Falcon Foundry

Extend the industry-leading CrowdStrike Falcon® platform with easy-to-build, low-code applications that use the same CrowdStrike data and infrastructure

Cybersecurity's first low-code application development platform

With cybersecurity tool sprawl on the rise, CrowdStrike Falcon® Foundry enables you to easily build low-code applications that operate as an extension of the CrowdStrike Falcon® platform, allowing your team to consolidate dozens of point products. With access to modern no-code and low-code app development tools and the same CrowdStrike data and infrastructure, your team is empowered to build mission-critical apps to solve the toughest cybersecurity challenges and stop adversaries.

Key capabilities

Empower your team to build security apps that strengthen your defenses

Falcon Foundry empowers your team to maximize your investment in the Falcon platform by reducing context switching during monitoring and remediation, stopping adversaries in their tracks.

- **Harness the power of CrowdStrike's data and infrastructure:** Falcon Foundry leverages CrowdStrike's high-fidelity data and cloud-scale infrastructure to build apps that reveal actionable insights and are accessible throughout your organization. Use automated workflows and scripts to close your security gaps, speed up threat detection, investigation and response, and stop adversaries.

- **Democratize app development with an easy-to-use, low-code app platform:** Empower your team to build applications and extend existing Falcon solutions with the intuitive, modern app development tools available in Falcon Foundry. Users are guided through the app development process with contextual help to enable security analysts to make decisions faster, build their confidence and reduce app development time.

Key benefits

- Consolidate solutions and drive more value from your CrowdStrike Falcon investment

- Leverage the same data and infrastructure as CrowdStrike to build low-code apps

- Democratize security app development with user-friendly developer tools

- Solve the most challenging security use cases to close gaps and stop adversaries

- **Increase speed and accuracy with automation:** Falcon Foundry leverages the native CrowdStrike Falcon® Fusion security orchestration, automation and response (SOAR) framework and Falcon Real Time Response (RTR) scripts to easily define workflow automation and execute response actions aligned with your business logic and third-party integrations.

Use a modular approach to successfully build low-code applications

As the first cybersecurity low-code application platform, Falcon Foundry takes a unique, modular approach to building security applications.

- **Build a data foundation for your apps that is easily integrated and normalized:** Falcon Foundry supports structured and unstructured data. It allows users to onboard third-party data through various ingestion mechanisms, such as APIs, Falcon RTR and OSquery, giving them the ability to fetch, transform and store any data. Users can also access CrowdStrike Falcon data from their existing modules or data stored in the Falcon platform to build their apps.

- **Define the business logic for your app to bring your use case to life:** Falcon Foundry users can capture their app logic with workflow automation that requires no code and gives them flexibility to define custom triggers, conditions and actions. Users can also leverage function as a service (FaaS) functions to execute code in response to events, all from the cloud.

- **Create intuitive user interfaces for your apps for an optimal usage experience:** Falcon Foundry's experience design studio offers an intuitive, no-code dashboard builder with numerous widgets to visualize your app data and improve the user experience. An optional low-code feature lets advanced developers extend their app interfaces with new pages or insertions into existing views to address unique requirements.

- **Safeguard your organization's apps with granular user permissions:** With embedded role-based access control defining user and group permissions, Falcon Foundry apps let users protect sensitive data by limiting who can create, access and manage apps while demonstrating compliance to auditors.

- **Close security gaps by seamlessly extending your Falcon platform modules:** Managed from the Falcon console and delivered from the cloud, Falcon Foundry apps harness the capabilities of Falcon modules, the single, powerful Falcon agent and the existing solutions within your ecosystem to boost your security posture. With Falcon Foundry, you can gather information, automate processes and execute response actions via internal tooling to improve security efficacy and efficiency.

Gain limitless potential to unlock cybersecurity innovation

Falcon Foundry lets you extend the Falcon platform to meet your unique challenges. It provides your team with modern app development tools to create applications that deliver a range of outcomes, from incremental productivity improvements to new, high-value solutions that transform your business. Some popular use cases include the following:

- **Deepen context and correlation in CrowdStrike Falcon® Next-Gen SIEM:** Integrate with any HTTP-based API to onboard data and orchestrate actions across your organization's third-party technologies to maximize the investment in your existing technology stack and extend the power of your Falcon Next-Gen SIEM deployment.

- **Visualize detection coverage against the MITRE ATT&CK® framework:** Safeguard your organization with comprehensive coverage against adversary tactics and techniques. By mapping your detections to the MITRE ATT&CK matrix, you will get a prioritized view of detection gaps to take immediate action.

The most integrated way to build low-code security apps

Falcon Foundry unlocks cybersecurity innovation through low-code apps that extend the power of the industry-leading, AI-powered Falcon platform to implement an unlimited array of security and IT use cases.

- **Reduce insider threat risk with proactive, automated threat hunting:** Lower the number of manual tasks that your team performs by automating threat hunting with a workflow that searches for suspicious events and correlates them against a watchlist. If a risky user is identified, it will trigger a multifactor authentication reset to lock them out.

- **Rapidly respond to critical vulnerabilities with emergency patching:** Stay up-to-date with critical software vulnerabilities by conducting emergency patching across hosts. You can easily schedule a job or run it immediately to take actions across your fleet of hosts, such as removing malicious files or uploading workaround or patch files as a preventive measure. You can then see the results, status and audit information of all of the jobs carried out within your organization.

- **Assess compliance across your fleet and validate audit information:** Enhance your organization's compliance by running recurrent assessments across your hosts to surface vulnerabilities and collect contextual information for investigations and audits.

Free trial →

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/

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