FORTRA

SOLUTION BRIEF

Agari Data Connector for Microsoft Azure Sentinel

Integrate Email Threat Data to Improve Threat Visibility and Accelerate Incident Response

Email is a primary vector for attacks on your business today—and email threats are evolving faster than ever. But actionable data about email attacks is often inaccessible to time-strapped security operations and incident response teams. That disconnect leaves your business vulnerable and unable to mitigate hidden email threats.

Improve Visibility with Integrated Email Threat Data

The Agari Data Connector for Microsoft Azure Sentinel solves this challenge and makes it easy to surface email threats by quickly integrating valuable Agari threat intelligence into the Azure Sentinel dashboard. Your team can analyze and correlate Agari data in workbooks and query logs to trigger custom alerts. Agari email threat intelligence also can be exposed via the Security Graph API to enable threat hunting in the Azure Sentinel environment.

Accelerate Incident Response and Drive SOC Efficiency

The Agari integration with Azure Sentinel empowers security teams to work more effectively to mitigate email threats. Leveraging Agari incident data and Azure Sentinel's orchestration tools, security analysts can incorporate email incidents in custom workflows to improve investigations and accelerate resolution—without needing to jump through hoops to transform syslog or STIX TAXXI feeds. With the ability to track and resolve security incidents through a single pane of glass, your team can focus on remediation of email threats, not repetitive labor and administrative overhead.

Leverage Your Strategic Microsoft and Agari Investments for Security

Agari is the first provider of email threat data for Microsoft's cloud-native SOAR. The integration leverages key Azure Sentinel capabilities such as Azure Functions and the Security Graph API to trigger actions in Microsoft Office 365, control users via Active Directory, and automate management of login, desktop, and security events.

AT A GLANCE

Agari Data Connector for Microsoft Azure Sentinel makes it easy to connect Agari email threat data to the Azure Sentinel SOAR, improving visibility into email threats, accelerating incident response, and driving SOC efficiency.

HIGHLIGHTS

First email threat data integration for Azure Sentinel
Agari is the first provider of email threat data for Microsoft's cloud-native SOAR and supports key Microsoft capabilities such as analytical workbooks, Azure Functions, and the Security Graph API.

Unlock email threat intelligence
Integrate Agari email threat data across applications and orchestrate workflows to manage security incidents through a single pane of glass.

Quickly connect and deploy
The pre-configured integration is easy to connect and get started, but is highly flexible to meet your organization's unique needs.

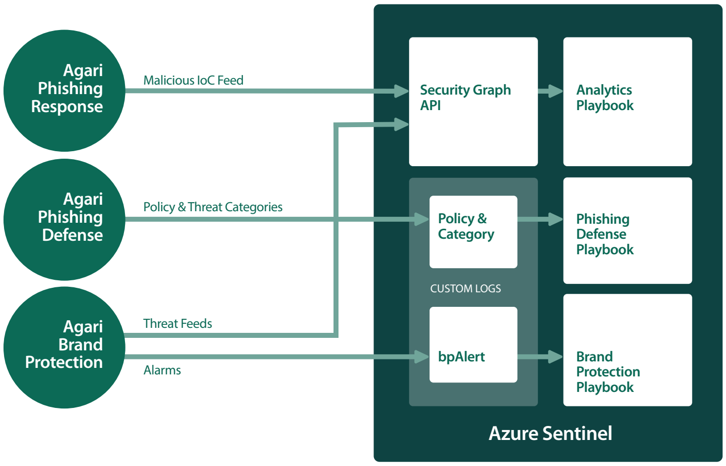
Integrate data from every Agari product
Integrate Agari Brand Protection, Agari Phishing Defense, and Agari Phishing Response with Azure Sentinel.

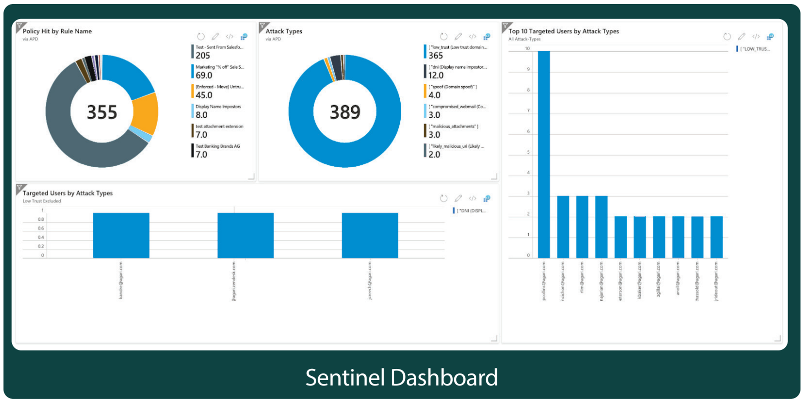
The Agari Data Connector for Microsoft Azure Sentinel supports every Agari product: Agari Brand Protection, Agari Phishing Defense, and Agari Phishing Response. Leveraging Agari data to enrich and share threat intelligence across multiple applications helps safeguard your entire infrastructure against email threats..

Build and Orchestrate Workflows to Quickly Deliver Results

The Agari Data Connector for Microsoft Azure Sentinel helps your team quickly operationalize email threat data to realize value for your organization by leveraging automated, orchestrated, and collaborative workflows; creating standard security and compliance playbooks; and simplifying incident tracking and case management. The integration reduces complexity to help you solve common needs such as:

- Simplify ingest without the need to transform syslog or STIX TAXXI feeds
- Operationalize indicators of compromise (IOC) and other threat data directly from Agari
- Enable fast, active sharing of IOCs and threat intelligence into Sentinel to find other events that match
- Create rules and triggers to reduce remediation and response time
- Leverage Security Graph API to query risks detected by the Identity Protection Tool
- Create of custom logs via the Kusto query language
- Customize dashboards to enable quick visual inspection and identity policy hits on:
  - Top attacks
  - Top users attacked
  - Previously undetected phishing emails
  - RUF data from the Agari Brand Protection Threat Feed to monitor for domain abuse





Sentinel Dashboard

Get Started Today

The Agari Data Connector is available to install from the Azure Sentinel portal today. Contact your Agari representative to learn more.

The Company We Keep

Top 3 Social Networks | 6 of the Top 10 Banks | Top Cloud Providers

Learn More: www.agari.com/products

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.