ARGOS by The Birdling

One for all - cybersecurity and compliance

Overview

Businesses are under increased pressure to stay afloat in a highly competitive business environment, continuously taking business initiatives to make operations more efficient and deliver services that leave a mark on customers. As they continue to step toward digital transformation, they face cyber risks that are more sophisticated in nature. To make it more challenging, they find it difficult to address threats in a highly volatile threat environment. They cannot gain clear visibility from siloed security solutions that give them little context to act with more precision. They need a holistic solution that augments their cyber resilience and gives them much-needed centralized visibility and control.

ARGOS is a comprehensive solution that blends the best of both worlds - cutting-edge AI/ML technology and human expertise. It is a machine learning-based multi-tenant, open architecture-based security solution that unifies endpoint, network, identity, and cloud security into a single human intelligence-led platform. It helps organizations make the most of all of their existing security solutions. It breaks siloes that limit security teams to gain clear visibility of their cybersecurity posture, offering centralized control and meaningful insights to make informed decisions. By offering a one-stop solution for cybersecurity, it empowers businesses across industries to seamlessly transcend digitally without any disruptions from cyber threats or non-compliance.

Endpoint

ARGOS is a highly customizable endpoint security solution that renders machine learning based accelerated incident investigations across a multi platform environment that reduces detection time significantly. It utilizes threat INTEL and root cause analysis to achieve a complete picture of threats for precise response. It empowers security teams to take action on the go when it comes to endpoint security.

| Network

Through a powerful machine accelerated human led approach, ARGOS enables organizations to detect threats across their internal and external network, helping teams to take action based on network vulnerability scanning and threat intel from multiple sources. It gives a centralized control of security, offering greater visibility of threats across your network.

| Identity

ARGOS renders superior detection capabilities with multi source ingestion and analysis of data with User Entity and Behavior Analytics (UEBA for more accurate action against suspicious user activity. It defends all the assets across your IT infrastructure against advanced identity based attacks to stop perpetrators from getting some of your most valuable information stored across IT infrastructure.

| Cloud

Keep all of your enterprise data including all your workload stored across private and public cloud environments safe from cyber criminals with The Birdling's continuous monitoring, real -time threat detection and automated response. It secures all your organizational data across virtual machines, containers, Kubernetes clusters, servers and provides you the OS-level visibility that you need to proactively detect suspicious activity, hunt and avert threats.

| Values Delivered

Manage

ARGOS is fully managed by cybersecurity experts, analysts, and incident responders who engage in an in-depth contextual and root cause analysis of alerts categorizing them for accurate response.

Detect

It integrates seamlessly with your IT infrastructure with all the current security investments, using AI, ML, and threat intel for quick and accurate detection

Respond

It reduces alert fatigue significantly by automating responses on AI/ML based decisions. Our security team works dedicatedly to render security actions such as configurations and rules. They help by channeling their threat expertise to triage and step-by-step guidance with the response.

Comply

By offering a team of cybersecurity and compliance experts with customizable reports, it has everything your organization needs to achieve all compliance goals.

Core Capabilities

Feature	Description
Next-Generation SIEM/XDR	A powerful AI driven detection engine that does more than just visibility with automated response to advanced threats based on multi source dingestion of threat INTEL and UEBA. With a dedicated team of cybersecurity experts it contextually renders precision in threat detection and response through seamless triage and rules optimization.
File Integrity Monitoring (FIM)	It is the ARGOS feature that detects changes from the baseline system files, registries, or application software that may indicate the occurrence of a cyber attack. It tracks file and registry changes. It is a must in many compliance standards like ISO and PCI DSS.
Vulnerability Management	Experience quick and intelligent prioritization of vulnerabilities on the most critical assets with comprehensive risk assessment score based on multi-source evaluation and recommendations to mitigate risk with the help of built-in assessment and remediation tools. Predict emerging threats and stop imminent threats from damaging your high-value assets.
CIS Benchmark-based Configuration Assessment	Get an active periodical assessment of configurations across your current security setup against CIS benchmarks and compliance guidelines your organization is subjected to. These configuration recommendations are prescribed for more than 25+ vendor families. Gain expert-based recommendations to address gaps in configurations.
Threat Detection & Response	ARGOS leverages a robust AI and ML based detection engine that engages in continuous monitoring of the IT infrastructure for cyber risks It renders context through threat INTEL based analysis and empowers businesses with quick threat response with the help of AI/ML.
Security Automation	ARGOS offers the capability to augment security operations through AI and Machine learning based automation of routine security tasks that assist security teams to work more efficiently. It offers capabilities such as automated threat detection, response and file retrieval and deletion in case of suspicious activity.
Full-cycle Incident Response	Get round-the-clock full-cycle unmetered incident response support with a team of security experts and incident responders working actively to keep your IT infrastructure. Prepare an in-depth plan and implement measures to control damage, remediate, and contain an attack from further damaging your most valuable assets and reputation.
Real-time Dashboards	ARGOS works superfluously in proactively securing your IT infrastructure by providing you with much-needed actionable insights on cybersecurity posture. It not only helps you make meaningful decisions on cybersecurity but also generates forensic reports that can help you with the achievement of globally renowned compliance certifications.

Feature	Description
Incident Management	ARGOS offers features for smooth incident management and triage features to address incidents more efficiently. It offers a unique feature to collaborate with the clients throughout the process of incident resolution with ease of classification based on impact and severity of the incident
User Entity Behavior and Analytics (UEBA)	ARGOS utilizes AI and ML to detect, identify and prevent advanced internal network based and other attacks on users and assets connected. Through continuous cyber risk analysis, collecting data from endpoints, identity, servers and cloud determining the level of risk exposure and predicting suspicious activity.
Network Detection & Response	ARGOS predicts and detects suspicious network activity based on multi-source collection and analysis of data. Based on the latest threat intel, it predicts and engages in automated AI and ML based response to threats rendering context based visibility of network posture in real-time.
Dark Web Monitoring	ARGOS offers in depth insights on the latest threat activity and the tactics, techniques and procedures of threat actors based on monitoring of the dark web. The Birdling's security experts engage in dark web analysis studying whether data has been published or sold on the dark web.
Deception Technology	ARGOS' next gen deception technology unlocks early threat detection with low false positives through deployment of real-world breadcrumbs like apps, servers, credentials etc alongside assets to act as lures for the attacker. Once the attacker interacts with the lures, the technology alerts incident responders for quick and precise response.

Use Cases

SIEM-as-a-service (Platform+People)

Enable your organization with round-the-clock security with a platform that offers a perfect blend of technology and human expertise. Centralize all the security data, and gain complete visibility & control of your cybersecurity operations.

XDR

Avert cyber threats with a supercharged platform built to deliver speed and high precision with AI/ML-based detection and response. Gain enhanced cross-platform visibility and control backed with real-time security analytics, enabling you to make meaningful decisions. Predict and prevent future attacks, detect vulnerabilities across endpoints, and correlate and prioritize alerts with XDR.

MDR

Experience increased ROI from all your existing cybersecurity investments with a robust open architecture platform that seamlessly integrates with your infrastructure. With file integrity monitoring, in-depth alert analysis, guided remediation, and expert-designed work flows.

NDR

Enable round-the-clock internal and external network monitoring with a platform that integrates easily with your firewall, next-generation firewall, and web application firewall backed by a team of cyber experts engaging in identifying and implementing network security best practices. Leverage behavioral analytics to detect suspicious user activity across network traffic.

Security Operations

Gain holistic fulfillment of your cybersecurity scope through a platform backed by a dedicated round-the-clock security operations center that caters to all your security operations. With 24x7 support for incident response backed by security experts who assist with guided remediation.

Risk Management

Identify and implement security best practices and controls to address the most potent cyber risks across your organizational environment to meet all your cybersecurity compliance requirements. Tailor your cybersecurity posture to address the most sophisticated internal and external cyber risks.

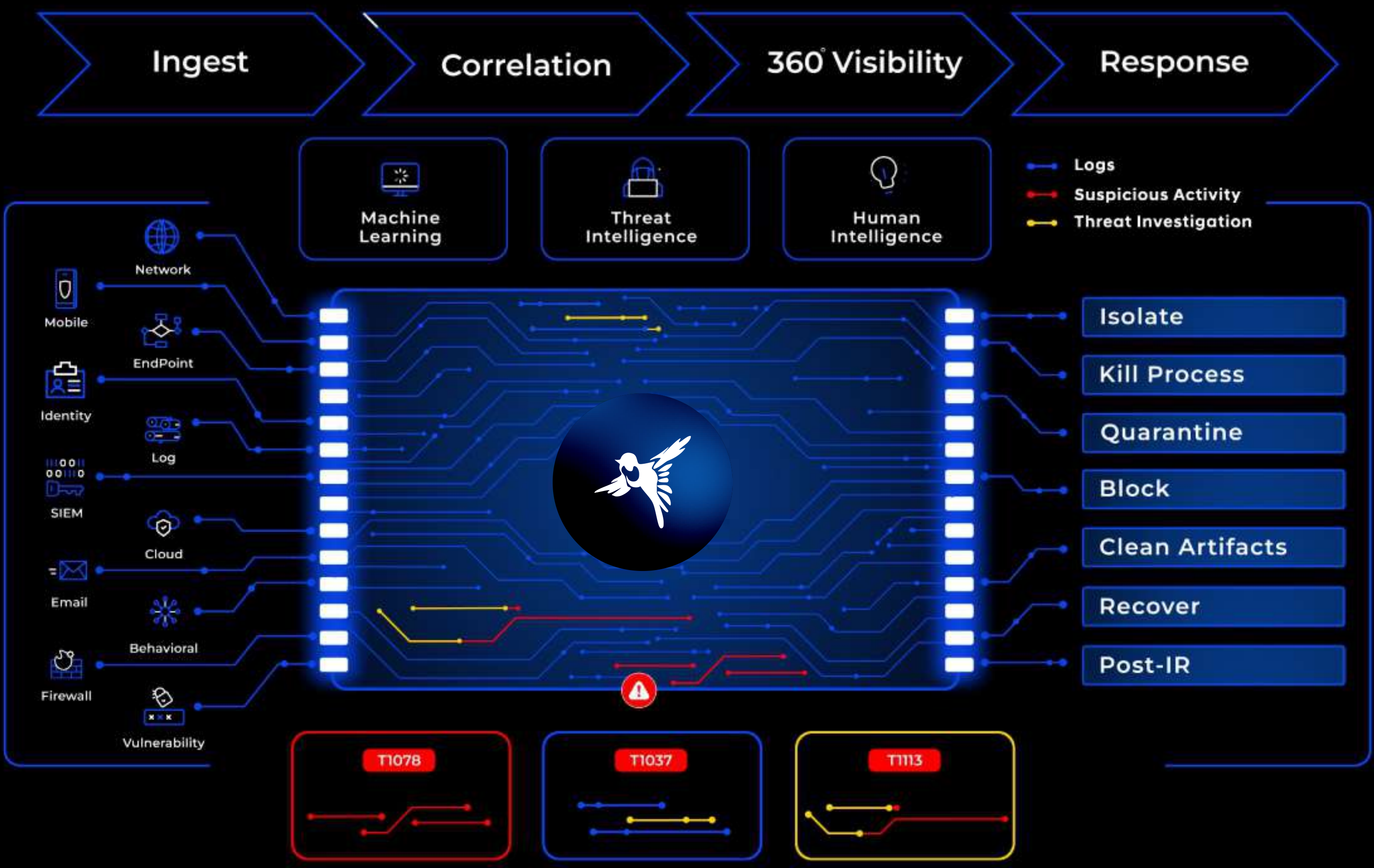
Vulnerability Management

Identify and address vulnerabilities in your IT infrastructure through assessments and reports for a detailed view of your cybersecurity posture. Test how different aspects of your IT infrastructure react to real-world attack techniques with experts categorizing vulnerabilities as per their severity.

Compliance Management

Take measures for risk and vulnerability management with our highly robust platform. Gain expertise for meeting all your compliance-specific objectives. Generate reports that are customizable to meet compliance requirements.

ARGOS Platform



About Us

The Birdling is a trailblazing cybersecurity organization with a mission to simplify cybersecurity for our partners across industries through our technologically driven human-led open architecture platform ARGOS. We seek to cater to some of the industry's most immediate challenges such as siloed cybersecurity, increasing cost of cybersecurity solutions, changing regulatory environment, and increasing reliance on multiple vendors for multiple aspects of cybersecurity and compliance. With ARGOS, we are able to assist our network of partners and customers through effective augmentation of cybersecurity posture as per use cases, extending visibility, compliance management, and round-the-clock support for incident response.

Through a team of threat-striking experts, we have made our presence across MEA.

In league with the finest, Globally trusted.

Phone: +234 912 489 9990
Email: hi@thebirdling.com
Website: www.thebirdling.com