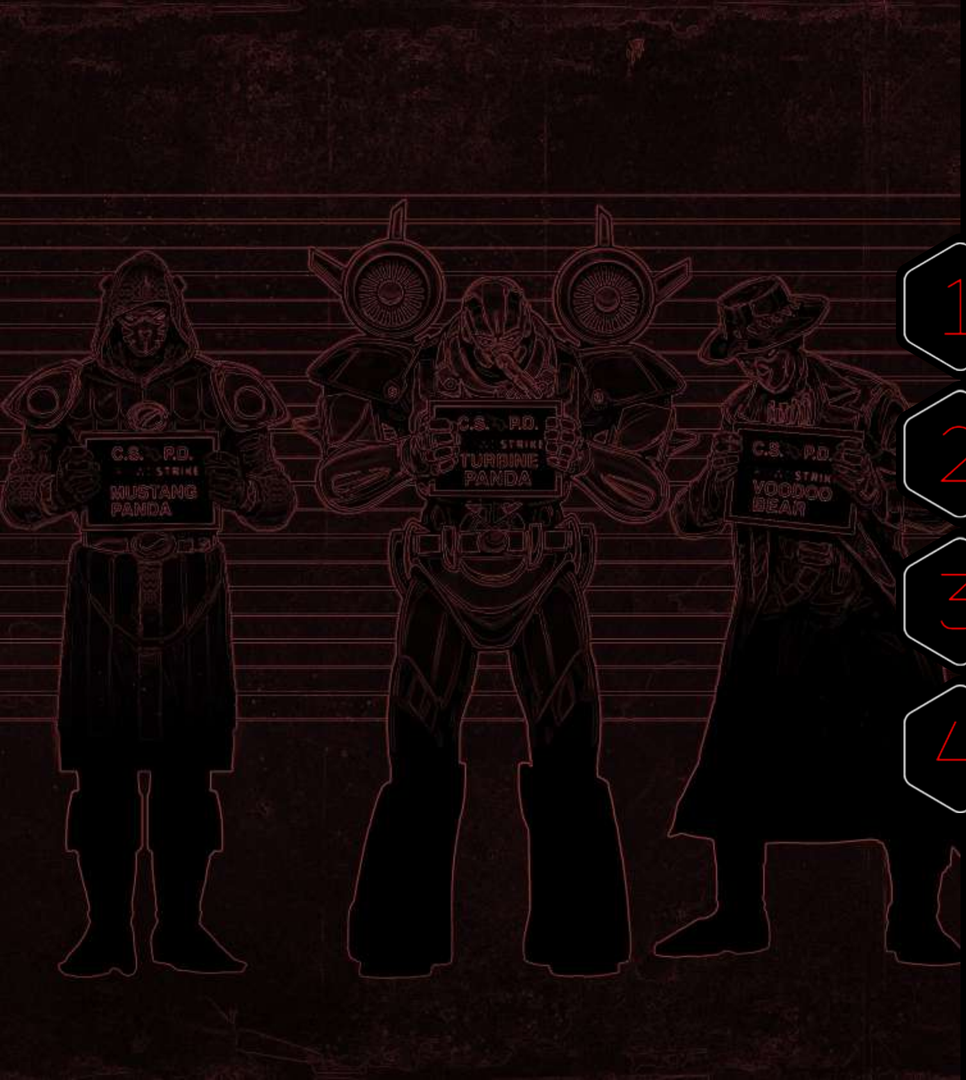
CROWDSTRIKE

SOFTPROM SECURITY FORUM BAKU

Philippe FARHAT
Regional Sales Engineer



AGENDA

1 GENERAL TRENDS & OBSERVATIONS

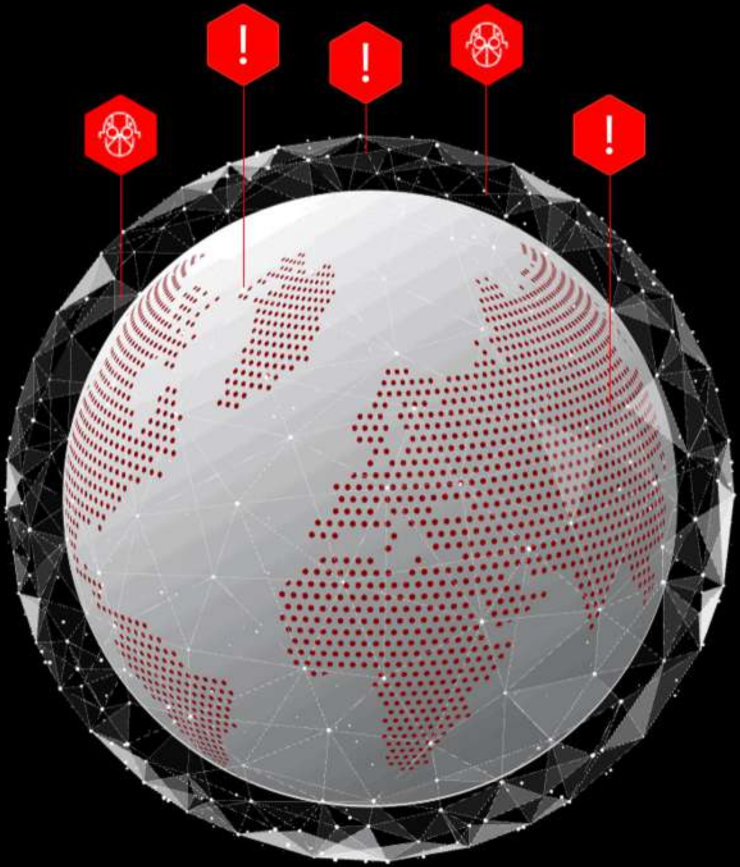
2 KEY THREATS HIGHLIGHT

3 UNIFIED PLATFORM

4 CONCLUSION

We Stop Breaches

Protection that powers you.



CROWDSTRIKE

YOU NO LONGER HAVE A MALWARE PROBLEM
YOU HAVE AN ADVERSARY PROBLEM

CRIMINAL

Alchemist Spider
Aviator Spider
Bitwise Spider
Carbon Spider
Chariot Spider
Clockwork Spider
Cyborg Spider
Doppel Spider
Feral Spider
Graceful Spider
Hidden Spider
Hive Spider
Indrik Spider
Knockout Spider
Lunar Spider
Mallard Spider
Mummy Spider
Narwhal Spider
Night Spider
Outbreak Spider
Outlaw Spider
Percussion Spider
Pinchy Spider
Prophet Spider
Salty Spider
Samba Spider
Scully Spider
Slippy Spider
Smoky Spider
Solar Spider
Sprite Spider
Traveling Spider
Venom Spider
Wizard Spider
Vice Spider

CHINA

Aquatic Panda
Cascade Panda
Circuit Panda
Emissary Panda
Ethereal Panda
Jackpot Panda
Karma Panda
Kryptonite Panda
Lotus Panda
Mustang Panda
Nomad Panda
Phantom Panda
Puzzle Panda
Shattered Panda
Sunrise Panda
Vapor Panda
Vertigo Panda
Vixen Panda
Wicked Panda

NORTH KOREA

Labyrinth Chollima
Ricochet Chollima
Silent Chollima
Stardust Chollima
Velvet Chollima

IRAN

Charming Kitten
Chrono Kitten
Haywire Kitten
Imperial Kitten
Nemesis Kitten
Pioneer Kitten
Refined Kitten
Spectral Kitten
Static Kitten
Tracer Kitten

INDIA

Hazy Tiger
Outrider Tiger
Quilted Tiger
Razor Tiger
Viceroy Tiger

RUSSIA

Berserk Bear
Cozy Bear
Ember Bear
Gossamer Bear
Fancy Bear
Primitive Bear
Venomous Bear
Voodoo Bear

PAKISTAN

Mythic Leopard
Fringe Leopard

VIETNAM

Ocean Buffalo

SOUTH KOREA

Shadow Crane

SYRIA

Deadeye Hawk

COLOMBIA

Galactic Ocelot

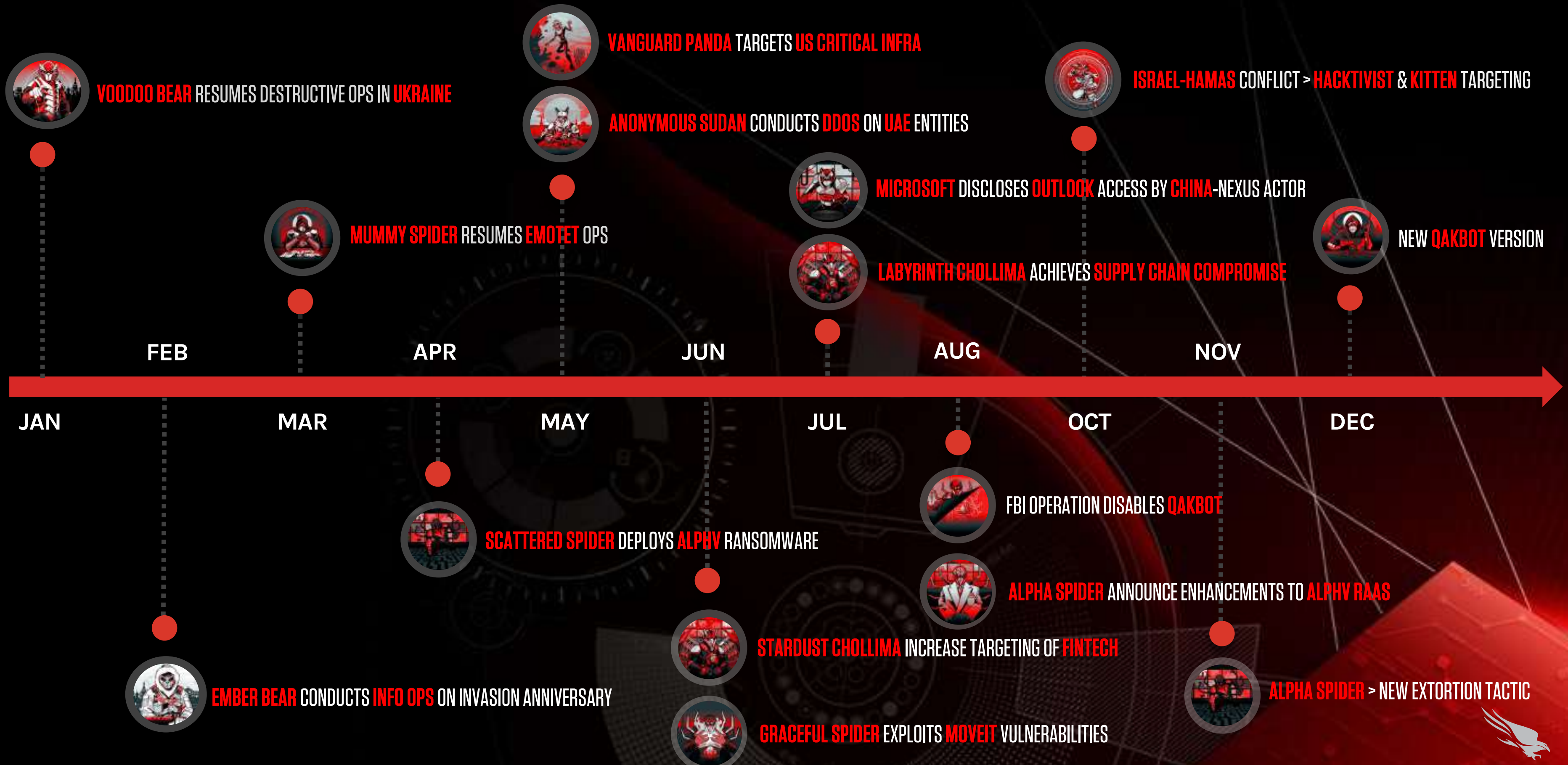
TURKEY

Cosmic Wolf

HACKTIVISM

Curious Jackal
Frontline Jackal
Intrepid Jackal
Partisan Jackal
Regal Jackal
Renegade Jackal

NOTEWORTHY DEVELOPMENTS IN 2023



VOODOO BEAR RESUMES DESTRUCTIVE OPS IN UKRAINE

EMBER BEAR CONDUCTS INFO OPS ON INVASION ANNIVERSARY

MUMMY SPIDER RESUMES EMOTET OPS

SCATTERED SPIDER DEPLOYS ALPHV RANSOMWARE

VANGUARD PANDA TARGETS US CRITICAL INFRA

ANONYMOUS SUDAN CONDUCTS DDOS ON UAE ENTITIES

STARDUST CHOLLIMA INCREASE TARGETING OF FINTECH

GRACEFUL SPIDER EXPLOITS MOVEIT VULNERABILITIES

MICROSOFT DISCLOSES OUTLOOK ACCESS BY CHINA-NEXUS ACTOR

LABYRINTH CHOLLIMA ACHIEVES SUPPLY CHAIN COMPROMISE

FBI OPERATION DISABLES QAKBOT

ALPHA SPIDER ANNOUNCE ENHANCEMENTS TO ALPHV RAAS

ISRAEL-HAMAS CONFLICT > HACKTIVIST & KITTEN TARGETING

ALPHA SPIDER > NEW EXTORTION TACTIC

NEW QAKBOT VERSION

2024 Threat Landscape

+34

232

34 new adversaries tracked by CrowdStrike, raising the total to **232**

110%

Cloud-conscious cases increased by **110% YoY**

$$$

84%

84% of adversary-attributed cloud-conscious intrusions were focused on eCrime

75%

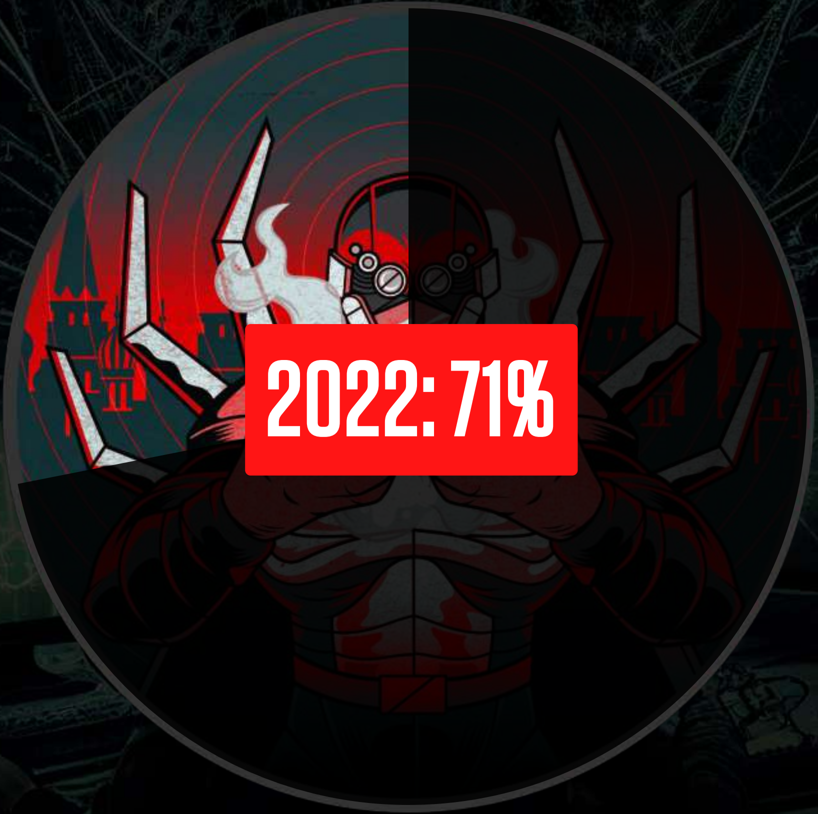
Cloud environment intrusions increased by **75% YoY**

76%

76% YoY increase in victims named on eCrime dedicated leak sites

ADVERSARIES CONTINUE TREND BEYOND MALWARE

ADVERSARIES CONTINUE TREND BEYOND MALWARE



ADVERSARIES CONTINUE TREND BEYOND MALWARE

2023: 75%

AVERAGE ECRIME BREAKOUT TIME

582

2019

62

2023

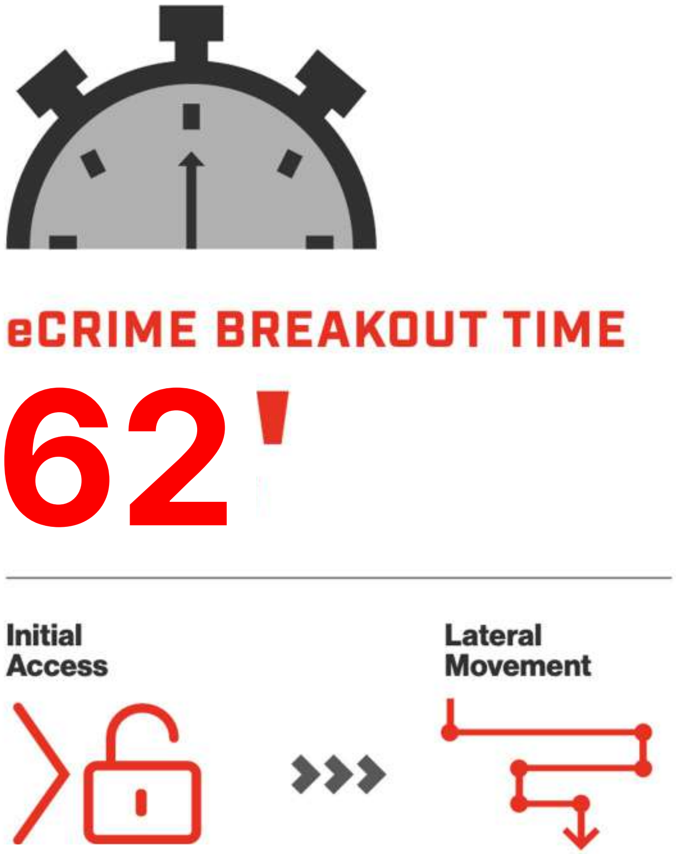
79

2022

INITIAL ACCESS

LATERAL MOVEMENT

CROWDSTRIKE



Adversaries Increasing in Speed and Precision

Defenders must act quickly

To contain the threat and minimize cost and damage, defenders must respond within the breakout time

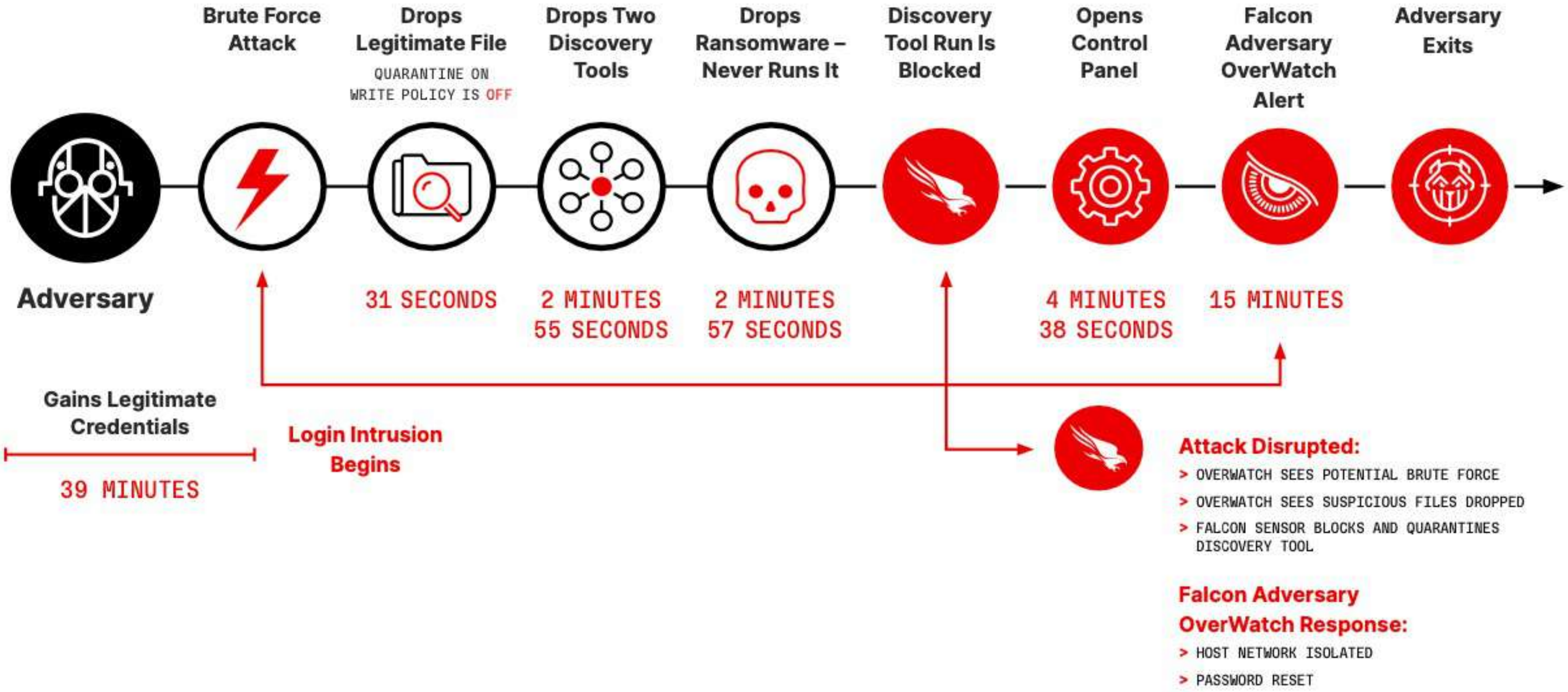
They weaponize YOUR tools and accounts

Adversaries use valid accounts and tools to move laterally, making it nearly impossible to detect abnormal activity and a potential breach

Fastest breakout time: 2 min, 7 sec

Nearly all security teams are not equipped to respond in less than 2 minutes

Identity Is the Critical Battleground



Adversary

Brute Force Attack

Drops Legitimate File

QUARANTINE ON WRITE POLICY IS OFF

31 SECONDS

Drops Two Discovery Tools

2 MINUTES 55 SECONDS

Drops Ransomware – Never Runs It

2 MINUTES 57 SECONDS

Discovery Tool Run Is Blocked

Opens Control Panel

4 MINUTES 38 SECONDS

Falcon Adversary OverWatch Alert

15 MINUTES

Adversary Exits

Gains Legitimate Credentials

39 MINUTES

Login Intrusion Begins

Attack Disrupted:

- OVERWATCH SEES POTENTIAL BRUTE FORCE
- OVERWATCH SEES SUSPICIOUS FILES DROPPED
- FALCON SENSOR BLOCKS AND QUARANTINES DISCOVERY TOOL

Falcon Adversary OverWatch Response:

- HOST NETWORK ISOLATED
- PASSWORD RESET

IDENTITY THREATS BECOME MAINSTREAM

GOING BEYOND USER CREDENTIALS

BEYOND USERNAMES AND PASSWORDS

- Username and password or PIN
- Smart card and PIN
- Valid account and Active Directory certificates
- APIs and secret keys
- Identity providers and protocols such as SAML and OAuth
- Session-based authentication, cookie-based authentication and JSON Web Tokens (JWT)
- Kerberos and Kerberos tickets
- Biometrics such as facial recognition, voice recognition, fingerprint recognition
- Hardware and software tokens or time-based one-time password (TOTP)

583% INCREASE IN KERBEROASTING

62% OF INTERACTIVE INTRUSIONS INVOLVE STOLEN CREDENTIALS

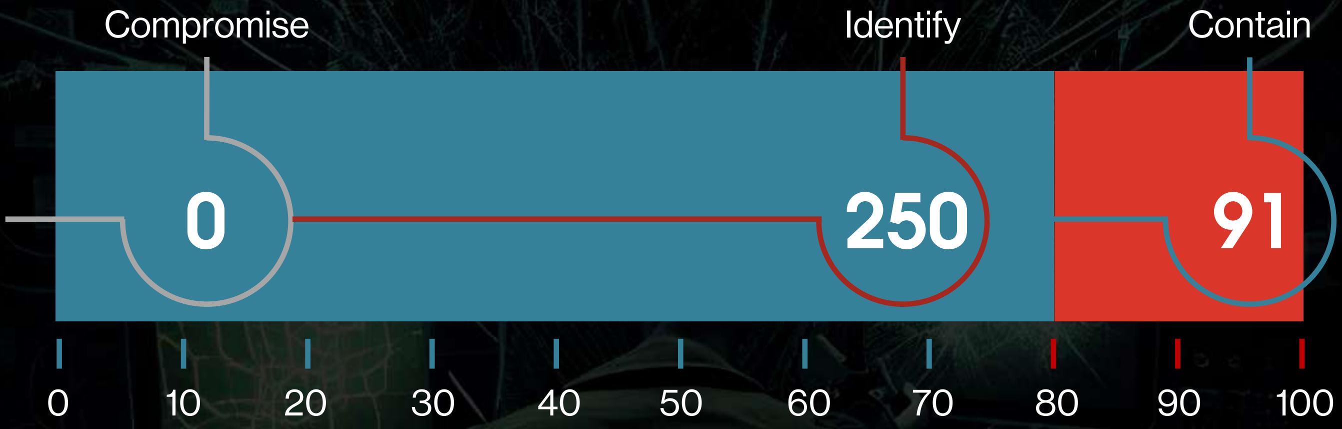
147% INCREASE IN ACCESS BROKER ADVERTISEMENTS ON DARK WEB

SMART CARD PIN, ACTIVE DIRECTORY CERTS, API/SECRET KEYS

PROPHET SPIDER AS PROLIFIC ACCESS BROKER

SCOURGE OF IDENTITY-BASED ATTACKS

IDENTITY IS AN ELEMENT OF THE VAST MAJORITY OF ALL INTRUSIONS



BREACHES CAUSED BY STOLEN CREDENTIALS TAKE 341 DAYS TO CONTAIN

IDENTITY-BASED AND SOCIAL ENGINEERING ATTACKS

Adversaries expanded beyond valid accounts

Also targeted API keys and secrets, session cookies and tokens, one-time passwords and Kerberos tickets

COZY BEAR

Conducted regular credential phishing using Microsoft Teams messages to solicit multifactor authentication tokens for Microsoft 365 accounts

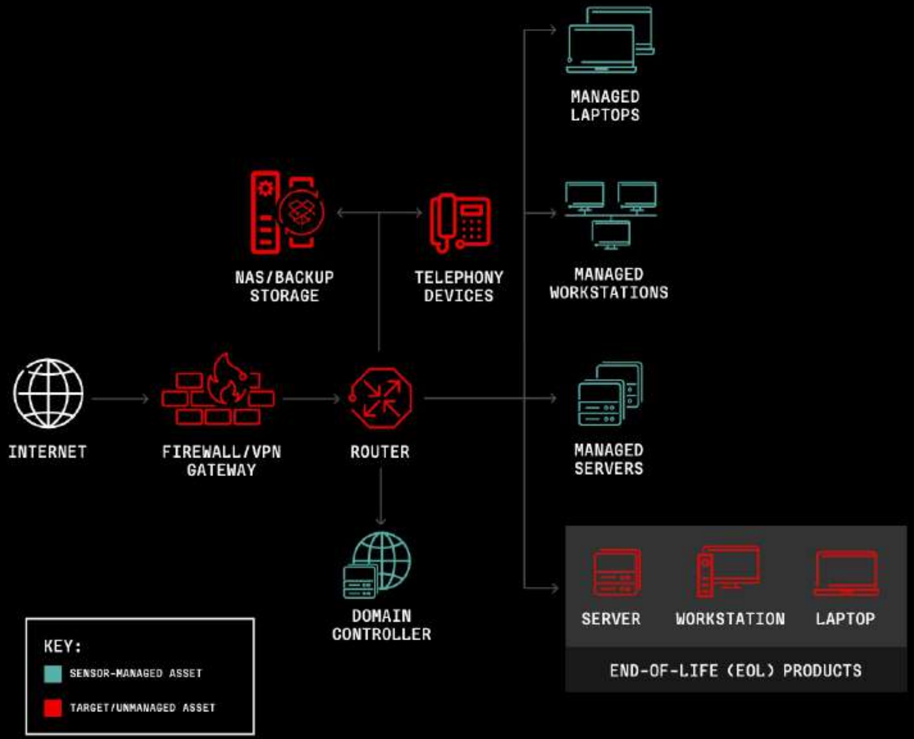
SCATTERED SPIDER

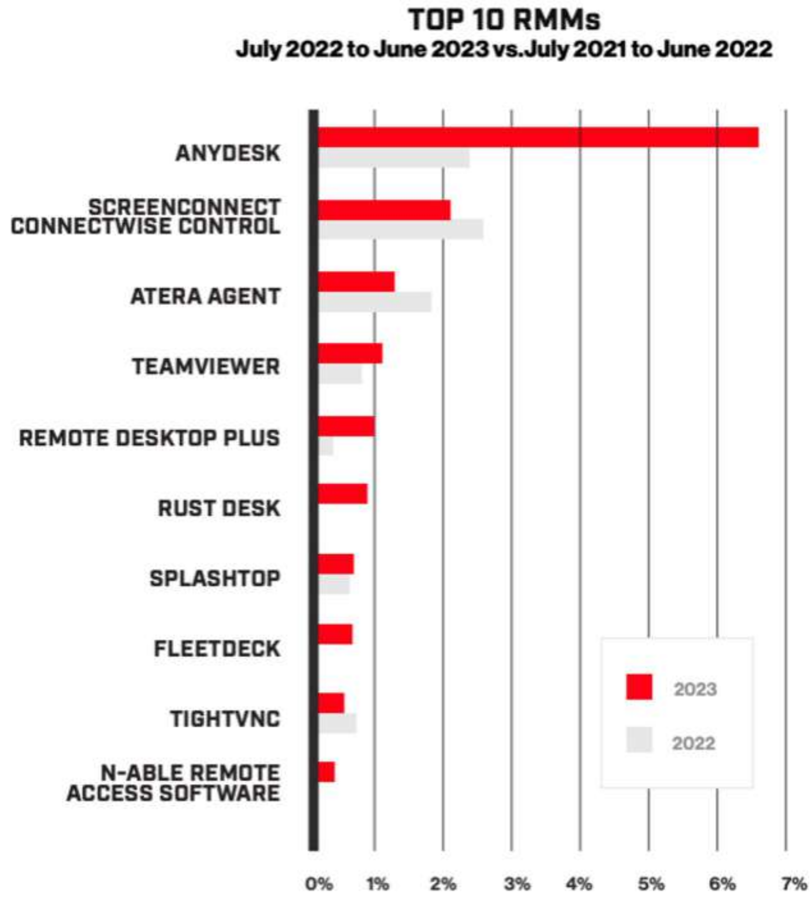
Conducted sophisticated social engineering campaigns

UNMANAGED NETWORK APPLIANCES – PARTICULARLY EDGE GATEWAY DEVICES – REMAINED THE MOST ROUTINELY OBSERVED INITIAL ACCESS VECTOR FOR EXPLOITATION DURING 2023.

THREAT ACTORS ARE ACTIVELY DEVELOPING EXPLOITS FOR EOL PRODUCTS THAT CANNOT BE PATCHED AND OFTEN DO NOT ALLOW FOR MODERN SENSOR DEPLOYMENT.

VULNERABILITY LANDSCAPE: "UNDER THE RADAR" EXPLOITATION





ABUSE OF LEGITIMATE ENTERPRISE TOOLS

REMOTE MONITORING & MANAGEMENT TOOLING

- 312% INCREASE IN ADVERSARY USE OF RMM TOOLING
- BLEND INTO ENTERPRISE NOISE TO AVOID DETECTION
- GAINED POPULARITY – FREE LICENSE, ROBUST GUI, PRIVELEGED ACCESS
- INCREASINGLY ADOPTED AS PERSISTENCE MECHANISM
- SCATTERED SPIDER EMPLOYS >20 RMM TOOLS FOR DIFFERENT TARGETS

eCrime Breakout Time

62 min

Every Second Counts

Adversaries are getting faster, defenders must accelerate

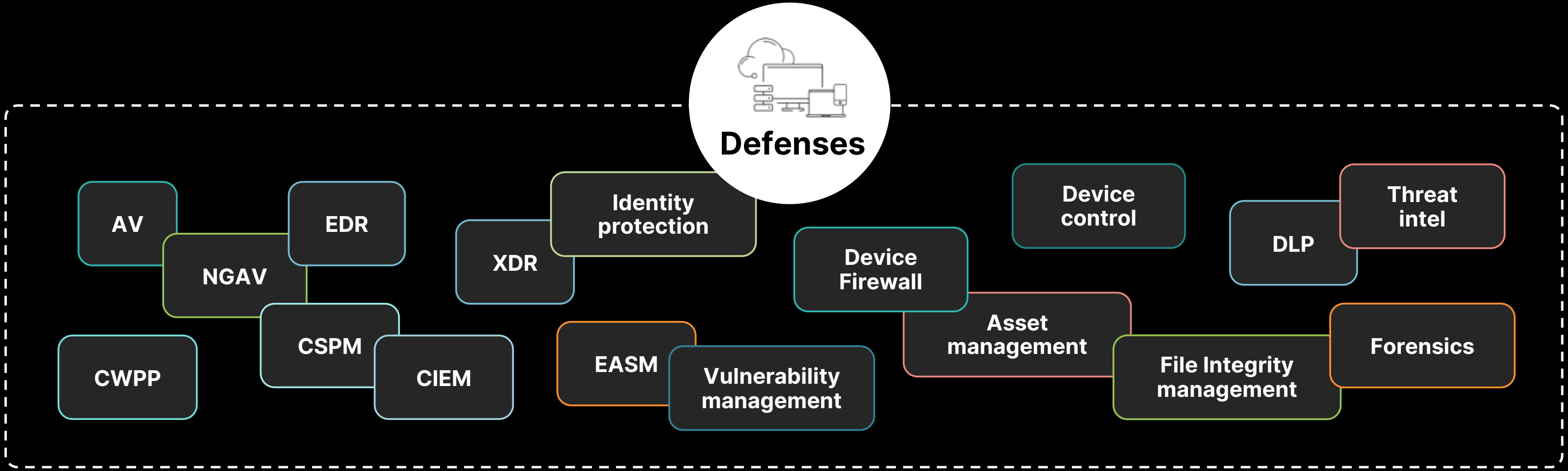
Breakout time dropped from

582 min in 2019 to **79 min** in 2022

79 min in 2022 to **62 min** in 2023

What is the PROBLEM

Adversaries Live in the Gaps Between Traditional Siloed Tools



Defenses

AV

EDR

NGAV

XDR

Identity protection

CSPM

CWPP

CIEM

EASM

Vulnerability management

Device Firewall

Device control

Asset management

DLP

Threat intel

File Integrity management

Forensics

▲ Cost

▲ Complexity

▼ Ease of **Deployment & operations**

What is NEEDED

Superior security outcomes

Continuous Validation
Highest detection & protection coverage

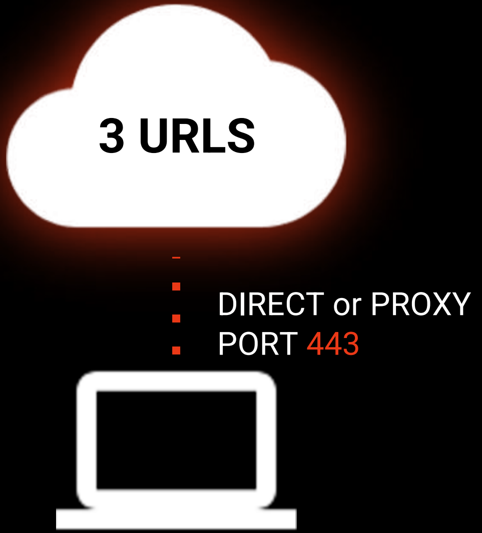
Reduce costs

Easy to deploy & manage
Zero reboots, no downtime, & no manual tuning

Consolidate point products

Eliminate agents
Unify standalone tools to cut complexity and sprawl

The Falcon Platform Architecture
Footprint & Communication



SUPPORTED PLATFORM(S)
WINDOWS | LINUX | MACOS
IOS | ANDROID | DOCKER |
KUBERNETES

LESS THAN
1% CPU

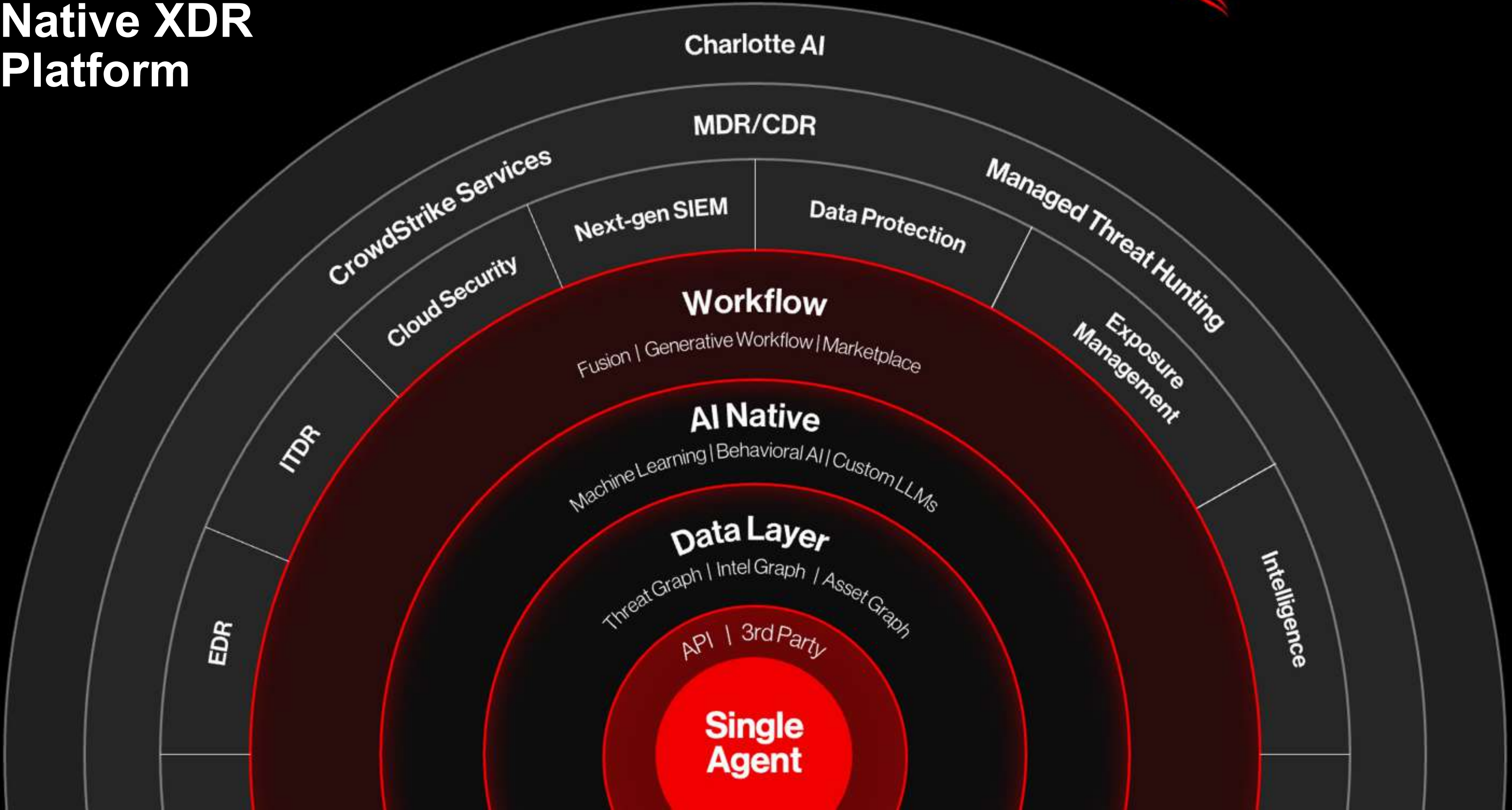
~155MB
MEMORY

~5MB-7MB
NETWORK
(DEVICE/DAY)

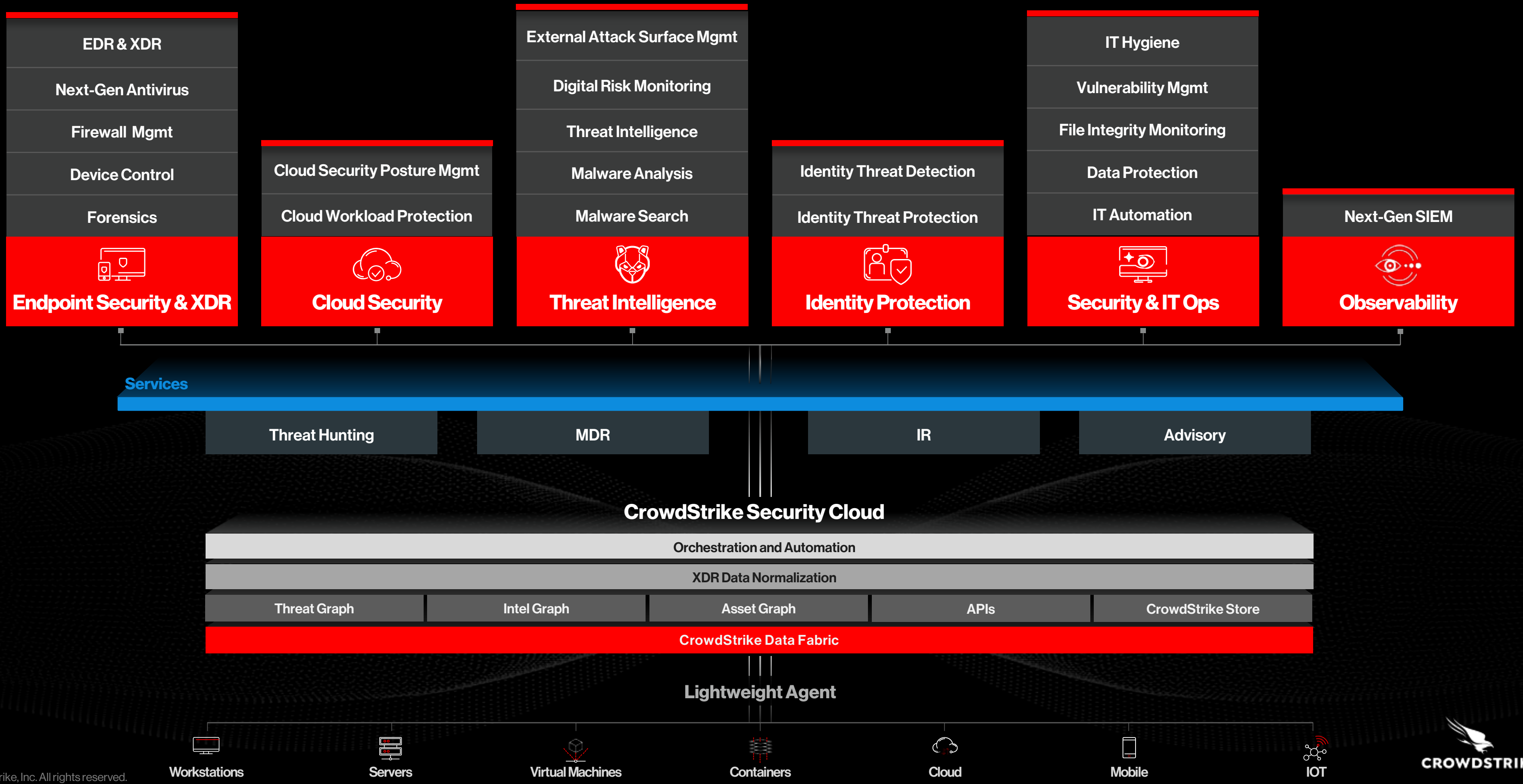
- Single Agent Architecture
- Native Cloud Management
- **No Reboot** Required
- Auto-Update Sensors
- No signatures updates
- No Scanning

Cybersecurity's AI-Native XDR Platform

CROWDSTRIKE



The Falcon Platform



Endpoint Security & XDR
- EDR & XDR
- Next-Gen Antivirus
- Firewall Mgmt
- Device Control
- Forensics

Cloud Security
- Cloud Security Posture Mgmt
- Cloud Workload Protection

Threat Intelligence
- External Attack Surface Mgmt
- Digital Risk Monitoring
- Threat Intelligence
- Malware Analysis
- Malware Search

Identity Protection
- Identity Threat Detection
- Identity Threat Protection

Security & IT Ops
- IT Hygiene
- Vulnerability Mgmt
- File Integrity Monitoring
- Data Protection
- IT Automation

Observability
- Next-Gen SIEM

Services
- Threat Hunting
- MDR
- IR
- Advisory

CrowdStrike Security Cloud
- Orchestration and Automation
- XDR Data Normalization
- Threat Graph | Intel Graph | Asset Graph | APIs | CrowdStrike Store
- CrowdStrike Data Fabric

Lightweight Agent
- Workstations
- Servers
- Virtual Machines
- Containers
- Cloud
- Mobile
- IOT

CROWDSTRIKE

Game-changing Security Outcomes

Reduce Patch Work
Attack Paths focus
on work that matters

Seconds to Investigate
Unified Enterprise
Asset + Threat Graph

Proactive Security

Active Protection

One Agent Everywhere

Minutes to Global Fix

Control Risk via Policy, RTR, Automations

Reduce Intrusion Noise

Less Noise for Security Operations

Falcon Identity Protection

Protect

See **like the adversary**; attack path visibility

Prevent

Detect **and** block, in real-time identity specific threats; dynamic policy

Enable

Verify only when the **risk changes**; frictionless conditional access

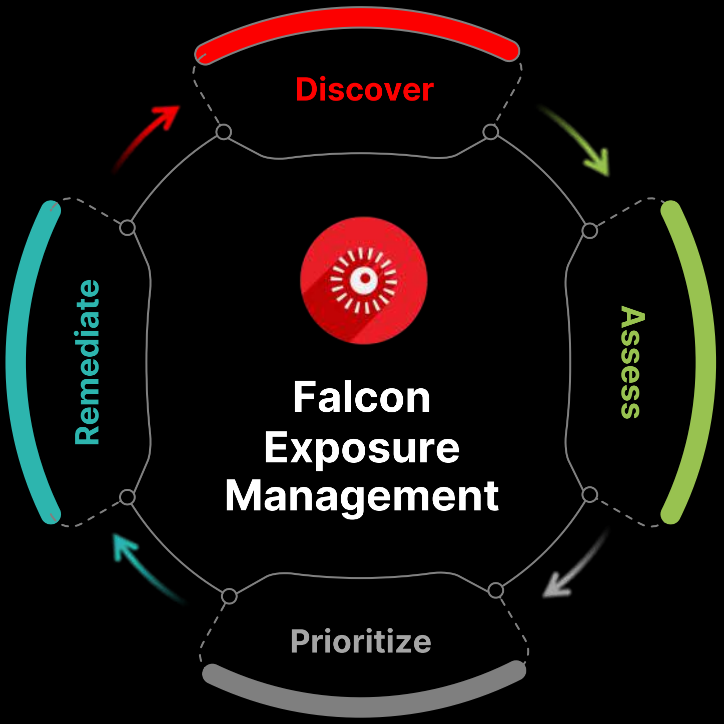
Falcon Identity + Endpoint Protection

Better Together Extending Your Protection and Investment

Improves Your Protection
at the endpoint and identity level
in a single solution

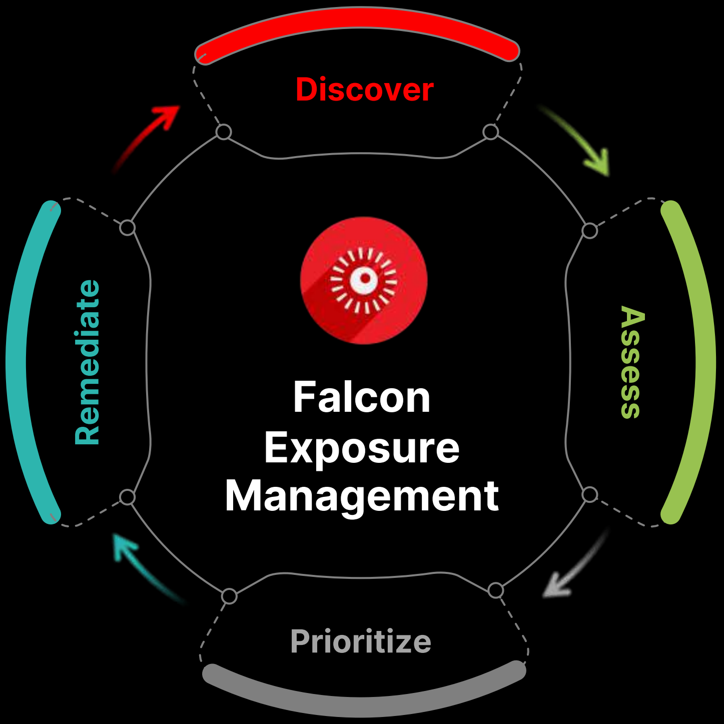
Reduces the Attack Surface
to help prevent lateral movement
across your network

Correlates Security
events across endpoints and identity
to provide real time, actionable insights



1	**Discover** **Instant visibility**	See and identify all assets from the inside-out and outside-in
2	**Assess** **Real-time exposure insight**	Know every weakness with no additional agents
3	**Prioritize** **Adversary-driven prioritization**	Real-world intrusion risk by likelihood of lateral movement
4	**Remediate** **Platform-based response**	Guided and automated response with RTR, SOAR and 3rd party integrations

CROWDSTRIKE



1
- Active Discovery NEW
- External Attack Surface NEW
- Passive Discovery
- Applications
- Accounts

2
- CIS Benchmark NEW
- 3rd Party Vulnerability Ingestion NEW
- Native Vulnerability Coverage
- EoL Software
- Software Misconfigurations

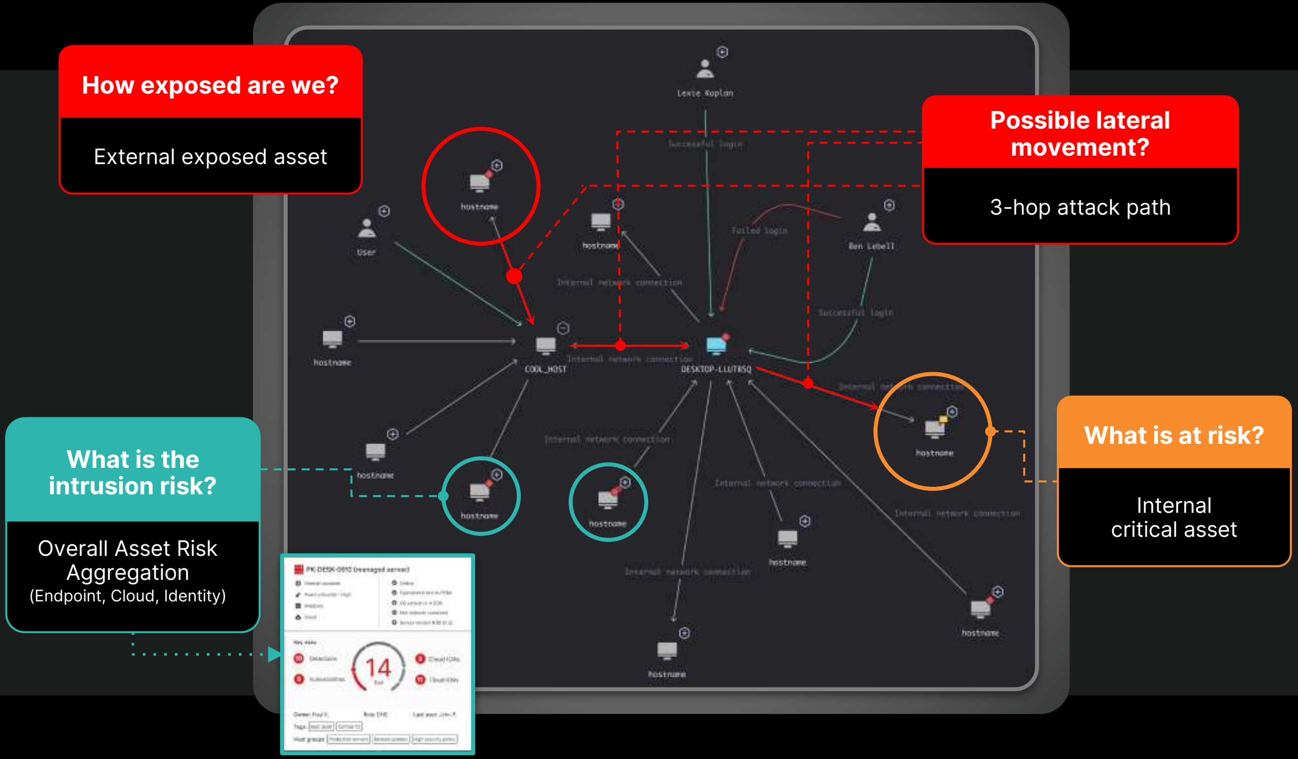
3
- Attack Path Analysis NEW
- Asset Criticality NEW
- Internet Exposure NEW
- ExPRT.AI Ratings
- Active Adversary Context

4
- Native SOAR Integration Falcon Fusion
- Real Time Response (RTR)
- Rule-based Policies
- Ticketing Integration
- Patching Integration

CROWDSTRIKE

Prioritize

Adversary-Driven Prioritization



How exposed are we?

External exposed asset

Possible lateral movement?

3-hop attack path

What is the intrusion risk?

Overall Asset Risk Aggregation
(Endpoint, Cloud, Identity)

What is at risk?

Internal critical asset

Visualize intrusion risk across endpoint, cloud and Identity assets

Understand lateral movement through critical hosts and user accounts

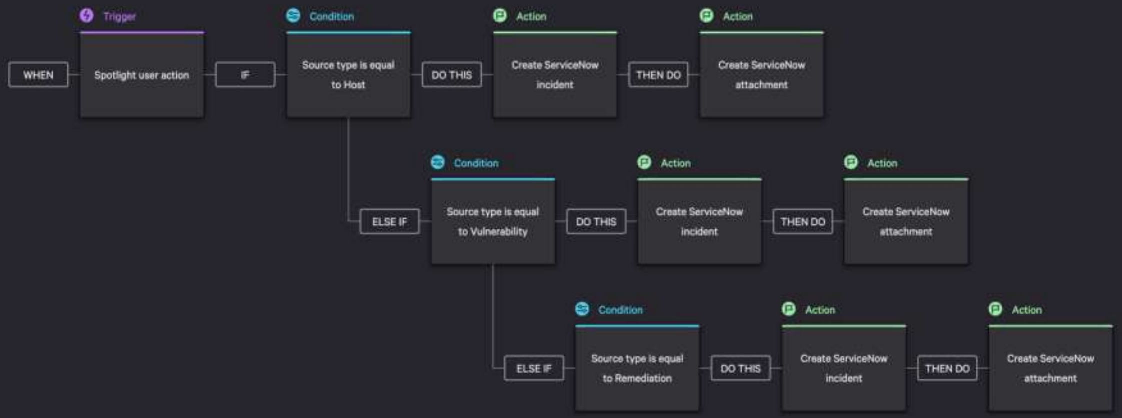
Fine-tune policies and respond with RTR (Real-Time Response) and Falcon® Fusion playbooks

Automatically unveil internet exposures

Remediate

Platform-based Response

Falcon® Fusion


Trigger
Condition
Action
Action
WHEN
Spotlight user action
IF
Source type is equal to Host
DO THIS
Create ServiceNow incident
THEN DO
Create ServiceNow attachment
Condition
Action
Action
ELSE IF
Source type is equal to Vulnerability
DO THIS
Create ServiceNow incident
THEN DO
Create ServiceNow attachment
Condition
Action
Action
ELSE IF
Source type is equal to Remediation
DO THIS
Create ServiceNow incident
THEN DO
Create ServiceNow attachment

Deploy emergency windows patches with one-click on managed systems and monitor the progress

Protect without patching by activating compensating controls directly on managed assets

Automated and Orchestrate playbooks with native SOAR Falcon Fusion

Guided remediation workflows across the Falcon® Platform and 3rd-party tools

Remedeiate

Delivering comprehensive compensating controls

Compute

- Kill Running Process
- Block File Execution
- Patchless Config Scripts

Network

- Close Ports
- Restrict IP
- Restrict DNS
- Restrict Network Storage

Identity

- Restrict Accounts
- Suspend Logins

Hardware

- Restrict USB devices
- Restrict Bluetooth

Replace Fragmented Point-solutions with CrowdStrike

Reduce Cost and Complexity with a Single Agent and Unified Console

CrowdStrike Falcon Platform

Endpoint	Cloud	Identity	SIEM	Threat Intel	MDR	Exposure Management
Microsoft	WIZ	Microsoft	splunk>	Recorded Future	ARCTIC WOLF	Qualys
SentinelOne	PRISMA BY PALO ALTO NETWORKS	SentinelOne	elastic	MANDIANT	expel	tenable
paloalto NETWORKS	Lacework	SILVERFORT	Chronicle	ZEROFOX	Secureworks	RAPID7
Trellix	aqua	semperis	sumo logic	digital shadows_ a ReliaQuest company	RELIAQUEST	censys
SOPHOS	orca security		securonix	INTEL471	red canary	CYCOGNITO
cybereason					SOPHOS	AXONIUS
TREND MICRO						
Symantec						
kaspersky						

CROWDSTRIKE

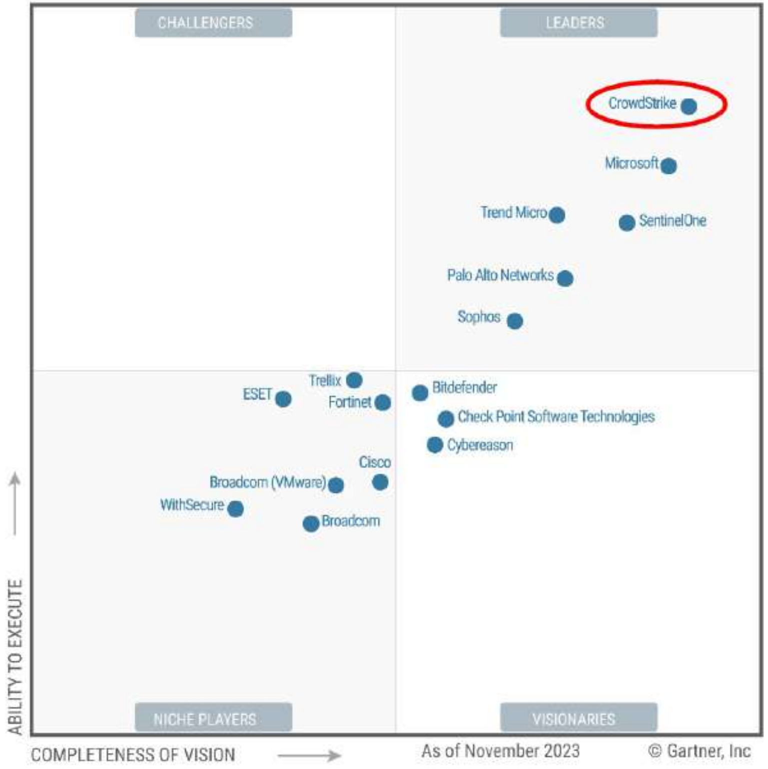
CrowdStrike is named A Leader in the 2023 Gartner® Magic Quadrant for Endpoint Protection Platforms

Positioned Highest on Ability to Execute and Furthest Right on Completeness of Vision

First time since 2018 for One Company to Lead on both Axes

Leader and Positioned Furthest Right on Completeness of Vision for the Fourth Consecutive Time

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (December 2023)

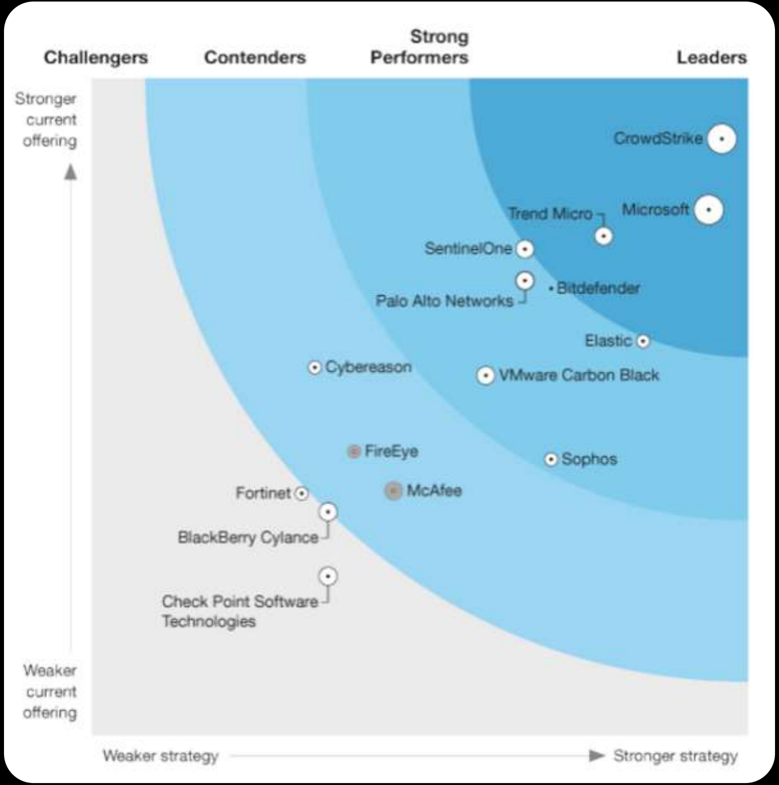
This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from CrowdStrike.

Third Consecutive Time as a Leader

Leading the EDR Market in Forrester's EDR Wave

> "CrowdStrike **dominates in EDR** while building its future in XDR and Zero Trust.

FORRESTER



The Forrester Wave™: Endpoint Detection And Response Providers, Q2 2022, April 6, 2022

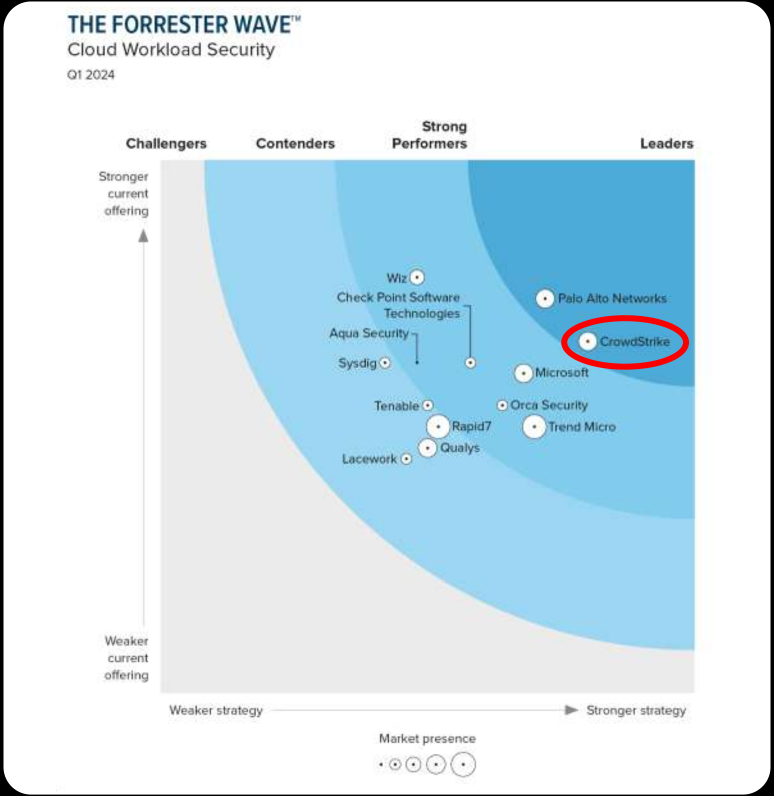
CROWDSTRIKE

CrowdStrike Named a Leader

The Forrester Wave™: Cloud Workload Security, Q1 2024

“Best position in the Strategy category and highest scores possible in the Innovation and Vision criteria

FORRESTER®



The Forrester Wave™: Cloud Workload Security, Q1 2024, January 30, 2024

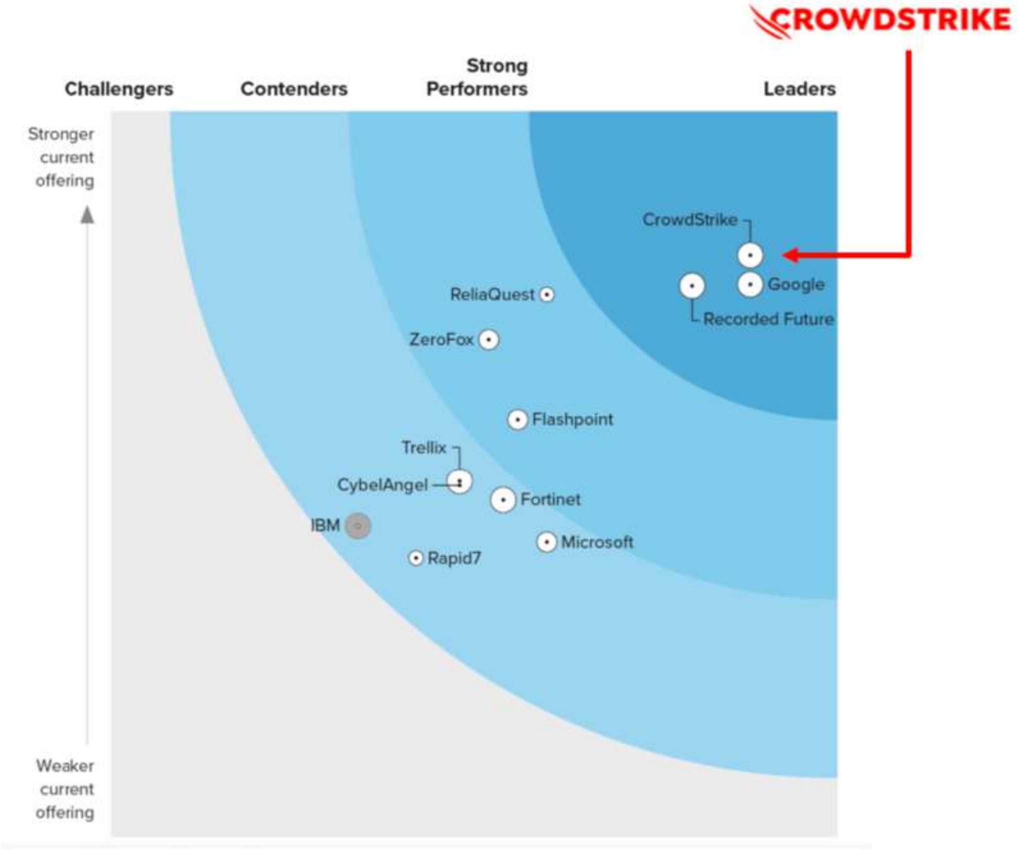
CROWDSTRIKE

Leading the Intel Market

Received highest score in Current Offering and top scores in 16 criteria, surpassing all other vendors

“CrowdStrike **delivers world-class** Threat Intelligence.”

FORRESTER



The Forrester Wave™:
External Threat Intelligence Service Providers, Q3 2023

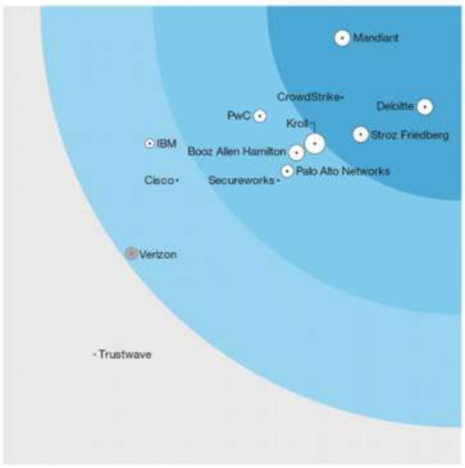
CROWDSTRIKE

Who are we?

A leading

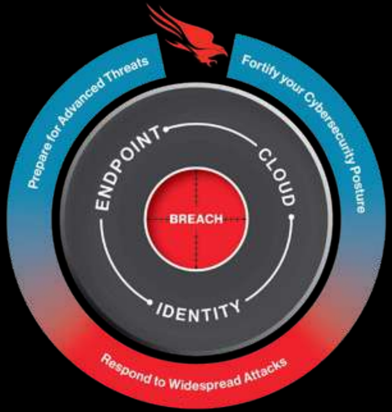
Digital Forensics and Incident Response

firm



Forrester Wave 2022
Cybersecurity Incident Response Services

CrowdStrike Professional Services



Prepare for Advanced Threats
Fortify your Cybersecurity Posture
Respond to Widespread Attacks
ENDPOINT
CLOUD
IDENTITY
BREACH

Respond

Incident Response
Forensic Investigation
Endpoint Recovery
Compromise Assessment
Adversary Exposure Assessment
Network Detections

CrowdStrike Incident Response Services

More than a decade of experience in breach response and investigations

"The team assembled for our forensic assessment engagement was outstanding. From project management to technical engagement, everyone was exceptional."

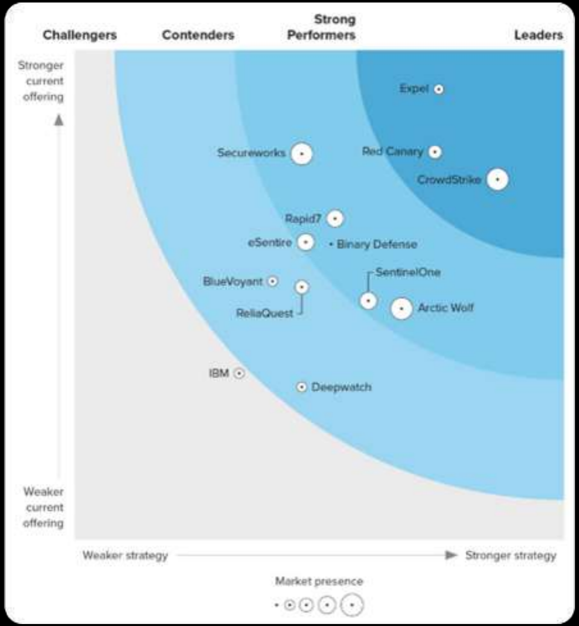
Getting our clients back to business faster with minimal business disruption

Second Consecutive Time as a Leader

> “CrowdStrike delivers **an exceptional MDR service**... blends products, platforms and services seamlessly for customers.

FORRESTER®

The Forrester Wave™: Managed Detection And Response, Q2 2023



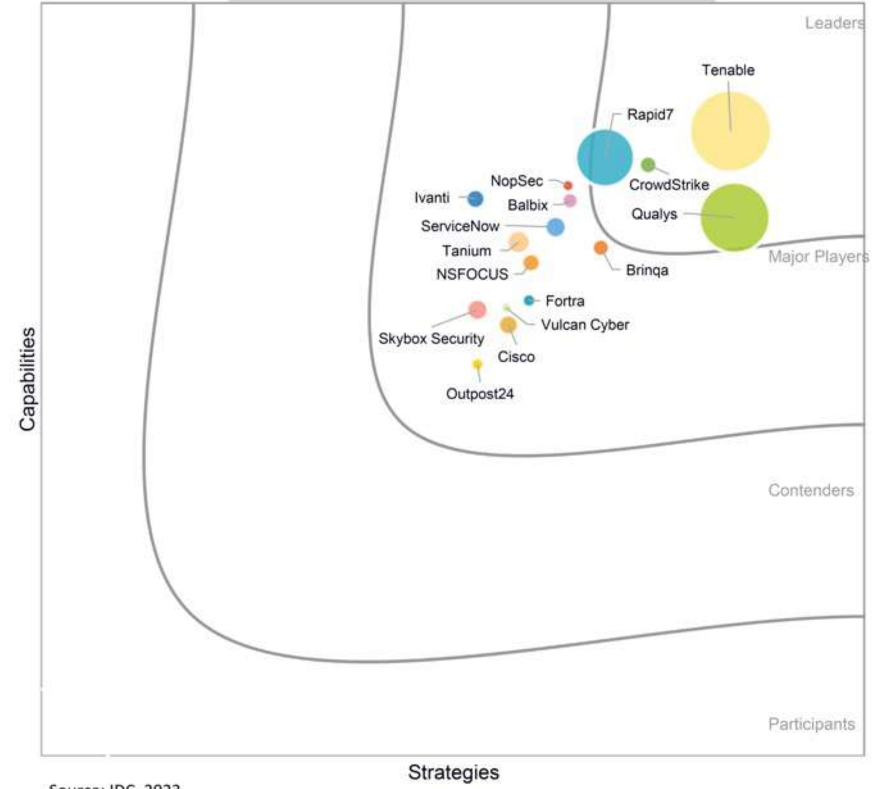
CROWDSTRIKE

CROWDSTRIKE

CROWDSTRIKE NAMED A LEADER

2023 IDC MarketScape for Risk-Based Vulnerability Management Software

IDC MarketScape Worldwide Risk-Based Vulnerability Management Platforms, 2023



Source: IDC, 2023

CROWDSTRIKE

Conclusion

5 STEPS TO BE PREPARED

1 Identity Protection

2 Effective Cloud Security

3 Cross-Domain Visibility

4 Speed: Outpace the Adversary

5 Practice Makes Perfect

TOWARDS ROBUST & PROACTIVE SECURITY

COMPREHENSIVE VISIBILITY

ATTACK SURFACE
ASSET DISCOVERY
ATTACK PATHS

SECURE CROWN JEWELS

ENDPOINTS
WORKLOADS
IDENTITIES

THREAT HUNTING

24/7/365
HUMAN-BASED
& AT SCALE

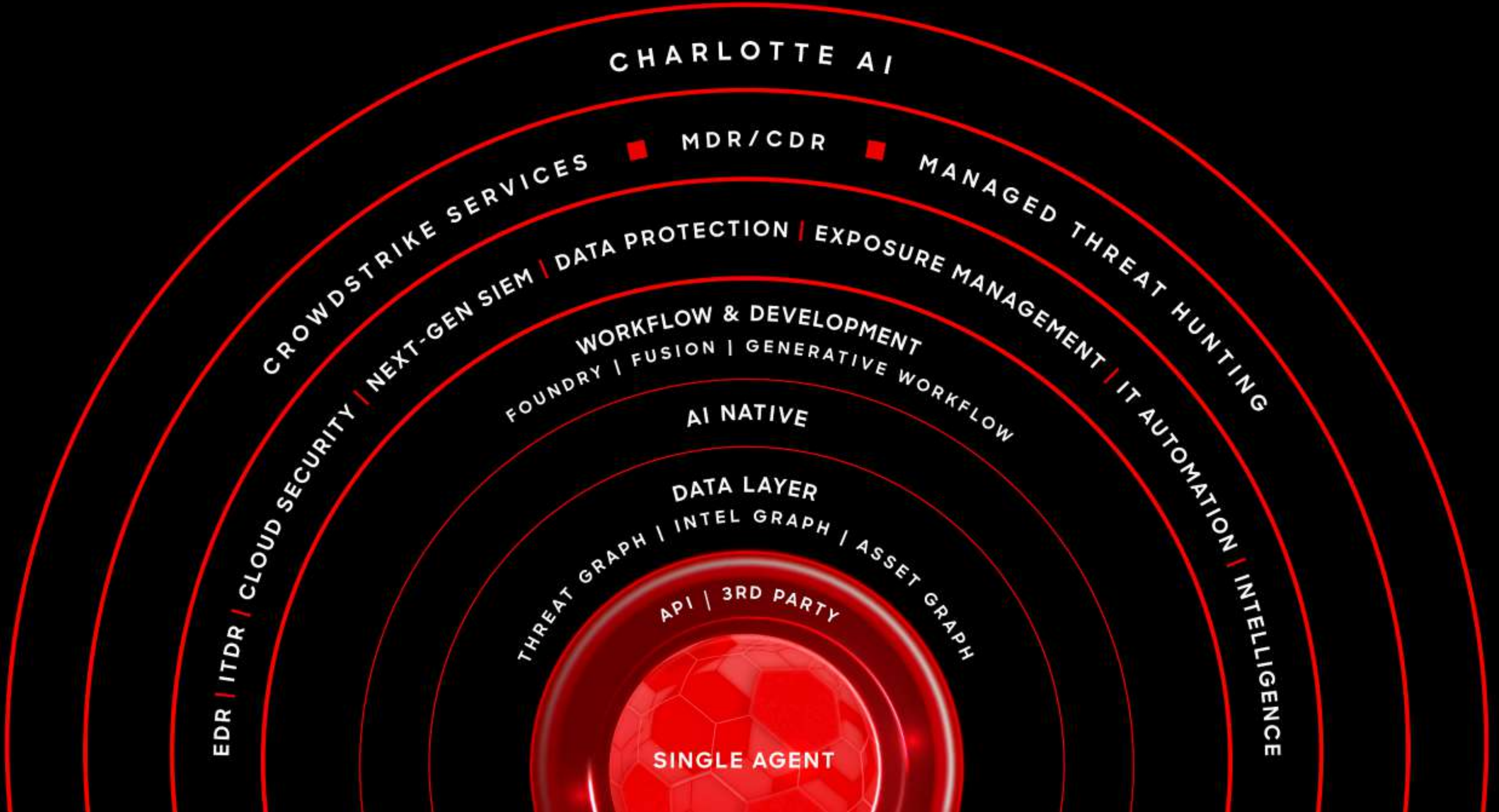
INTELLIGENCE ADOPTION

ENRICHMENT
THREAT MODEL
DDW MONITORING

SECURITY AWARENESS

EDUCATION
SIMULATION
PREPAREDNESS

CROWDSTRIKE'S FALCON XDR PLATFORM STOPS BREACHES


CHARLOTTE AI
CROWDSTRIKE SERVICES ■ MDR/CDR ■ MANAGED THREAT HUNTING
EDR | ITDR | CLOUD SECURITY | NEXT-GEN SIEM | DATA PROTECTION | EXPOSURE MANAGEMENT | IT AUTOMATION | INTELLIGENCE
WORKFLOW & DEVELOPMENT
FOUNDRY | FUSION | GENERATIVE WORKFLOW
AI NATIVE
DATA LAYER
THREAT GRAPH | INTEL GRAPH | ASSET GRAPH
API | 3RD PARTY
SINGLE AGENT