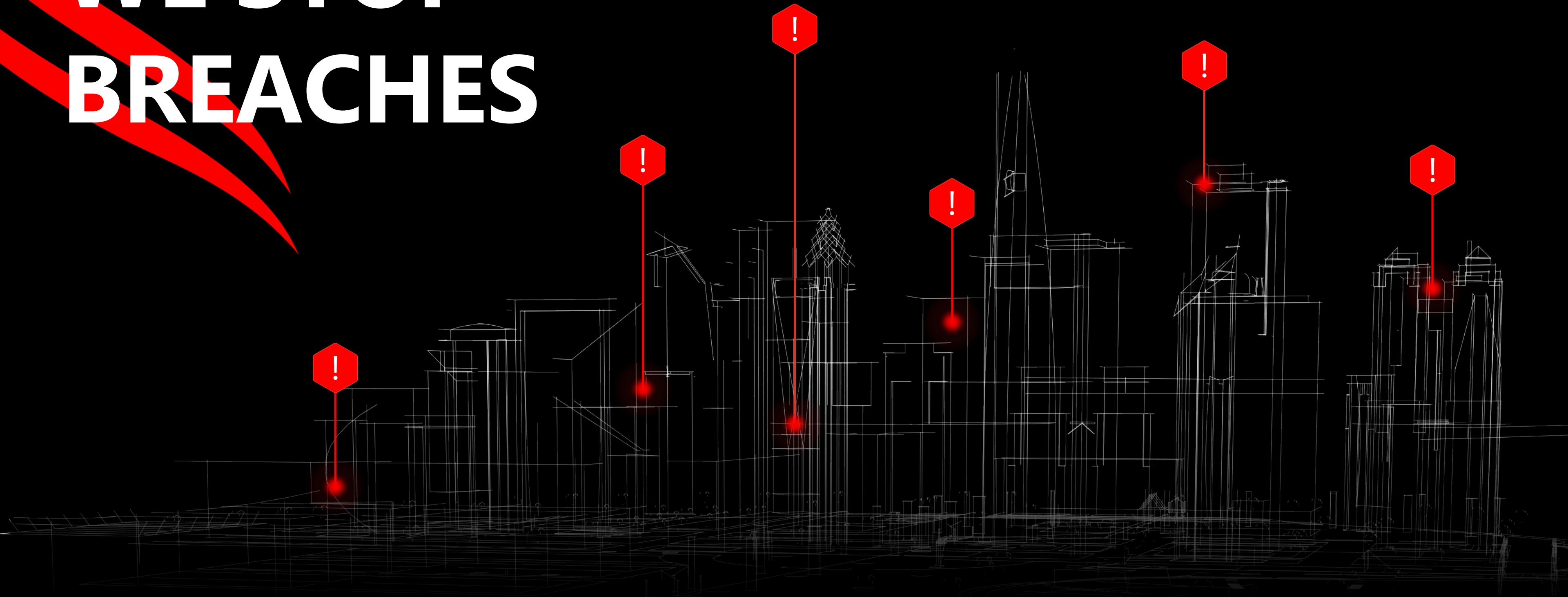
CROWDSTRIKE
CLOUD-DELIVERED ENDPOINT SECURITY

The image cannot be displayed. Your computer may not have enough

WE STOP BREACHES



CROWDSTRIKE

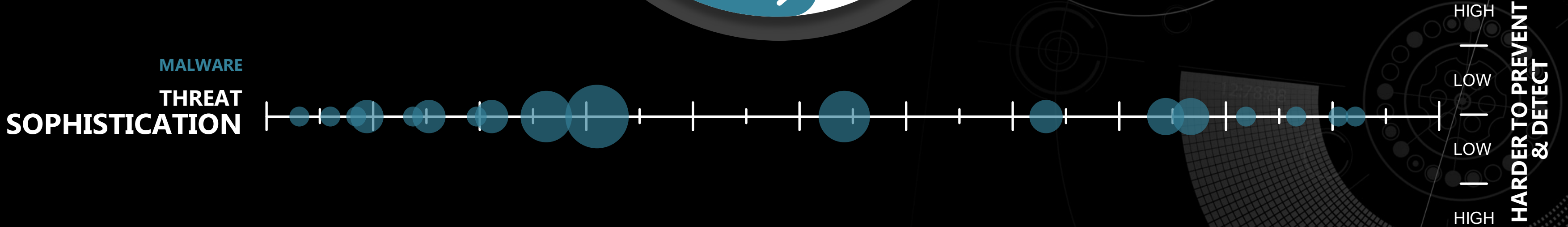
OUTMODED DEFENSES

MALWARE

38%

STOPPING MALWARE

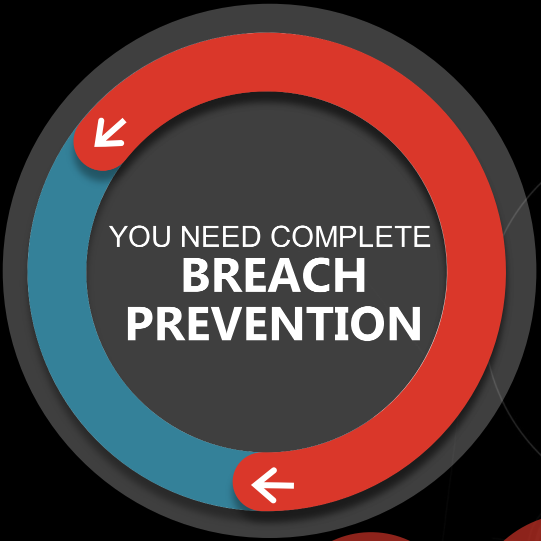
IS NOT ENOUGH



OUTMODED DEFENSES

MALWARE

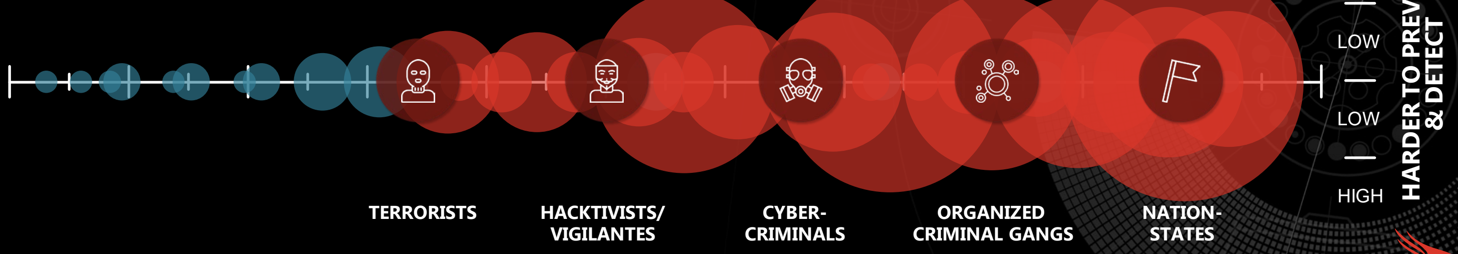
38%



YOU NEED COMPLETE
BREACH PREVENTION

MALWARE-FREE

62%

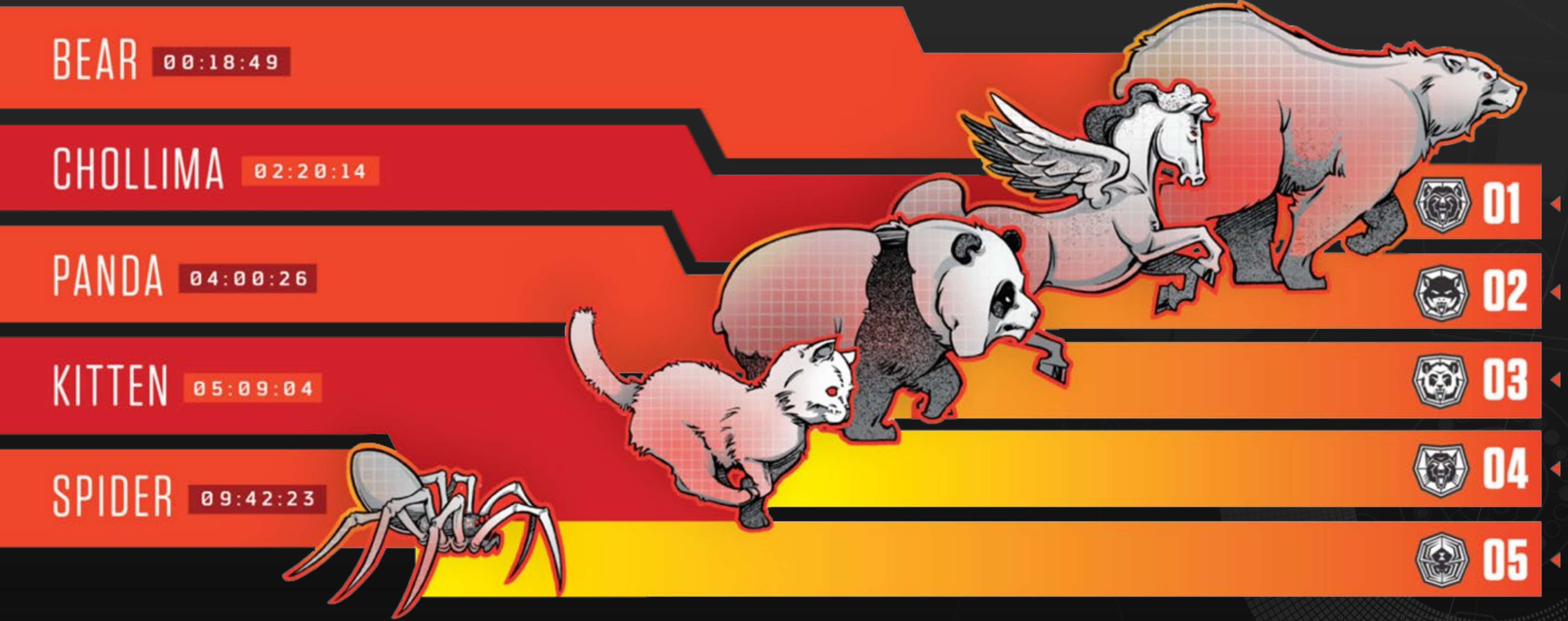


AT THE HEART OF EVERY ATTACK IS A HUMAN ADVERSARY.

FALCON INTELLIGENCE REVEALS THEIR MOTIVATION AND TRADECRAFT TO KEEP YOU ONE STEP AHEAD.

8'0"
7'5"
7'0"
6'5"
6'0"
5'5"
5'0"
C.S. P.D. CROWDSTRIKE GOBLIN PANDA
C.S. P.D. CROWDSTRIKE COZY BEAR
C.S. P.D. CROWDSTRIKE STARDUST CHOLLIMA
C.S. P.D. CROWDSTRIKE HELIX KITTEN
C.S. P.D. CROWDSTRIKE DEEP PANDA
C.S. P.D. CROWDSTRIKE COBALT SPIDER
C.S. P.D. CROWDSTRIKE VENOMOUS BEAR

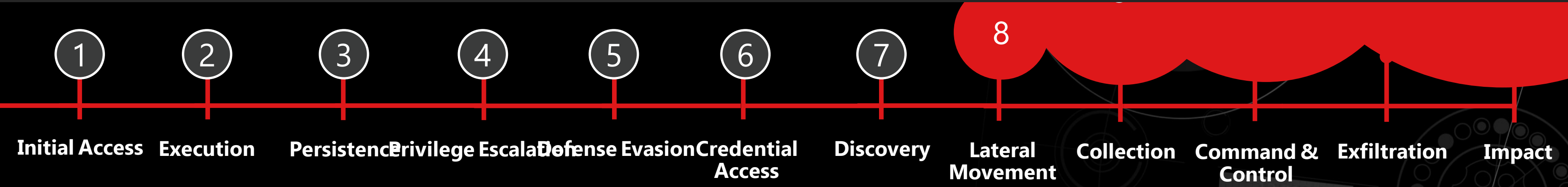
THE ADVERSARY IS SWIFT



SURVIVAL OF THE FASTEST

TO STAY AHEAD YOU MUST:

DETECT IN	INVESTIGATE IN	RESPOND IN
1min	10min	60min



1 Initial Access

2 Execution

3 Persistence

4 Privilege Escala

5 Defense Evasion

6 Credential Access

7 Discovery

8 Lateral Movement

Collection

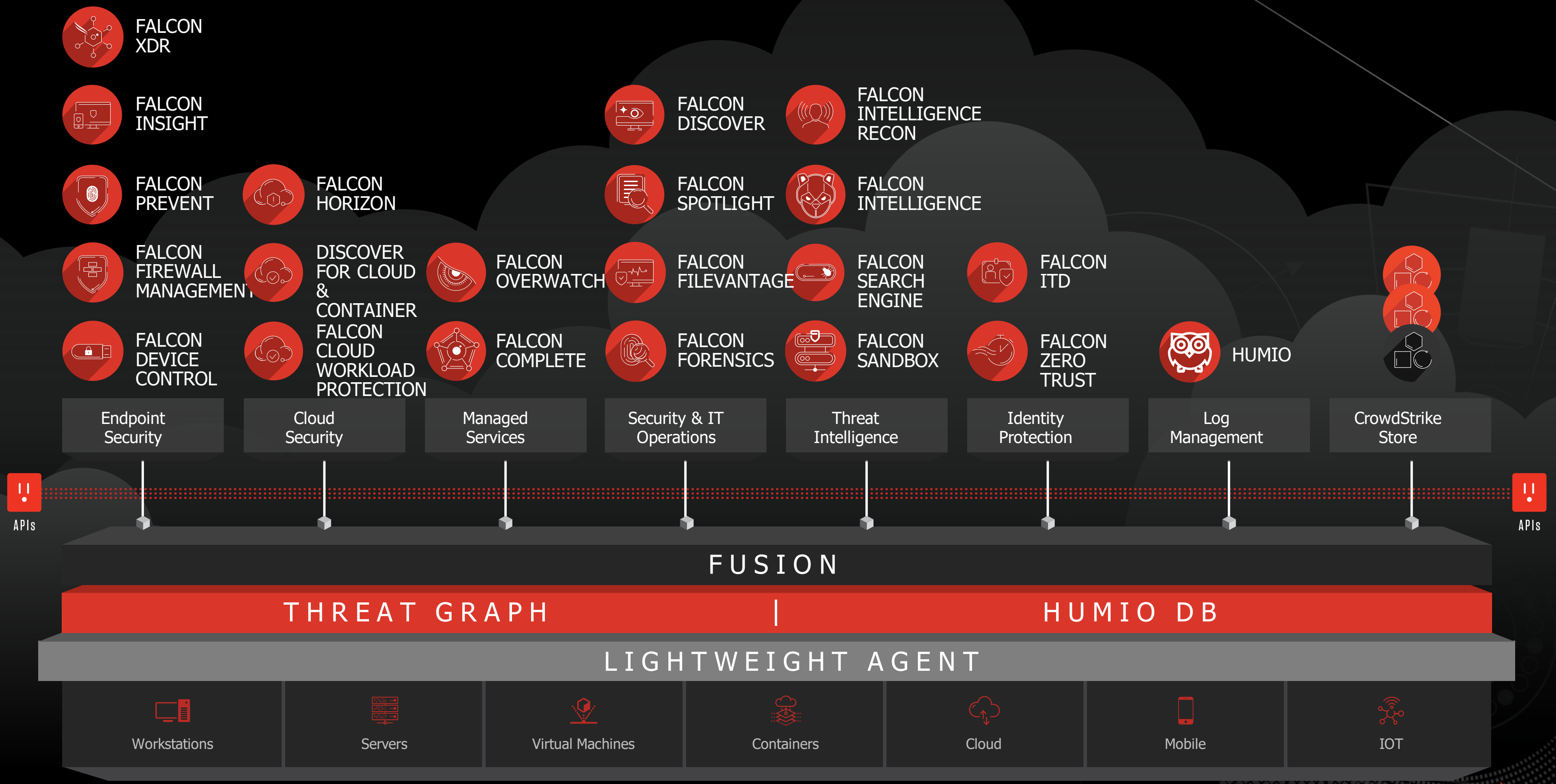
Command & Control

Exfiltration

Impact

MITRE ATT&CK PHASE

Falcon Platform: Defining the Security Cloud



FALCON XDR
FALCON INSIGHT
FALCON PREVENT
FALCON FIREWALL MANAGEMENT
FALCON DEVICE CONTROL
Endpoint Security

FALCON HORIZON
DISCOVER FOR CLOUD & CONTAINER
FALCON CLOUD WORKLOAD PROTECTION
Cloud Security

FALCON OVERWATCH
FALCON COMPLETE
Managed Services

FALCON DISCOVER
FALCON SPOTLIGHT
FALCON FILEVANTAGE
FALCON FORENSICS
Security & IT Operations

FALCON INTELLIGENCE RECON
FALCON INTELLIGENCE
FALCON SEARCH ENGINE
FALCON SANDBOX
Threat Intelligence

FALCON ITD
FALCON ZERO TRUST
Identity Protection

HUMIO
Log Management

CrowdStrike Store

APIs

APIs

FUSION

THREAT GRAPH | HUMIO DB

LIGHTWEIGHT AGENT

Workstations
Servers
Virtual Machines
Containers
Cloud
Mobile
IOT

SIMPLE-
NO SETUP/
ONE AGENT

CROWDSTRIKE

ONE AGENT FULL VISIBILITY

Falcon Agent

Prevent • Predict • Detect • Respond

Endpoints

Workstations

Mobile

Servers

IOT

Clouds

Data Centers

Red Hat

Google Cloud

Microsoft Azure

ORACLE

amazon webservices

aws

docker

Workloads

Containers

Identities

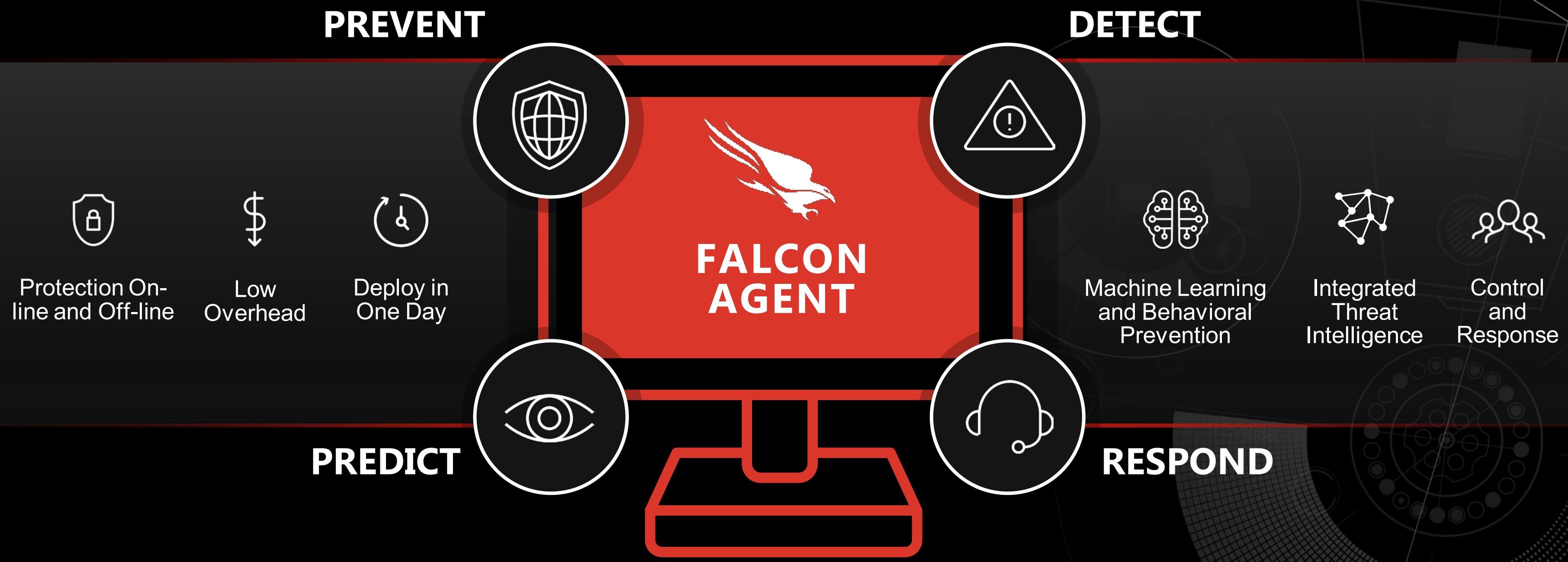
Active Directory

User Accounts

3rd Parties

CROWDSTRIKE

SINGLE LIGHTWEIGHT AGENT



PREVENT

Protection On-line and Off-line

Low Overhead

Deploy in One Day

DETECT

Machine Learning and Behavioral Prevention

Integrated Threat Intelligence

Control and Response

FALCON AGENT

PREDICT

RESPOND

3 SMALL STEPS TO REPLACE YOUR AV

No infrastructure setup

No fine-tuning, rule writing

1 Install the Falcon Agent

2 Verify the installation

No reboot

No signatures updates

No scan

3 Remove legacy products

Financial Institution

77,000 AGENTS
1 DAY

Hospitality Chain

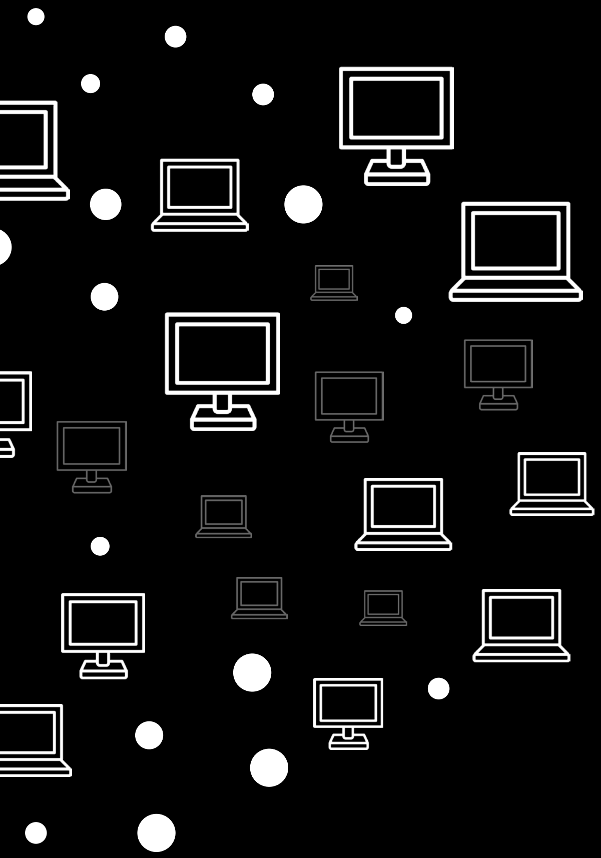
40,000 AGENT
5 DAYS

Technology Company

55,000 AGENTS
5 DAYS

Financial Institution

300,000 AGENTS
90 DAYS



CLOUD-NATIVE

REDUCED COST AND COMPLEXITY

PROTECTION OF THE CROWD

EFFORTLESS SCALABILITY

WORKS ON DAY ONE

NEXT-GEN AV
FALCON PREVENT

Machine Learning

Block Known Bad

IOA Behavioral Blocking

Exploit Blocking

CROWDSTRIKE FALCON CERTIFIED AS LEGACY AV REPLACEMENT

BUSINESS VALUE

Improves protection

Reduces number of incidents

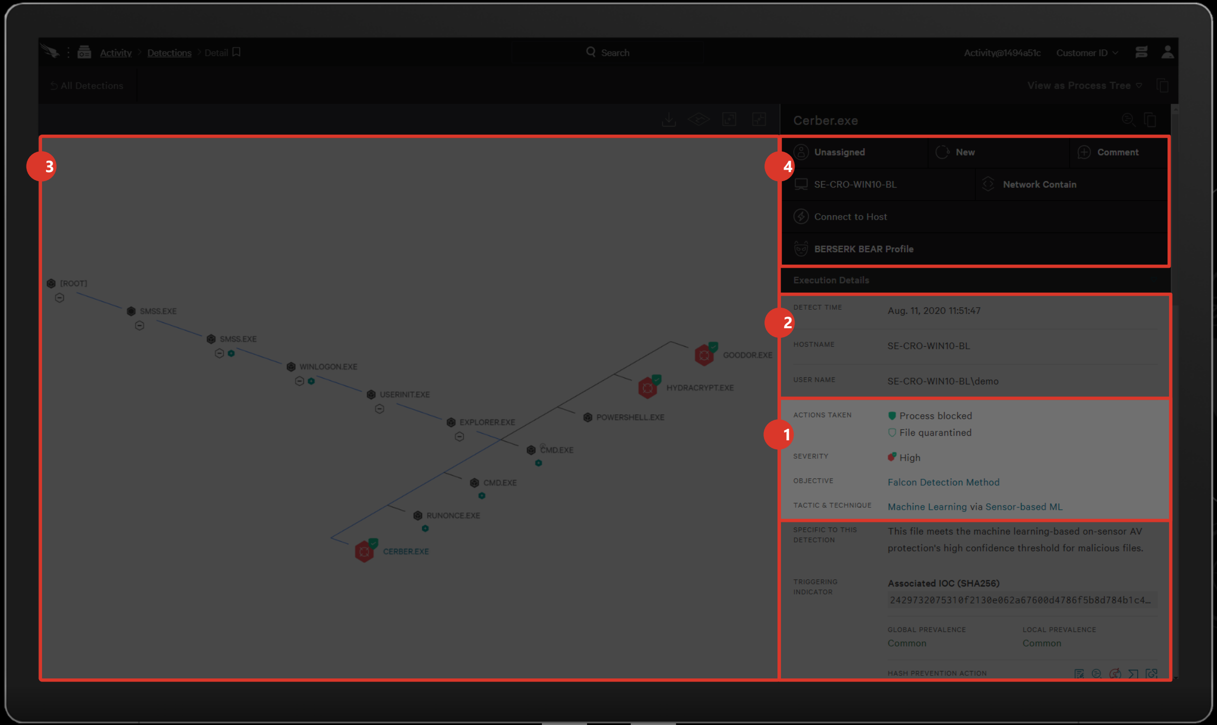
Improves user productivity – no user impact

Reduces complexity

Delivers security efficiency and efficacy

CROWDSTRIKE

SiS



DETECT TIME	Aug. 11, 2020 11:51:47
HOSTNAME	SE-CRO-WIN10-BL
USER NAME	SE-CRO-WIN10-BL\demo
ACTIONS TAKEN	Process blocked File quarantined
SEVERITY	High
OBJECTIVE	Falcon Detection Method
TACTIC & TECHNIQUE	Machine Learning via Sensor-based ML
SPECIFIC TO THIS DETECTION	This file meets the machine learning-based on-sensor AV protection's high confidence threshold for malicious files.
TRIGGERING INDICATOR	Associated IOC (SHA256) 2429732075310f2130e062a67600d4786f5b8d784b1c4…

GLOBAL PREVALENCE: Common

LOCAL PREVALENCE: Common

HASH PREVENTION ACTION

OVERVIEW OF THE FALCON UI

1. The malware was blocked by Machine Learning

2. See the all the details

3. You can see more than just a detection. You can view the entire flow of events attack, step by step

4. Take action and manage the alert

ENDPOINT DETECTION AND RESPONSE
FALCON INSIGHT

Real-time and Historical Search
Record Everything
Real-time Response and Containment
Threat Hunting

BUSINESS VALUE

Reduce time-to-respond

Improve SOC productivity

Reduced time to remediation

Augment skills and expertise

Reduce risk

Gain security efficiency and efficacy

FALCON ENDPOINT PROTECTION SOLUTIONS

FALCON PRO

Next Gen Antivirus

Remote Response

Integrated Threat Intel

Device Control

Firewall Management

FALCON ENTERPRISE

Next Gen Antivirus

Endpoint Detection & Response

Integrated Threat Intel

Managed Threat Hunting

Device Control

Firewall Management

FALCON ELITE

Next Gen Antivirus

Endpoint Detection & Response

Integrated Threat Intel

Managed Threat Hunting

Identity Protection

Device Control

Firewall Management

IT Hygiene

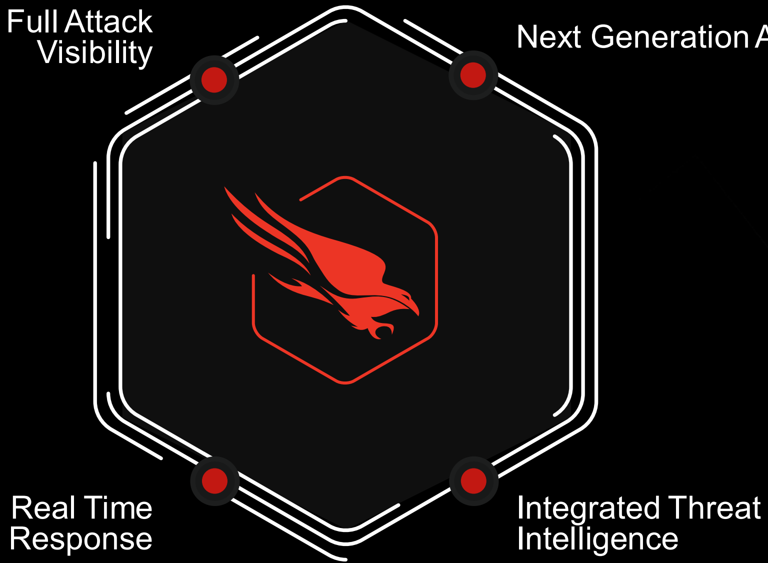
FALCON COMPLETE

Falcon Endpoint Protection

Delivered as a Service

Breach Prevention Warranty

FALCON ENDPOINT PROTECTION PRO



BUSINESS VALUE

Replace legacy antivirus suites

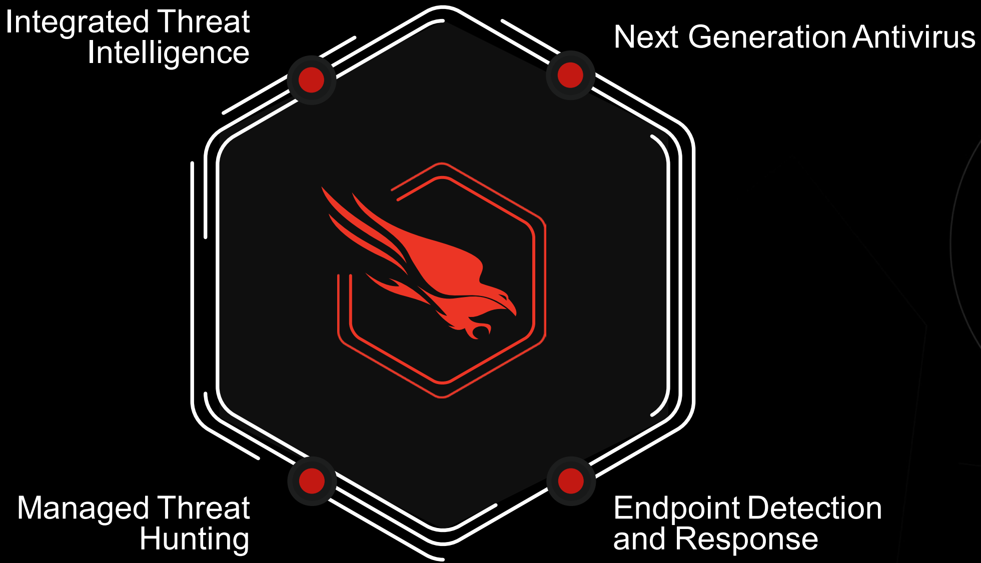
Stop known and unknown malware

Remediate incidents quickly

Restore system performance and productivity

Empower analysts to operate more efficiently

FALCON ENDPOINT PROTECTION ENTERPRISE


Integrated Threat Intelligence
Next Generation Antivirus
Managed Threat Hunting
Endpoint Detection and Response

BUSINESS VALUE

Unify NGAV and EDR for full endpoint protection

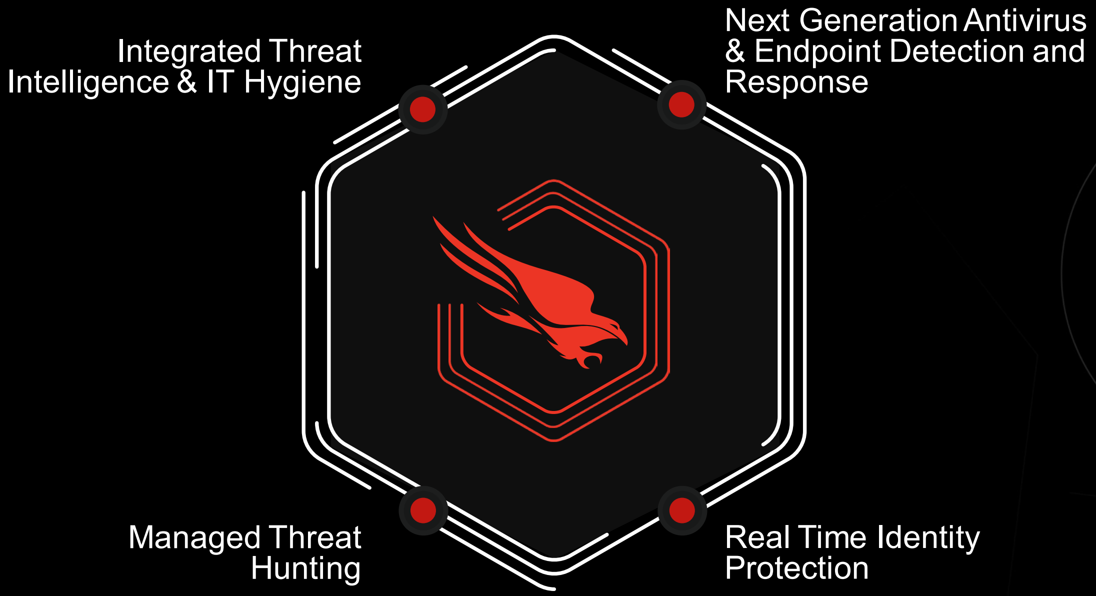
Enable threat hunting and real time visibility

Uncover stealthy attacks

Speed investigation and response

Automatic analysis and orchestrated IOC sharing

FALCON ENDPOINT AND IDENTITY PROTECTION ELITE


Integrated Threat Intelligence & IT Hygiene
Next Generation Antivirus & Endpoint Detection and Response
Managed Threat Hunting
Real Time Identity Protection

BUSINESS VALUE

Protection that unifies NGAV, EDR, Identity and IT Hygiene

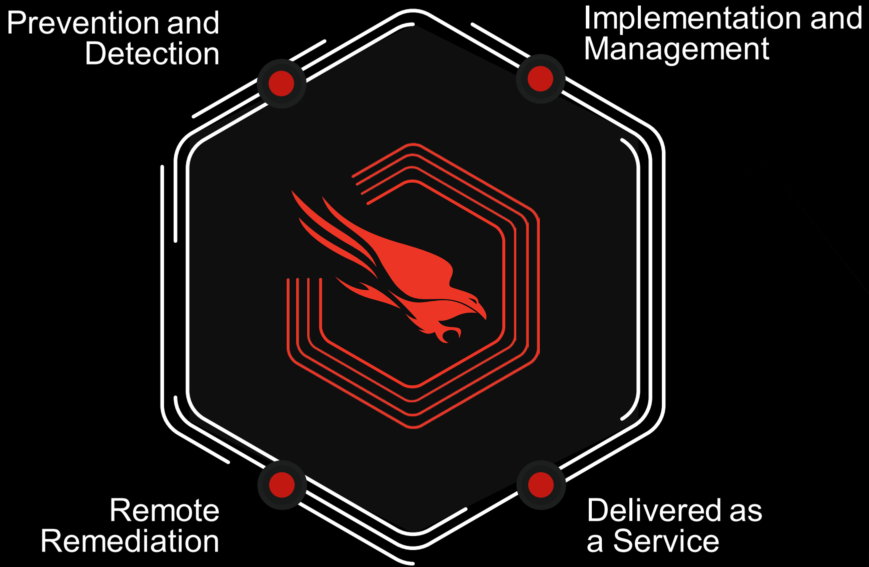
Enable threat hunting and real time visibility

Expanded visibility & control

Speed investigation and response

Discover unprotected systems, risky applications and users

FALCON COMPLETE



BUSINESS VALUE

Reduce costs of managing endpoint protection

Increase security effectiveness

Optimize your team

Back to business swiftly with surgical remediation

Gain confidence with industry's strongest breach prevention warranty

CROWDSTRIKE

SIS

CROWDSTRIKE IS REDEFINING SECURITY FOR THE CLOUD ERA

BETTER PROTECTION

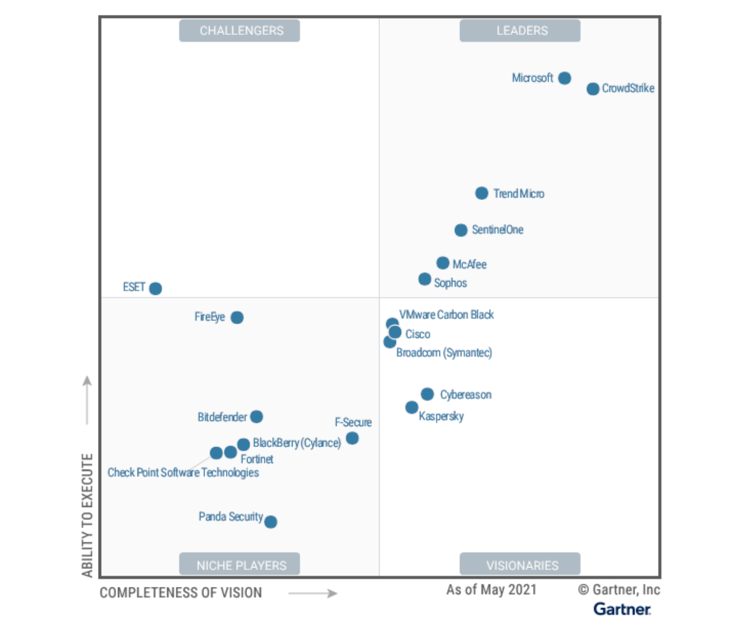
BETTER PERFORMANCE

BETTER TIME TO VALUE

GARTNER RECOGNITION

Expert Recognition

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)

Gartner® Magic Quadrant™ for Endpoint Protection Platforms, May 2021

Customer Recognition

Gartner peerinsights customers' choice 2021 ™

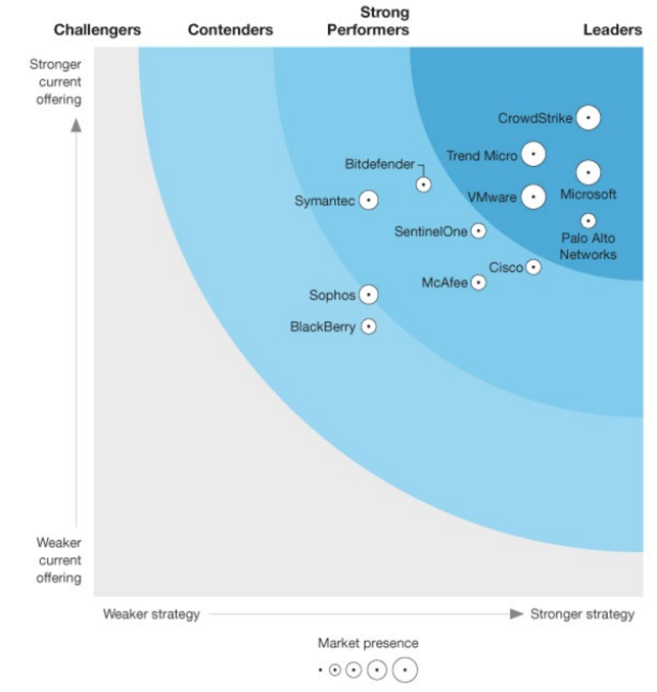
Endpoint Protection Platforms

Gartner peerinsights customers' choice 2020 ™

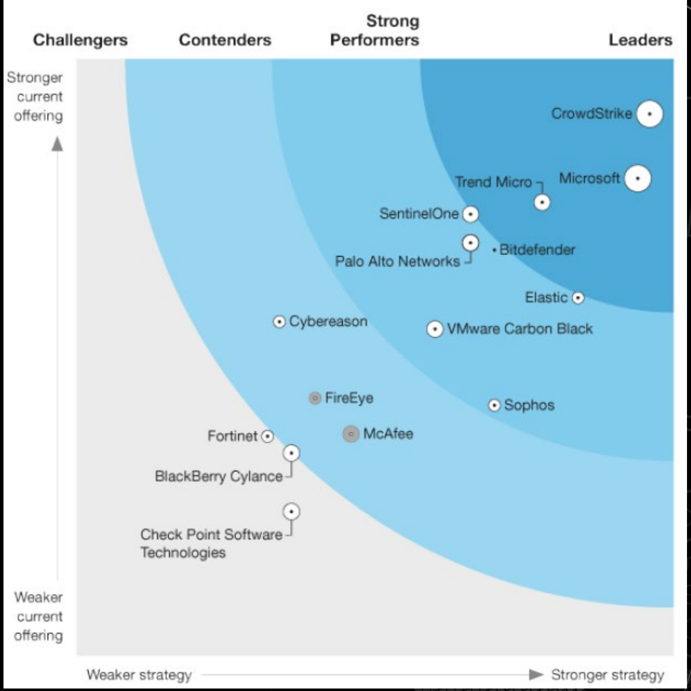
Endpoint Detection and Response Solutions

Gartner Magic Quadrant for Endpoint Protection Platforms,Paul Webber, Peter Firstbrook, Rob Smith, Mark Harris, Prateek Bhajanka,5th May 2021
This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Crowdstrike. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The GARTNER PEER INSIGHTS Logo is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences and do not represent the views of Gartner or its affiliates.. https://www.gartner.com/reviews/customers-choice/endpoint-protection-platforms and https://www.gartner.com/reviews/customers-choice/endpoint-detection-and-response-solutions

FORRESTER WAVES



Forrester Wave: Endpoint Security Software As A Service, Q2 2021



Forrester Wave™: Endpoint Detection And Response Providers, Q2 2022

CROWDSTRIKE

SiS

TESTING AND COMPLIANCE

AV comparatives

99%+ Malware Block Rate

Proven on Windows and Mac

Negligible Performance Impact

MITRE

Broad Proactive Detections

Comprehensive Visibility

Deep Context

SE Labs

AAA Rating

100% Legitimate Accuracy

0% False Positives

COMPLIANCE

Privacy Shield Framework

FedRAMP

PCI

HIPAA Health Insurance Portability & Accountability Act

aws competency

MEMBER amtso Anti-Malware Testing Standards Organization

CROWDSTRIKE

SiS

A PROVEN SECURITY LEADER

Leader In

Gartner • FORRESTER • IDC

Validated

MITRE • AV comparatives • SE Labs

Compliance & Certifications

Privacy Shield Framework · FedRAMP · PCI · aws competency · MEMBER amtso · FIEC · CYBER ESSENTIALS CERTIFIED · PRODUCTO SEGURIDAD TIC CCN CUALIFICADO · STAR LEVEL TWO · CREST

TRUSTED BY CUSTOMERS EVERYWHERE

"CrowdStrike Falcon is one of the most important tools in my organization's security toolbox."

Gartner peerinsights customers' choice™

Highest Ratings

4.9/5	in EDR
4.8/5	in Endpoint Protection Platforms

AMG PETRONAS MOTORSPORT

CREDIT SUISSE

Goldman Sachs

ADP

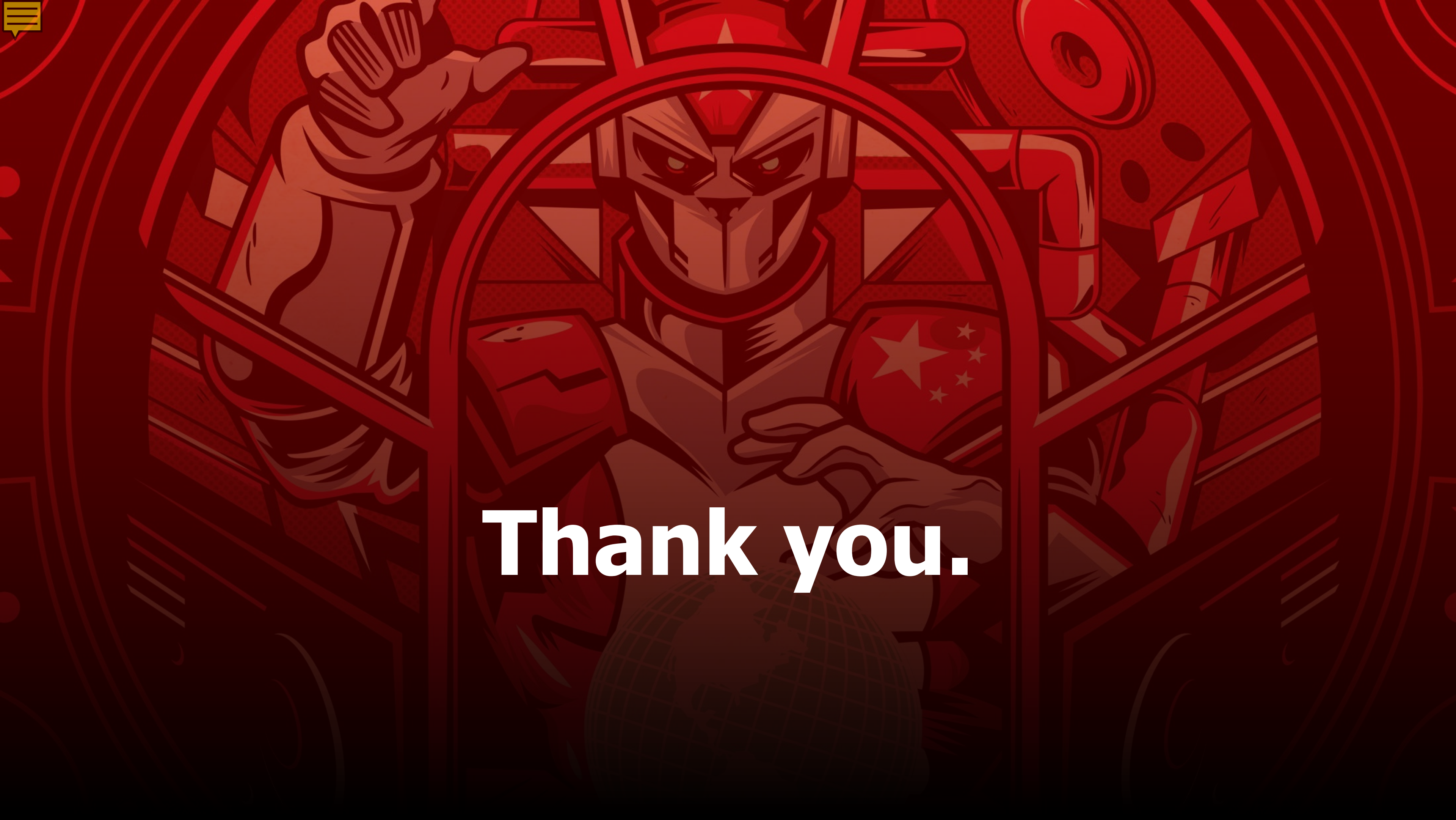
254 of 500
of the Fortune 500

526 of 2000
of the Global 2000

15 of the Top 20
Global Banks

5 of the Top 10
Largest Healthcare Providers

7 of the Top 10
Largest Energy Institutions



Thank you.