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–starting with the network, which reveals the entire attack surface, like IoT devices and including traditional endpoints that often serve as the vectors for attack. The integration of network and endpoint security enables the most effective defense-in-depth against even the most advanced cyber threats.

The Arista NDR Platform, the world's leading network detection and response platform integrates fully and easily with the SentinelOne Singularity Platform 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 your enterprise.

Better Together: The Benefits

- Visibility & detection for managed and unmanaged devices
- Investigations across the kill chain with endpoint and network detection and response
- 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.

SentinelOne™

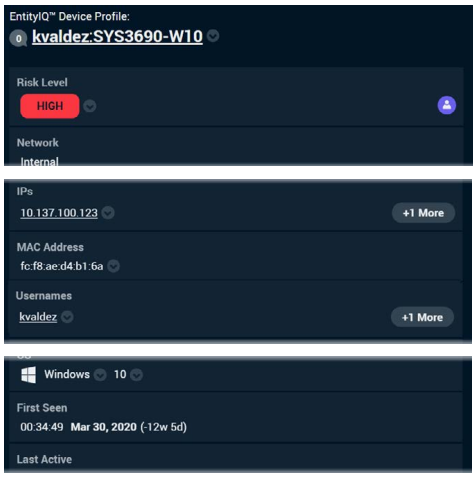
SentinelOne unites endpoint protection, detection, response and remediation. Software agents on the endpoints continuously monitor and collect data pertaining to all aspects of the managed device—how it's configured, what's running on it, where it reaches out to internally and externally, and more.

The platform uses AI engines to identify file-based malware, malicious scripts, weaponized documents, lateral movement, file-less malware, and even zero-days on the endpoints. When malicious activities are detected, the agent responds automatically to contain the threat.

How They Complement Each Other

With this integration, endpoint data from SentinelOne 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 both network and endpoint context. The optimized and integrated workflow also reduces human errors and minimizes operational overheads from repeated context switches.

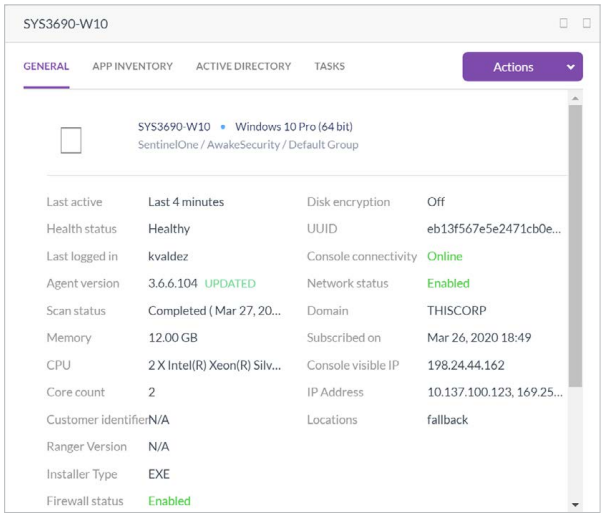
Arista NDR's network visibility picks up devices, users, and applications that SentinelOne doesn't see. For example, in a recent attack, Arista NDR discovered an externally accessible IoT device that was compromised and then used for lateral movement across managed endpoints. The threat was discovered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



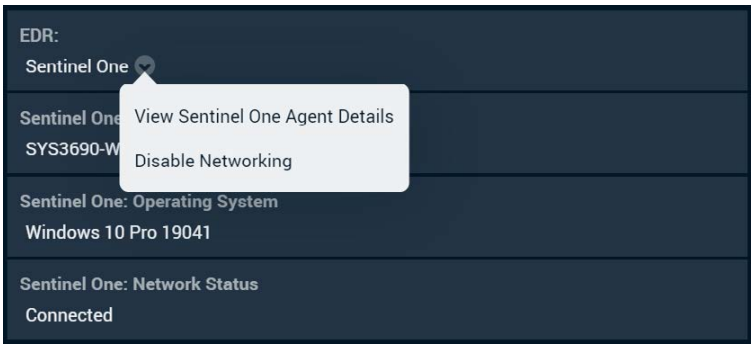
The Devil in the Details: An Integration Case Study

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.

Pivot to SentinelOne.
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 SentinelOne without requiring the analyst to manually search and match timestamp 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.



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 SentinelOne 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