Zscaler MDR for Zscaler Internet Access (ZIA)

Bring critical ZIA context into investigations to save time and accelerate response

KEY BENEFITS

- **Accelerate investigations**
- **Focus on true positives**
- **Respond quickly and precisely**

The challenge

When suspicious activity occurs, security analysts are often forced to manually correlate multiple data sources. This can be an extremely tedious process where one or multiple members of your team find themselves:

Pivoting between consoles:
Jumping from your alerting system to your Zscaler environment.

Hunting for answers:
Manually searching ZIA logs for related activity from that specific user or endpoint, trying to piece together what happened before and after the initial alert.

Wasting time on false positives:
ZIA might have already blocked the activity, meaning your investigation into that specific alert could be unnecessary.

This manual correlation consumes valuable time, slows down your response, and can leave significant gaps in your understanding of an incident's full scope.

Our solution

Our MDR integrates directly with the Zscaler Data Fabric, allowing us to enrich investigations and consolidate vast context automatically, without SIEM forwarding delays or costs. The integration allows you to:

Unify visibility:
Relevant ZIA web data are automatically visible within Zscaler MDR, allowing your team and ours to focus on analysis and action, not manual data collection.

Increase signal, decrease noise:
We only notify you of active threats, not activity that's already been mitigated by ZIA. Common investigative questions are automatically asked and answered for you.

Respond faster:
No 15–20 minute NSS log delays, richer context, and fewer false positives means improved efficiency, decision-making, and response.

Solution Architecture

When Zscaler MDR detects suspicious activity or begins an investigation, we immediately and automatically look up relevant ZIA data from your Zscaler Data Fabric instance. This happens behind the scenes, enriching our investigations without any extra steps from your team. This approach ensures that our platform integrates the full picture of user, endpoint and network activity for you before we notify you of a threat.

Integration details

Valuable ZIA context is organized and is fully transparent for every MDR investigation where relevant ZIA web data exist. You can find the context in the “Related data (by query)” and “Related data insights” tabs of your MDR investigations.

Related data: Provides raw ZIA web log transactions, offering a detailed timeline of internet activity around suspicious events.

Related data insights: Provides concise, high-level summaries that point out unusual or suspicious activity. Our system runs a series of predefined queries to help answer critical questions, such as:

- **For user activity:** Was the affected user seen on multiple devices, from unexpected locations, or with unusual browser information? Were they observed connecting from a country considered risky?
- **For endpoint activity:** Was the affected device seen in multiple locations or using unexpected browser details? Is its observed location in a high-risk country?
- **For transaction details:** Was traffic to a suspicious destination blocked by ZIA (meaning a potential threat was stopped) or allowed (suggesting a need for further investigation)? Was the web traffic encrypted in a way that ZIA couldn’t inspect, potentially hiding malicious activity? Did Zscaler detect malware within the transaction? Did the transaction bypass the Zscaler Client Connector, which could indicate a gap in your security controls?

Teams gain immediate access to all critical ZIA data directly within Zscaler MDR, eliminating disruptive pivots and dramatically accelerating investigations.

Automated ZIA responses

Block/unblock URLs, IPs, file hashes, or other IOCs using no-code playbooks configurable directly within Zscaler MDR.

DO YOU QUALIFY?

- **Activated Authentication Service**
- **US-based data fabric instance**