Dynatrace and CrowdStrike: Better Together

Connect security findings with logs, application, and infrastructure context

Dynatrace and CrowdStrike unify security, logs, and observability workflows to help teams investigate incidents with shared context while reducing duplicate telemetry and cost.

Outage, incident, or breach? Get the context to investigate faster

Key benefits:

- Engage the right team with context that helps distinguish an attack from an outage, incident or breach.
- Identify root cause faster with security, log, and application context in one place.
- Add Dynatrace context to CrowdStrike Falcon investigations without moving the underlying data.
- Reduce duplicate telemetry by routing logs and other telemetry to the right platforms.

Challenges

When an incident occurs, security and operations teams can see different parts of the same problem. Security teams investigate threat activity in CrowdStrike Falcon, while IT operations, platform engineering, and SRE teams investigate application and infrastructure behavior in Dynatrace.

Connecting security and observability context across separate workflows can slow investigation. Organizations may also collect and ingest overlapping logs and telemetry across platforms, increasing data volume and cost.

Solution: Bring CrowdStrike context into Dynatrace

Bring CrowdStrike security context into Dynatrace so operations teams can investigate security activity alongside log, application, infrastructure, and topology data.

Bring Dynatrace context into CrowdStrike Falcon: Use Federated Search to query Dynatrace telemetry from CrowdStrike Falcon and add observability context to security investigations without moving the underlying data.

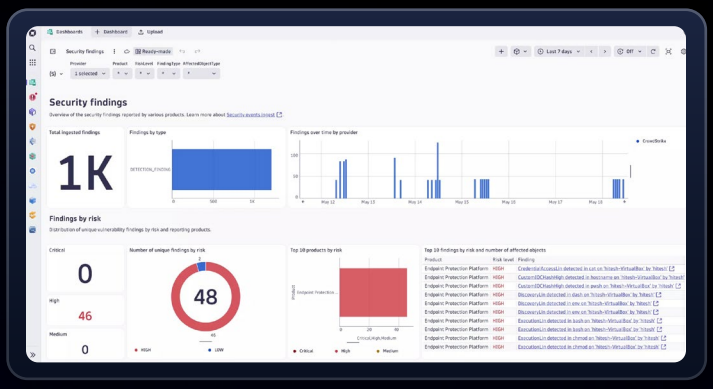
Reduce telemetry costs with Bindplane by Dynatrace: Collect, process, and route logs and other telemetry before ingestion to control what data reaches Dynatrace, CrowdStrike Falcon, or other destinations.

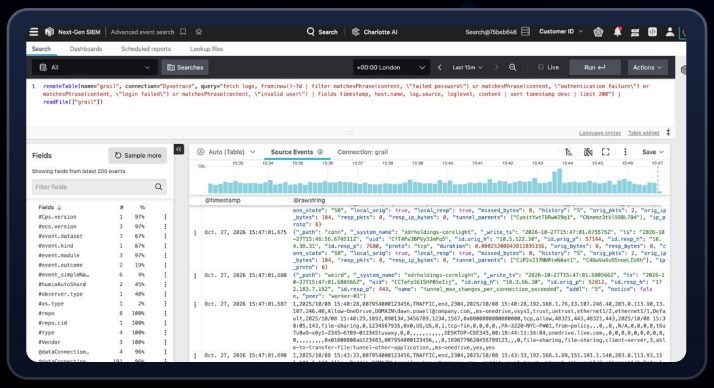
Business Value

Use Case / Challenge	Solution	Benefits
Security sees the threat, not the application impact	Federated Search brings Dynatrace logs and observability context into the CrowdStrike Falcon investigation	Investigate root cause with broader context without moving the underlying Dynatrace data
Operations need to determine whether an issue is an outage or an attack	CrowdStrike endpoint security context in Dynatrace can be investigated alongside logs, application and infrastructure data	Help teams determine who should investigate and reduce unnecessary escalations
Duplicate log and telemetry collection increases data volume and cost	Bindplane by Dynatrace collects, processes, and routes logs and other telemetry before ingestion	Reduce duplicate data ingestion and cost while controlling where logs and other telemetry go.

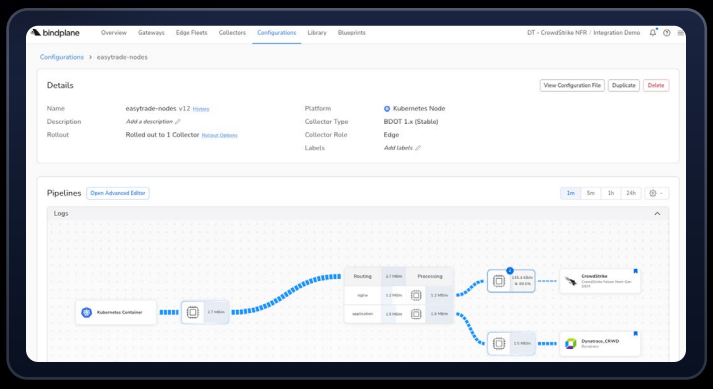
Technical Solution: Three integrations connect Dynatrace and CrowdStrike

The Falcon Insight XDR connector brings endpoint detection and response (EDR) telemetry into Dynatrace.





CrowdStrike Federated Search for Dynatrace lets analysts query Dynatrace from Falcon Next-Gen SIEM without moving data.



Bindplane by Dynatrace routes logs and other telemetry before platform ingestion.

Key Capabilities

- **CrowdStrike endpoint security telemetry in Dynatrace:** Investigate CrowdStrike security context alongside logs, application, infrastructure, and topology data in Dynatrace.
- **Dynatrace context in CrowdStrike Falcon:** Query Dynatrace observability data from CrowdStrike Falcon through Federated Search without moving the underlying data and added egress cost.
- **Log and telemetry routing:** Use Bindplane by Dynatrace to route logs and other telemetry before ingestion. Route security events to CrowdStrike Falcon and observability data to Dynatrace, or send telemetry to both.
- **Telemetry volume control:** Filter, transform, and reduce telemetry before it reaches downstream platforms to help control ingestion volume and cost.

ABOUT DYNATRACE

Dynatrace is advancing observability for today's digital businesses, helping to transform the complexity of modern digital ecosystems into powerful business assets. By leveraging AI-powered insights, Dynatrace enables organizations to analyze, automate, and innovate faster to drive their business forward. Learn more at www.dynatrace.com.

ABOUT CROWDSTRIKE

CrowdStrike has redefined security with the world's most advanced cloud-native platform for protecting critical areas of risk — endpoints and cloud workloads, identity, and data. The Falcon® platform harnesses real-time threat intelligence and enterprise telemetry to automate threat prevention, detection, remediation, hunting, and vulnerability observability through a single, intelligent, lightweight agent. Try it for free. ©2024 CrowdStrike, Inc. All rights reserved.

dynatrace

dynatrace.com/blog @dynatrace linkedin.com/company/dynatrace @dynatrace

11.02.26 BAE30055_WP_USLet_mt