

# The Power of Integrated Network & Endpoint Detection and Response

## Get a Holistic View of Your Entire Environment

Detecting and responding to an attacker's tactics, techniques and procedures (TTPs) benefits from 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.

The Arista NDR platform, 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.

## How They Complement Each Other

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

EntityIQ™ Device Profile:  
0 **SYS777-W10** ✓  
+ Add Tag   + Add Note

Risk Level  
**MEDIUM** ✓

Network  
Internal

Type  
Windows Device ✓

OS  
Windows ✓ 10 ✓

First Seen  
17:50:09 **Dec 15, 2020** (-12w 6d)

Management Detected  
Yes ✓

20:15:57 Jun 10, 2020

1 **Stage 1: Initial Access** ✓

Malicious java script was delivered to kvaldez upon access.

Initial Access\_Malicious javascript  
13.226.253.194 → kvaldez.SYS3099-W7

21:26:23 Jun 10, 2020

2 **Stage 2: Lateral Movement** ✓

Lateral Movement\_data transfer from internal ...  
kvaldez.SYS3099-W7 → npstroy.SYS777-W10

21:57:26 Jun 10, 2020 > through >  
21:57:27 Jun 10, 2020

3 **Stage 3: Exfiltration** ✓

Unregistered chrome extension implanted on system is exfiltrating data to a high quality domain

Unregistered\_Chrome\_Extension\_Exfiltrating\_Data  
kvaldez.SYS3099-W7 → jak-245621.appspot.com

22:55:11 Jun 10, 2020

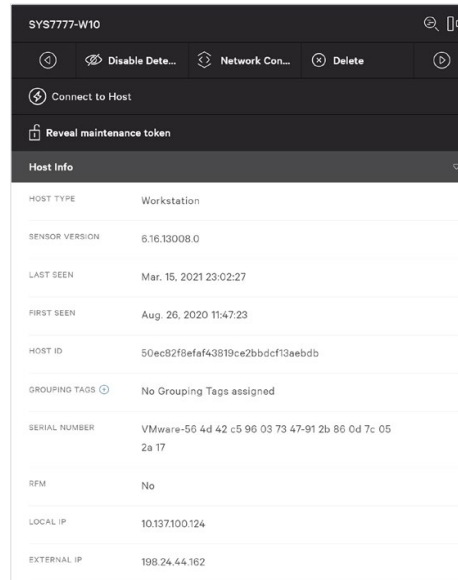
4 **Stage 4: C2** ✓

C2 commands to unregistered chrome extension

C2\_Command\_and\_Control  
kvaldez.SYS3099-W7 → trendmd.co

### 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.



Host Info	
HOST TYPE	Workstation
SENSOR VERSION	6.16.13008.0
LAST SEEN	Mar. 15, 2021 23:02:27
FIRST SEEN	Aug. 26, 2020 11:47:23
HOST ID	50ec82f8efaf43819ce2bbdcf13aebdb
GROUPING TAGS	No Grouping Tags assigned
SERIAL NUMBER	VMware-56 4d 42 c5 96 03 73 47-91 2b 86 0d 7c 05 2a 17
RFM	No
LOCAL IP	10.137.100.124
EXTERNAL IP	198.24.44.162

## 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](mailto: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



Copyright © 2022 Arista Networks, Inc. All rights reserved. CloudVision, and EOS are registered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. 9/15