**Data Sheet**

# PERCEPTION POINT: X-RAY

Providing 360-degree threat containment
and remediation

## CHALLENGES

With the frequency, variety and sophistication of today's cyberattacks, it is inevitable that some malicious content will reach the endpoint. Vast damage can be caused by just one successful attempt, and already stretched SOC teams are challenged to consistently identify and quarantine every attack before it spreads.

## SOLUTION

Perception Point's X-Ray seamlessly plugs into CrowdStrike Falcon® to contain and remediate malicious incidents that successfully breach the enterprise and are subsequently detected on the endpoint. Instant and automated, X-Ray scans all channels (email, CRM, cloud storage and more) to identify where else the content was sent and prevent further transmission.

Here's how it works. CrowdStrike® Falcon sends hashes of malicious files discovered at the endpoint to X-Ray. X-Ray automatically scans all organizational content-exchange channels to map the extent of the breach across users. Within minutes, the SOC team receives a full channel audit while X-Ray actively remediates and contains the incident to prevent further spread.

## BUSINESS VALUE

| Use Case/Challenge | Solution | Benefit |
|---|---|---|
| Your SOC team is attempting to chase down incidents following endpoint detection | Automated transmission from Falcon's detection to X-Ray enables rapid scan of all channels | Dramatically reduces pressure on the SOC team and shortens containment time |
| There can be a lack of visibility across all channels | X-Ray maps all affected users through an analysis of cloud content exchanges across the organization | Provides full visibility on where else the attack may have spread |
| Additional layer of protection is provided using CrowdStrike threat intelligence | Based on hashes from Falcon, X-Ray modifies the verdict to "malicious" | Prevents reinfection across email and collaboration channels |

## KEY BENEFITS

Automated incident containment and remediation

Lightning-fast response time and unlimited scale

360-degree user and collaboration channel coverage

Software-as-a-service (SaaS) application that deploys within minutes on the Falcon platform

Gartner-recognized solution trusted by global enterprises
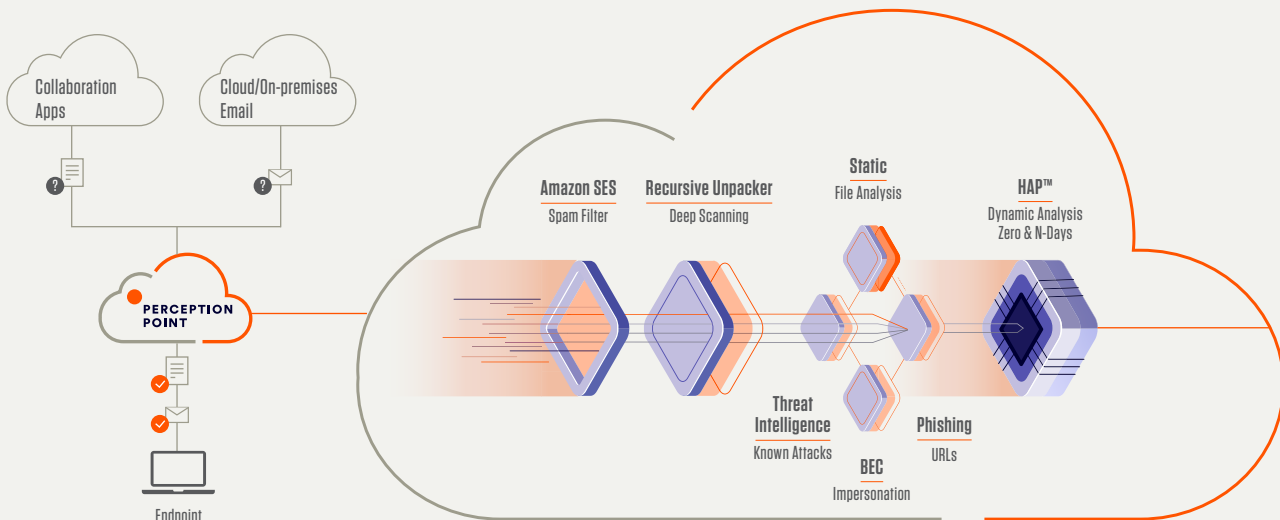
# HOW X-RAY WORKS WITH FALCON

The instant Falcon detects malicious content, it sends the hash to X-Ray. Then X-Ray searches for the hash to see if there are any file matches across all collaboration channels, including cloud storage platforms, email, instant messaging apps and more. Once a file is identified, the SOC team immediately receives an alert, and the system automatically contains the malware, preventing it from spreading.

X-Ray deploys onto Falcon within minutes, with zero fuss to the IT team, and conforms to any existing policies and playbooks.



Endpoint

File Hash

PERCEPTION POINT

Containment & Remediation

# THE X-RAY SECURITY PLATFORM

The X-Ray application for Falcon is only one part of the offering of Perception Point. X-Ray comprises seven layers of next-generation static and dynamic engines that work together to identify any content-based attacks. Techniques covered include zero-days, N-days, BEC, phishing, spam, malware and evasion. Hosted on Amazon Web Services (AWS), X-Ray's cloud technology enables shorter scan times by up to 40x, unlimited scale and rapid updates as the threat landscape evolves.

## WHY IS IT UNIQUE?

X-Ray provides automated incident containment and remediation across all users, email and collaboration channels.

Lightning-speed scans and unlimited scale ensure that the full collaboration network is fully analyzed — no path is left unscanned.

X-Ray is source-agnostic and can analyze and contain the threat regardless of where it originated.

Deployed in the cloud, X-Ray integrates with Falcon in minutes, with zero fuss to the IT team.

X-Ray contains every type of technique including zero-days, known vulnerabilities (N-days), business email compromise (BEC), phishing, spam, malware and evasion.

You gain access to experienced cybersecurity personnel that provides in-depth post-breach analysis.

Attackers will not rest until they find a way to breach their target's perimeter. With Perception Point's X-Ray deployed with CrowdStrike Falcon, you can ensure they are stopped in their tracks — even if an endpoint has been compromised.



Collaboration Apps

Cloud/On-premises Email

PERCEPTION POINT

Endpoint

**Amazon SES**
Spam Filter

**Recursive Unpacker**
Deep Scanning

**Static**
File Analysis

**HAP™**
Dynamic Analysis
Zero & N-Days

**Threat Intelligence**
Known Attacks

**BEC**
Impersonation

**Phishing**
URLs

## KEY CAPABILITIES

X-Ray provides true 360-degree user, channel and threat coverage to ensure incidents are contained quickly and seamlessly across your organization. Combining seven layers of detection with a unique cloud technology enables X-Ray to rapidly scan across 100% of the organization's users and content exchanges, regardless of size or volume, and regardless of attack techniques. No shortcuts. No filtering. No exchange left unturned. Attackers are stopped in their tracks.

## ABOUT PERCEPTION POINT

Perception Point™ is a prevention-as-a-service company, built to enable digital transformation. Trusted by global enterprises, its Gartner-recognized, revolutionary platform offers 360-degree protection against any type of content-based attacks, such as phishing, BEC, spam, malware, Zero-days and N-days, across all collaboration channels, in one simple solution. Built by and for IT and security experts, the service is incredibly easy to deploy, maintain and update according to the newest attack techniques.

Learn more at **www.perception-point.io.**

## ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 4 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Learn more **www.crowdstrike.com**