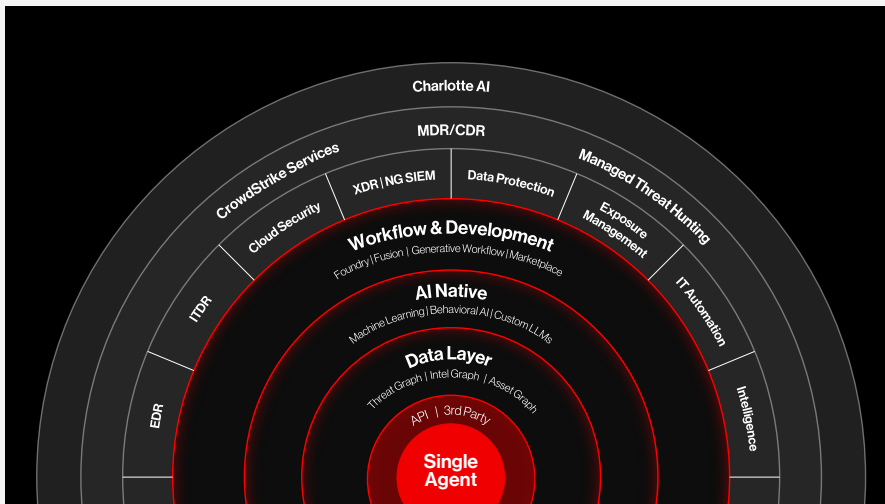# CROWDSTRIKE

fal.con :

CrowdStrike Ushers In the Future of Cybersecurity

Since its founding, CrowdStrike has revolutionized cybersecurity by focusing on the security outcome that customers need most: stopping breaches. This year at Fal.Con, we delivered innovations across the unified CrowdStrike Falcon® platform to help organizations reduce risk, consolidate point products and harness data for generative AI and extended detection and response (XDR).

Platform Innovations: Enabling the Future of Generative AI and XDR

Raptor release for the CrowdStrike Falcon® platform

The CrowdStrike Falcon platform's latest release, Raptor, delivers the petabyte-scale, lightning-fast data collection, search and storage needed to fuel the next era of generative AI-powered cybersecurity. The Raptor release is powered by the same technology as CrowdStrike's next-gen SIEM offering, CrowdStrike Falcon LogScale, and includes:

- **First AI-powered incident creator with Charlotte AI Investigator:** Charlotte AI Investigator automatically correlates related context into a single incident and generates a large language model (LLM)-powered incident summary for understanding by security analysts of all skill levels.

- **XDR for all:** All CrowdStrike Falcon® Insight XDR endpoint detection and response (EDR) customers now get native XDR to accelerate investigations with comprehensive endpoint, identity, cloud and data protection telemetry from across the CrowdStrike Falcon platform.

- **XDR Incident Workbench:** Dramatically accelerate investigation and response times with a reimagined and lightning-fast user experience for EDR/XDR that is designed around incidents, not stand-alone alerts.

- **Collaborative Incident Command Center:** Work on incidents in real time with security analysts from any location, at any time, from a unified source of truth.

Charlotte AI: Generative Workflows for Better Outcomes

Charlotte AI accelerates cybersecurity with generative AI workflows that help everyone — from novices to experts — become a power user of the CrowdStrike Falcon platform. With Charlotte AI, anything the platform can do is only a question away, with example use cases including:

- Summarizing thousands of pages of intelligence reports in an instant to better understand adversaries targeting your organization, industry and region

- Quickly identifying exposures to vulnerabilities and getting custom remediation guidance

- Hunting for signs of adversary activity to speed incident investigation and response

- Filtering millions, billions or trillions of data points without building custom queries to get the answers you need — fast

Disrupting Legacy Markets: Better Security by Consolidating Point Products with a Tightly Integrated Platform

CrowdStrike Falcon® Exposure Management

Stop breaches before they start by proactively reducing an adversary's opportunity for compromise and lateral movement. Falcon Exposure Management allows IT and security teams to prioritize the problems making the biggest impact and effectively stop breaches instead of spending their time on a stream of low-priority fixes. Falcon Exposure Management allows these teams to:

- Reduce risk with complete visibility into every asset and real-time assessments of potential exposures — from the inside out and outside in — by leveraging existing CrowdStrike endpoint agents and natively integrated external attack surface management (EASM)

- Automatically visualize all potential adversary intrusion paths, including lateral movement, to proactively identify and stop attacker activity

- Assess critical configuration settings with Secure Configuration Assessment (SCA) to demonstrate compliance posture against Center for Internet Security (CIS) benchmarks

- Automate closed-loop remediation through native integration with CrowdStrike's industry-leading EDR, Falcon Real Time Response (RTR) and CrowdStrike Falcon® Fusion security orchestration automation and response (SOAR)

CrowdStrike Falcon® Data Protection

Falcon Data Protection stops data theft with dynamic data protection policies that automatically follow content, even as it moves across files or SaaS applications.

Benefits include:

- Consolidate legacy data loss prevention (DLP) point products on the unified CrowdStrike Falcon platform, with one agent for data protection and endpoint security.

- Accelerate detection and response by extending EDR/XDR from initial compromise through data exfiltration, with unified visibility across endpoints and data in a single console and workflow.

- Stop data theft with dynamic data protection policies that automatically follow content, even as it moves across files or SaaS applications, to protect data as it's being copied or shared.

CrowdStrike Falcon® for IT

Falcon for IT extends the CrowdStrike Falcon platform with built-in IT automation in an end-to-end, visibility-to-action life cycle. With Falcon for IT, teams can immediately leverage the platform's single lightweight agent to:

- **Ask a question:** With Charlotte AI, use plain-language generative AI prompts to run queries and get real-time visibility for any system and compliance and performance data on any asset — across any operating system.

- **Get an answer:** Instantly understand the current state of all enterprise assets to rationalize the IT estate, support a remote and global workforce, and optimize the employee experience by resolving problems remotely.

- **Take an action:** Automate remediation directly on assets to rapidly fix issues, such as installing missing patches or changing endpoint policies, with an out-of-the-box Quick Fix library and custom workflows via Falcon Fusion SOAR.

- **Monitor the problem:** Continuously monitor the state of CrowdStrike-managed assets — including system utilization, compliance status, running services and performance — with intuitive, flexible dashboards.

CrowdStrike Falcon® Foundry

Falcon Foundry, the cybersecurity industry's first no-code application development platform, gives customers and partners the ability to harness the data, automation and cloud-scale infrastructure of the CrowdStrike Falcon platform to easily create their own custom applications to solve an infinite number of security and IT challenges. New capabilities and benefits include:

- **No-code application development:** Build no-code apps in minutes with an intuitive, modern app development interface with step-by-step instructions and a drag-and-drop visual application studio.

- **Native access to the highest-fidelity data:** Get data and threat intelligence from across the CrowdStrike Falcon platform, including third-party telemetry stored in CrowdStrike® Falcon LogScale™ next-gen security information and event management (SIEM).

- **Built-in automation with end-to-end response:** Falcon Fusion — the platform's native SOAR framework — and Falcon RTR scripts work together to easily define automated workflows and execute fast response on endpoints and beyond.

CrowdStrike to Acquire Bionic to Extend Cloud Security Leadership with the Industry's Most Complete Code-to-Runtime Cybersecurity Platform

CrowdStrike announced an agreement to acquire Bionic, the pioneer of application security posture management (ASPM). The acquisition will extend CrowdStrike's leading cloud-native application protection platform (CNAPP) with ASPM to deliver comprehensive risk visibility and protection across the entire cloud estate, from cloud infrastructures to the applications and services running inside of them. As part of the industry's most complete code-to-runtime cybersecurity platform, customers will be able to experience:

- **Real-time, frictionless application visibility:** Discover and map all application services, databases, microservices, third parties, APIs and data flows across cloud service providers and both hybrid and on-premises application deployments via an agentless approach. Applications are automatically deconstructed while seamlessly integrating with continuous integration/continuous delivery (CI/CD) pipelines, removing the requirement for sensitive source code access.

- **Instant prioritization of application-level vulnerabilities:** Eliminate up to 95% of vulnerability noise and prioritize the top business-critical risks that can be exploited in production applications so teams know what to fix first based on business impact.

- **Complete visibility for serverless infrastructure:** Reduce your overall cloud risk with vulnerability scanning for serverless infrastructure, such as Azure Functions and AWS Lambda.

Availability on Future Products

For information on timing and availability of the products and features announced at Fal.Con, please contact your CrowdStrike representative. Some products are currently only available in private beta. The product descriptions above include forward-looking statements including, but not limited to, statements concerning feature availability, the benefits and capabilities of our current and future products and services, and our strategic plans and objectives. Such statements are subject to numerous risks and uncertainties and actual results could differ from those statements. Any future products, functionality and services may be abandoned or delayed, and customers should make decisions to purchase products and services based on features that are currently available.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike 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.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches

Learn more: https://www.crowdstrike.com/

Follow us: Blog | Twitter | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/