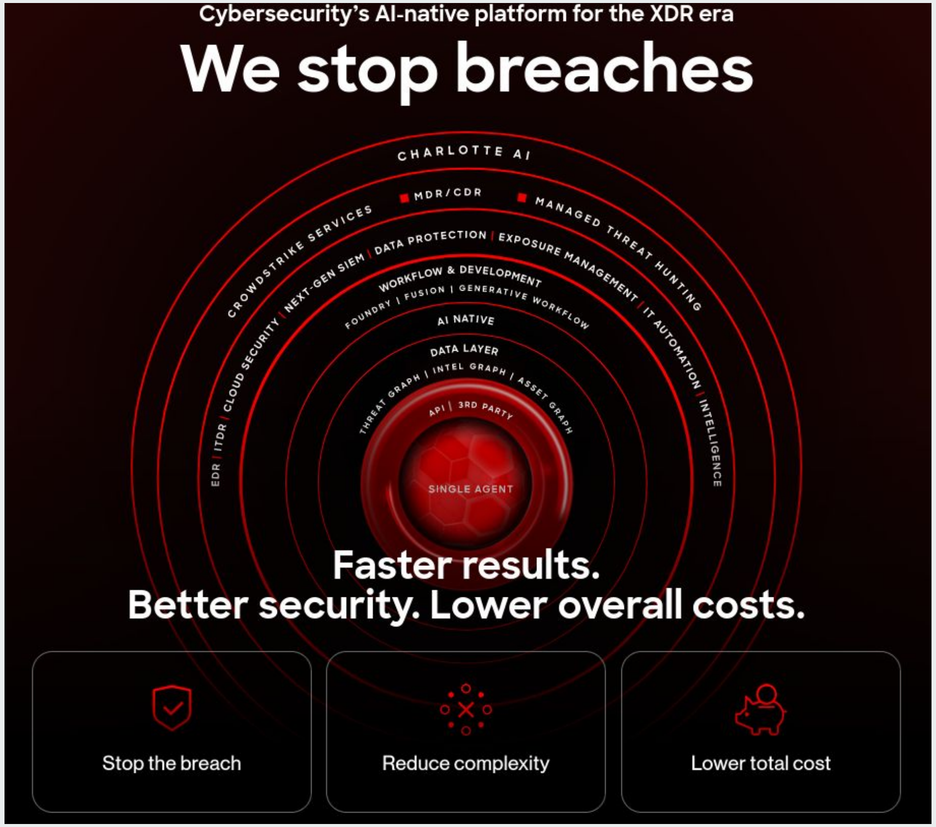
CrowdStrike Falcon

CrowdStrike Falcon is the foundation of next-generation endpoint protection.


Cybersecurity's AI-native platform for the XDR era
We stop breaches
CHARLOTTE AI
MDR/CDR
MANAGED THREAT HUNTING
CROWDSTRIKE SERVICES
EDR | ITDR | CLOUD SECURITY | NEXT-GEN SIEM | DATA PROTECTION | EXPOSURE MANAGEMENT | IT AUTOMATION | INTELLIGENCE
WORKFLOW & DEVELOPMENT
FOUNDRY | FUSION | GENERATIVE WORKFLOW
AI NATIVE
DATA LAYER
THREAT GRAPH | INTEL GRAPH | ASSET GRAPH
API | 3RD PARTY
SINGLE AGENT
Faster results.
Better security. Lower overall costs.
Stop the breach
Reduce complexity
Lower total cost

Outline

What is Crowdstrike Falcon

Solutions provided by Falcon

How to install Falcon

Real life case study of falcon being used in enterprises

What is CrowdStrike?

CrowdStrike contains various product modules that connect to a single SaaS environment. Endpoint Security Solutions are enacted on the endpoint by a single agent, known as the CrowdStrike Falcon Sensor. The Falcon Platform is broken out into Endpoint Security Solutions, Security IT & Operations, Threat Intelligence, Cloud Security Solutions, and Identity Protection Solutions.

Solution Provided by Crowdstrike

Endpoint Security Solutions

- **Falcon Insight - Endpoint Detection and Response (EDR):** Outpace the adversary with comprehensive visibility into what is happening on your endpoints, extended across all key data sources through integrated XDR.
- **Falcon Prevent - Next-Generation Antivirus (NGAV):** Stop attacks with the power of cutting-edge artificial intelligence (AI) and machine learning (ML) - from commodity malware to fileless and zero-day attacks.
- **CrowdStrike Falcon Device Control - USB Device Control:** Enhance visibility of USB device use and activity to monitor, proactively hunt, and investigate data loss incidents through comprehensive user activity context, deep file visibility, and automatic source code identification.
- **Falcon Firewall Management - Host Firewall Control:** Defend against network threats and gain instant visibility to enhance protection and inform action.
- **Falcon for Mobile - Mobile Endpoint Detection and Response**
- **Falcon Forensics - Forensic Data Analysis**

Security & IT Operations

- **CrowdStrike Falcon Discover**
  - Provides insight into your endpoint environment. This allows administrators to view real-time and historical application and asset inventory information.
- **CrowdStrike Falcon OverWatch**
  - Provides an around-the-clock managed threat hunting and email notification from the Falcon OverWatch team, alerting administrators within moments of an indicator that there is an emerging threat.
- **CrowdStrike Falcon Spotlight**
  - Offers vulnerability management by leveraging the Falcon Sensor to deliver Microsoft patch information or active vulnerabilities for devices with Falcon installed, and for nearby devices on the network.

Threat Intelligence

- **CrowdStrike Falcon Search Engine**
  - CrowdStrike Falcon MalQuery is an advanced, cloud-native malware research tool that enables security professionals and researchers to quickly search a massive dataset of malware samples, validating potential risks and stay ahead of would-be attackers.
- **CrowdStrike Falcon Sandbox**
  - Allows for controlled malware execution to provide detailed reports of threats that have been seen within your environment and gather additional data on threat actors worldwide.
- **CrowdStrike Falcon Intelligence**
  - Automatically investigate incidents and accelerate alert triage and response. Built into the Falcon platform, it is operational in seconds.

Cloud Security Solutions

- **Falcon Cloud Workload Protection - For AWS, Azure, and GCP**
  - Falcon Cloud Security delivers comprehensive breach protection for workloads, containers, and Kubernetes enabling organizations to build, run, and secure cloud-native applications with speed and confidence.
- **Falcon Horizon - Cloud Security Posture Management (CSPM)**
  - Falcon Cloud Security delivers continuous agentless discovery and visibility of cloud-native assets from the host to the cloud, providing valuable context and insights into the overall security posture and the actions required to prevent potential security incidents.
- **Container Security**

Identity Protection Solutions

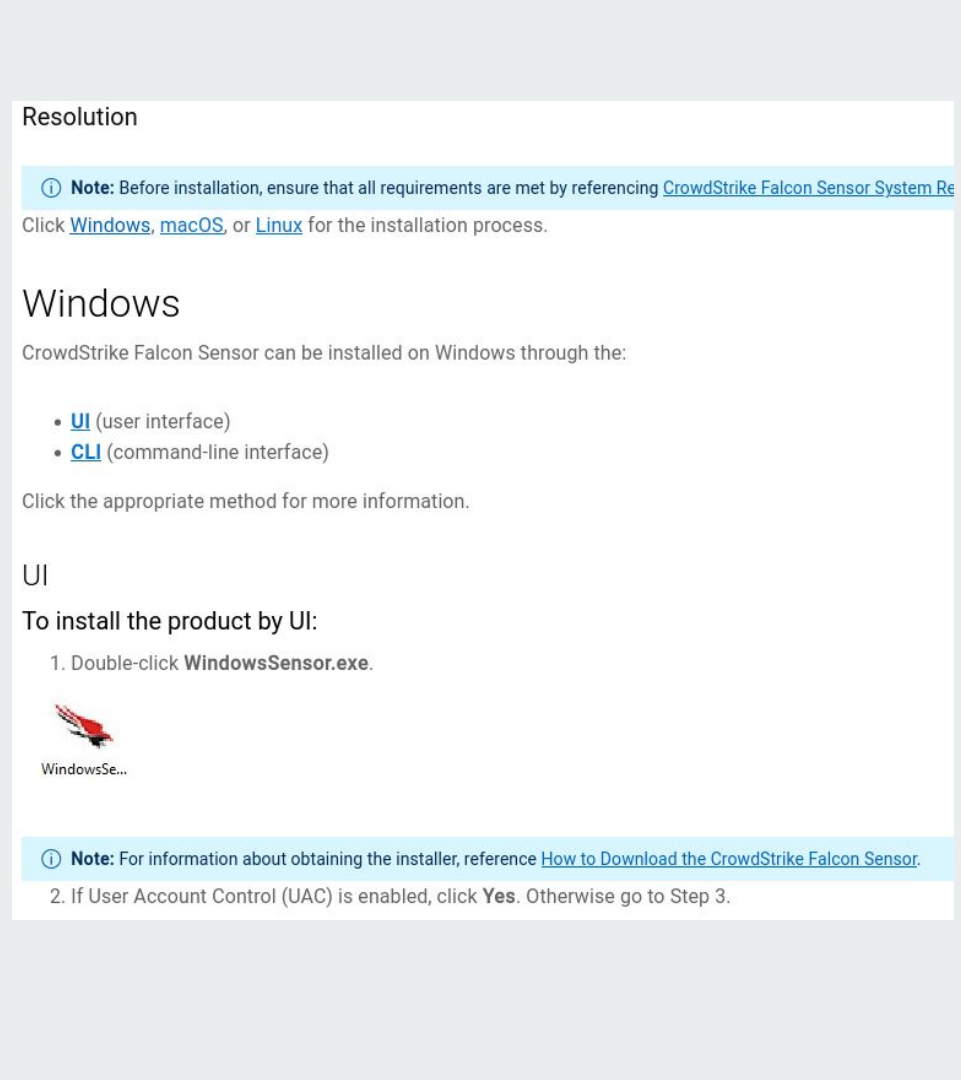
- **Falcon Identity Threat Detection (ITD)**
  - **CrowdStrike Falcon Identity Threat Detection** - Provides deep visibility into identity-based incidents and anomalies across a complex hybrid identity landscape, comparing live traffic against behavior baselines and policies to detect attacks and lateral movement in real time.

  - **CrowdStrike Falcon Identity Threat Protection** - Using a single sensor and unified threat interface with attack correlation across endpoints, workloads, and identity, Falcon Identity Threat Protection stops identity-driven breaches in real time.

Falcon Platform Bundles

- Falcon Go
- Falcon Pro
- Falcon Enterprise
- Falcon Elite
- Falcon Complete

How to install Falcon?



Resolution

ⓘ **Note:** Before installation, ensure that all requirements are met by referencing CrowdStrike Falcon Sensor System Re

Click Windows, macOS, or Linux for the installation process.

Windows

CrowdStrike Falcon Sensor can be installed on Windows through the:

- **UI** (user interface)
- **CLI** (command-line interface)

Click the appropriate method for more information.

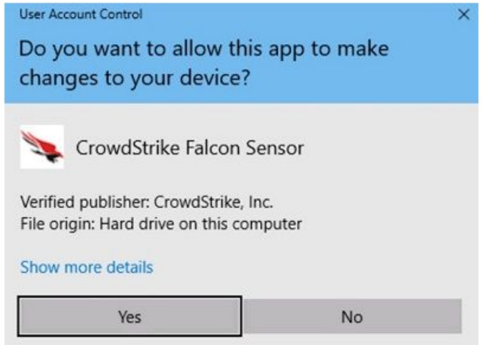
UI

To install the product by UI:

1. Double-click **WindowsSensor.exe**.

ⓘ **Note:** For information about obtaining the installer, reference How to Download the CrowdStrike Falcon Sensor.

2. If User Account Control (UAC) is enabled, click **Yes**. Otherwise go to Step 3.



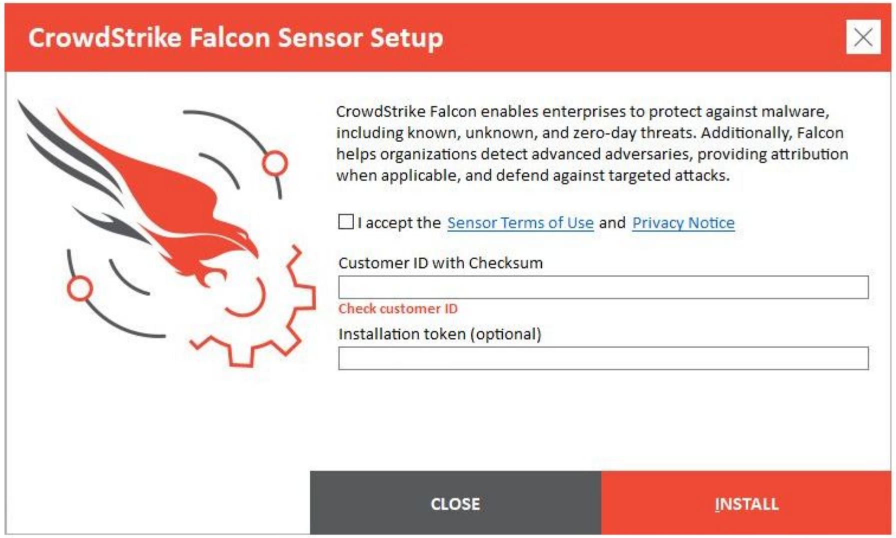
User Account Control

Do you want to allow this app to make changes to your device?

CrowdStrike Falcon Sensor

Verified publisher: CrowdStrike, Inc.
File origin: Hard drive on this computer

3. In the install UI:
   A. **Accept the license agreement.**
   B. Populate the **Customer ID**.
   C. Click **Install**.



CrowdStrike Falcon Sensor Setup

CrowdStrike Falcon enables enterprises to protect against malware, including known, unknown, and zero-day threats. Additionally, Falcon helps organizations detect advanced adversaries, providing attribution when applicable, and defend against targeted attacks.

□ I accept the Sensor Terms of Use and Privacy Notice

Customer ID with Checksum

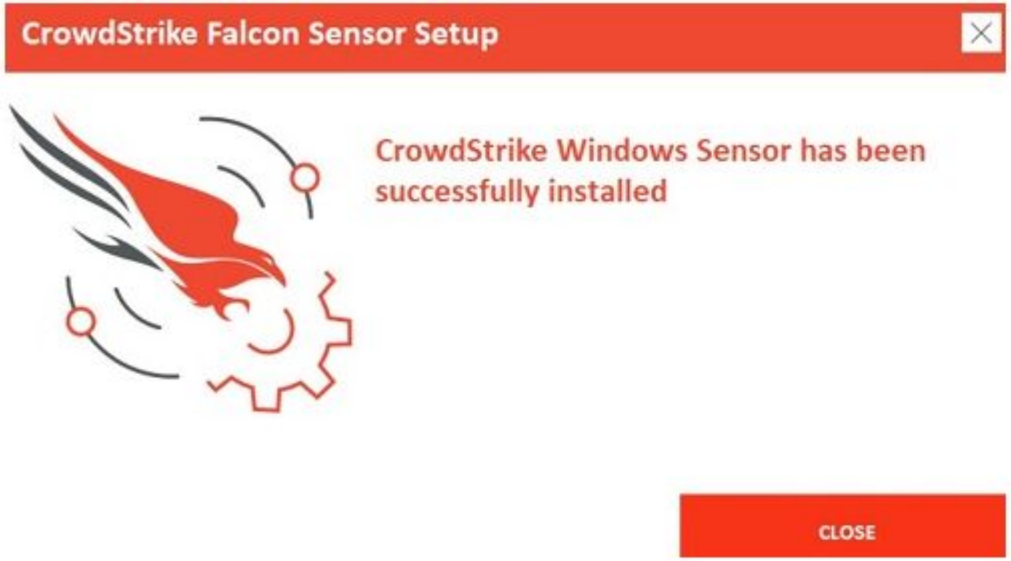
Check customer ID

Installation token (optional)

ⓘ **Note:**

- To locate the Customer ID (CID), reference How to Obtain the CrowdStrike Customer Identification (CID).
- The CID is used to associate the endpoint to the CrowdStrike Falcon Console.

4. On successful installation, click **Close**.



CrowdStrike Windows Sensor has been successfully installed

Case Study:
How Investment Banking Firm, Greenhill, Uses Falcon

GreenHill

INVESTMENT REPORTING

About GreenHill

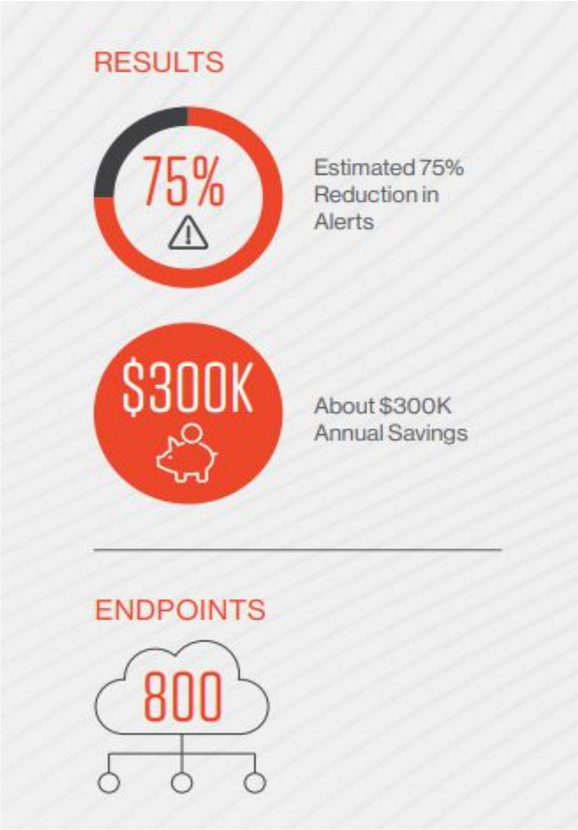
Greenhill is a global independent investment bank that advises corporations, partnerships, institutions and governments on matters that include financing, restructuring, raising capital, and mergers and acquisitions. From 17 offices on five continents, the firm uniquely focuses on client services versus investing, trading, underwriting or lending.

Greenhill's team of managing directors averaging over 25 years' experience provides seasoned insight to all major industries and markets. They have built a reputation for independence, discretion and providing unconflicted advice, particularly in cases of shareholder activism

Integration of CrowdStrike Falcon

Greenhill witnessed significant business value with an estimated **75% reduction in alerts** and **cost savings of $300K per year**.

Greenhill leveraged CrowdStrike solutions for its detection and forensics capabilities, leading to additional security deployments including complete endpoint detection and response (EDR), managed services and consulting services.



RESULTS

75%

Estimated 75% Reduction in Alerts

$300K

About $300K Annual Savings

ENDPOINTS

800

Why GreenHill chose Falcon

“At first, the lightweight single agent attracted us to CrowdStrike,” he says. “It was incredibly **easy to implement and roll out globally**. We were able to deploy agents and have the system running in an hour. And the agents continually update, which is fantastic. We are in a constant battle to keep our security updated and CrowdStrike is not one that we have to worry about.”

As the CrowdStrike Falcon® platform evolved to stay ahead of the threat landscape, Greenhill added extra capabilities including endpoint protection, next-gen antivirus and Falcon Firewall Management™. “CrowdStrike does a really **good job of looking into the future and delivering solutions** that our business needs,” he says.

The Falcon platform was **built from the ground up rather than through acquisitions**, a factor that has given Shaffer the confidence to trust CrowdStrike as “an extension of our security department.”

Features of CrowdStrike Falcon

Features

- ➔ Falcon Complete adds a team of security experts that handle every aspect of CrowdStrike's endpoint security technology for Greenhill. They assist with all security tasks, including deploying and managing the Falcon platform from the initial onboarding and configuration stages, to prevention health checks, maintenance and operations, incident triage, and hands-on remote remediation.
- ➔ Another benefit is the day-to-day guidance from CrowdStrike engineers. "The team has been incredibly responsive. Without that support we would be doing that on our own, with any tool, and it would be trial by fire."

Result

Greenhill’s long-standing partnership with CrowdStrike enables the investment bank to spend less time on security and more time providing value to its end users.

“Our needs are focused and targeted,” Shaffer explains. “We want to make sure our applications and laptops work and that we can conduct business remotely. All the behind-the-scenes security CrowdStrike does to make sure our environment is safe means we can spend time on projects that are more meaningful and more effective for our end users.”

References

https://www.dell.com/support/kbdoc/en-in/000126839/what-is-crowdstrike

https://www.crowdstrike.com/resources/customer-stories/greenhill/

https://www.crowdstrike.com/falcon-platform/