

Falcon Shield: Covering the Low- Code/No-Code Attack Surface

Low-code/no-code (LCNC) programming is revolutionizing application development, empowering non-programmers to rapidly create microprograms at a fraction of the cost. But even though LCNC applications can improve workflows and optimize processes, the proliferation of these applications is raising security concerns.

LCNC applications are used to access sensitive information, but they are built without critical safeguards. They lack scalability, security controls, logs, or runtime protection, significantly increasing an enterprise's attack surface.

CrowdStrike Falcon® Shield monitors the software as a service (SaaS) applications used to build LCNC apps (such as Power Apps) and the LCNC apps themselves. It helps ensure that the security features available within tools like Power Apps are configured correctly, providing organizations with the best chance to keep their LCNC apps secure.

Use cases



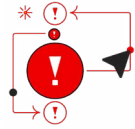
Prevent data leakage

Limiting access to sensitive databases and information within the company's network is critical to preventing LCNC applications from leaking data. The permissions granted to the application are based on the permissions of the user who created the application. Falcon Shield helps app owners manage and monitor users who build apps, ensuring that only authorized users are able to develop applications that access this sensitive data.

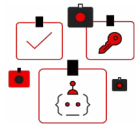
Falcon Shield: Covering the Low-Code/No-Code Attack Surface

**Manage configurations**

Configurations in the parent application (such as Power Apps) are passed down to the LCNC app. Falcon Shield's automated monitoring alerts app owners when configurations drift and high-risk permissions are passed down to the LCNC app in operational use.

**Monitor suspicious behavior**

Falcon Shield's threat detection capabilities trigger alerts when LCNC apps or their users behave suspiciously. This could include activities such as late-night operations, anomalous app behavior, or changes to configurations.

**Stop insider abuses**

Falcon Shield alerts app owners when there are too few or too many admins managing the LCNC development software. Having too few owners could create situations where a single admin has unfettered access to sensitive data without oversight, and having too many admins makes it difficult to manage all of the users.

[Learn More](#)**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](#) | [X](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

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