

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, AI agents, and CrowdStrike data and infrastructure, your team is empowered to build mission-critical apps to solve the toughest cybersecurity challenges and stop adversaries.

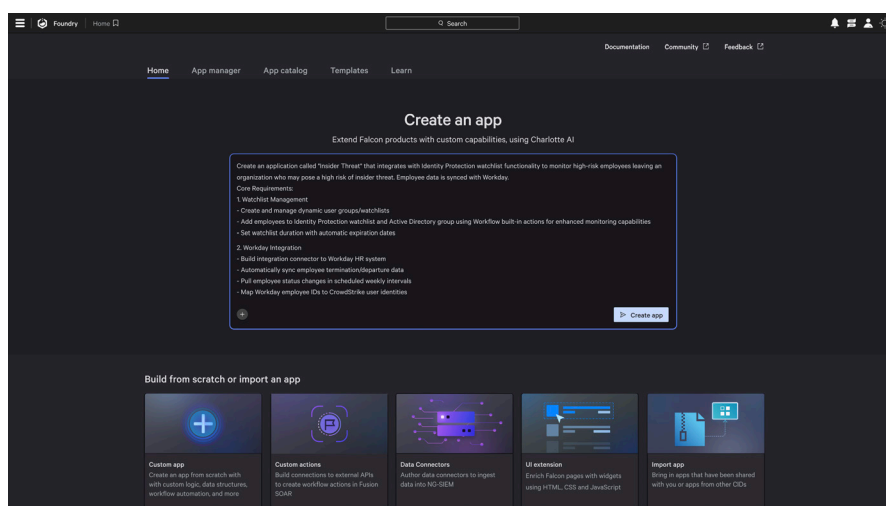


Figure 1. Falcon Foundry empowers you to build low-code applications with modern development tools and AI agents.

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 CrowdStrike® Charlotte AI™-powered agents
- Solve the most challenging security use cases to close gaps 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 to reduce context switching during monitoring and remediation to stop adversaries in their tracks.

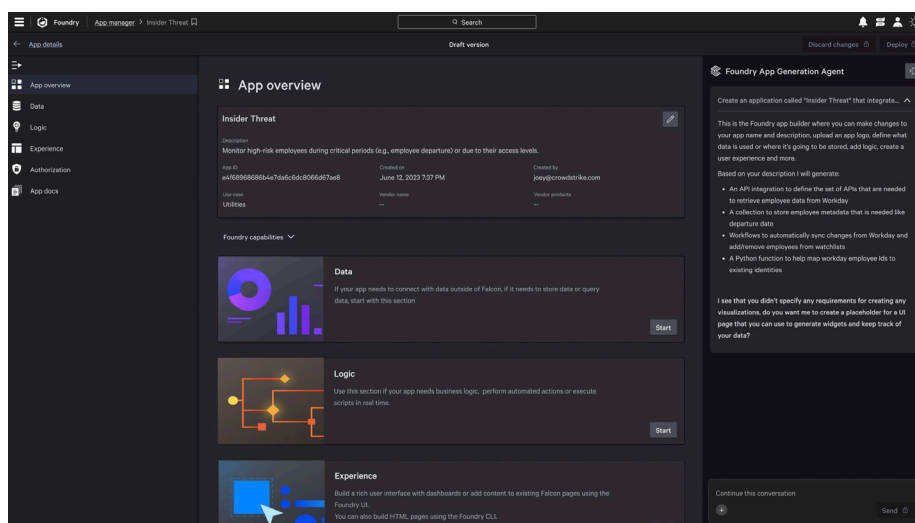


Figure 2. The Foundry App Generation Agent enables users to write a prompt describing their use case.

- 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 modern development tools and Charlotte AI:** Empower your team to build applications and extend existing Falcon solutions with the intuitive, modern app development tools available in Falcon Foundry. Users can now leverage the Foundry App Generation Agent — an AI assistant powered by Charlotte AI — that streamlines the application development process. This powerful combination enables security analysts to make decisions faster, builds their confidence, and significantly reduces app development time through AI-assisted development.
- Increase speed and accuracy with automation:** Falcon Foundry leverages the native CrowdStrike Falcon® Fusion SOAR 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.

The most integrated way to build low-code security apps

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

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. The Foundry App Generation Agent allows users to simply describe their desired use case and app functionality in natural language, helping them create the app structure and build necessary components.

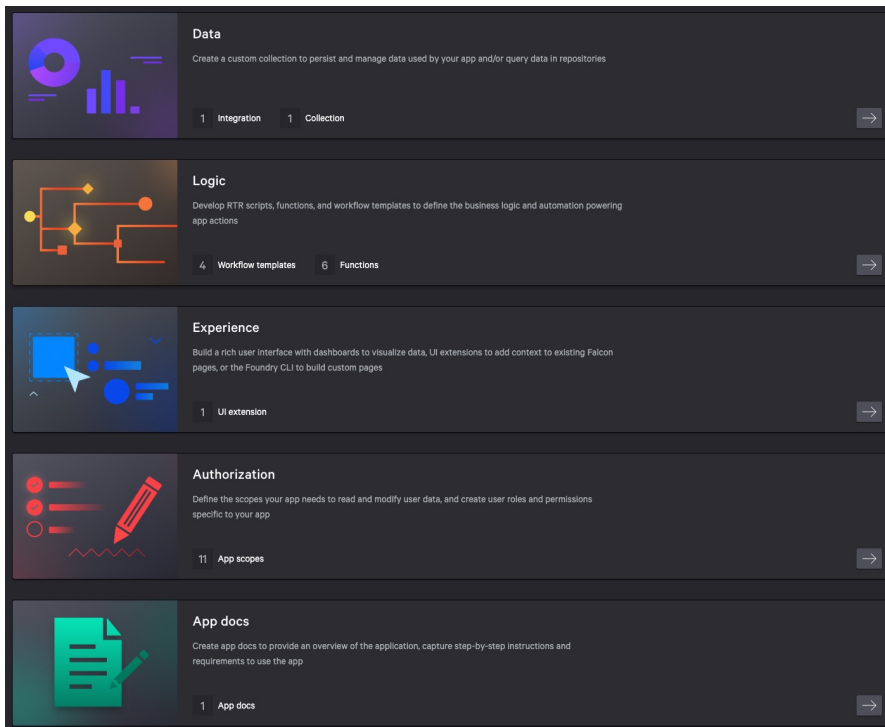


Figure 3. Falcon Foundry's modular building approach allows users to choose and build the different components for their application with AI and modern development tools.

- 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 and Falcon RTR, 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 FaaS functions to write and execute Python or Golang 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 a no-code extension builder to customize 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 sensor, 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 solutions that extend native modules in the Falcon platform to new, high-value business transformation. Some popular use cases include the following:

- **Safeguard data during offboarding with automated insider risk monitoring:** Integrate with Workday to track users with a departure date, add high-risk users to watchlists and AD groups for enhanced oversight, and automatically remove them after 30 days. Streamline offboarding, maintain visibility into privileged access, and reduce insider threat risk with data-driven protection.
- **Automate threat intelligence imports to strengthen detection and speed response:** Continuously pull and process data from open-source threat feeds, convert it to CSV, and upload it as CrowdStrike Falcon® Next-Gen SIEM lookup files using FalconPy. This keeps Falcon Next-Gen SIEM updated with the latest malicious IPs, domains, and hashes, improving accuracy and enabling faster, intelligence-driven investigations.
- **Strengthen web control with automated, category-based URL filtering:** This Falcon Foundry application automates domain block rule creation, streamlines category-based blocking, and delivers real-time insights into domain activity. It transforms CSV domain data into actionable categories, updates rule groups automatically, and visualizes relationships for efficient, intelligence-driven firewall management.
- **Unify access management across ServiceNow and identity protection:** Connect CrowdStrike Falcon® Next-Gen Identity Security with ServiceNow CMDB to automatically align configuration rules and access policies. By synchronizing approvals with policy enforcement, it eliminates manual updates, ensures users only access authorized resources, and helps prevent lateral movement across the network.
- **Ensure continuous identity protection with proactive infrastructure monitoring:** Monitor domain controllers, multifactor authentication (MFA), and identity-as-a-service (IDaaS) connectors to keep authentication services healthy and secure. Get automatic alerts when issues arise so teams can quickly fix problems, avoid downtime, and maintain strong, reliable identity protection across the environment.

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/>

