



# CrowdStrike Endpoint Security



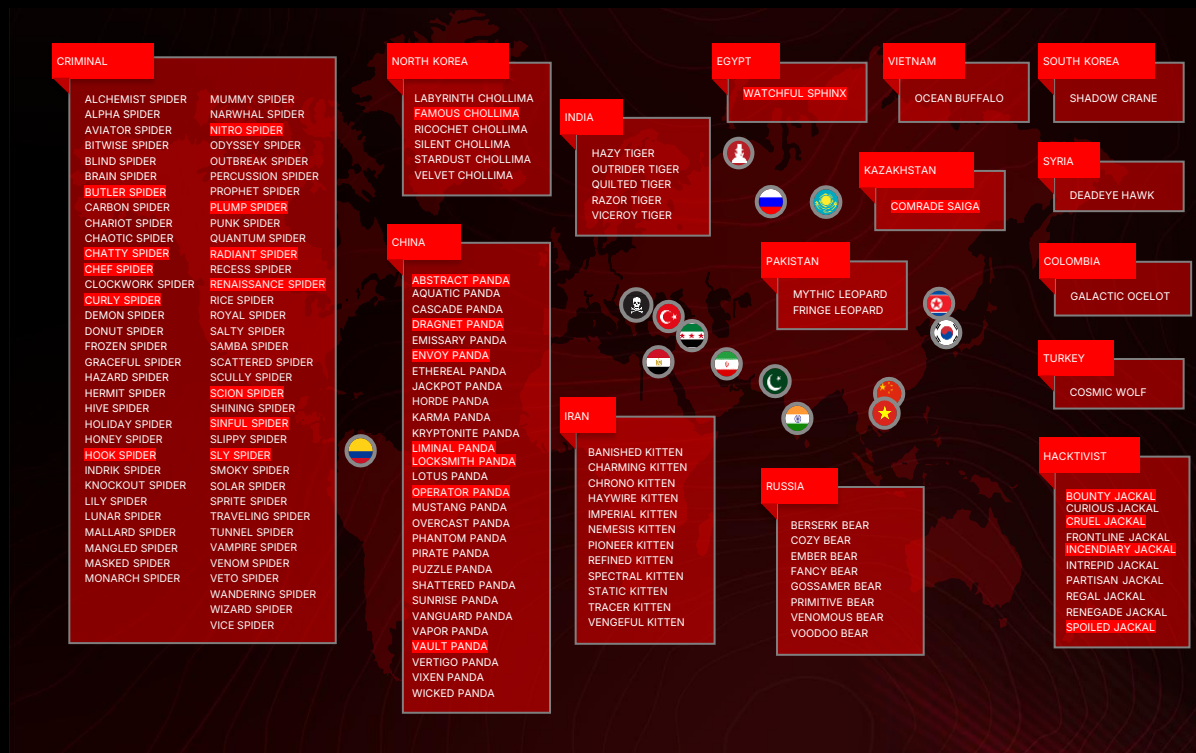
# Global Adversaries

The growing threat actor landscape

26 New Adversaries

257 Total Tracked

140+ Malicious Activity Clusters



# Threat Landscape **by the Numbers**

## INITIAL ACCESS

**442%**

Increase in voice phishing (vishing) between the first and second half of 2024

**50%**

Increase in access broker advertisements in 2024

**52%**

Of vulnerabilities observed by CrowdStrike in 2024 were related to initial access

## LATERAL MOVEMENT

**51s**

Fastest breakout time in 2024

## STEALTH

**79%**

Of detections in 2024 were malware-free



ADVERSARY PROFILE:

# PUNK SPIDER

Objective  
**Financial Gain**

Motivation  
**Criminal**

Type  
**eCrime**

## **Legitimate Tool Abuse**

Uses legit software and open-source tools

## **Privilege Escalation**

Copies privileges to new or compromised accounts

## **Lateral Movement**

Pivots across systems to evade detection

## **Data Exfiltration**

Steals user and group data for later use

## **Ransomware**

Deploys ransomware to extort victims

**Adversaries are faster and more evasive.**  
Your endpoints are the critical attack vector.

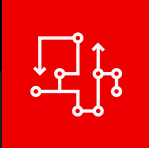
# Outdated Defenses Can't Stop Modern Threats



Outdated Security Approaches



Limited Visibility and Coverage Gaps



Complex, Heavy, Hard to Operate





# CrowdStrike's Modern Endpoint Approach

Unmatched protection.  
Unrivaled security.  
Proven results.



## One Agent. One Platform.

Protect endpoints, identities, and workloads.



## Instant Coverage. Immediate Value.

Fast, frictionless protection from Day One.



## Smarter Detection. Modern Protection.

AI-powered detection for stealthy threats.



## Intelligence-Fueled. Continuously Informed.

Adversary-driven intelligence for critical threat context.



## CrowdStrike® Charlotte AI™. Real-Time Answers.

Accelerate security operations with an AI security analyst.

# Deploy with Ease, Defend with Confidence

Delivered via one agent

## Falcon Platform

- ✓ Easy to install and manage
- ✓ Extends across on-premises, hybrid, and cloud
- ✓ AI-powered platform
- ✓ Cloud-native interface
- ✓ Simple and unified management

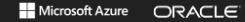
### Clouds



Data Centers



Workloads



Containers

Servers

### Endpoints



Workstations



Mobile Devices



Servers



IoT Devices



ChromeOS

### Identities



Active Directory  
Entra ID  
Okta



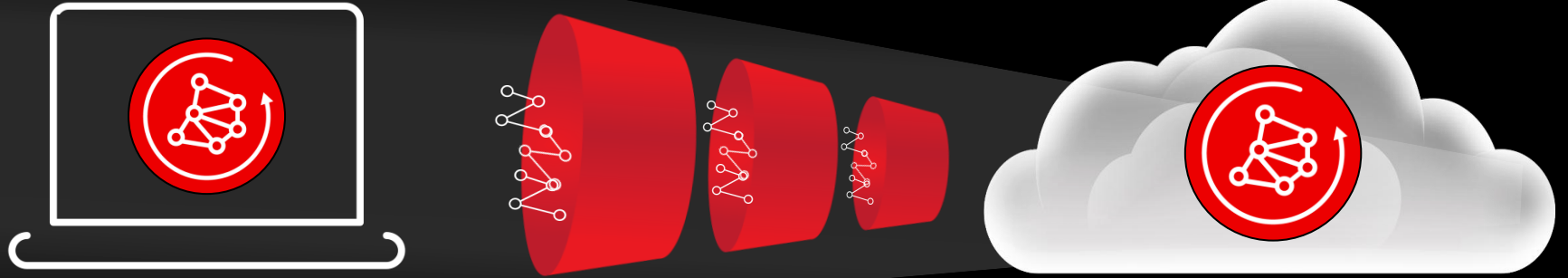
Human and  
Service  
Accounts



Third Parties

# AI-Native Prevention and Detection

From the sensor to the cloud



## On the sensor

Sensor ML

*Core models for inline malware prevention*



## In the cloud

AI-Powered Indicators of Attack  
*Advanced behavioral IOAs plus cloud ML for high-fidelity detection*

Cloud ML

*Wide array of models run at cloud scale*

# Integrated Threat Intelligence. Superior Endpoint Protection.

## Collect

Trillions  
of events per week

## Enrich

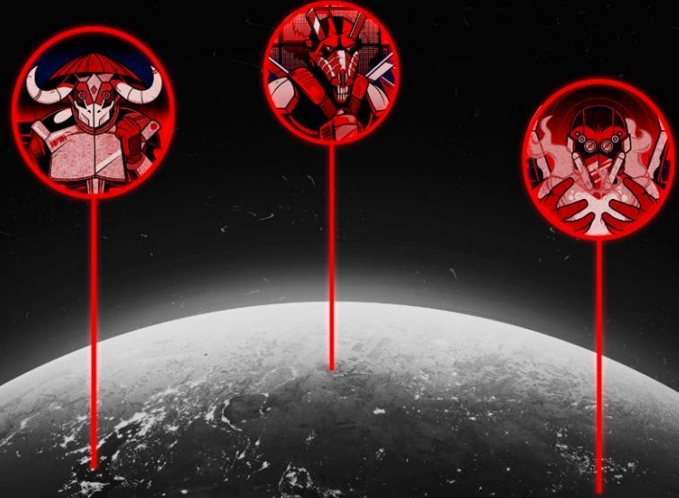
257  
global adversaries tracked

## Evolve

800K+ Indicators of Compromise (IOCs)  
published per week

## Protect

180M+  
IOA decisions per second



FORRESTER®

**#1 in Intelligence Collection**

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

*Figures from the Falcon platform, CrowdStrike 2024 Threat Hunting Report and  
CrowdStrike 2025 Global Threat Report.*

# Unified Cross-Domain Detection and Protection

How are endpoint detections related?

Connect endpoint detections

Are identities compromised?

Integrated identity events

Accelerate security operations across the Falcon platform

Find answers faster with generative AI

Investigate incidents with Charlotte AI

Take immediate action

Leverage integrated native response actions

Where are adversaries attacking?

Know your adversary

Rapid investigation

Instantly pivot from detections to search with easy AI-powered workflows

Complete understanding

Visualize the full attack path and explore other potentially impacted hosts

Full context

Get an integrated view with all related threat intel, context, and artifact relationships

10GB per day of free third-party data ingest

# Powering the Next Evolution of the SOC

Transcends “ask-and-respond” copilots with autonomous reasoning and action across the SOC

✓ **EXPERT-GRADE PRECISION**  
**> 98%**  
Accuracy in autonomous triage

✓ **COMPOUNDING TIME SAVINGS**  
**40+ hours**  
Avg. analyst hours reclaimed weekly


✓ **AUTONOMOUS ACTION**  
**Round the clock**  
Drive outcomes around the clock

**CHARLOTTE AI**  
**DETECTION TRIAGE**  
*Autonomous, cross-domain triage*




- Consistently triage with expert-level precision
- Offload manual triage and surface only what matters

**CHARLOTTE AI**  
**AGENTIC RESPONSE**  
*AI-guided investigations*



- Apply front-line expertise to every investigation
- Accelerate analyst decisions with faster, richer context

**CHARLOTTE AI**  
**AGENTIC WORKFLOWS**  
*LLM-powered SOAR*



- Adapt seamlessly to edge cases and unknowns
- Tailor outputs to fit any team, audience, or mission

Accuracy rating is a measure of Charlotte AI triage decisions that match the expert decisions from the CrowdStrike Falcon Complete Next-Gen MDR team. Time savings represents the amount of time an analyst would have spent triaging detections but can now use that time for other skilled work while Charlotte triages the detections. Individual results may vary based on factors such as total alert volume.

# CrowdStrike Named a Leader

2025 Gartner® Magic Quadrant™ for  
Endpoint Protection Platforms

Positioned **Furthest Right** for  
Completeness of Vision and  
**Highest** in Ability to Execute

Gartner®

Gartner, 2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms (EPP), Evgeny Mirolyubov, Franz Hinner, and Deepak Mishra, July 14, 2025.

GARTNER is a registered trademark and service mark of Gartner and Magic Quadrant™ is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

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 research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

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.

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Gartner®

# Unmatched Innovation. Unparalleled Protection.

## Proven Leadership.

### Tested

**100%** total accuracy

2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test

**100%** ransomware protection

2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test

### Trusted

By more than **74,000** direct and MSSP end customers worldwide

### Validated

Leader in:

Forrester Wave for XDR

Forrester Wave for Endpoint

GigaOm Radar for XDR

GigaOm Radar for Ransomware

*Named a Leader in The Forrester Wave: Extended Detection And Response Platforms, Q2 2024*

*Named a Leader in The Forrester Wave: Endpoint Security, Q4 2023*

*Named a Leader in the 2025 GigaOm Radar for Extended Detection and Response*

*Named a Leader in the 2024 GigaOm Radar for Ransomware Prevention*

# You Don't Have to Do It Alone

## Augment your team with world-class experts



### Managed detection and response

Full 24/7/365 management  
or team augmentation



### Managed threat hunting

Proactively uncover hidden,  
sophisticated attacks with AI  
and human expertise



### Incident response and advisory

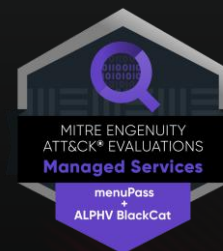
Pre-breach hardening and post-breach  
response with world-class experts

## 2024 MITRE Engenuity ATT&CK® Evaluations: Managed Services, Round 2

**4 min** Mean time to detect  
(MTTD)



Comprehensive  
detection coverage and  
rapid threat detection





# Thank You

# Appendix

# CROWDSTRIKE'S AI-NATIVE PLATFORM STOPS BREACHES



# Endpoint Adversary



ADVERSARY PROFILE:

# PUNK SPIDER

Objective  
**Financial Gain**

Motivation  
**Criminal**

Type  
**eCrime**

## **Legitimate Tool Abuse**

Uses legit software and open-source tools

## **Privilege Escalation**

Copies privileges to new or compromised accounts

## **Lateral Movement**

Pivots across systems to evade detection

## **Data Exfiltration**

Steals user and group data for later use

## **Ransomware**

Deploys ransomware to extort victims



# PUNK SPIDER: Attempted Data Exfil and Ransomware Deployment

Target: North American technology company

Attack Sequence

## Initial Access

Exploited CVE-2024-3400 on an unmanaged Palo Alto GlobalProtect VPN appliance to gain access using compromised credentials



## Lateral Movement

Used Remote Desktop Protocol (RDP) with a service account to move to another internal system



## Credential Access

Attempted to dump credentials and escalate privileges by adding users to local and ESX Admins groups



## Persistence and Defense Evasion

Attempted to deploy proxy-tunneling and remote access tools



## Reconnaissance

Used SharpShares and Invoke-ShareFinder.ps1 to enumerate network shares



## Collection and Impact

Used WinRAR to archive data and attempted exfiltration via FileZilla. Final step: Akira ransomware deployment attempt



Data exfiltration  
Ransomware



# PUNK SPIDER: Attempted Data Exfil and Ransomware

## Deployment

Outcome: Fully blocked by Falcon sensor and Falcon Adversary OverWatch detection  
Target: North American technology company

Attack Sequence

### Initial Access

Exploited CVE-2024-3400 on an unmanaged Palo Alto GlobalProtect VPN appliance to gain access using compromised credentials



VPN appliance was unmanaged (i.e., no Falcon sensor was installed).

### Lateral Movement

Used Remote Desktop Protocol (RDP) with a service account to move to another internal system



Initial Falcon detection. Activity was also detected by Falcon Adversary OverWatch.

### Credential Access

Attempted to dump credentials and escalate privileges by adding users to local and ESX Admins groups



Falcon sensor blocked the privilege escalation attempts.

### Persistence and Defense Evasion

Attempted to deploy proxy-tunneling and remote access tools



Falcon sensor blocked the execution of these tools, preventing persistence mechanisms from taking hold.

### Reconnaissance

Used SharpShares and Invoke-ShareFinder.ps1 to enumerate network shares



Falcon sensor prevented both reconnaissance tools from executing. Activity was also detected by Falcon Adversary OverWatch.

### Collection and Impact

Used WinRAR to archive data and attempted exfiltration via FileZilla. Final step: Akira ransomware deployment attempt



Falcon Adversary OverWatch detected FileZilla being used to exfiltrate data and notified the customer, who immediately contained the host. Akira ransomware was also blocked by Falcon before any encryption could occur.

# Key Capabilities

# Automated Leads

## Powered by CrowdStrike® Signal

The screenshot displays the CrowdStrike Signal interface for automated leads. At the top, there are navigation tabs for 'Detections', 'Automated leads' (which is selected), 'Cases', and 'Incidents'. Below the tabs, it shows '18 results (18 total)'. A filter bar includes 'Confidence', 'Assigned to', 'Status', 'Tags', 'Add/remove filters +', and 'Clear all'. A 'List is up to date' indicator is present, along with a 'Sort by Confidence: Highest to lowest' dropdown and a refresh icon. The main table has columns for 'Confidence', 'Detections', 'Name', 'Hosts', 'Start time', 'Last activity', 'Assigned to', 'Type', 'Resolution', and 'Status'. The first row shows a lead with a confidence of 100/100, 30 total detections, and a name 'XDR-STH-WIN10-2 at 2025-07-11T14:37:52Z'. Below the table, a detailed view of the selected lead is shown, including a 'Lead actions' dropdown. The detailed view contains a list of behaviors: 'An unusual process accessed lsass. This might indicate an attempt to dump credentials. Investigate the process tree.', 'A process gathered information about one or more system users. Adversaries can use this to guide future behaviors. Review the process tree.', and 'A process has scheduled an unusual task. Some malware schedules tasks to maintain persistence. If this task unexpected, review it.' There is also a 'Show more' link and a 'History' section with a small bar chart showing a single data point at the time of the lead.

Uses AI to surface stealthy threats others often miss

Catches threats early, spotting trouble before it escalates

Adapts to your environment making leads uniquely relevant

# Automated Leads

powered by CrowdStrike® Signal



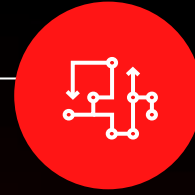
## Simpler Detection

- **AI-powered** starting point for investigations
- **Prioritizes** automated leads to accelerate triage



## Earlier Detection

- **Elevates** subtle early indicators of an attack
- **Uncovers** early-stage threats before they cause significant harm



## Adaptive Detection

- **Automatically** adapts to your environment
- **Ensures** automated leads are relevant and actionable

# Track and Stop the Adversary with Complete Visibility



## See More

Deep endpoint visibility across your enterprise to reveal the full scope of attacks



## Know More

Critical adversary-driven threat intelligence and real-time analyst collaboration



## Do More

Instant response with automated SOAR workflows from a unified command console

## Key native telemetry for cross-domain visibility



Endpoint



Identity



Cloud



Mobile



Data

# Interactive Workbench

Reduce time to contain and time to remediate



## Centralized Investigations

Interactive graph view to support hunting and investigation workflows without having to leave the console



## Collaborative Command Center

Support for real-time, multi-user collaboration; tagging analysts; and adding notes and inputs to entities or cases



## Enrichment and Remediation

Built-in automated enrichment and remediation options to run workflows and playbooks

# All Falcon Insight XDR Customers: 10GB per day of free third-party data ingest



Falcon  
Platform

100+

one-click connectors  
with parsers

## Robust Partner Ecosystem

ExtraHop

mimecast

zscaler

PingIdentity

CLOUDFLARE

VECTRA

MENLO  
SECURITY

okta

FORGEROCK

Skyhigh  
Security

proofpoint

CISCO

corelight

FORTINET

THREAT  
WARRIOR

servicenow

CLAROTY

Google Cloud

ARMIS

Abnormal

netskope

Cribl

zeek


# Charlotte AI

## From GenAI assistance to agentic operations

Streamline hands-on investigations  
**WITH EMBEDDED GENAI**

Get fast answers to plain questions  
**WITH CONVERSATIONAL AI**

Automate complex tasks  
**WITH AGENTIC AI**

 **mimikatz.exe on BILK-DUCK-USR1 by natasha**  
2025-04-17T03:37:59.441Z

**Detection description:**  
A process appears to be launching mimikatz, a password dumping utility. mimikatz's primary purpose is to steal passwords. If credentials were dumped, change your passwords and investigate further.

**Triage verdict from Charlotte AI:**  
The detection was labeled as a true positive because it involves the execution of "mimikatz.exe" with specific commands aimed at extracting sensitive information from the system. Mimikatz is a well known post exploitation tool used by attackers to dump credentials from memory, escalate privileges, and perform other malicious activities. The command line "mimikatz.exe \"/>


There were no authentication events found on the host "BILK-DUCK-USR1" (agent ID a31dde9bf8d745b4b2d290d6c32d0592, domain workshop.bilk-duck.cs-labs.net) over the past seven days, from 2025-04-10 to...

What network connections were established within 15 minutes after the mimikatz execution?

What network connections were initiated by processes such as PowerShell after the detection?

Using LogScale, what processes initiated on the host within 15 minutes around the detection had parent processes such as explorer.exe, cmd.exe, or powershell.exe?

Using LogScale, did the user 'natasha' initiate remote login events to other hosts within 15 minutes after the detection?

 Curating the questions to select the best lead

# Charlotte AI Agentic Workflows for Endpoint Security

Automate the analysis of datasets to conduct evaluations, send reports, translate outputs, etc.

## PowerShell Command Triage

“Triage all encoded PowerShell commands run in the last 24 hours and send a report for anything suspicious”

## RDP Impossible Travel Detection

“Examine RDP activity over the past week and send a report showcasing any impossible travel”

## Executive Security Reporting

“Produce an executive summary of security detections in the past week as compared to the previous week, and output the summary as a PDF to a Slack channel”

## Multilingual Alert Summarization

“Summarize any critical severity alerts from host groups A, B, and C, and send the summary in Brazilian Portuguese”

# Case Studies

## Case Study



### Coventry University Achieves First-Class Results with Enhanced Endpoint Security Strategy



Improved incident  
response time



Eliminated endpoint  
reimaging



Freed up IT resources

### Challenge

- Struggled with a reactive and inefficient approach to endpoint security that was unable to keep up with a fast-changing threat landscape
- Faced difficulty securing a diverse and globally distributed IT environment, including remote and hybrid setups
- Had a time-consuming incident response process

### Solution

- Deployed multiple Falcon platform modules, including Falcon Prevent (NGAV), Falcon Insight XDR, and Falcon Complete Next-Gen MDR
- Consolidated security operations into a single-agent, cloud-native platform
- Dramatically reduced time to respond and recover

### Key Results

**94% decrease**

In time spent resolving threats

**2-3 days to < 1 hour**

Average time to resolve security incidents

**"The visibility we have now is a powerful asset in keeping the university secure. We're able to use the detailed reports to show our senior management team threat and risk levels across the entire environment."**

— Steve Rogers, Enterprise Cloud, Infrastructure, and Security Architect

## Case Study



### Pegasystems Consolidates Endpoint, Identity, and Cloud Security with CrowdStrike

- ✓ Unified security visibility with one platform
- ✓ Simplified operations
- ✓ 24/7 managed detection and response

#### Challenge

- Needed to consolidate fragmented security tools that lacked integration
- Required a way to protect identities, cloud workloads, and endpoints under a unified strategy
- Faced gaps in detecting compromised credentials and lateral movement

#### Solution

- Deployed the Falcon platform to integrate endpoint, identity, and cloud security in a single solution
- Gained real-time visibility into service accounts, admin misuse, and compromised credentials
- Streamlined security operations with a single-agent, cloud-native architecture

#### Key Results

**100%**

Malware detection rate during POC

**Rapid deployment**

Across 5,000 endpoints and 6,000 servers

**"[Deploying] CrowdStrike EDR and identity protection from the same platform and sensor saves us time while closing security gaps."**

— Steve Tieland,  
Director of Corporate Security Operations

## Case Study



### From Endpoint to Cloud, CoreWeave Consolidates Security Stack with CrowdStrike

- ✓ Zero performance impact
- ✓ Scalable, unified security
- ✓ Improved attack surface visibility

#### Challenge

- Needed to secure a rapidly scaling cloud infrastructure supporting high-performance computing workloads
- Faced increased threat complexity and volume while expanding service offering
- Required strong visibility and control across endpoints and workloads without sacrificing performance

#### Solution

- Deployed the Falcon platform to consolidate endpoint and cloud workload protection with a single agent
- Achieved seamless security scaling alongside business growth without compromising customer performance expectations
- Gained full visibility into the attack surface, enhancing security posture while supporting complex, high-throughput environments.

#### Key Results

**100x**

Reduction in false positive

**Hundreds**

Of hours saved every year

**“CrowdStrike is the star of the show in our security operations center. Our detections dashboard shows us anything CrowdStrike deems malicious ... giving us end-to-end visibility and protection.”**

— Matt Bellingeri, CISO

## Case Study



### Anywhere Real Estate Flips Security Posture with CrowdStrike



Faster, unified response



Enhanced endpoint and  
identity protection



Stronger enterprise-wide  
visibility

### Challenge

- Operated a decentralized IT environment with multiple brands and platforms, complicating threat visibility and response
- Faced rising ransomware risks and needed stronger endpoint and identity protection
- Required a scalable, cloud-native security solution to support digital transformation across its enterprise

### Solution

- Deployed the Falcon platform to unify endpoint detection, response, and identity threat protection
- Leveraged Falcon Identity Protection to stop credential-based attacks and lateral movement attempts
- Gained real-time threat visibility and response across a highly distributed organization

### Key Results

**500x**

Fewer alerts

**98% of alerts**

Are true positives

**"We have the best of the best with CrowdStrike.**

**For us, using the Falcon platform along with OverWatch puts us in the 99th percentile for security."**

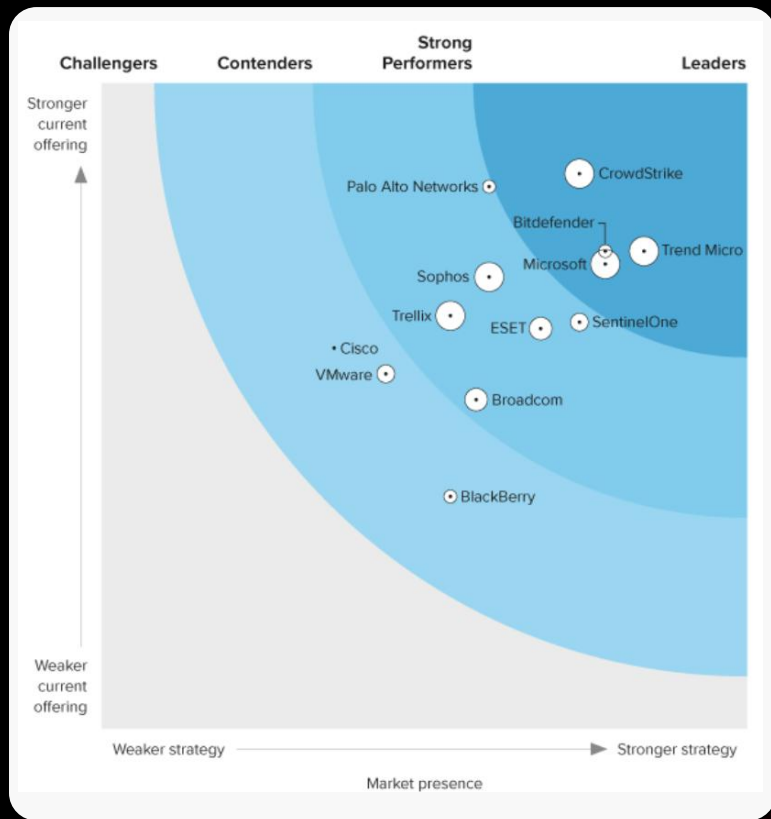
— Brett Fernicola, Senior Director of Security Operations

# Validation

# Endpoint Security Leader

Received highest score in Current Offering and top scores in 15 criteria, surpassing all other vendors

CrowdStrike recognized for its **"dominant endpoint"** solution with **"superior vision"**



The Forrester Wave:  
Endpoint Security, Q4 2023

FORRESTER

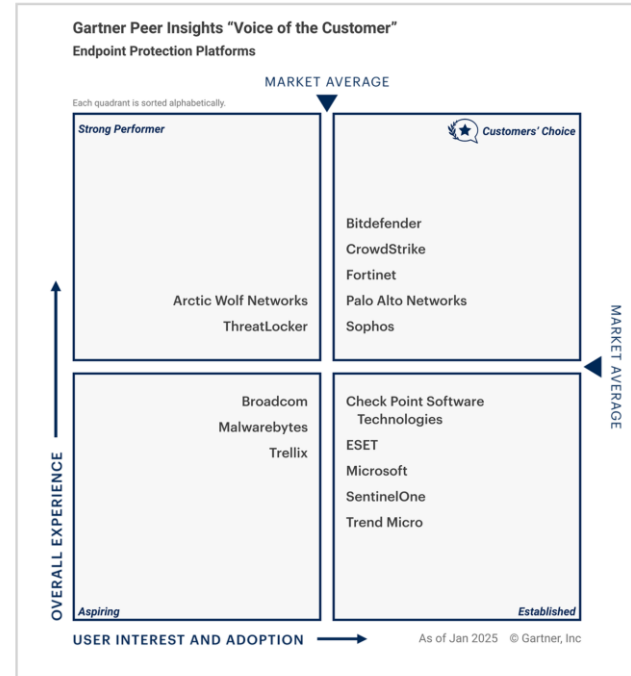
# CrowdStrike is a 2025 Customers' Choice for EPP

A Customers' Choice in the 2025 Gartner Peer Insights™ Voice of the Customer for Endpoint Protection Platforms (EPP) report

**97%** willing to recommend.<sup>2</sup>  
**601** reviews.  
**One** unified platform.

**Gartner**

Figure 1. Voice of the Customer for Endpoint Protection Platforms



Source: Gartner (May 2025)

Gartner

<sup>1</sup>As of January 2025. Gartner, Voice of the Customer For Endpoint Protection Platforms, Peer Editors, May 23, 2025

GARTNER is a registered trademark and service mark, and Peer Insights is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

<sup>2</sup>Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties.

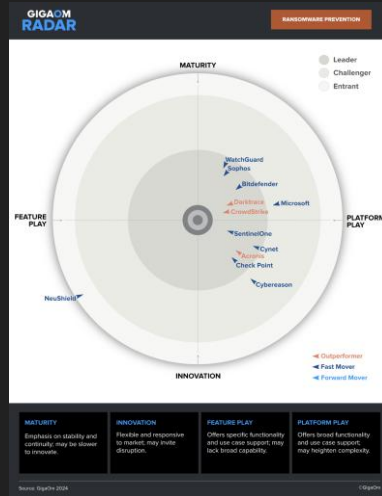
EXPRESSLY GRANTED. IN NO EVENT SHALL GARTNER BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, OF ANY NATURE, ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS CONTENT. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from CrowdStrike.

# Validated by Ransomware Testing



2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test

**CrowdStrike Falcon Achieves 100% Ransomware Detection, Prevention, and Accuracy**



2024 GigaOm Radar for Ransomware Prevention

**CrowdStrike Named a Leader and Outperformer in Ransomware Prevention**



SE Labs Q3 2024 Enterprise Advanced Security Test

**CrowdStrike Wins AAA Award, Lone 100% Total Accuracy Score Winner**

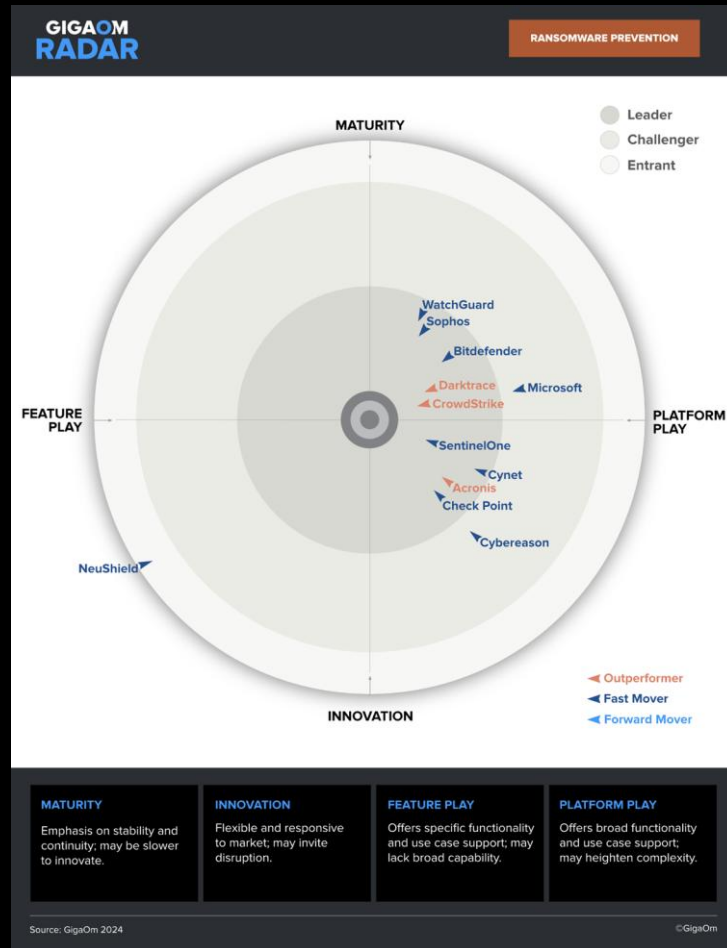
# CrowdStrike Named a Leader and Outperformer in Ransomware Prevention

2024 GigaOm Radar for Ransomware Prevention

10 perfect scores and the top average score among all vendors evaluated

“The Falcon platform enables comprehensive ransomware detection, prevention, and protection.”

# GIGAOM



# CrowdStrike Wins AAA Award, Lone 100% Total Accuracy Score Winner

SE Labs Q3 Enterprise Advanced Security Test

100% Detection Accuracy  
100% Legitimate Accuracy  
100% Total Accuracy  
0 False Positives



“CrowdStrike Falcon achieved perfect results in this test, detecting every element of each threat, and making no mistakes with legitimate applications.”

# Endpoint Security Modules

# A Leader in Endpoint Security

## Industry-Leading Protection

Falcon Prevent (Next-Gen AV)

Falcon Forensics

Falcon Device Control

Falcon Insight XDR (EDR)

Falcon Firewall Management

Falcon for Mobile

## Endpoint Security



## Industry-Leading Services



24/7 MDR &  
Threat Hunting



Incident  
Response



Proactive  
Security Services

Single Agent | Unified Platform

# Falcon Device Control

Ensuring Safe and  
Accountable Device Usage

## Mitigate USB device risk

by gaining insights and granular control to enable safe use and protect against external and internal threats.

## Get automatic threat visibility

by enhancing USB device monitoring, proactive hunting, and data loss investigation.

## Streamline policy management

through intuitive dashboards without extra endpoint agents, software, or hardware.

**100%**

Cloud-delivered device control

**40+**

Number of source code languages for USB data loss ML detections

**1**

One agent, one console, and one platform

Device Control

Mobile

Next-Gen AV

EDR

Firewall Management

Forensics

Mobile

# Falcon for Mobile

**Advanced mobile security**  
by the industry leader in  
endpoint protection

**Advanced protection against mobile attacks** that stays ahead of threats, with an adversary-focused approach designed to prevent data leakage, credential theft, and lateral movement.

**Natively integrated with industry-leading EDR/XDR**

to accelerate mobile endpoint detection and response with a unified view and integrated threat intelligence.

**Seamless adoption that delivers peace of mind** with fast onboarding, zero-touch enrollment, and UEM integrations, offering mobile threat defense while protecting data and minimizing resource use.

Device Control

Next-Gen AV

EDR

Firewall Management

Forensics

Next-Gen AV

EDR

Firewall Management

Mobile

# Falcon Prevent

**Unrivaled prevention**  
with world-class AI and  
integrated adversary  
intelligence

**State-of-the-art prevention**  
using AI/ML to stop malware, fileless attacks,  
and zero-day attacks. Elite threat intelligence  
and advanced scanning detect and block  
malicious behaviors early.

**Secure your estate in seconds**  
with instant protection from our lightweight  
agent, which provides coverage for all major  
operating systems, online or offline.

**Streamline operations and boost productivity**  
with high-fidelity alerts, integrated threat  
intelligence, and automated workflows.

Device Control

Forensics

**100%**  
Ransomware  
prevention<sup>1</sup>

**100K+**  
Agents deployed in  
one day<sup>2</sup>

**< 1 year**  
To realize  
ROI<sup>3</sup>

# Falcon Insight XDR

**A Leader in endpoint security**  
Leader, 2025 Gartner Magic  
Quadrant for EPP

**EDR**

**Pioneered EDR**

with AI-powered protection backed by industry-leading adversary intelligence.

**Complete coverage**

for all major OSs, editions, and versions.

**Lightweight, unified agent**

deploys and secures in minutes, with no complex tuning required.

**Industry-leading protection:**

100% total accuracy detecting real-world cross-domain tradecraft in the 2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test.

**100%**

Total Accuracy  
(2024 SE Labs Enterprise  
Advanced Security (EDR)  
Ransomware Test)

**95%**

Faster MTTR, reduced triage  
from 4 hours to  
10 minutes

**100%**

Ransomware protection  
(2024 SE Labs Enterprise  
Advanced Security (EDR)  
Ransomware Test)

# Falcon Firewall Management

**Easily create and enforce**  
host firewall policies with one  
agent

**Simple firewall policy management**  
for Windows and macOS, with templates,  
reusable rule groups, and rapid change  
propagation.

**Reduced complexity**  
with the lightweight Falcon agent and unified  
console, allowing quick deployment and  
minimal host impact.

**Instant visibility**  
with automatic network monitoring, threat  
identification, and anomaly detection, plus  
application and location-aware firewall  
policies for enhanced security.

Device Control

Mobile

Next-Gen AV

EDR

Firewall Management

Forensics

# Falcon Forensics

**Respond and recover**  
with automated forensic data collection, enrichment, and correlation

## **Reduce complexity**

with automated forensic data collection and comprehensive dashboards, augmenting the analyst expertise for robust incident analysis.

## **Get a unified platform**

for maximum efficiency, with built-in threat intelligence, rich context for investigations, and swift response actions for containment and remediation.

## **Gain value with diverse use cases**

including threat hunting, compromise assessments, and asset risk analysis during mergers and acquisitions.

**1**

Lightweight, dissolvable collector

**6**

Comprehensive dashboards to accelerate workflows

**3**

Platforms supported: Windows, macOS, and Linux

Device Control

Mobile

Next-Gen AV

EDR

Firewall Management

Forensics