CROWDSTRIKE

Data Sheet

FALCON FORENSICS

Streamlining triage data collection and analysis

TRIAGE LARGE-SCALE INVESTIGATIONS QUICKLY IN A SINGLE SOLUTION

Falcon Forensics is CrowdStrike's powerful forensic data collection solution. It allows threat hunters and responders to speed up investigations and conduct periodic compromise assessments, threat hunting and monitoring.

With CrowdStrike® Falcon Forensics, responders are able to streamline the collection of point-in-time and historic forensic triage data for robust analysis of cybersecurity incidents. Responders gain the ability to research and investigate incidents faster and with greater precision. Falcon Forensics leverages a dissolvable executable and the CrowdStrike cloud, which leaves a minimal trace on endpoints. Streamlined management via the Falcon Forensics console and dashboards makes triage fast and easy.

KEY CAPABILITIES

Falcon Forensics is a robust solution that simplifies forensic data analysis by eliminating the need for multiple tools or data ingestion methods. Analysts can quickly gather and analyze large quantities of historical data to triage incidents and accelerate compromise assessments.

IMPROVE EFFICACY AND TIME-TO-RESPOND

Zero in on attacker activity with preset dashboards. Live and historical deep-level triage data served up in preset dashboards eliminates lengthy research time to respond to incidents, speeding analysis and triage. Responders can target attacker activity with convenient filters, queries and dashboards to quickly gain essential insights. Dashboard capabilities include:

- **Deployment status:** Gain visibility over collections and trends for the past 24 hours across your enterprise.
- **High-level telemetry view of a single system:** See contextual information about an attacker's activity outside a single query, with pictorial histograms within a given timeframe.

KEY BENEFITS

Simplify forensic data collection and analysis in one single solution

Dive into vast amounts of organized data quickly, including historical artifacts

Accelerate triage analysis of an incident with the use of preset dashboards

Save valuable time by targeting incident analysis using customizable dashboards, filters and queries

Download and export data via Falcon Data Replicator (FDR)

- **Quick Wins displaying high signal-to-noise ratios:** Quickly identify potential misconfigurations and hacker activity with preset panel groupings. Customize the dashboard by selecting groupings relevant to your analysis.
- **Timeline format for a single system:** Gather and analyze multiple artifacts for a single system and timeframe. Use this host timeline dashboard to get a visual representation of artifacts for a specific timeline of events.

REDUCE WORKFLOW COMPLEXITY

Harness the power of CrowdStrike Real Time Response and Falcon Forensics with their simple, large-scale deployment ability. Easy to deploy, Falcon Forensics can get you up and running in a minimal amount of time, from a single workstation to tens of thousands of endpoints.

- Operate with a single solution and eliminate time-consuming efforts to collect and consolidate forensics data.
- Deploy Falcon Forensics via CrowdStrike's Real Time Response for quick and easy deployment.
- Leverage the cloud for data processing, freeing up systems to continue business-critical functions.
- Gather collected data from ten to hundreds of thousands of endpoints with large-scale deployment capability.
- Avoid ongoing maintenance and management. The Falcon Forensics dissolvable agent performs the collection of artifacts and then removes itself from the system, leaving minimal trace. It does not persistently remain as yet another agent to maintain and manage on systems.

SIMPLIFY DATA COLLECTION AND RESEARCH

Falcon Forensics provides the ability to automate data collection while also providing a convenient console that gives responders detailed information about an incident.

- Tap into full threat context without lengthy queries or full disk image collections.
- Uncover attacker activity that may have occurred before Falcon endpoint detection and response (EDR) monitoring.
- Take advantage of advanced query capabilities for in-depth research. In addition to preset and packaged dashboards, Falcon Forensics makes the raw event data available so responders can customize their queries.
- Track attacker activity by analyzing the Master File Table (MFT), shim cache, shellbags and other artifacts within your organization.
- Gain critical contextual data on threats and specific threat actors by combining historical forensics data with CrowdStrike's advanced threat intelligence — giving a holistic picture of specific attack methods and techniques an attacker might use.

A SINGLE SOLUTION FOR FAST FORENSIC COLLECTION AND ANALYSIS

Reduce deployment complexity by integrating CrowdStrike's Real Time Response

Tap into the full power of contextual data by using incident analysis in conjunction with CrowdStrike threat actor intelligence

See the detailed threat context of an incident without the need for lengthy queries

Keep business systems functioning at a high level with a dissolvable executable and cloud processing

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint 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 on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.