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

proofpoint

Pre-delivery sandboxing analysis of attachments

Post-delivery detection and remediation of malicious attachments

Proofpoint queries CrowdStrike Intelligence for known threats, blocking and sharing threat intelligence

Proofpoint sends malicious hash information to CrowdStrike list of custom IOCs

CROWDSTRIKE

Leverage CrowdStrike Intelligence to block files at the email gateway

Defend against future attacks across endpoints

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

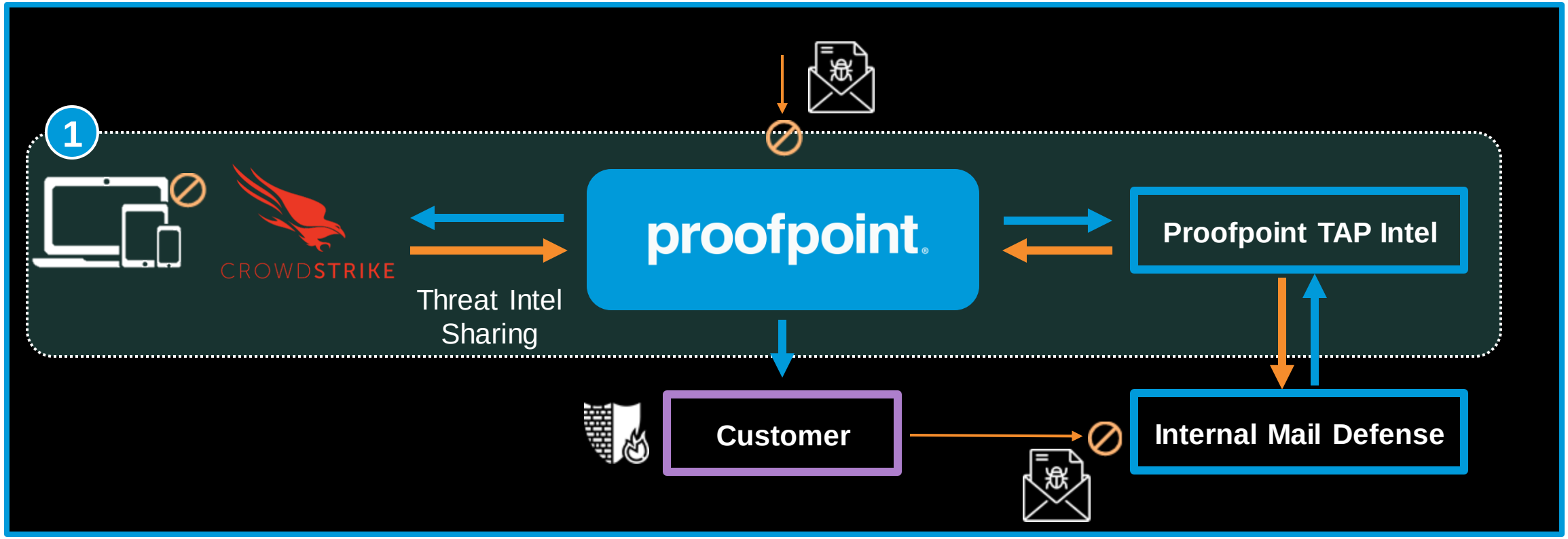
Pre-Delivery Attachment Defense

proofpoint.

Pre-Delivery Attachment Defense: Internal and External Threats

1

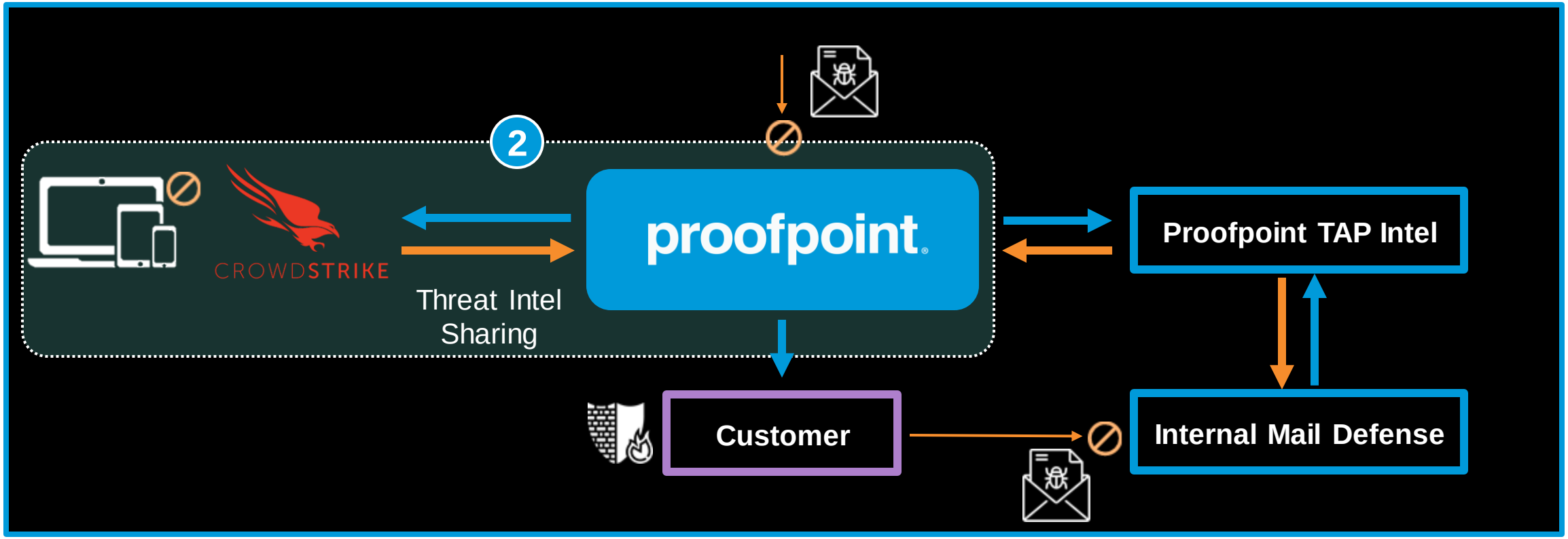
Proofpoint begins sandboxing file and will also query the CrowdStrike Intelligence API for file reputation.



Pre-Delivery Attachment Defense: Internal and External Threats

2

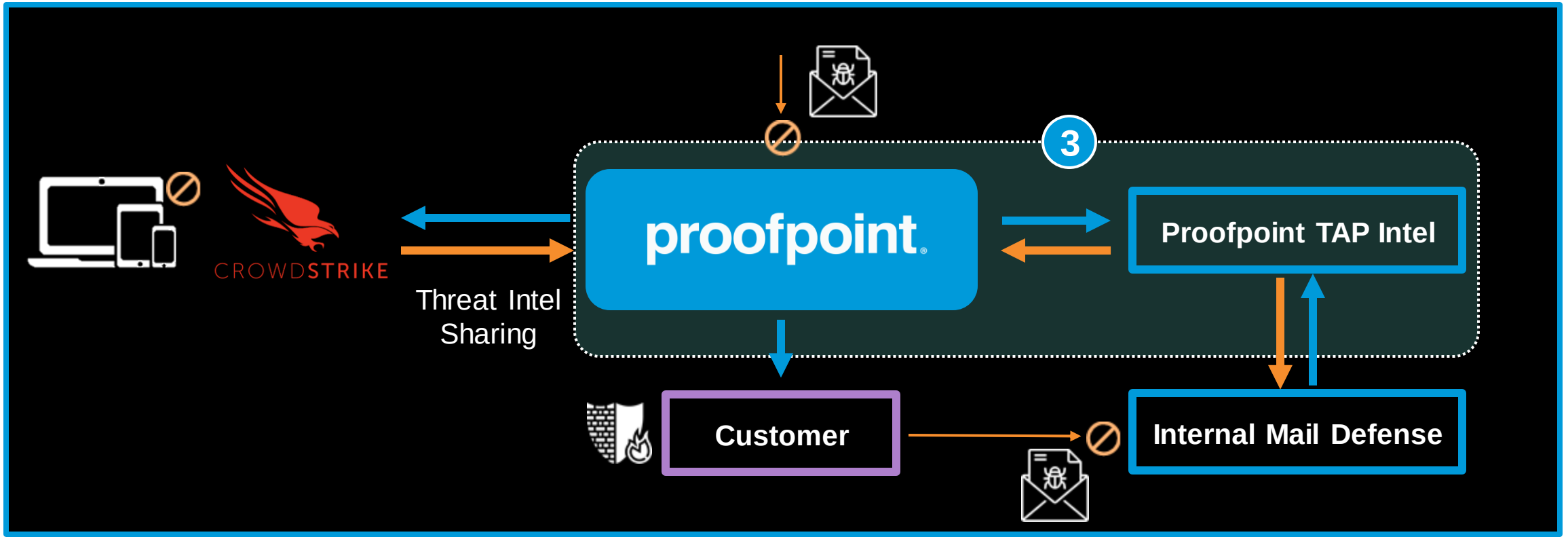
If CrowdStrike knows the file to be malicious, this threat intel will be shared with Proofpoint and file will be blocked within TAP. Never delivered to end-user.



Pre-Delivery Attachment Defense: Internal and External Threats

3

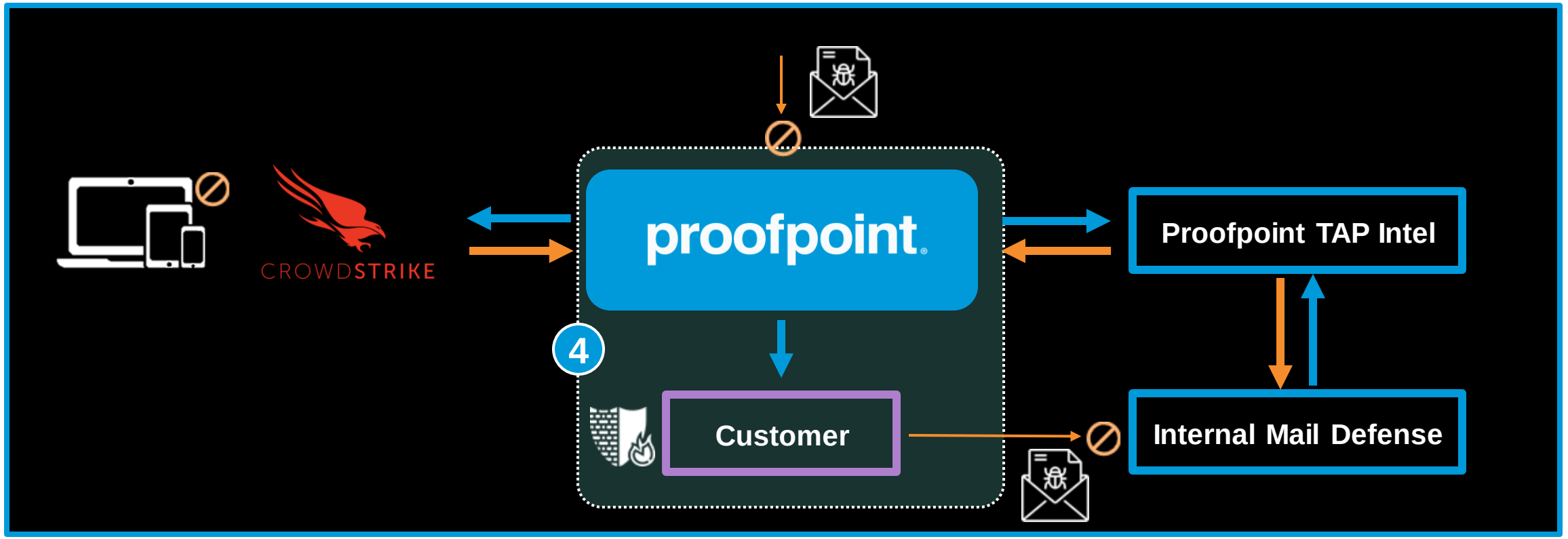
Proofpoint TAP will simultaneously sandbox the file. If file found malicious during investigation, it will be blocked.



Pre-Delivery Attachment Defense: Internal and External Threats

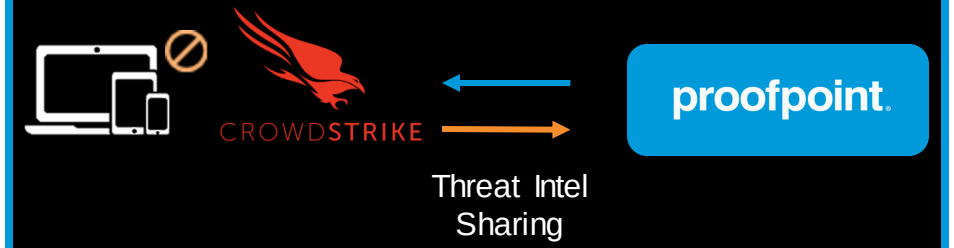
4

Improved protection for customer through threat intelligence sharing

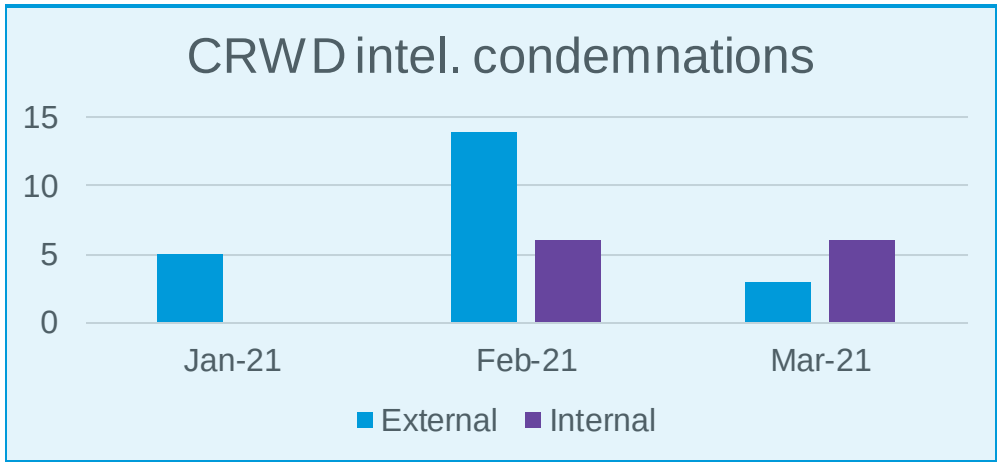


Proofpoint + CrowdStrike: Pre-Delivery Attachment Defense

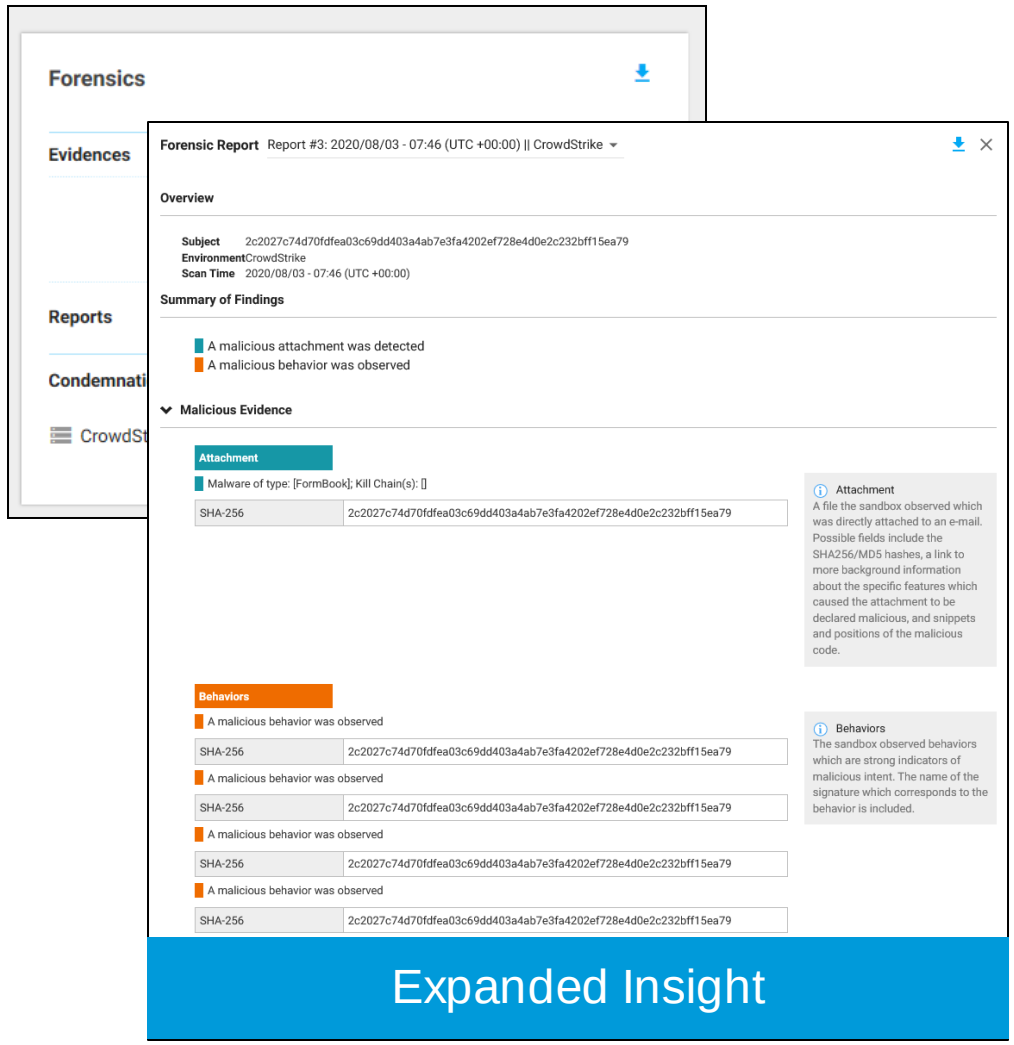
Improved Efficacy



Example: BioTech. customer (4500+ FTEs)



Forensics on TAP Dashboard



proofpoint.

CROWDSTRIKE

Proofpoint and CrowdStrike: Multi-layered Protection

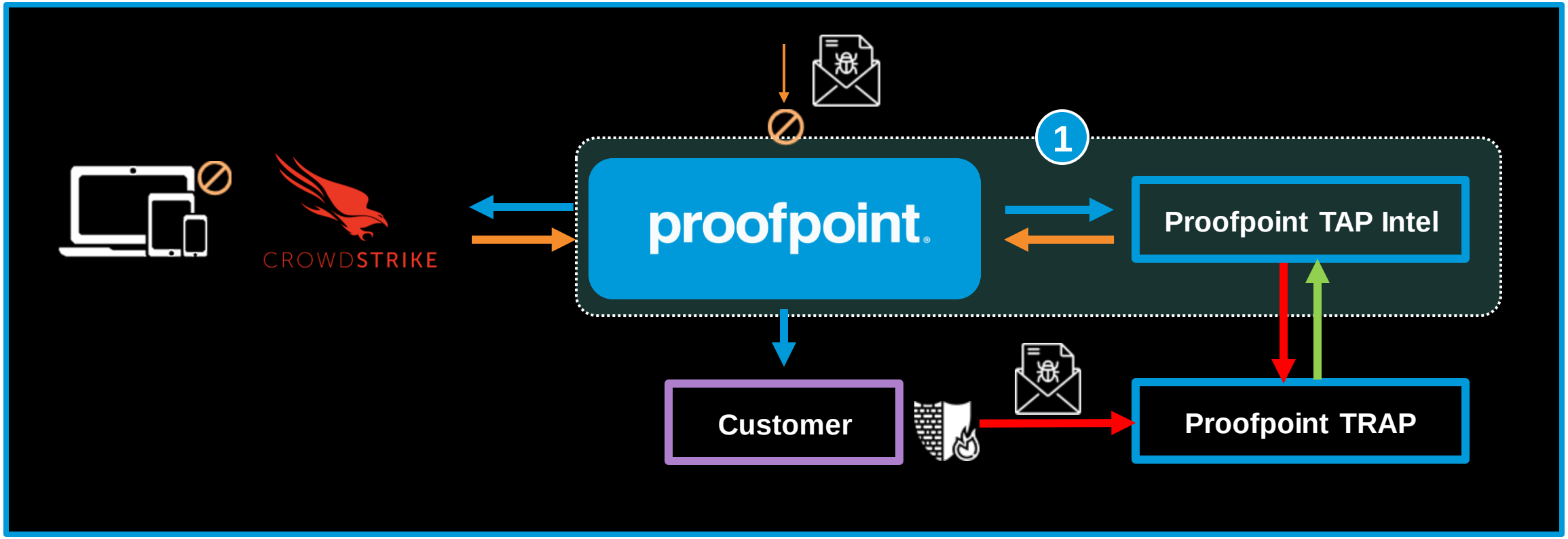
Post Delivery Attachment Defense

proofpoint.

Post Delivery Detection and Protection

1

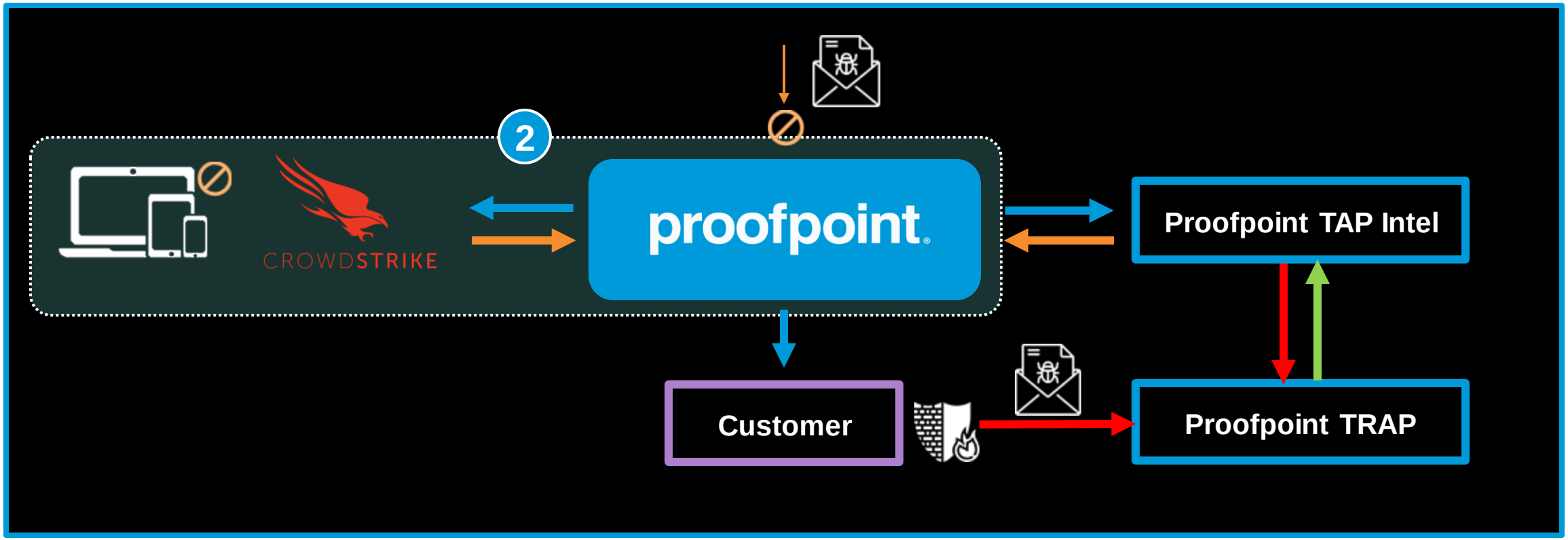
Proofpoint TAP detects a malicious file has been delivered, TRAP enables automated remediation for the user mailboxes



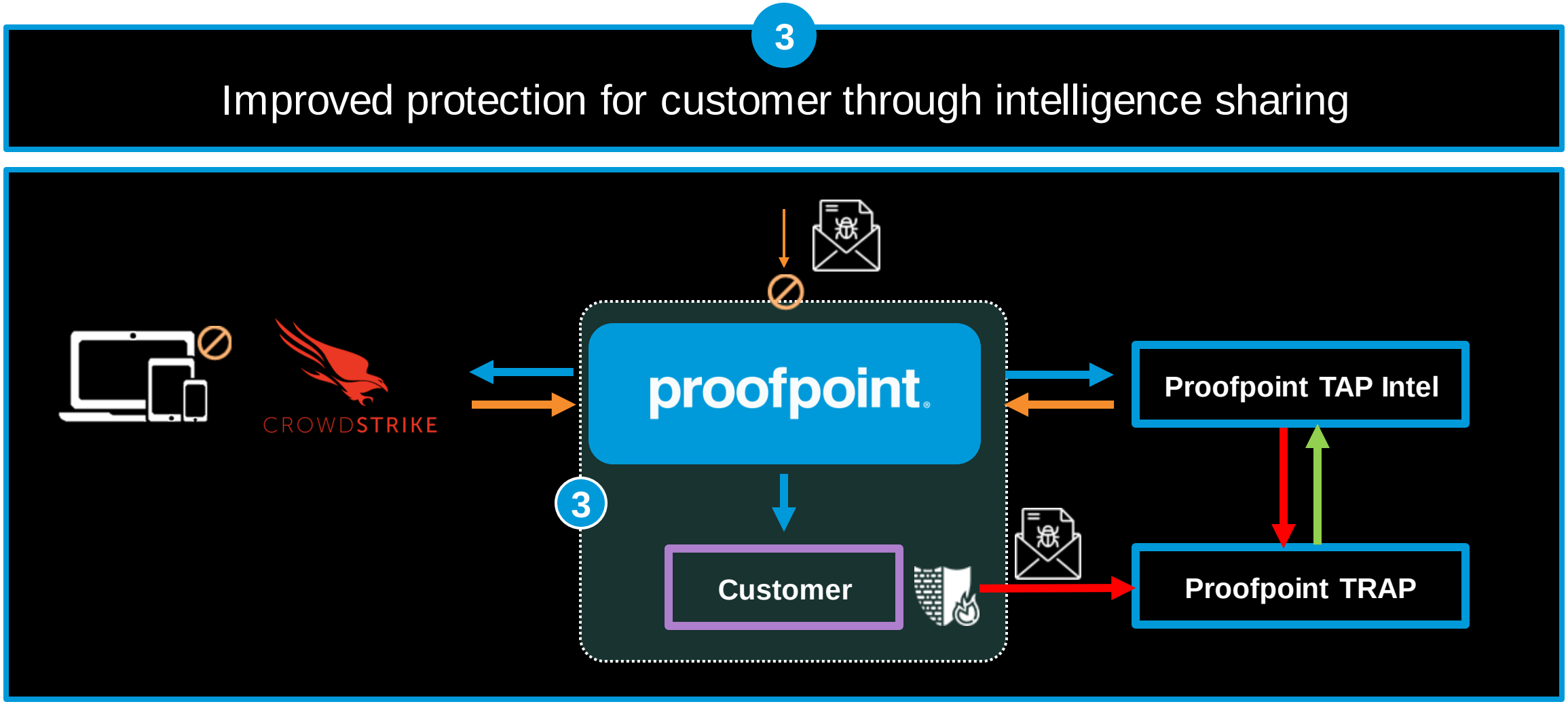
Post Delivery Detection and Protection

2

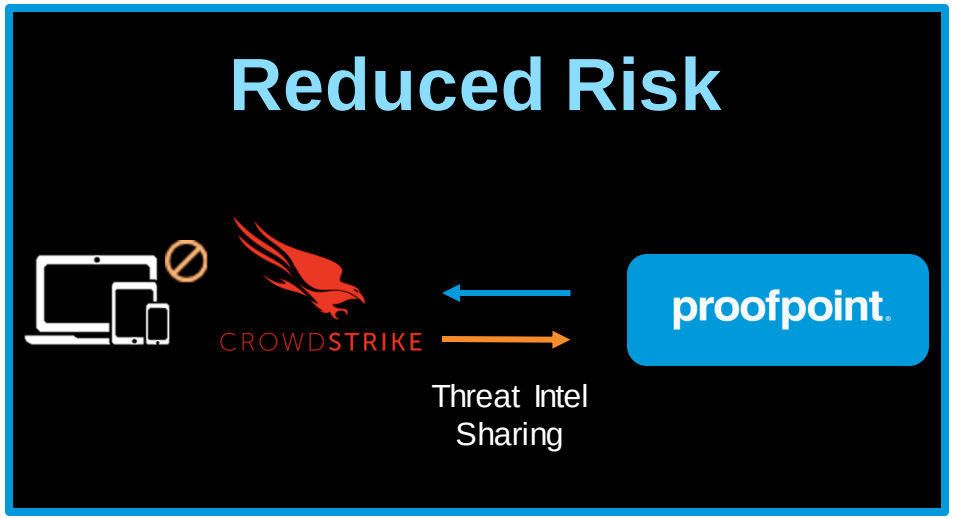
If unknown to CrowdStrike, file hash gets added to CrowdStrike Custom Indicator



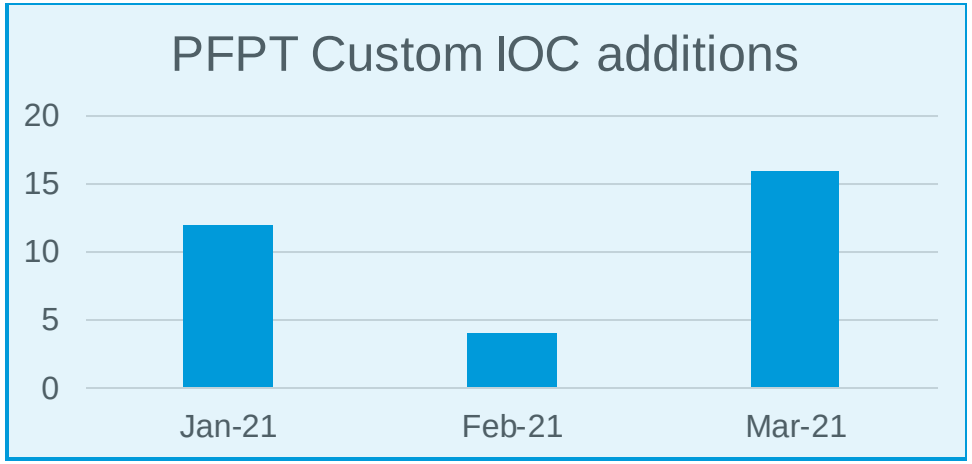
Post Delivery Detection and Protection



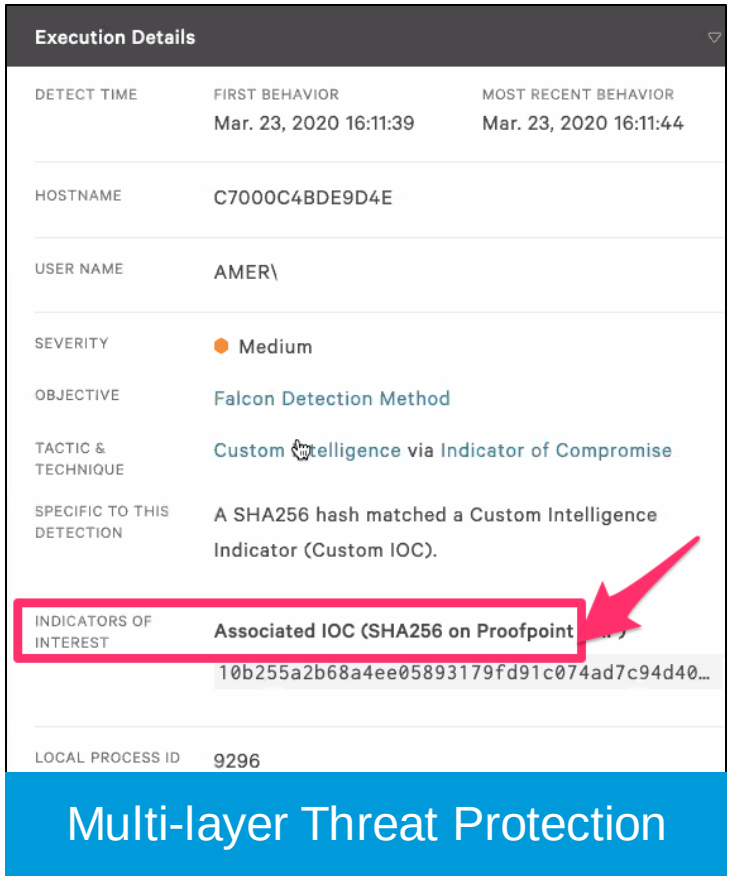
Proofpoint + CrowdStrike: Post Delivery Detection and Protection



Example: BioTech. customer (4500+ FTEs)



CrowdStrike Falcon Platform

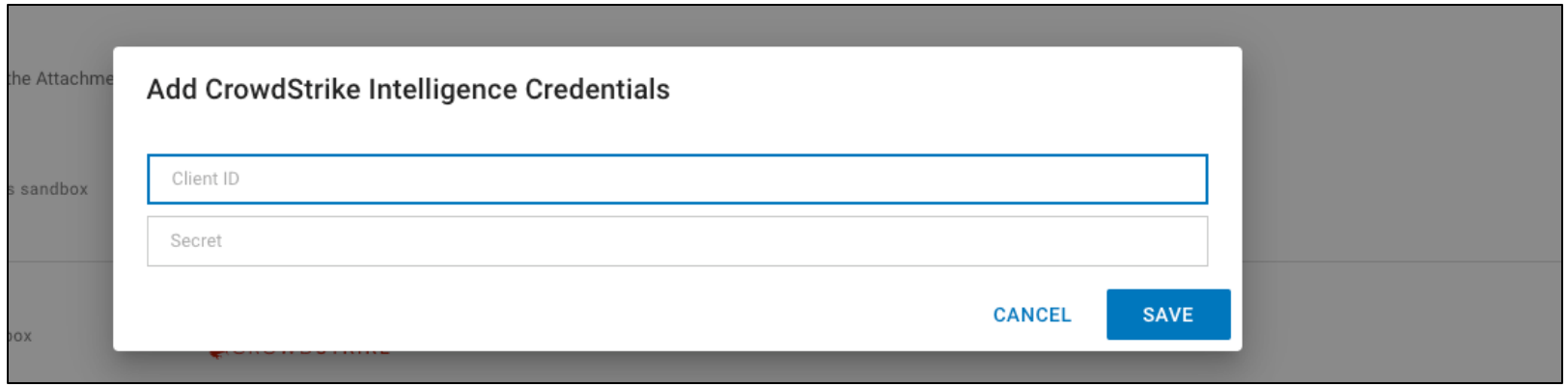


proofpoint.

CROWDSTRIKE

Activate the threat intelligence integration in seconds

Proofpoint TAP dashboard



CLOUD NATIVE

NO EXTRA COST AND COMPLEXITY

EFFORTLESS SCALABILITY

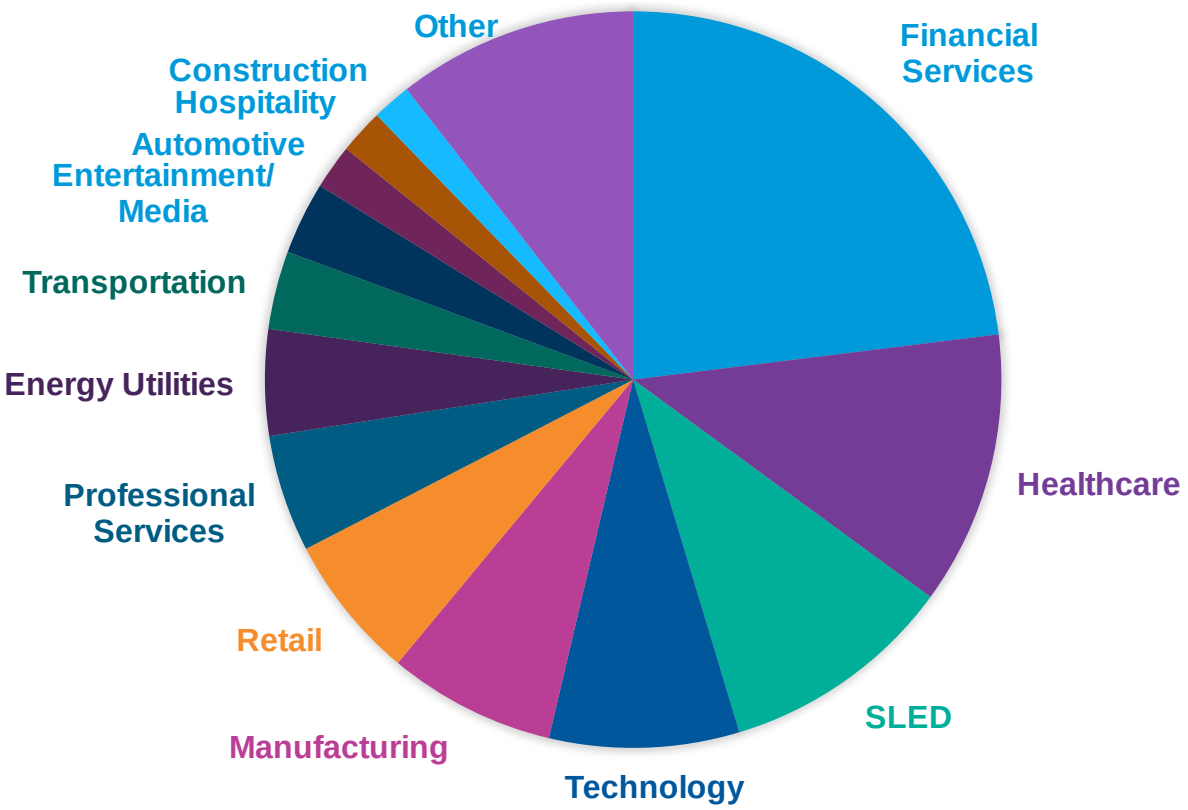
WORKS ON DAY ONE

proofpoint.

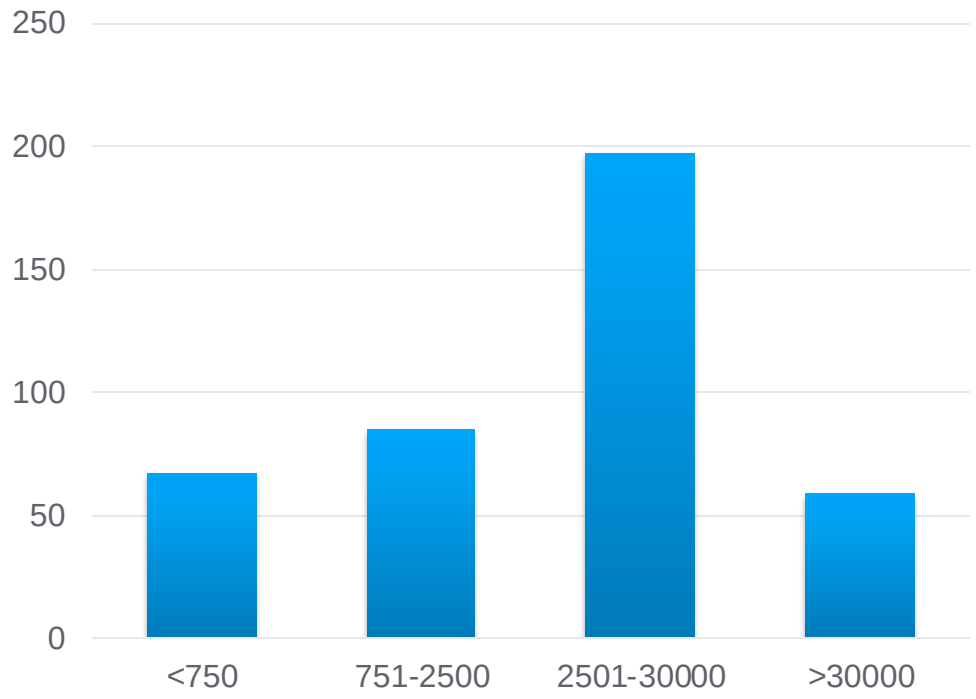
CROWDSTRIKE

400+ customers now benefiting from the integration

Breakdown by Industry



Breakdown by Customer Mailboxes



Q&A

Thank you!

Learn more about our partnership

Sign up for free people-centric risk assessments

proofpoint.

CROWDSTRIKE