

Integrated Security Operations: Arista NDR with Zscaler

Shared Intelligence to Lower Time to Detection and Response

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, insider threats, lateral movement, and privilege escalation to the edge and cloud often act as the initial entry point for attacks. The integration of Arista NDR with Zscaler Internet Access (ZIA) enables effective defense-in-depth against even the most advanced cyber threats.

The Arista NDR platform, named a leader in the Network Detection and Response market by Forrester, integrates easily with Zscaler Internet Access to provide comprehensive threat detection, rapid and effective response as well as containment and forensic analysis capabilities. This combination delivers visibility for threats across both north-south and east-west attack paths and helps customers strengthen their security posture across the enterprise. The integration of network detection and response (NDR) with the security service edge (SSE) also drives zero trust maturity, ensuring organizational security policies are enforced whether users and devices are on or off-premises.

Better Together: The Benefits

- Visibility & detection irrespective of where the users or devices are located
- Threat intelligence sharing ensures rapid enterprise-wide risk mitigation
- Automated blocking of command and control and data exfiltration helps lower the impact of threats like ransomware

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 and thus detects threats, reacting within seconds if necessary.



Zscaler Internet Access (ZIA) includes a comprehensive suite of AI-powered security and data protection services to help organizations stop cyberattacks and data loss. ZIA dynamically computes a risk score and then inspects traffic inline to secure users as well as workloads and IoT/OT devices as they access the internet or SaaS destinations.

How They Complement Each Other

With this integration, alert categorization and domain intelligence data from Zscaler are factored into Arista NDR's risk analysis of north-south traffic. This enables Arista NDR to quickly detect attacker command and control infrastructure as well as data exfiltration. Similarly, intelligence about domains identified as malicious within the customer's network is shared by Arista NDR with ZIA, enabling the blocking of malicious inbound and outbound access not just for the initial victim but across the rest of the organization's digital assets.

Arista NDR's network visibility picks up east-west behaviors like lateral movement, credential abuse, and privilege escalation that stay purely within the organization's internal network. For example, in a recent attack, Arista NDR discovered a compromised device performing credential brute force on the internal network as part of a larger ransomware threat. By working in conjunction with Zscaler, Arista NDR prevented the device from engaging in command and control as well as any potential data exfiltration. Moreover, this also allowed the attacker infrastructure to be blocked at the perimeter from all corporate devices and users.

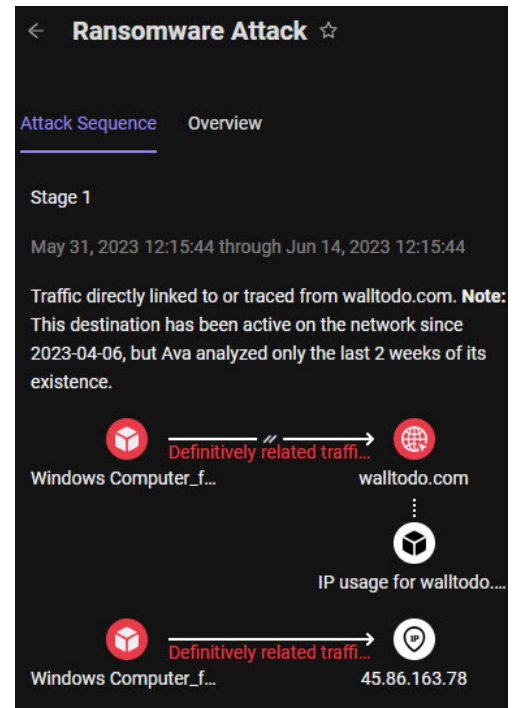
The Devil in the Details: An Integration Case Study

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.

Ingest global classification and custom category data from ZIA.

Domain intelligence data from ZIA is ingested into Arista NDR and is factored into the risk analysis as well as to identify stages in the attack lifecycle such as command and control and data exfiltration.



ARISTA NDR

Search

Artifacts / walltodo.com

← walltodo.com EntityIQ™ Domain Profile

+ Add to Situation

Yes View Details

First Seen: 2022-04-20T19:03:18

Last Seen: 2023-10-09T07:39:03

Registered: Oct 25, 2022

Expires: Oct 25, 2023

Registrar: DropCatch.com 1092 LLC

Nameserver: JM1.DNS.COM

IP: 68.233.239.85 View Details

Domain Policy Lists: None

Zscaler : ZIA Categorization
custom cats: None; alerts: None; classificati...

5.0.6

Search extracted data

Top 1 device accessing this domain

Device Name	Activities	Data Volume	Protocols	Last Accessed
Windows Desktop_...	469	12MB	HTTP, UNKNOWN_TCP	2023-10-09T07:39:03.653051Z

Subdomains Accessed (0)

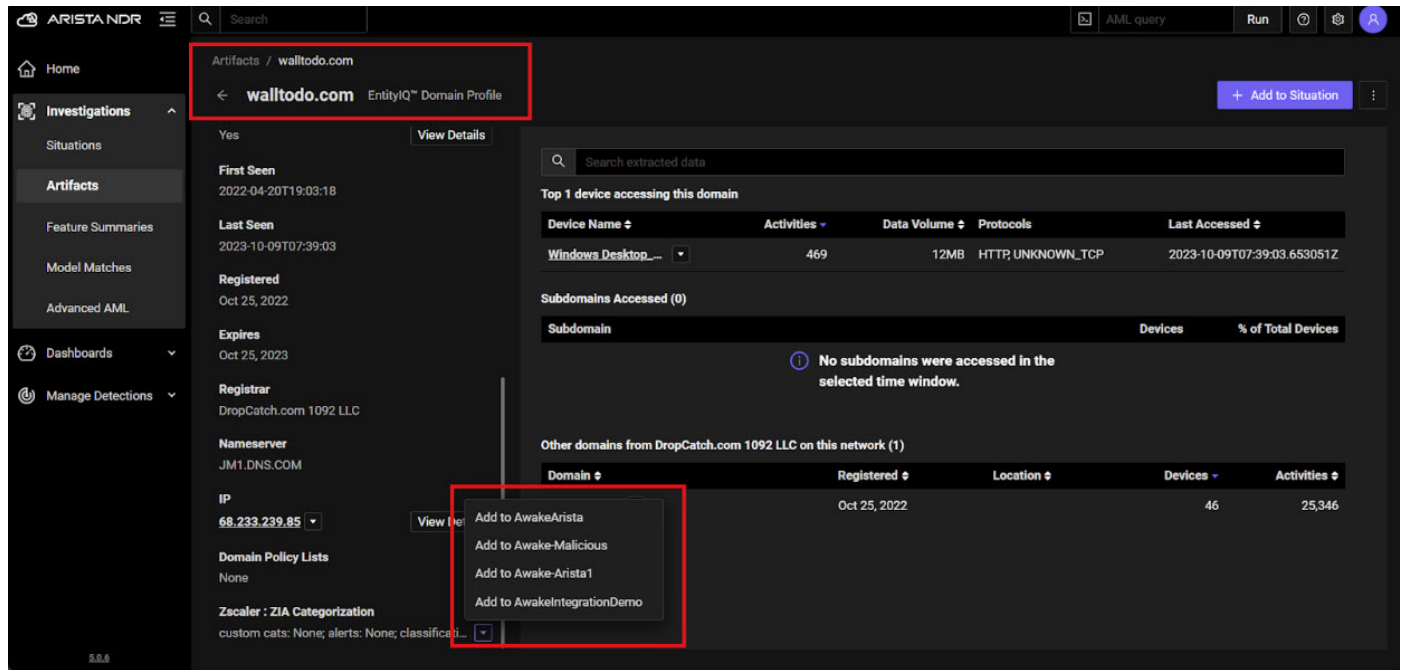
No subdomains were accessed in the selected time window.

Other domains from DropCatch.com 1092 LLC on this network (1)

Domain	Registered	Location	Devices	Activities
walltodo.com	Oct 25, 2022		46	25,346


Mitigate risk enterprise-wide

The integration also enables one-click risk mitigation to block access to any other domains identified as malicious. This extends protection to the entire enterprise, not just for the initially compromised device.




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, URL, Username and password for your ZIA deployment.



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

