
CROWDSTRIKE
Breaches Stop Here
Cloud-Delivered Protection
Across Endpoints,
Cloud Workloads,
Identity and Data

CrowdStrike Falcon

PROTECTION THAT POWERS YOU

Automatically predict and prevent threats in real time

Purpose-built in the cloud with a single lightweight-agent architecture, the **CrowdStrike Falcon®** platform protects the most critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the Falcon platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.

THE CROWDSTRIKE DIFFERENCE

CrowdStrike Threat Graph

Uses cloud-scale artificial intelligence (AI) to correlate trillions of data points from multiple telemetry sources to identify shifts in adversarial tactics and map tradecraft in **CrowdStrike Threat Graph®** to automatically predict and prevent threats in real time across CrowdStrike's global customer base

Single Lightweight Agent

Provides frictionless and scalable deployment and stops all types of attacks while eliminating agent bloat and scheduled scans

Cloud-Native Platform

Leverages the network effect of crowdsourced security data while eliminating the management burden of cumbersome on-premises solutions

CrowdStrike Asset Graph

Solves one of the most complex customer problems today: identifying assets, identities and configurations accurately across all systems including cloud, on-premises, mobile, IoT and more, and connecting them together in a graph form

Falcon Fusion Integrated Security Orchestration Automation and Response (SOAR)

Integrates with the Falcon platform to allow you to collect contextually enriched data and automate security operations, threat intelligence and incident response — all in a single platform and through the same console — to mitigate cyber threats and vulnerabilities

CrowdStrike Falcon

SECURE YOUR CRITICAL AREAS OF RISK: ENDPOINT, CLOUD, IDENTITY AND DATA

They said it was impossible to provide complete cloud-native protection using a single lightweight agent with no impact on user performance.

CrowdStrike proved them wrong. The cloud-native **CrowdStrike Falcon** platform uniquely combines technology, intelligence and expertise to deliver comprehensive end-to-end security across the critical areas of enterprise risk: endpoints, cloud workloads, identity and data.

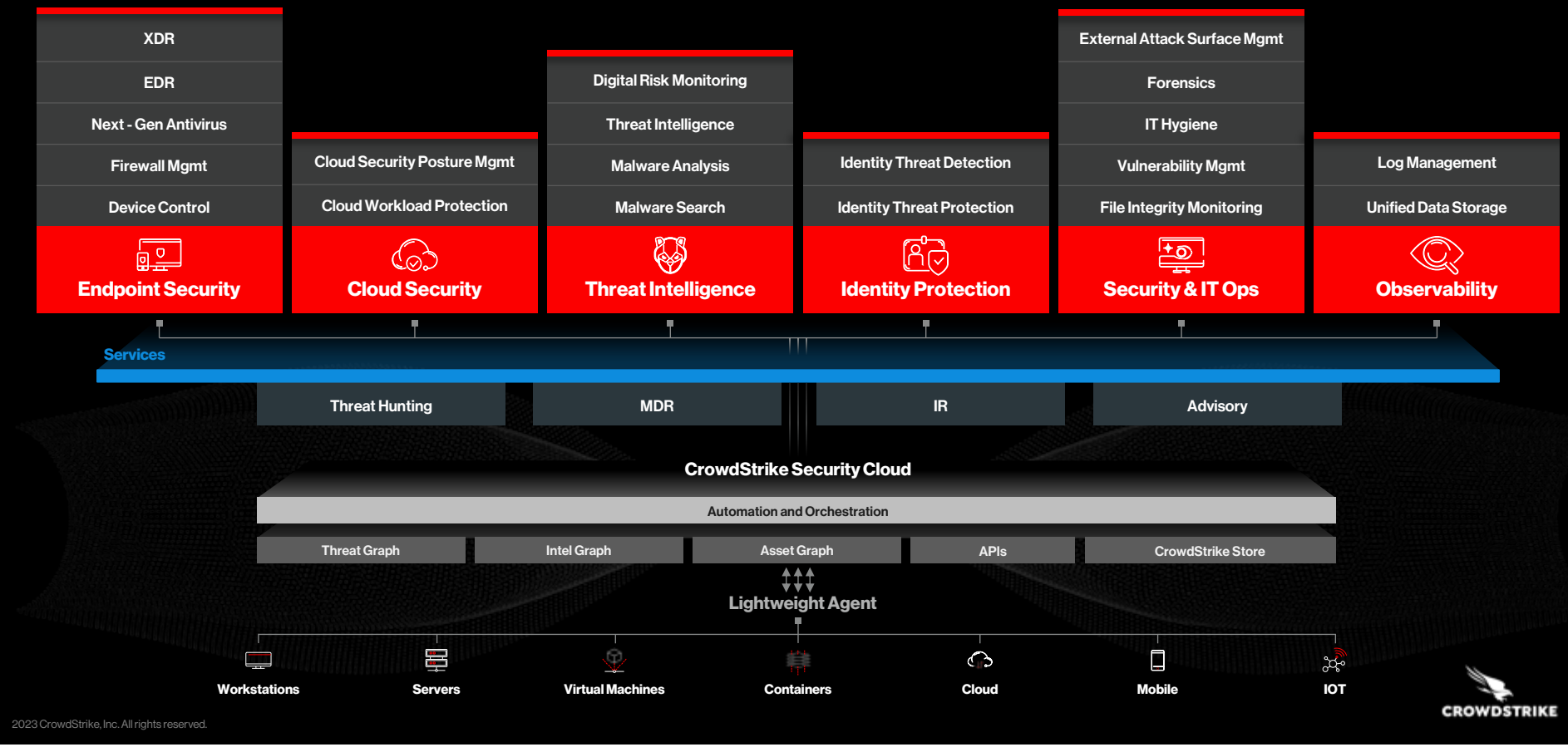
By leveraging the **CrowdStrike Security Cloud** and the lightweight Falcon agent to collect data once and use it many times, the Falcon platform addresses the complete gamut of security challenges while simultaneously eliminating cost and complexity.

The **Falcon platform** continues to grow, delivering industry-leading protection covering:

- Endpoint and cloud security
- Identity protection
- Extended detection and response (XDR)
- Security and IT operations
- Managed services
- Log management
- Threat intelligence
- Data protection

With the Falcon platform, customers receive rapid and scalable deployment, superior protection and performance, reduced complexity, and immediate time-to-value.

The CrowdStrike Falcon Platform



CROWDSTRIKE STORE

CLOUD-SCALE OPEN ECOSYSTEM

Offers an enterprise marketplace of technology partners where you can discover, try, buy and deploy trusted CrowdStrike and partner applications that extend the CrowdStrike Falcon platform, without adding agents or increasing complexity

CROWDSTRIKE UNIVERSITY

TRAINING AND CERTIFICATION

Provides online and instructor-led training courses and certifications focused on implementing, managing, developing and using the CrowdStrike Falcon platform

CROWDSTRIKE ZERO TRUST

Natively enforces Zero Trust protection at three critical layers: device, identity, and data, providing frictionless Zero Trust security with real-time threat prevention and IT policy enforcement that uses identity, behavioral and risk analytics to stop breaches for any endpoint, workload or identity

ENDPOINT SECURITY

FALCON PREVENT | NEXT-GENERATION ANTIVIRUS

Protects against all types of threats, from malware and ransomware to sophisticated attacks, and deploys in minutes, immediately protecting your endpoints

FALCON INSIGHT XDR | DETECTION AND RESPONSE FOR ENDPOINT AND BEYOND

Offers industry-leading endpoint detection and response (EDR) and extended detection and response (XDR) in a single solution, and customers can easily expand from EDR to XDR using XDR connector packs

FALCON INSIGHT XDR | ENDPOINT DETECTION AND RESPONSE

Delivers continuous, comprehensive endpoint visibility and automatically detects and intelligently prioritizes malicious activity to ensure nothing is missed and potential breaches are stopped

FALCON INSIGHT XDR CONNECTOR | EXTENDED DETECTION AND RESPONSE (XDR)

Extends detection, investigation and response across your enterprise, easily synthesizing cross-domain telemetry from Falcon modules and third-party sources to activate extended capabilities from a single console

FALCON COMPLETE XDR | MANAGED EXTENDED DETECTION AND RESPONSE (MXDR)

Expands Falcon Complete's industry-leading MDR service with cross-domain XDR protection, run by CrowdStrike's elite 24/7 expertise, proactive threat hunting and native threat intelligence

FALCON FIREWALL MANAGEMENT | HOST FIREWALL

Delivers simple, centralized host firewall management, making it easy to manage and control host firewall policies

FALCON DEVICE CONTROL | USB SECURITY

Provides the visibility and precise control required to enable safe usage of USB devices across your organization

FALCON FOR MOBILE

Protects against threats to iOS and Android devices, extending XDR/EDR capabilities to your mobile devices, with advanced threat protection and real-time visibility into app and network activity

THREAT INTELLIGENCE

FALCON INTELLIGENCE | AUTOMATED THREAT INTELLIGENCE

Enriches the events and incidents detected by the CrowdStrike Falcon platform, automating intelligence so security operations teams can make better, faster decisions

FALCON INTELLIGENCE PREMIUM | CYBER THREAT INTELLIGENCE

Delivers world-class intelligence reporting, technical analysis, malware analysis and threat hunting capabilities, enabling organizations to build cyber resiliency and more effectively defend against sophisticated nation-state, eCrime and hacktivist adversaries

FALCON INTELLIGENCE ELITE | ASSIGNED INTELLIGENCE ANALYST

Maximizes your investment in Falcon Intelligence Premium with access to a CrowdStrike threat intelligence analyst whose mission is helping you defend against adversaries targeting your organization

FALCON INTELLIGENCE RECON | DIGITAL THREAT MONITORING

Monitors potentially malicious activity across the open, deep and dark web, enabling you to better protect your brand, employees and sensitive data

FALCON INTELLIGENCE RECON+ | MANAGED THREAT MONITORING

Provides CrowdStrike experts to manage the monitoring, triaging, assessing and mitigating of threats across the criminal underground

FALCON SANDBOX | MALWARE ANALYSIS

Uncovers the full malware attack lifecycle with in-depth insight into all file, network, memory and process activity, and provides easy-to-understand reports, actionable IOCs and seamless integration

MANAGED SECURITY

FALCON OVERWATCH™ | MANAGED THREAT HUNTING

Partners you with a team of elite cybersecurity experts to hunt continuously within the Falcon platform for faint signs of sophisticated intrusions, leaving attackers nowhere to hide

FALCON OVERWATCH™ ELITE | ASSIGNED MANAGED THREAT HUNTING ANALYST

Extends your team with an assigned CrowdStrike threat hunting analyst, providing dedicated expertise, tactical day-to-day insights into your threat landscape and strategic advisory to help drive continuous improvement

FALCON COMPLETE | MANAGED DETECTION AND RESPONSE (MDR)

Stops and eradicates threats in minutes with 24/7 expert management, monitoring, surgical remediation, proactive threat hunting and integrated threat intelligence — all backed by the industry's strongest Breach Prevention Warranty

CLOUD SECURITY

FALCON CLOUD SECURITY

Provides breach protection including threat intelligence, detection and response, workload runtime protection and cloud security posture management across AWS, Azure and GCP

FALCON CLOUD SECURITY FOR CONTAINERS

Delivers cloud and container security and breach protection: cloud security posture management, threat detection and response across on-premises, hybrid and multi-cloud environments, and cloud workload protection, including container security and Kubernetes protection

FALCON CLOUD SECURITY FOR MANAGED CONTAINERS

Provides cloud and container security, including threat intelligence, detection and response, container image security and Kubernetes protection

FALCON OVERWATCH™ CLOUD THREAT HUNTING | MANAGED SERVICES

Unearths cloud threats, from unique cloud attack paths with complex trails of cloud IOAs and indicators of misconfiguration (IOMs) to well-concealed adversary activity in your critical cloud infrastructure — including AWS, Azure and Google Cloud Platform

FALCON COMPLETE CLOUD SECURITY | MDR FOR CLOUD WORKLOADS

Provides a fully managed cloud workload protection service, delivering 24/7 expert security management, threat hunting, monitoring and response for cloud workloads, backed by CrowdStrike's industry-leading Breach Prevention Warranty

SECURITY AND IT OPERATIONS

FALCON DISCOVER | IT HYGIENE

Identifies unauthorized accounts, systems and applications anywhere in your environment in real time, enabling faster remediation to improve your overall security posture

FALCON SPOTLIGHT | VULNERABILITY MANAGEMENT

Offers security teams an automated, comprehensive vulnerability management solution, enabling faster prioritization and improved remediation workflows without resource-intensive scans

FALCON SURFACE | EXTERNAL ATTACK SURFACE MANAGEMENT

Continuously discovers and maps all internet-facing assets to shut down potential exposure with guided mitigation plans to reduce the attack surface

FALCON FILEVANTAGE| FILE INTEGRITY MONITORING

Provides real-time, comprehensive and centralized visibility that boosts compliance and offers relevant contextual data

FALCON FORENSICS | FORENSIC CYBERSECURITY

Automates collection of point-in-time and historic forensic triage data for robust analysis of cybersecurity incidents

IDENTITY PROTECTION

FALCON IDENTITY THREAT DETECTION

Enables hyper-accurate detection of identity-based threats in real time, leveraging AI and behavioral analytics to provide deep actionable insights to stop modern attacks like ransomware

FALCON IDENTITY THREAT PROTECTION

Enables hyper-accurate threat detection and real-time prevention of identity-based attacks by combining the power of advanced AI, behavioral analytics and a flexible policy engine to enforce risk-based conditional access

FALCON COMPLETE IDENTITY THREAT PROTECTION

Provides a fully managed identity protection solution delivering frictionless, real-time identity threat prevention and IT policy enforcement, monitoring and remediation — powered by CrowdStrike's team of experts

OBSERVABILITY

FALCON LOGSCALE | LOG MANAGEMENT

Purpose-built for large-scale logging and real-time analysis of all of your data, metrics and traces, providing live observability for organizations of all sizes

FALCON LONG TERM REPOSITORY | UNIFIED DATA STORAGE

Reduces cost and improves visibility with long-term scalable storage of historical and real-time Falcon platform data

FALCON COMPLETE LOGSCALE | MANAGED DATA LOGGING AND OBSERVABILITY

Delivers expertise and continuous guidance for log management and observability programs to ingest, aggregate and analyze massive volumes of streaming log data at petabyte scale.

CROWDSTRIKE SERVICES

Delivers pre- and post-incident response (IR) services 24/7 to support you before, during and after a breach, with skilled teams to help you defend against and respond to security incidents, prevent breaches and optimize your speed to remediation

PREPARE: ADVISORY SERVICES

Helps you prepare to defend against sophisticated threat actors with real-life simulation exercises

- TABLETOP EXERCISE
- ADVERSARY EMULATION EXERCISE
- RED TEAM / BLUE TEAM
- PENETRATION TESTING

RESPOND: BREACH SERVICES

Helps you stop breaches, investigate incidents, and recover from attacks with speed and surgical precision

- INCIDENT RESPONSE (DFIR)
- ENDPOINT RECOVERY
- COMPROMISE ASSESSMENT
- ADVERSARIAL EXPOSURE ASSESSMENT
- NETWORK SECURITY MONITORING

FORTIFY: ADVISORY SERVICES

Helps you enhance your cybersecurity posture with actionable recommendations to fortify your defenses

- CYBERSECURITY MATURITY ASSESSMENT
- CLOUD SECURITY ASSESSMENT
- TECHNICAL RISK ASSESSMENT
- SOC ASSESSMENT
- AD SECURITY ASSESSMENT
- CYBERSECURITY ENHANCEMENT PROGRAM
- SECURITY PROGRAM IN DEPTH ASSESSMENT

CLOUD SECURITY SERVICES

Helps you recover from a cloud data breach and secure your cloud platform configurations

- INCIDENT RESPONSE FOR CLOUD
- CLOUD SECURITY ASSESSMENT
- CLOUD COMPROMISE ASSESSMENT
- RED TEAM / BLUE TEAM EXERCISE FOR CLOUD
- FALCON OPERATIONAL SUPPORT SERVICES FOR CLOUD SECURITY

TECHNOLOGY SERVICES

- ENDPOINT SECURITY SERVICES
- IDENTITY PROTECTION SERVICES
- NETWORK MONITORING SERVICES

CrowdStrike: Tried, Tested, Proven

With CrowdStrike, you can be confident that your organization is finally protected from cyberattacks — known or unknown, with or without malware. Hear what the experts are saying about the **CrowdStrike Falcon platform:**

NAMED A LEADER IN THE FORRESTER WAVE™:
ENDPOINT DETECTION AND RESPONSE PROVIDERS, Q2 2022

NAMED A LEADER IN THE FORRESTER WAVE:
CYBERSECURITY INCIDENT RESPONSE SERVICES (CIRS), Q1 2022

NAMED A STRONG PERFORMER IN THE FORRESTER WAVE:
CLOUD WORKLOAD SECURITY, Q1 2022

NAMED A LEADER IN THE IDC MARKETSCAPE:
WORLDWIDE MODERN ENDPOINT SECURITY FOR ENTERPRISE 2022 VENDOR ASSESSMENT

NAMED A LEADER AND THE SECURITY VENDOR PLACED FURTHEST FOR COMPLETENESS OF VISION:
GARTNER® MAGIC QUADRANT™ FOR ENDPOINT PROTECTION PLATFORMS (EPP), 2022

NAMED A LEADER IN THE FORRESTER WAVE:
ENDPOINT SECURITY SOFTWARE AS A SERVICE, Q2 2021

*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, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

CROWDSTRIKE

info@crowdstrike.com | sales@crowdstrike.com | crowdstrike.com
Experienced a breach? Contact us at (855) 276-9347 or services@crowdstrike.com