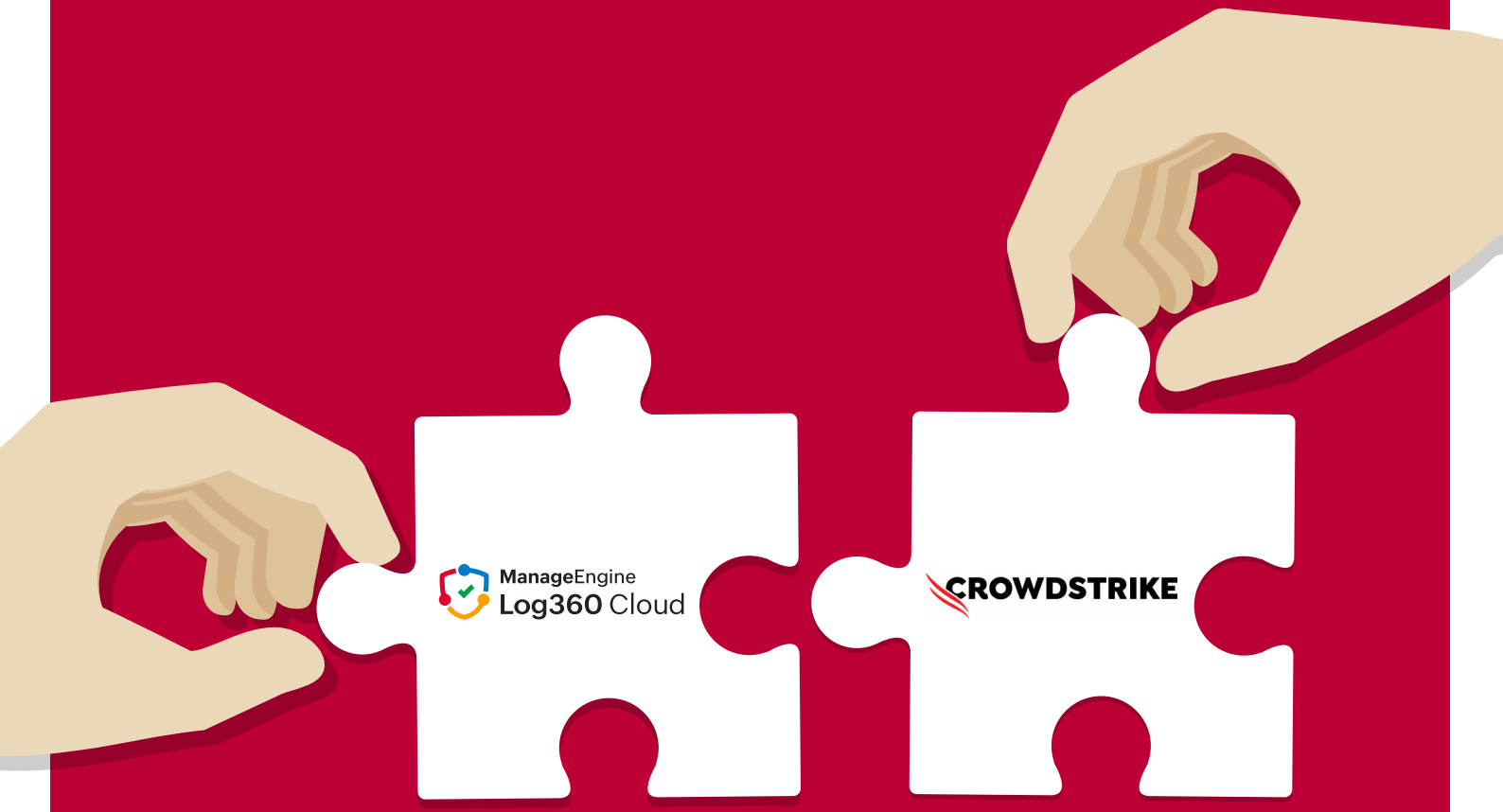
ManageEngine
Log360 Cloud

DATASHEET

CrowdStrike Falcon integration with Log360 Cloud



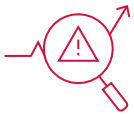
Overview

CrowdStrike Falcon is a cloud-based endpoint protection platform that generates high-volume detection, audit, and response telemetry.

The CrowdStrike Falcon Event Streams integration enables Log360 Cloud to ingest Falcon detection and audit events for centralized analysis, correlation, and long-term retention. This integration focuses on visibility and investigation, extending endpoint detections into SIEM-driven correlation and response workflows.

Data collected

The integration ingests Falcon events using the Event Streams API, including:



Detection summary events

Authentication audit events

User activity audit events

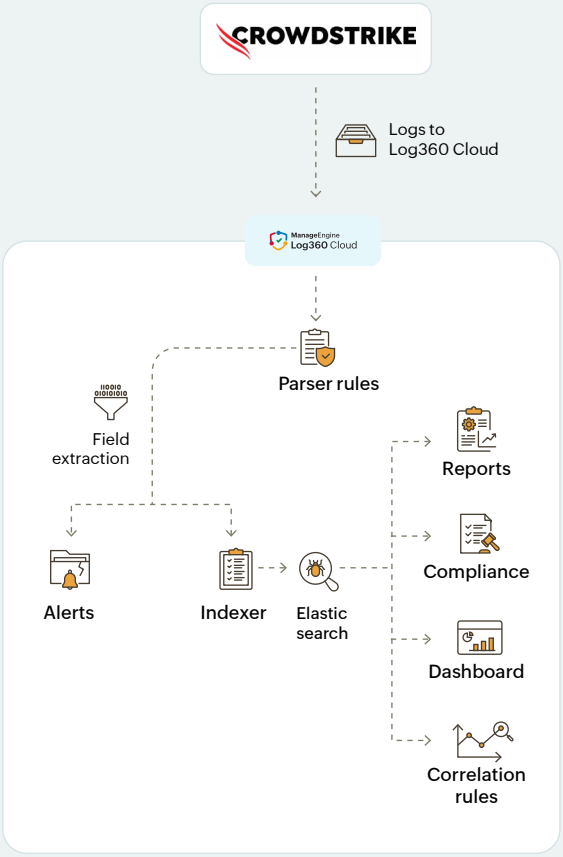
Firewall match events

Remote response session events

These events are parsed, indexed, and stored in Log360 Cloud for search, reporting, correlation, and investigation.

How it works

1. Log360 Cloud connects to CrowdStrike Falcon using OAuth2 API credentials.
2. Falcon Event Streams continuously push detection and audit events.
3. Events are parsed and normalized by Log360 Cloud.
4. Data is made available for:
   - Search and investigation
   - Correlation with other SIEM sources
   - Detection rules and alerts
   - Incident Workbench analysis
   - SOAR actions



Use cases and challenges | How Log360 Cloud helps

Use case / challenge	How the integration helps
Isolated endpoint detections	Centralizes Falcon detections with network, identity, and cloud logs.
High alert volume	Enables correlation to reduce noise and false positives.
Limited investigation context	Enriches Falcon alerts with user, device, and historical activity.
Compliance log retention	Stores Falcon audit and detection logs long term.
Manual cross-tool analysis	Enables pivoting across Falcon, SIEM, and other sources in one console.

Analytics available

Once CrowdStrike Falcon is integrated, Log360 Cloud extends endpoint telemetry into centralized visibility, correlated threat detection, investigation context, and automated response workflows.

Detection Visibility and Trend Analysis

Falcon detection, authentication, audit, and policy events are transformed into searchable summaries and trend views that help teams understand activity patterns across devices and users.

This includes reports on:

- Detection volume trends over time to identify spikes
- Severity distribution across endpoints
- Device-based detection summaries to highlight impacted systems
- Authentication and audit activity tracking

Examples:

Detection Trend View

Displays detection count changes over selected timeframes to identify unusual surges.

Device Activity Summary

Highlights endpoints generating the highest detection volume to prioritize investigation.

Security Posture Monitoring

The integration continuously evaluates Falcon configuration and protection states to identify risk conditions and alert in Log360 Cloud.

This includes monitoring:

- Disabled credential protection mechanisms
- Tamper protection status
- Privilege or policy changes that impact endpoint security

Examples:

- Credential dumping protection disabled
- Falcon sensor tamper protection turned off

These controls help detect misconfigurations and evasion attempts early.

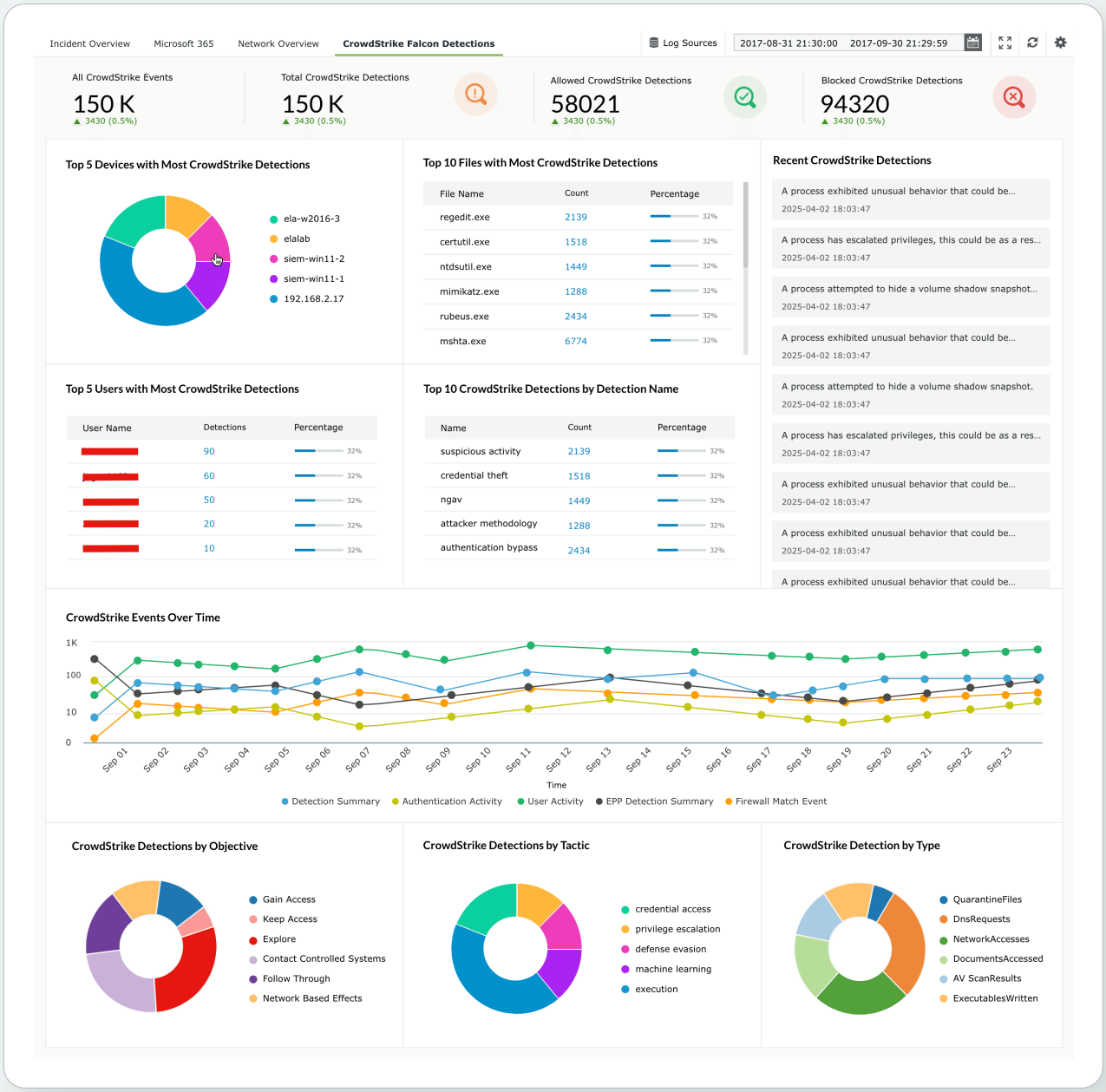
Real-Time Operational Visibility

Gain instant insight into detection distribution, affected entities, and tactical breakdowns through a prebuilt dashboard for Crowdstrike.

This includes:

- Detection trends by tactic and objective
- Top affected devices and users
- Frequently triggered files
- Detection status distribution (blocked vs allowed)

These views allow SOC teams to assess impact at a glance.



Correlated Threat Detection

Falcon detections are correlated with Windows events and other SIEM sources to uncover multi-stage or fileless attack chains that may not be visible from endpoint data alone.

This enables identification of:

- Credential theft preparation activity
- Fileless LOLBin-based execution chains
- Registry modifications linked to attack techniques

Examples:

- Registry modification + Falcon “credential theft” detection → flags credential dumping preparation
- Suspicious regsvr32 execution + high-severity Falcon execution detection → flags fileless attack chain

This reduces noise and surfaces high-confidence threats.

Incident investigation support

CrowdStrike-specific context is embedded inside the Incident Workbench, allowing analysts to pivot across endpoint telemetry and SIEM data without switching tools.

This provides:

- Device-level threat summaries
- Recent detection timelines
- Frequently involved files
- Historical alert correlation

This accelerates root-cause analysis and scope assessment.

Automated Playbooks (Response & Remediation)

Native SOAR actions and pre-built playbooks in Log360 Coud allow automated enrichment, investigation, containment, remediation, and policy changes directly from Falcon detections.

Actions Category	Example Actions	Example in a Playbook
Threat Containment and Active Response	Isolate Endpoint, Kill Process, Delete File, Apply Quarantine File Action	If a high-severity Falcon detection is confirmed, automatically isolate the endpoint, kill the malicious process, delete the dropped file, and notify SOC before lifting containment.
Detection and Incident Management	Search Detection, List Detection Summaries, Get Detections for Incident, Resolve Detection, List Incident Summaries	When a detection is triggered, fetch detection details, correlate with related incidents, update status to "Resolved" after containment, and document the response automatically.
Endpoint and Policy Administration	Create/Update/Delete Host Group, Create ML Exclusion, Update ML Exclusion, Delete ML Exclusion, Create Scheduled ODS Scan	During an active campaign, move affected endpoints to a restricted host group, apply stricter policies, or create an ML exclusion for validated false positives.
Investigation and Remote Forensics	List Processes, List Network Stats (netstat), Read Registry, Retrieve File, List Host Files, Get Script	Upon suspicious behavior, automatically retrieve running processes, inspect registry keys, collect suspicious files, and attach findings to the incident for deeper analysis.

Outcomes

By integrating CrowdStrike Falcon with Log360 Cloud, organizations gain:

- Centralized visibility into endpoint detections
- Better investigation context through correlation
- Improved audit and compliance readiness
- Reduced manual effort during incident analysis

ManageEngine
Log360 Cloud

About Log360 Cloud

ManageEngine Log360 Cloud, a unified cloud SIEM solution with integrated CASB capabilities, helps enterprises secure their network from cyberattacks. With its security analytics, threat intelligence and incident management capabilities, Log360 Cloud helps security analysts spot, prioritize and resolve threats in both on-premises and cloud environments. The solution is highly scalable and helps drive down infrastructure and storage costs.

For more information about Log360 Cloud, visit www.manageengine.com/cloud-siem/.

Sign-up for free

Get a personalized walk-through