Protecting Organizations’ People and Their Devices
Executive Summary

• People and their endpoints are key variables in the rapidly evolving cybersecurity threat landscape
  - Email is a key source for malware getting on endpoints, 92% of all malware delivered by email
  - Modern threat landscape is focused on targeting people, malware increasingly used in multi-stage threats
  - It is hard to accomplish security goals when attacks are sophisticated, solutions are complex and skills are in short supply

• In order to better mitigate risk, organizations need to deploy best in class security products that work together
  - Collaboration required between security leaders to successfully defend against sophisticated attacks
  - Together, Proofpoint and CrowdStrike deliver exceptional business value to customers
  - Our threat intelligence integrations enable customers to reduce their overall risk

• Proofpoint and CrowdStrike are working together to transform security programs
  - Easy integration that gets activated in seconds, is cloud native and scales effortlessly
  - 180+ customers already getting unparalleled protection for the users and their endpoints
  - Engage us to deliver on end to end (people and device) security outcomes for your enterprise
Modern threat campaigns focus on human vulnerabilities

99% threats rely on users and their devices

- Identity Deception
- Phishing
- Account Compromise
- Malware
- Data Exfiltration
- Insider Threat
Security programs need to prevent breaches from malware and non-malware attacks.

60% MALWARE BREACH PREVENTION

40% NON-MALWARE ATTACKS

Malware and non-malware threats require complete breach prevention.

Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary
Fast and effective response is critical

TO STAY AHEAD YOU MUST:

1. DETECT IN 1min
2. INVESTIGATE IN 10min
3. RESPOND IN 60min

MITRE ATT&CK PHASE

Initial Access  Execution  Persistence  Privilege Escalation  Defense Evasion  Credential Access  Discovery  Lateral Movement  Collection  Exfiltration  Command & Control  Impact
Today’s security can’t keep up

Attacks are sophisticated

Solutions are complex

Skills are in short supply
Expect leaders to solve for end to end security outcomes

Email Security Example

- Allow employees to safely access personal email while complying with privacy regulations
- Automate response against time-delayed attacks where attackers weaponize URLs after the email has been delivered
- Educate employees against potential email threats while creating a feedback loop that enables them to report suspicious emails
Collaborative leaders improve your security posture

Proofpoint’s Magic Quadrant leadership:

- Secure Email Gateway: Leader for 7 consecutive years
- Security Awareness Training: Leader for 6 consecutive years

...confirmed by its most trusted partner status
to protect against the leading threat vector

#1

- Most deployed solution for the Fortune 100
- Most deployed solution for the Fortune 1000
- Most deployed solution for the Global 2000

CrowdStrike is setting the standard in Endpoint Protection

Gartner
“CROWDSTRIKE NAMED A LEADER IN THE 2019 GARTNER MAGIC QUADRANT FOR ENDPOINT PROTECTION AND POSITIONED FURTHEST FOR COMPLETENESS OF VISION”

Forrester
“CROWDSTRIKE IS THE ONLY VENDOR TO BE NAMED A LEADER IN BOTH ENDPOINT SECURITY SUITE AND EDR WAVES”

IDC
“LEADER IN IDC MARKETSCAPE FOR US INCIDENT READINESS, RESPONSE AND RESILIENCY SERVICES”

CUSTOMER INSIGHTS
HIGHEST SCORE OF 4.9/5 IN BOTH EDR AND ENDPOINT PROTECTION PLATFORMS
Proofpoint delivers peace of mind to its customers

Typical Results: a month of analyzing O365 email at a large global consulting firm customer

Inbound Email
- 196M Emails
  - 100M Emails Blocked
    - IP Reputation Check

Proofpoint Protection Gateway
- Reputation
- Content
- Attachment
- URL
- Known Threats
- Targeted Threats

Targeted Attack Protection
- 6.4M Emails Blocked
  - TAP feeds
  - Signatures
  - Classifiers: Phish, Virus, Spam, Impostor, Bulk, etc.
- 14K Threats Blocked
  - Attachment detonation
  - Static/Dynamic/Protocol detection ensemble

Organization Mail Store
- 70K Threats Blocked
  - URL detonation
  - Static and behavioral detection of phishing kits
  - ML detection of phishing pages using HTML, URL
- 89.5M Emails Delivered
  - 1,985 attachments detected post-delivery and remediated
  - 35,980 URLs detected post-delivery and remediated
  - 1,866 clicks blocked

End Result:
- 80% fewer incidents get to the SOC

© 2020 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary
CrowdStrike transforms your security program

Automated Hunting Engine
Threat Graph

- **135 Million** IOA Decisions/Min
- **2.5 Trillion** Events/Week
- **130 Adversaries Tracked**
- **35,000 Potential Breaches Stopped**
- **ENRICHED DATA**
- **ANALYZED DATA**
- **Prevent Threats**
- **Investigate Faster**
- **Hunt Proactively**
- **Actionable Insights**

**IMPROVE YOUR PROTECTION**
Sophisticated technology
Built in threat intelligence
Deep human expertise

**REDUCE COMPLEXITY**
Consolidate agents
Simplify your architecture
Streamline operations

**GAIN EMBEDDED EXPERTISE**
Expert threat hunters
Fully managed protection & remediation
Threat intelligence

**GET IMMEDIATE VALUE**
A true turnkey solution
Deploy in one day
No consulting services required
Together, we deliver exceptional value to customers.

**US State Agency (35,000 endpoints, 28,000 mailboxes)**

**Before**
- Email Security Solution: Google (Proofpoint POC)
- Endpoint Security Solution: McAfee (CrowdStrike implementation planned)
- Problem: SecOps team unable to cover (respond to) all the security alerts being generated

**After**
- Dramatic (>50%) reduction in alerts escalated to SecOps once Proofpoint’s email security solution was in production
- SecOps team was able to better focus on alerts that needed investigation using CrowdStrike’s Security Analytics and EDR capabilities

- Gain security efficiency and efficacy
- Reduce time-to-respond
- Improve SOC productivity
- Reduced time to remediation
- Reduce risk
Proofpoint queries CrowdStrike Intelligence for known threats, blocking and sharing threat intelligence. Proofpoint sends malicious hash information to CrowdStrike list of custom IOCs.

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.
Activate the threat intelligence integrations in seconds

Proofpoint TAP dashboard

CrowdStrike Intelligence
Leverage CrowdStrike Intelligence in addition to Proofpoint’s sandbox
Add API Credentials

Add CrowdStrike Intelligence Credentials
- Client ID
- Secret

CANCEL   SAVE

CrowdStrike Intelligence (On)
Leverage CrowdStrike Intelligence in addition to Proofpoint’s sandbox
Replace API Credentials | Remove API Credentials

© 2020 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary

CLOUD NATIVE
NO EXTRA COST AND COMPLEXITY
EFFORTLESS SCALABILITY
WORKS ON DAY ONE
180+ customers now benefiting from the integration
Together we can protect your people and their devices

Proofpoint solutions protect you against people-centric attacks
- Email
- ZTNA
- SOAR
- Security Awareness Training
- CASB
- Insider Threat Management
- Compliance
- Digital Risk

CrowdStrike solutions protect you against endpoint-based attacks
- Cloud Security
- Endpoint Security
- Security & IT Ops
- Threat Intelligence

© 2020 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary
Proofpoint and CrowdStrike: Threat Intelligence Sharing
Pre-Delivery Attachment Defense
Proofpoint + CrowdStrike: Pre-Delivery Attachment Defense

1. Proofpoint begins sandboxing file and will also query the CrowdStrike Intelligence API for file reputation.
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.
Proofpoint TAP will simultaneously sandbox the file. If file found malicious during investigation, it will be blocked.
Proofpoint + CrowdStrike: Pre-Delivery Attachment Defense

Improved protection for customer through threat intelligence sharing
Improved Efficacy

Threat Intel Sharing

Forensics on TAP Dashboard

Expanded Insight
Proofpoint and CrowdStrike: Multi-layered Protection

Post Delivery Attachment Defense
Proofpoint TAP detects a malicious file has been delivered, TRAP enables automated remediation for the user mailboxes.
Proofpoint + CrowdStrike: Post Delivery Detection and Protection

If unknown to CrowdStrike, file hash gets added to CrowdStrike Custom Indicator
Improved protection for customer through intelligence sharing
Proofpoint + CrowdStrike: Post Delivery Detection and Protection

CrowdStrike Falcon Platform

<table>
<thead>
<tr>
<th>Execution Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>DETECT TIME</td>
</tr>
<tr>
<td>FIRST BEHAVIOR</td>
</tr>
<tr>
<td>MOST RECENT BEHAVIOR</td>
</tr>
<tr>
<td>HOSTNAME</td>
</tr>
<tr>
<td>USER NAME</td>
</tr>
<tr>
<td>SEVERITY</td>
</tr>
<tr>
<td>OBJECTIVE</td>
</tr>
<tr>
<td>TACTIC &amp; TECHNIQUE</td>
</tr>
<tr>
<td>SPECIFIC TO THIS DETECTION</td>
</tr>
<tr>
<td>INDICATORS OF INTEREST</td>
</tr>
<tr>
<td>LOCAL PROCESS ID</td>
</tr>
</tbody>
</table>

Multi-layer Threat Protection
Step by Step Integration Guide
Threat Intelligence Integrations with Crowdstrike
Steps to activate the Threat Intel. integrations (1/3)

**Step 1:** Log into Falcon account, click on API Clients and Keys under Support

**Step 2:** Under API clients, click Add new API client

- For detections, host, host groups, prevention policies, and sensor update policies

<table>
<thead>
<tr>
<th>API clients</th>
<th>Client name</th>
<th>Created</th>
<th>Last modified</th>
<th>Client ID</th>
<th>Actions</th>
</tr>
</thead>
</table>

**Step 3:** After giving appropriate name and description, save the following selections by clicking ADD
- Indicators (Falcon X): READ permission
- IOCs (Indicators of Compromise): READ and WRITE permissions

Crowdstrike API’s Needed

<table>
<thead>
<tr>
<th>Crowdstrike</th>
<th>Indicators (READ)</th>
<th>IOCs (READ and WRITE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration 1</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Integration 2</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
Steps to activate the Threat Intel. integrations (2/3)

**Step 4:** Copy and Save the generated Client ID and Client Secret, you will need them in Step 8 (key expires in 30 minutes)

- API client created
  - CLIENT ID
  - SECRET
  - Copy this to a safe place
  - This is the only time we'll show you this client secret

**Step 5:** Log into your TAP Dashboard, Click on Settings icon

Proofpoint customers need to have license for TAP-Attachment Defense
Steps to activate the Threat Intel. integrations (3/3)

Step 6: **Click on Connected Applications**

Step 7: **Under Integrations, look for Crowdstrike Intelligence and Click on Add API Credentials**

Step 8: **Add the Client ID and Client Secret that you got in Step 4, Select your Crowdstrike Cloud Environment and Save**
RESULT

SUCCESS, integration is working

FAILURE, reach out to Crowdstrike account team

Proofpoint TAP dashboard > Settings > Connected Applications

CrowdStrike Falcon Platform

Proofpoint TAP Dashboard

Execution Details

Forensics

Evidences

Total 35 evidences found across 6 categories

Malicious Attachments: 2
Network Activities: 2
Malicious URL: 1
Malware: 2
DNS Lookups: 2
Behaviors: 26

Condemnation Sources

CrowdStrike Intelligence
Join 1000’s of your peers at Proofpoint’s Annual Customer Event

Register for free at https://www.proofpoint.com/us/events/protect

Americas: Sep 9-10, 2020
Europe: Sep 15-16, 2020
Asia Pacific: Oct 13-14, 2020