CrowdStrike Products

CROWDSTRIKE

FALCON FUSION: UNIFIED EXTENSIBLE SOAR FRAMEWORK

Streamline IT and security operations with customizable and easy-to-use workflow automation

AUTOMATE COMPLEX WORKFLOWS

Achieving digital transformation to keep up with ever-changing business and market demands has caused organizations to rapidly increase IT and security stack complexity and, as a result, expand the threat surface. Doing so has compromised the security operations center's ability to meet the 1-10-60 challenge, wherein teams have an average of 1 minute to detect an attack, 10 minutes to understand it and 60 minutes to contain it. Every minute spent by security teams struggling with too many security point solutions, disparate data and not enough skills among their workforce means the risk of attack grows exponentially.

To simplify enterprise security and streamline security operations center (SOC) operations, security teams must implement solutions that can intuitively customize and build automated workflows based on real-world problems and desired outcomes. Falcon Fusion is a unified and extensible framework built on the CrowdStrike Falcon® platform to orchestrate and automate complex workflows, leveraging the power of the CrowdStrike Security Cloud and relevant contextual insights across endpoints, identities and workloads, in addition to telemetry from partner applications. Enterprises can build real-time active notification and response capabilities by leveraging complex sequencing and branching, as well as customizable triggers based on detection and incident categorizations. With Falcon Fusion's easy-to-use automation, complex enterprise security workflows are simplified, allowing analysts to more effectively understand workflows and optimize SOC performance.

KEY BENEFITS

Orchestrate and automate complex workflows using powerful data insights from Security Cloud and partner apps without leaving the console.

Simplify security operations based on threat detections, incidents and audit events

Accelerate incident triaging and real-time response by configuring custom response actions and notifications

Gain on-demand, cloud-scale extensibility with custom code or no-code options to create repeatable and reliable processes

Cut costs and resources: Free up skilled resources and budget by scaling workflows on demand with consistency and efficacy.

KEY CAPABILITIES

AUTOMATE FULL-CYCLE INCIDENT RESPONSE

Accelerate active response times and reduce mean time to remediate threats by building and deploying customized workflows.

- **Simplify SOC workstreams** with a customizable, intuitive framework built on the Falcon platform, using native and partner contextual data.
- **Build and run workflows in minutes** within the Falcon Fusion workflow builder by simply adding elements to the canvas that visualize workflow functionality.
- **Automate complex workflows** with any sets of triggers, conditions and actions using Falcon Fusion's complex conditional branching and sequencing logic.
- **Monitor workflow performance, execution and updates** made to workflows to achieve unparalleled visibility into performance.

GAIN THE POWER OF ENRICHED DATA

Achieve unparalleled visibility and control with contextual insights leveraging the CrowdStrike Security Cloud and trusted partners.

- **Leverage the Security Cloud** that is always online and works in real time with complete visibility into critical business entities — workloads, endpoints, identities and applications — across IaaS, PaaS and SaaS environments.
- **Seamlessly deploy partner applications from the CrowdStrike Store** to add telemetry that enriches detection and response logic.
- **Unify alerts, workflows and response capabilities** under a single console for complete visibility and active response.
- **Automate workflows based on contextual insights** across the entire threat surface to reduce analysts' threat caseloads through consistency.

Start Free Trial
of Next-Gen AV

ACCELERATE RESPONSE TIME WITH NOTIFICATION WORKFLOWS

For unparalleled alert context and visibility, Falcon Prevent:

- **Build and deploy customized notification workflows** for consistent alerts, faster response and remediation time.
- **Minimize alert fatigue** with automated workflows based on threat detections, incidents and audit events.
- **Speed up response** when new threats are detected, incidents are discovered or policies are modified.
- **Set up plugin applications** enabled through the CrowdStrike Store to configure customized notifications to be sent from communication tools.

SCALE WITH CONSISTENCY AND SIMPLIFIED MANAGEMENT

Improve SOC efficiency and efficacy with scale by creating repeatable, consistent and customizable workflows.

- **Simplify management and ensure comprehensive coverage** through a unified console delivered via the cloud-scale Falcon platform and a single, lightweight agent Streamline security processes and reduce
- **Free up time** by automating away repetitive and manual tasks to focus SOC analysts' efforts on critical activities.
- **Reduce incident response time** and control the impact of security incidents with contextual insights.
- **Eliminate blind spots** with an open security cloud ecosystem that unifies alerts, workflows and response capabilities in a single console.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates approximately 6 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Learn more at **www.crowdstrike.com**