CrowdStrike Falcon Platform and Gigamon ThreatINSIGHT

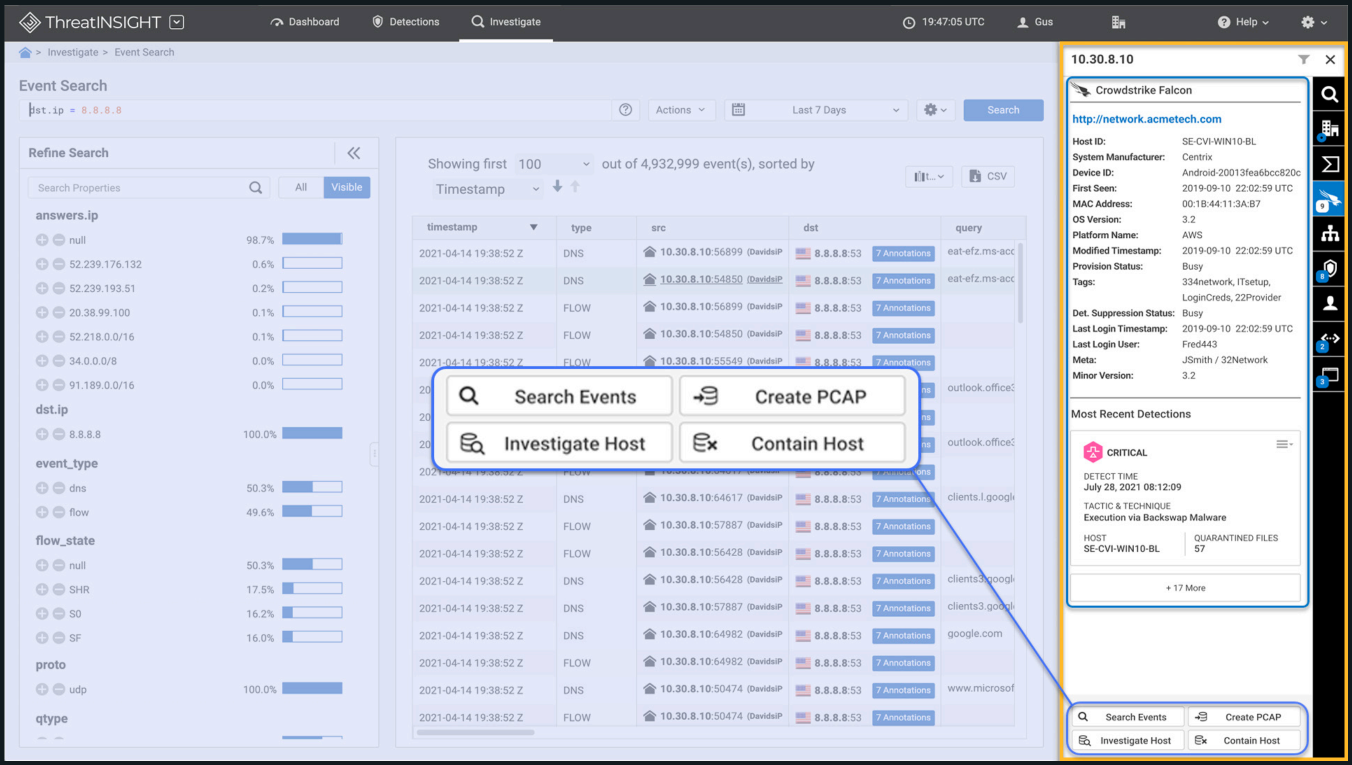
Seamless Net-to-End Visibility and Detection to Stop Attackers in Their Tracks

Without in-depth visibility into device activity and network traffic to identify adversary behaviors, security teams are at a loss to defend against cyberattacks. Aggregation of logs and alerts from frontline security tools don't provide SOC and IR teams the context necessary to effectively detect and respond to attackers who have already bypassed those same tools. Security teams seeking to address this SOC visibility gap and increase effectiveness have turned to network detection and response (NDR) and endpoint detection and response (EDR) solutions to establish the foundational visibility necessary to combat adversaries; however, not all NDR and EDR integrations provide the same level of integration, visibility, and detection.

THE OVERVIEW

Gigamon has partnered with CrowdStrike to provide users with a fully unified detection and response solution for active threats. As cyberattacks escalate in speed and sophistication, defenders need tools that help them stay ahead. The seamless cloud-to-cloud integration between Gigamon ThreatINSIGHT and the Falcon platform ensures the right data is available at the right time to the right people from within the ThreatINSIGHT web portal.

- Falcon X threat intelligence is applied against real-time network traffic for immediate detections
- Falcon Insight detections appear alongside ThreatINSIGHT machine learning and threat intelligence detections for fast adversary identification
- Falcon Insight endpoint telemetry appears alongside the ThreatINSIGHT solution's L2 – L7 network telemetry to speed triage, hunting, and investigations



Event Search

`dst.ip = 8.8.8.8`

answers.ip

null	98.7%
52.239.176.132	0.6%
52.239.193.51	0.2%
20.38.99.100	0.1%
52.218.0.0/16	0.1%
34.0.0.0/8	0.0%
91.189.0.0/16	0.0%

dst.ip

8.8.8.8	100.0%

event_type

dns	50.3%
flow	49.6%

flow_state

null	50.3%
SHR	17.5%
S0	16.2%
SF	16.0%

proto

udp	100.0%

qtype

Showing first 100 out of 4,932,999 event(s), sorted by Timestamp

timestamp	type	src	dst		query
2021-04-14 19:38:52 Z	DNS	10.30.8.10:56899 (DavidsiP	8.8.8.8:53	7 Annotations	eat-efz.ms-acc
2021-04-14 19:38:52 Z	DNS	10.30.8.10:54850 (DavidsiP	8.8.8.8:53	7 Annotations	eat-efz.ms-acc
2021-04-14 19:38:52 Z	FLOW	10.30.8.10:56899 (DavidsiP	8.8.8.8:53	7 Annotations	
2021-04-14 19:38:52 Z	FLOW	10.30.8.10:54850 (DavidsiP	8.8.8.8:53	7 Annotations	
2021-04-14 19:38:52 Z	FLOW	10.30.8.10:55549 (DavidsiP	8.8.8.8:53	7 Annotations	
20				ns	outlook.office3
20				ns	
20				ns	outlook.office3
2021-04-14 19:38:52 Z	FLOW		8.8.8.8:53	7 Annotations	
2021-04-14 19:38:52 Z	DNS	10.30.8.10:64617 (DavidsiP	8.8.8.8:53	7 Annotations	clients.l.googl
2021-04-14 19:38:52 Z	FLOW	10.30.8.10:57887 (DavidsiP	8.8.8.8:53	7 Annotations	
2021-04-14 19:38:52 Z	FLOW	10.30.8.10:56428 (DavidsiP	8.8.8.8:53	7 Annotations	
2021-04-14 19:38:52 Z	DNS	10.30.8.10:56428 (DavidsiP	8.8.8.8:53	7 Annotations	clients3.googl
2021-04-14 19:38:52 Z	DNS	10.30.8.10:57887 (DavidsiP	8.8.8.8:53	7 Annotations	clients3.googl
2021-04-14 19:38:52 Z	DNS	10.30.8.10:64982 (DavidsiP	8.8.8.8:53	7 Annotations	google.com
2021-04-14 19:38:52 Z	FLOW	10.30.8.10:64982 (DavidsiP	8.8.8.8:53	7 Annotations	
2021-04-14 19:38:52 Z	DNS	10.30.8.10:50474 (DavidsiP	8.8.8.8:53	7 Annotations	www.microsof
2021-04-14 19:38:52 Z	FLOW	10.30.8.10:50474 (DavidsiP	8.8.8.8:53	7 Annotations	

10.30.8.10

Crowdstrike Falcon

http://network.acmetech.com

Host ID:	SE-CVI-WIN10-BL
System Manufacturer:	Centrix
Device ID:	Android-20013fea6bcc820c
First Seen:	2019-09-10 22:02:59 UTC
MAC Address:	00:1B:44:11:3A:B7
OS Version:	3.2
Platform Name:	AWS
Modified Timestamp:	2019-09-10 22:02:59 UTC
Provision Status:	Busy
Tags:	334network, ITsetup, LoginCreds, 22Provider
Det. Suppression Status:	Busy
Last Login Timestamp:	2019-09-10 22:02:59 UTC
Last Login User:	Fred443
Meta:	JSmith / 32Network
Minor Version:	3.2

Most Recent Detections

CRITICAL

DETECT TIME
July 28, 2021 08:12:09

TACTIC & TECHNIQUE
Execution via Backswap Malware

HOST
SE-CVI-WIN10-BL

QUARANTINED FILES
57

THE CHALLENGE

Gaps in SOC visibility allow adversaries to persist, escalate privileges, move laterally, and exfiltrate data or cause damage, whether it be ransomware or a data breach.

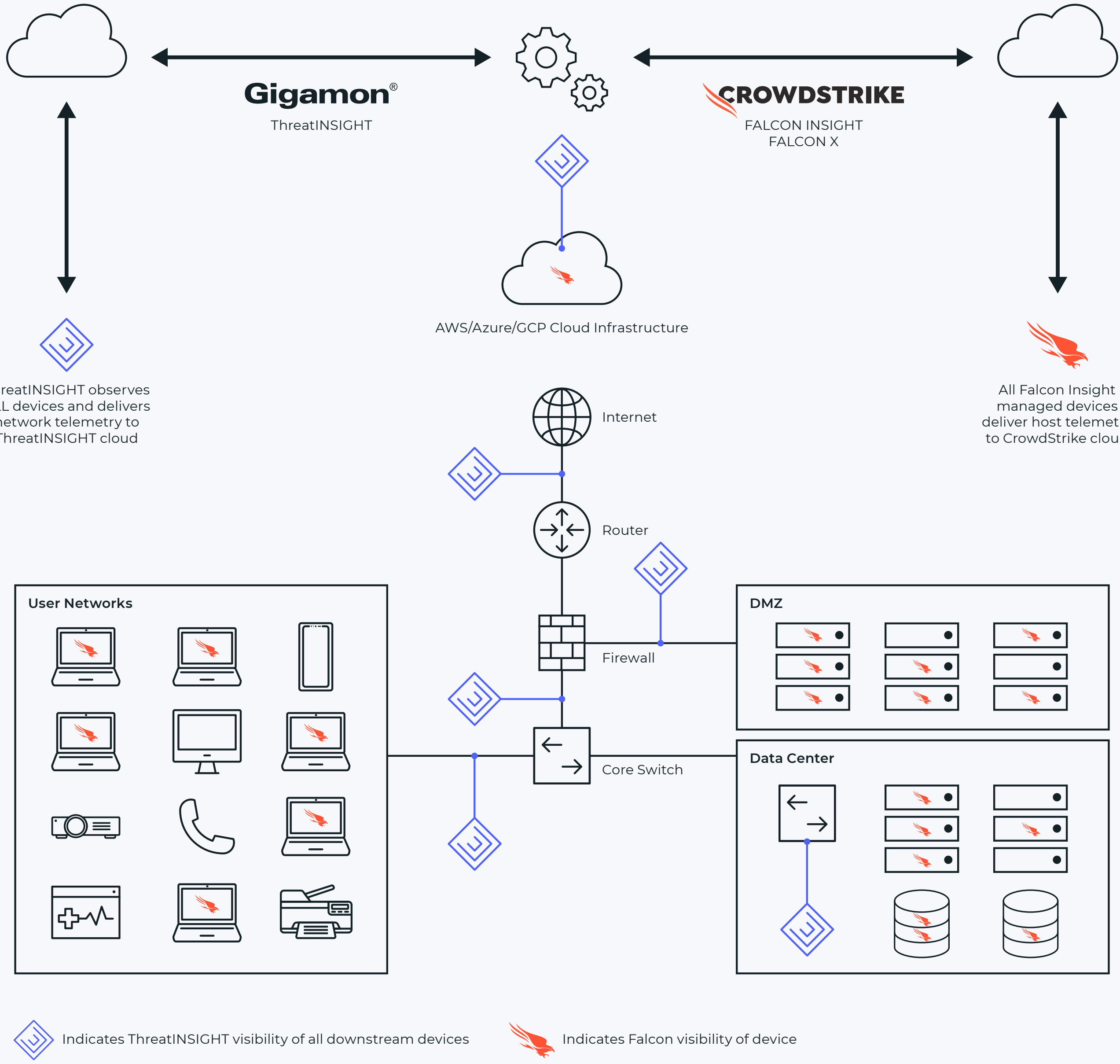
THE SOLUTION

To optimize effectiveness, ThreatINSIGHT NDR integrates with the Falcon platform, delivering seamless net-to-end visibility, combined threat intelligence, behavioral threat detection, and the tools and telemetry to stop attackers in their tracks.

JOINT SOLUTION BENEFITS

- Close the SOC visibility gap with in-depth host and L2–L7 network telemetry in a single console
- IoT, BYOD, and unmanaged host visibility for devices where Falcon is not present
- Indicate if host has Falcon agent present
- Correlated Gigamon and CrowdStrike ML and threat intel for quicker detections
- Efficient, effective access to data and tools for hunting/investigation within a single platform
- Contain compromised endpoints in real time from within ThreatINSIGHT
- Distraction-free, cloud-to-cloud integration, with zero maintenance

Cloud-to-Cloud Integration


Gigamon®
ThreatINSIGHT
CROWDSTRIKE
FALCON INSIGHT
FALCON X
AWS/Azure/GCP Cloud Infrastructure
ThreatINSIGHT observes ALL devices and delivers network telemetry to ThreatINSIGHT cloud
All Falcon Insight managed devices deliver host telemetry to CrowdStrike cloud
Internet
Router
Firewall
Core Switch
User Networks
DMZ
Data Center
Indicates ThreatINSIGHT visibility of all downstream devices
Indicates Falcon visibility of device

> The power of the CrowdStrike EDR/Gigamon NDR integration is twofold: It provides SOC and IR teams unparalleled, in-depth visibility and is a customer-inspired, feature-rich integration to combat adversaries.”

– MICHAEL DICKMAN, GIGAMON CHIEF PRODUCT OFFICER

SCENARIOS

	Technical Capabilities	Why SOC/IR Teams Should Care	Why Security Leaders Should Care
Avoid multi-vendor headaches	Out-of-the-box, cloud-to-cloud integration with both Falcon X threat intelligence and Falcon Insight EDR.	Fewer distractions with zero integration work or ongoing maintenance.	Fast time to value; security teams can focus on threats, not solutions management.
Close SOC visibility gaps	In-depth host telemetry for managed devices and L2-L7 network metadata for all devices within ThreatINSIGHT. NOTE: Most NDRs can only provide L2–L4 visibility for all devices.	Observe all devices (x-axis breadth) with rich host and network context (y-axis depth) within a single console to perform triage, hunting, and investigations across current and historical activity (z-axis time).	In-depth context for SOC teams on a single platform — for both efficiency and effectiveness.
Achieve IoT, BYOD, and unmanaged device visibility	ThreatINSIGHT observes the behavior of all managed and unmanaged devices and enumerates for any device whether the Falcon agent is present or not.	Secure all devices, plus make informed response decisions even when Falcon agent is not present.	Visibility into EDR gaps for better response decisions on all hosts, not just managed ones.
Faster threat intelligence detections	Utilize both ThreatINSIGHT's proprietary threat intelligence and the Falcon X threat intelligence on live network traffic.	Faster Falcon X threat intelligence detections via real-time matches for all network devices versus trying to match against historical log data within your SIEM.	Get more out of your Falcon X investment by applying matches on live traffic, not just SIEM history.
Behavioral detection corroboration	Observe, triage, and investigate both ThreatINSIGHT and Falcon Insight behavioral-based detections with correlated telemetry.	High-fidelity adversary behavior identification using CrowdStrike and Gigamon Machine Learning and Behavioral Analysis techniques.	Improve mean time to detect by combining network and endpoint adversary behavior identification techniques.
Hunting and incident investigations	Query the Falcon platform's host-based telemetry alongside enriched network metadata with ThreatINSIGHT advanced investigation capabilities.	Rich L2–L7 network and robust endpoint telemetry at your fingertips.	Data and tools for hunting teams on a single platform — for both efficiency and effectiveness.
Host management	For any host being explored within ThreatINSIGHT, right-click to pivot directly into CrowdStrike to manage that device.	ThreatINSIGHT detections can quickly be investigated within Falcon Insight.	Reduce complexity and drive faster mean time to respond.
Host isolation	For any host being explored within ThreatINSIGHT, easily isolate the device with a single click.	Mitigate risk quickly once a device has been triaged and confirmed infected from within ThreatINSIGHT.	Take swift action, improving mean time to contain.

Conclusion

Focused on enabling and empowering joint customers to detect and respond with certainty, the ThreatINSIGHT, Falcon Insight, and Falcon X products combine to provide a fully unified NDR and EDR integration to close the SOC visibility gap and dismantle adversaries.

For more information on Gigamon ThreatINSIGHT and CrowdStrike, please visit:

GIGAMON.COM/THREATINSIGHT | CROWDSTRIKE.COM

WHY GIGAMON?

Gigamon enables organizations to run fast, stay secure and innovate in the digital economy by providing complete visibility and intelligence on all data in motion across their hybrid cloud network. The numbers below highlight the Gigamon journey that started in 2004. Since then, we've been awarded over 60 technology patents and enjoy industry-leading customer satisfaction with more than 3,000 organizations around the world.

Take ThreatINSIGHT for a test drive, visit gigamon.com/demo

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com