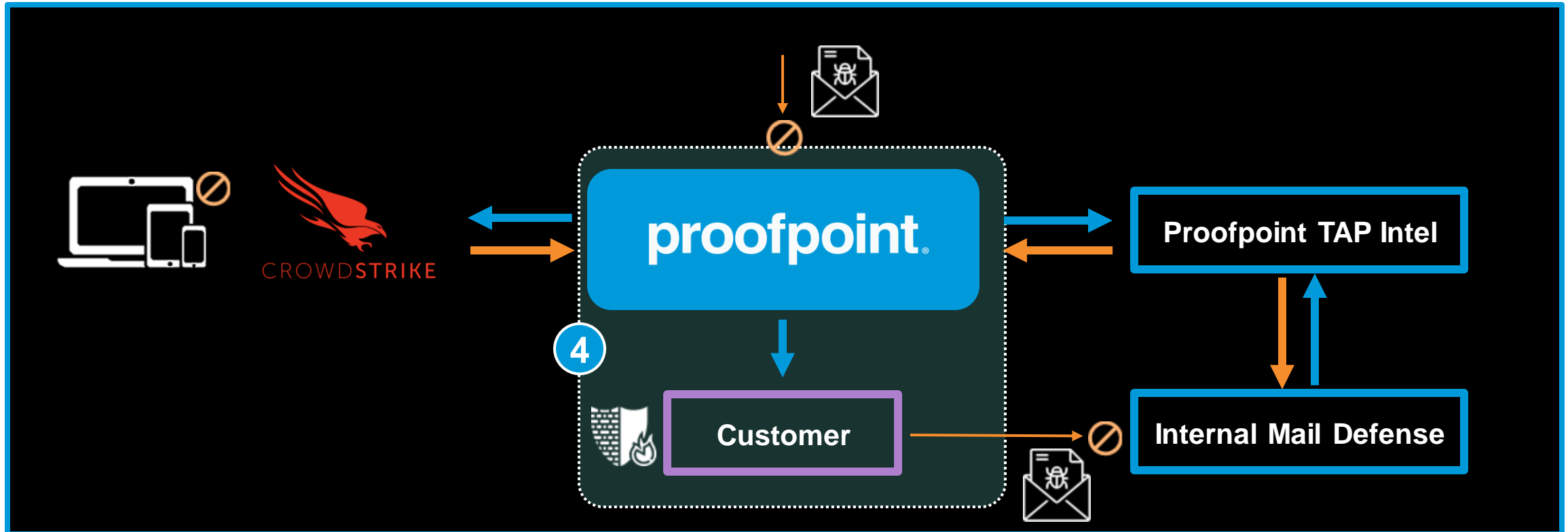
Proofpoint TAP will simultaneously sandbox the file. If file found malicious during investigation, it will be blocked.



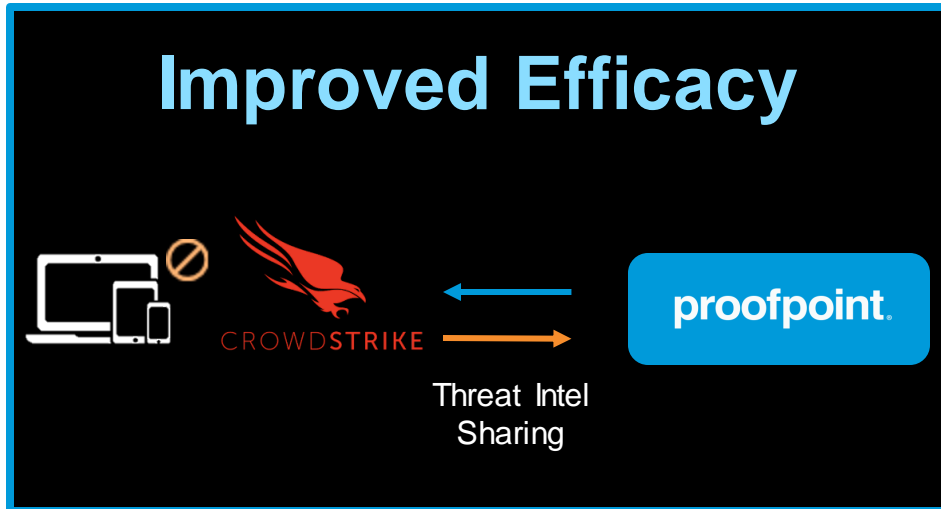
Pre-Delivery Attachment Defense: Internal and External Threats

4

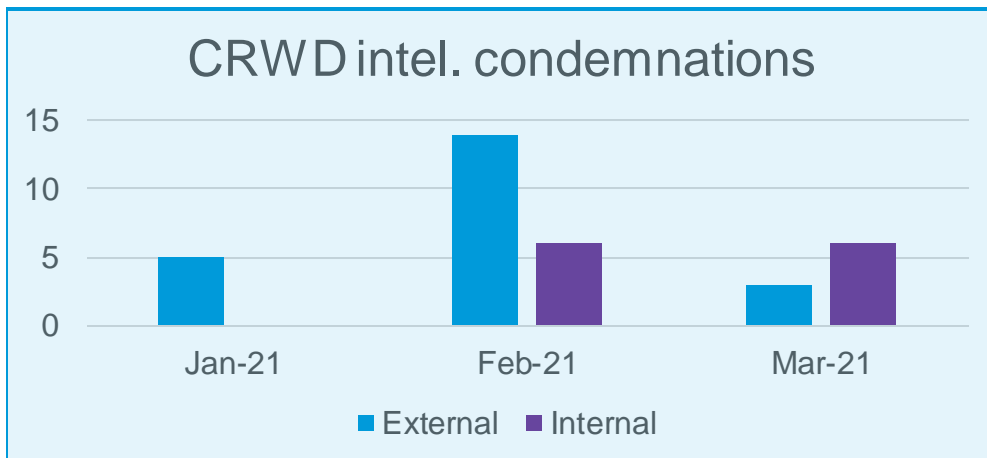
Improved protection for customer through threat intelligence sharing



Proofpoint + CrowdStrike: Pre-Delivery Attachment Defense



Example: BioTech. customer (4500+ FTEs)



Forensics on TAP Dashboard

Forensics

Forensic Report Report #3: 2020/08/03 - 07:46 (UTC +00:00) || CrowdStrike

Overview

Subject 2c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79
 Environment CrowdStrike
 Scan Time 2020/08/03 - 07:46 (UTC +00:00)

Summary of Findings

- A malicious attachment was detected
- A malicious behavior was observed

Malicious Evidence

Attachment

Malware of type: [FormBook]; Kill Chain(s): []

SHA-256	SHA-256
2c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79	2c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79

Behaviors

- A malicious behavior was observed
- A malicious behavior was observed
- A malicious behavior was observed
- A malicious behavior was observed
- A malicious behavior was observed

SHA-256	SHA-256
2c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79	2c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79
2c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79	2c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79
2c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79	2c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79
2c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79	2c2027c74d70fdfea03c69dd403a4ab7e3fa4202ef728e4d0e2c232bff15ea79

Expanded Insight

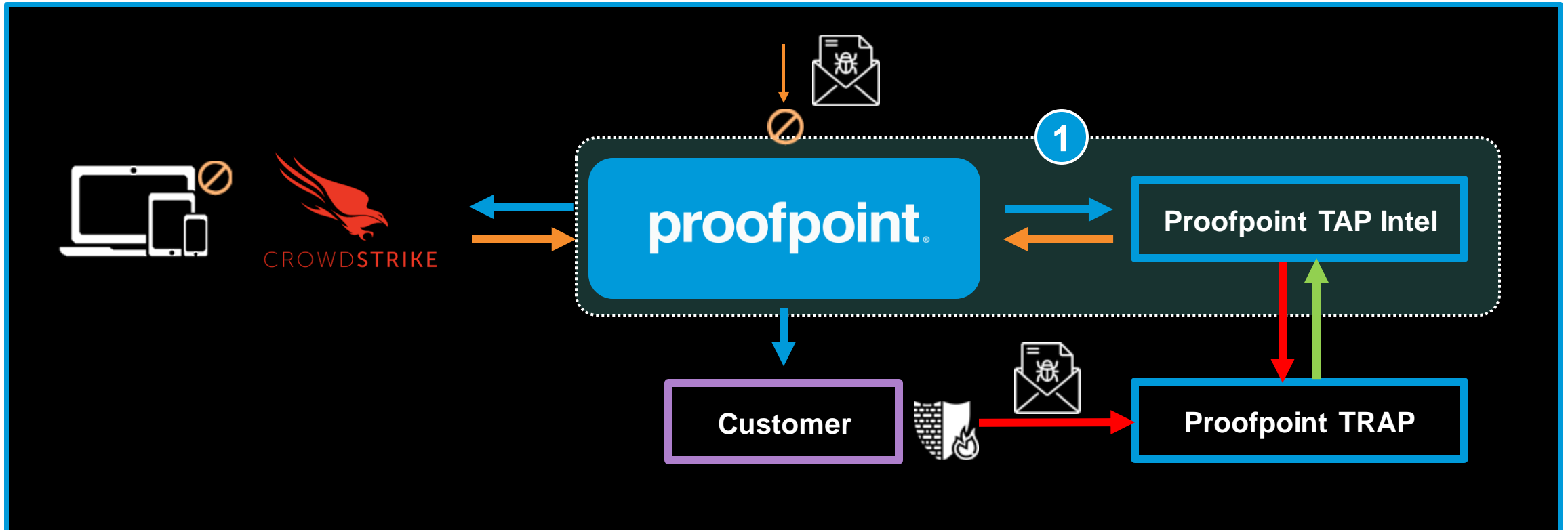
Proofpoint and CrowdStrike: Multi-layered Protection

Post Delivery Attachment Defense

Post Delivery Detection and Protection

1

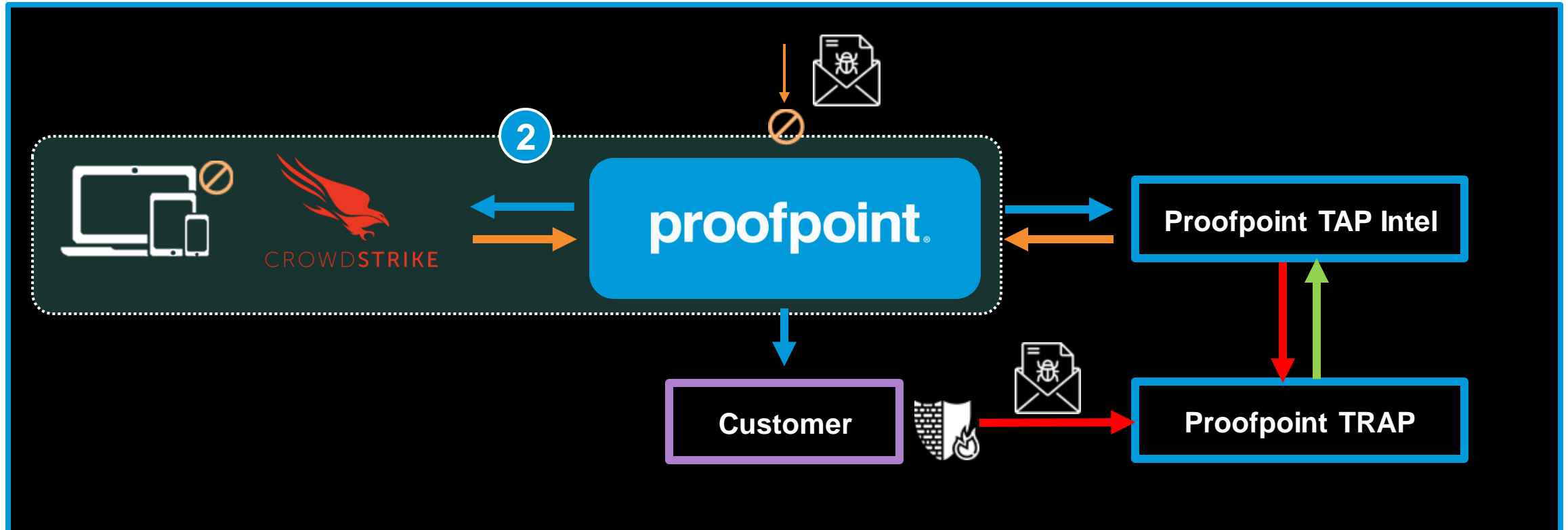
Proofpoint TAP detects a malicious file has been delivered, TRAP enables automated remediation for the user mailboxes



Post Delivery Detection and Protection

2

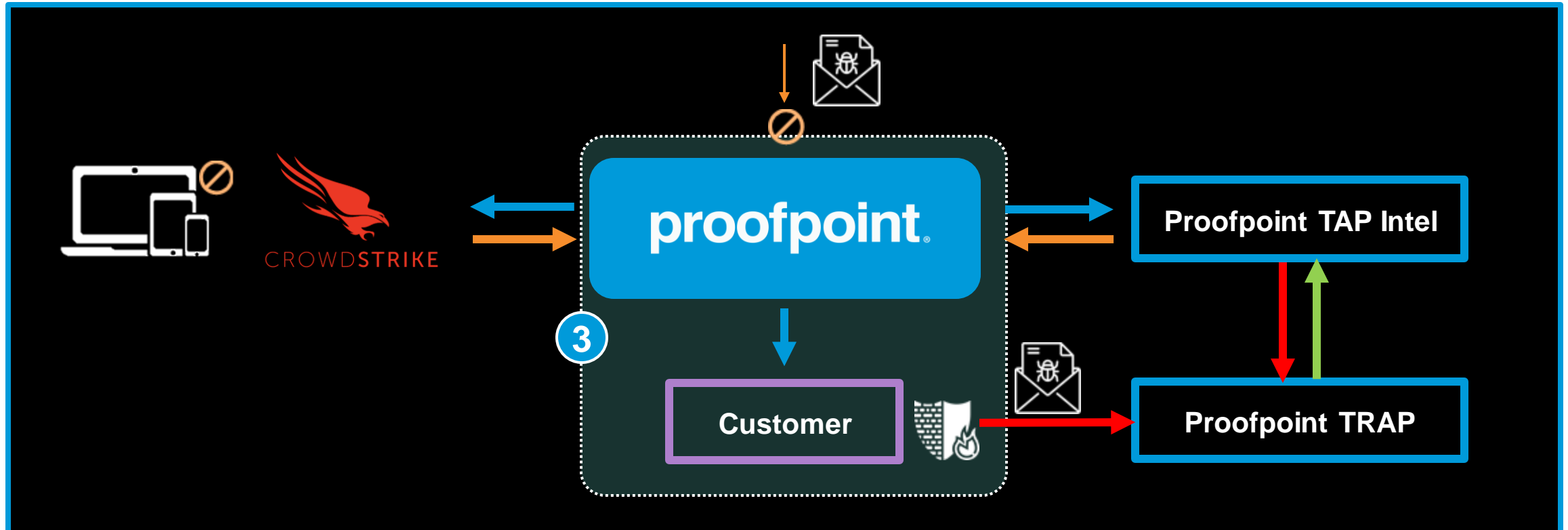
If unknown to CrowdStrike, file hash gets added to CrowdStrike Custom Indicator



Post Delivery Detection and Protection

3

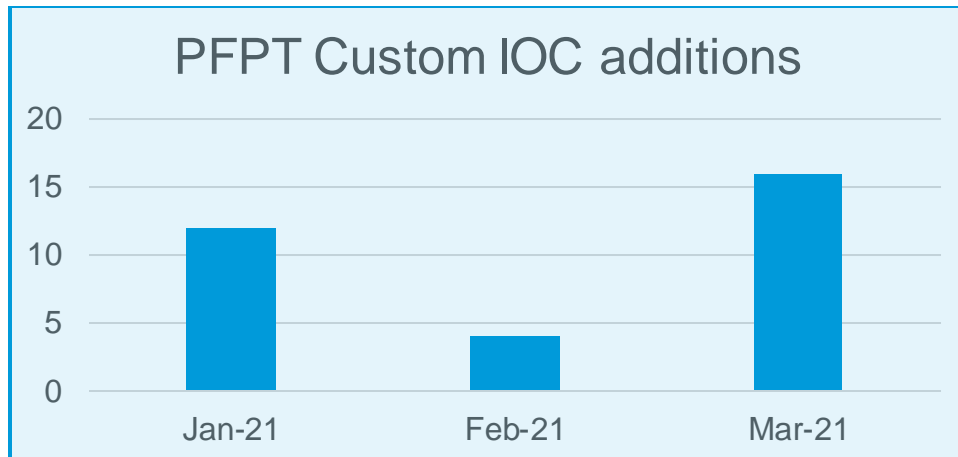
Improved protection for customer through intelligence sharing



Proofpoint + CrowdStrike: Post Delivery Detection and Protection



Example: BioTech. customer (4500+ FTEs)



CrowdStrike Falcon Platform

The screenshot shows the 'Execution Details' page in the CrowdStrike Falcon Platform. It displays various fields such as Detect Time, Hostname, User Name, Severity, Objective, Tactic & Technique, and Specific to this Detection. A red box highlights the 'INDICATORS OF INTEREST' section, which contains the text 'Associated IOC (SHA256 on Proofpoint)' and a long alphanumeric hash. A red arrow points to this section. At the bottom of the screenshot, there is a blue banner with the text 'Multi-layer Threat Protection'.

DETECT TIME	FIRST BEHAVIOR	MOST RECENT BEHAVIOR
	Mar. 23, 2020 16:11:39	Mar. 23, 2020 16:11:44

HOSTNAME	C7000C4BDE9D4E
USER NAME	AMER\
SEVERITY	● Medium
OBJECTIVE	Falcon Detection Method
TACTIC & TECHNIQUE	Custom Intelligence via Indicator of Compromise
SPECIFIC TO THIS DETECTION	A SHA256 hash matched a Custom Intelligence Indicator (Custom IOC).

INDICATORS OF INTEREST	Associated IOC (SHA256 on Proofpoint) 10b255a2b68a4ee05893179fd91c074ad7c94d40...
------------------------	--

LOCAL PROCESS ID	9296
------------------	------




Activate the threat intelligence integration in seconds

Proofpoint TAP dashboard

CrowdStrike Intelligence
Leverage CrowdStrike Intelligence in addition to Proofpoint's sandbox

[Add API Credentials](#)




the Attachme
s sandbox
box

Add CrowdStrike Intelligence Credentials

CANCEL SAVE

CrowdStrike Intelligence (On)
Leverage CrowdStrike Intelligence in addition to Proofpoint's sandbox

[Replace API Credentials](#) | [Remove API Credentials](#)



CLOUD NATIVE

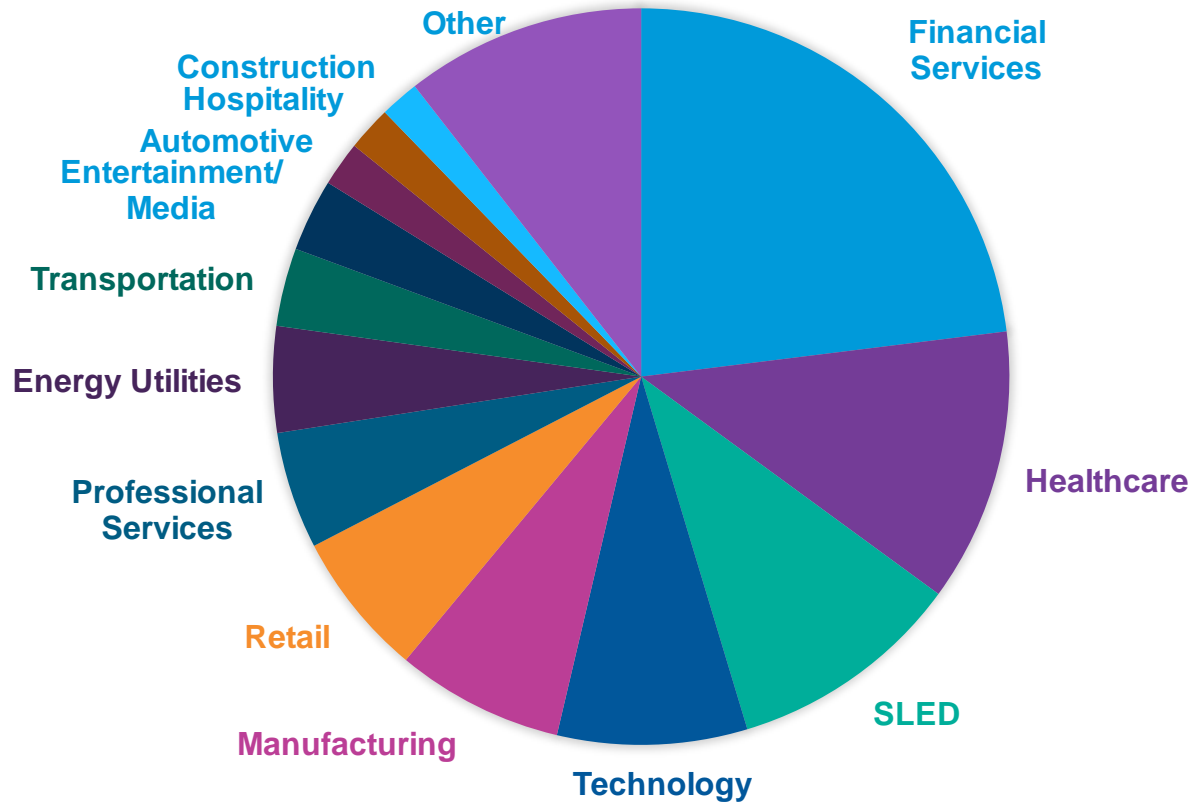
**NO EXTRA COST
AND COMPLEXITY**

**EFFORTLESS
SCALABILITY**

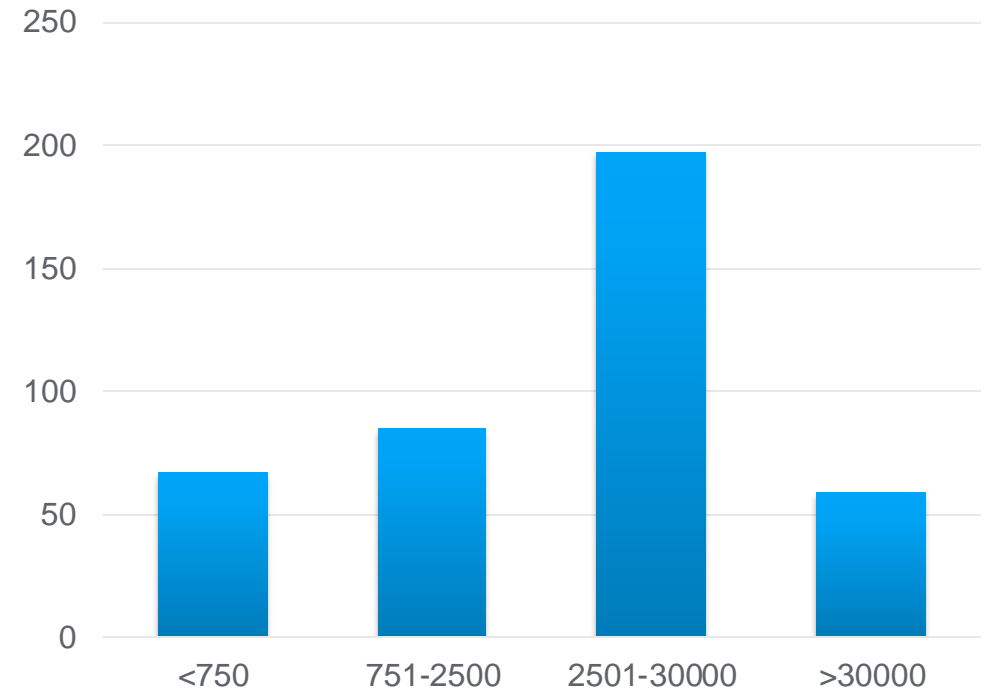
**WORKS ON
DAY ONE**

400+ customers now benefiting from the integration

Breakdown by Industry



Breakdown by Customer Mailboxes



proofpoint[®]

+

CROWDSTRIKE

Q&A

Thank you!

[Learn more](#) about our partnership

Sign up for free people-centric risk assessments

Email
Threats



People Risk



SaaS Apps
Risk



Digital
Brand Risk

