The Power of Integrated Network & Endpoint Detection and Response

Get a Holistic View of Your Entire Environment

Detecting and responding to modern attacker tactics, techniques, and procedures (TTPs) requires a holistic view of everything that is happening in your environment–from the network, which reveals the entire attack surface, like unmanaged IoT or contractor devices as well as managed endpoints that are often the end-target of the attack. The integration of network and endpoint security enables effective defenses against even the most advanced cyber threats.

Arista NDR, the world's leading advanced network detection and response platform integrates fully and easily with CrowdStrike Falcon Insight to provide the most comprehensive threat detection, rapid and effective response as well as containment and forensic analysis capabilities. This combination delivers the visibility and confidence you need to maintain a strong security posture across both the managed and unmanaged infrastructure within the enterprise.

Better Together: The Benefits

- Visibility, detection, and response for managed and unmanaged devices
- Investigations across the kill chain with endpoint and network context at your fingertips
- Integrated security operations that lower the cost of response
- Rapid and effective response and containment that speeds up time to remediation

The Strengths of Each Platform

ARISTA

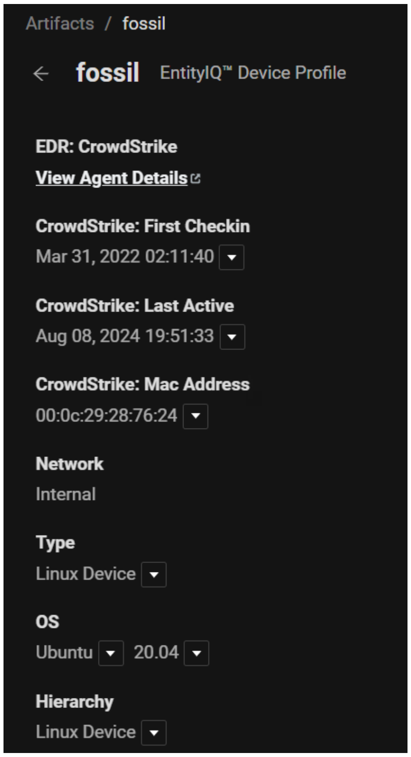
The Arista NDR platform provides broad context beyond managed endpoints to the 50+% of unmanaged infrastructure. Arista NDR thus provides a complete view of the potential attack surface and the business assets that are part of it.

By observing and analyzing every behavior on the network, Arista NDR tracks assets as they move across your network. It autonomously builds an understanding of the relationships and similarities between entities. The platform can sense abnormalities and threats, reacting within seconds if necessary.

CROWDSTRIKE

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike® Falcon Insight™ solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. All endpoint activity is also streamed to the CrowdStrike Falcon® platform so that security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.



Artifacts / fossil

← fossil EntityIQ™ Device Profile

EDR: CrowdStrike
View Agent Details

CrowdStrike: First Checkin
Mar 31, 2022 02:11:40

CrowdStrike: Last Active
Aug 08, 2024 19:51:33

CrowdStrike: Mac Address
00:0c:29:28:76:24

Network
Internal

Type
Linux Device

OS
Ubuntu 20.04

Hierarchy
Linux Device

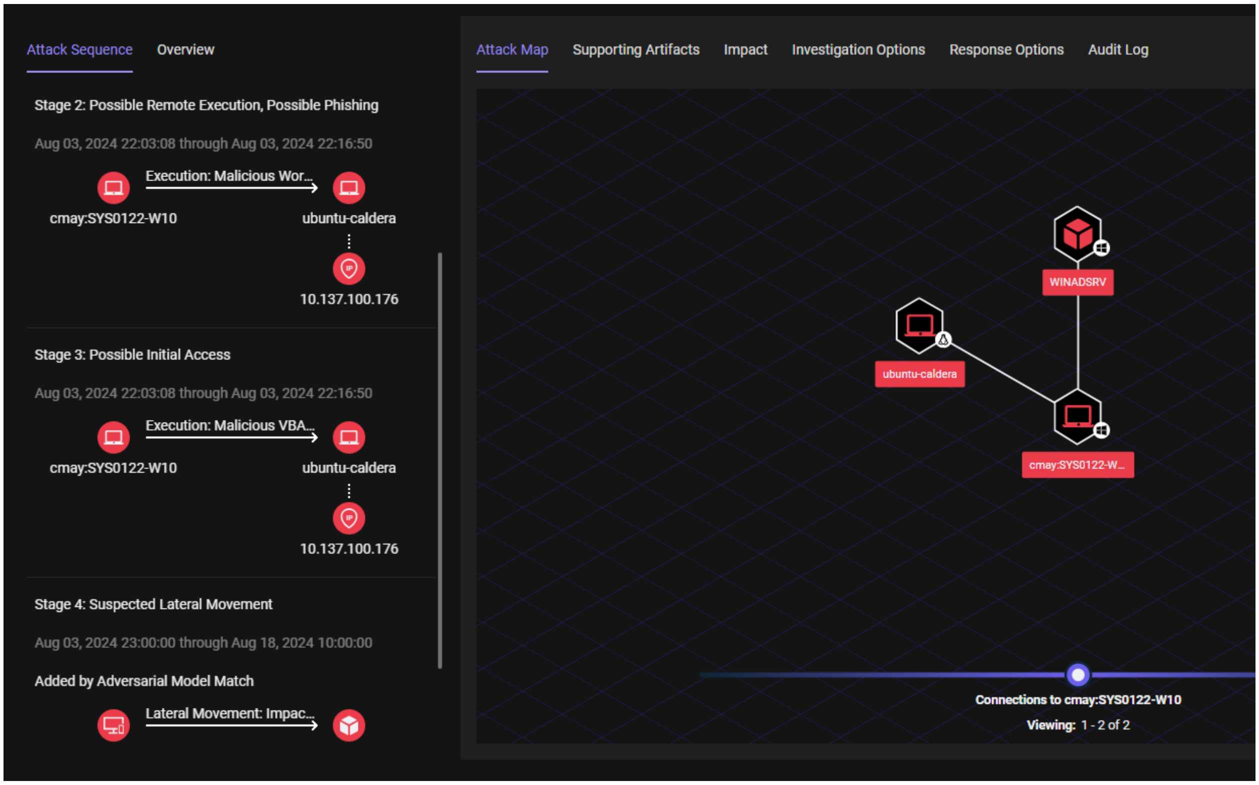
How They Complement Each Other

With this integration, endpoint data from Falcon Insight is automatically displayed in Arista NDR. A security analyst investigating a threat can thus make effective risk management decisions with the benefit of network and endpoint context on a single screen. The optimized and integrated workflow also reduces human errors and minimizes operational overheads from repeated context switches.

Importantly, Arista NDR's network visibility picks up devices, users, and applications that Falcon Insight does not manage. For example, in a recent attack, Arista NDR discovered an externally accessible IoT device that was compromised and then used for lateral movement across managed endpoints. The threat was discovered and quickly contained.

The Devil in the Details: An Integration Case Study

Automatically view a timeline of the breach.
Arista NDR automatically constructs a forensic timeline showing the series of activities flagged for the device in question as well as the broader attack map that identifies the entire kill chain along with other devices, destinations, and activities relevant to the investigation.



Stage 2: Possible Remote Execution, Possible Phishing
Aug 03, 2024 22:03:08 through Aug 03, 2024 22:16:50

cmay:SYS0122-W10 → Execution: Malicious Wor... → ubuntu-caldera
10.137.100.176

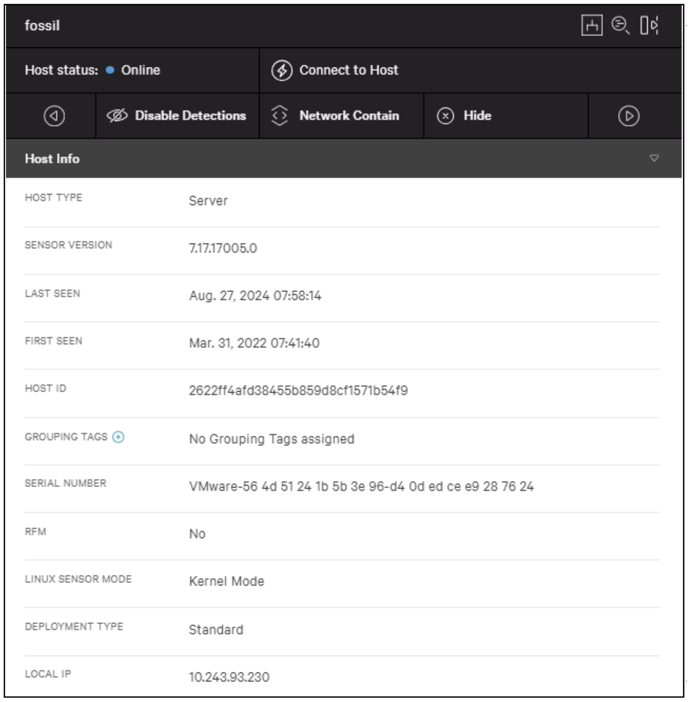
Stage 3: Possible Initial Access
Aug 03, 2024 22:03:08 through Aug 03, 2024 22:16:50

cmay:SYS0122-W10 → Execution: Malicious VBA... → ubuntu-caldera
10.137.100.176

Stage 4: Suspected Lateral Movement
Aug 03, 2024 23:00:00 through Aug 18, 2024 10:00:00
Added by Adversarial Model Match

Lateral Movement: Impac...

Connections to cmay:SYS0122-W10
Viewing: 1 - 2 of 2



fossil

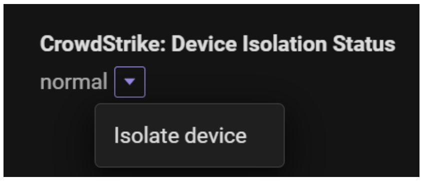
Host status: ● Online

Host Info

HOST TYPE	Server
SENSOR VERSION	7.17.17005.0
LAST SEEN	Aug. 27, 2024 07:58:14
FIRST SEEN	Mar. 31, 2022 07:41:40
HOST ID	2622ff4afd38455b859d8cf1571b54f9
GROUPING TAGS	No Grouping Tags assigned
SERIAL NUMBER	VMware-56 4d 51 24 1b 5b 3e 96-d4 0d ed ce e9 28 76 24
RFM	No
LINUX SENSOR MODE	Kernel Mode
DEPLOYMENT TYPE	Standard
LOCAL IP	10.243.93.230

Pivot to Falcon Insight.
With one click, view endpoint data such as process listings, registry information, and other device specifics. The integration automatically tracks down the correct device in CrowdStrike without requiring the analyst to manually search and match timestamps and IP addresses.

Isolate and remediate.
The integration enables one-click remediation of endpoints to quarantine the device and prevent lateral movement, command and control and data exfiltration.



CrowdStrike: Device Isolation Status

normal

Get Started — Set Up the Integration to Get a Holistic View of Your Environment

Setup the integration in two quick steps:

1 Obtain an API key and URL for access to the CrowdStrike platform.

2 Arista NDR's customer success handles the rest to turn on the integration.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062

September 11, 2024