FULL-STACK CLOUD SECURITY FOR ALL IDENTITIES, INFRASTRUCTURE AND SERVICES

Ariksa

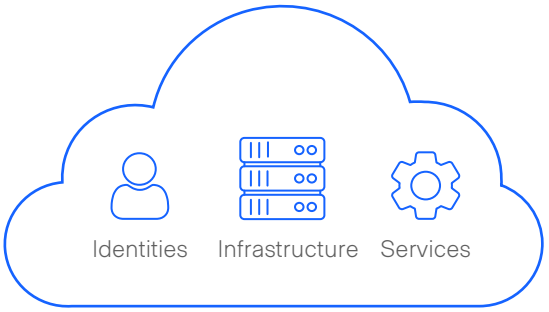
SOLUTION OVERVIEW

WHY ARIKSA IS DIFFERENT

- ASSESSES RISKS ACROSS IDENTITIES, INFRASTRUCTURE & SERVICES
- ELIMINATES POINT TOOLS & SILOED INSIGHTS TO DELIVER HIGH-QUALITY ALERTS
- DEEP OBSERVABILITY AND VISUALLY RICH CONTEXT FOR THREATS

Ariksa simplifies how you secure your cloud

Ariksa provides a radically new approach to securing your cloud for all your identities, infrastructure and services – 100% coverage, deep contextual detection of threats, visually rich investigation and custom workflow automation for response. Ariksa identities broadest assessment for insider and outside threats. It enables continuous least-privilege management and separation of duties, detects high-risk combination of resource misconfigurations that create attack paths, and provides automatic compliance assessment. Ariksa works across organizational silos and eliminate point-solutions to deliver high-quality findings that help you focus on what matters most to secure your cloud.



Legacy approach requires multiple tools to manage user and non-user identities, infrastructure and services. This limits threat assessment, creates tool sprawl and generates low-quality alerts. Ariksa looks across siloes and delivers holistic, big picture view and alerts based on deeper contextual assessment of risks and threats from usually hidden dependencies and activity. Instead of hundreds of meaningless alerts, Ariksa delivers prioritized list of alerts.

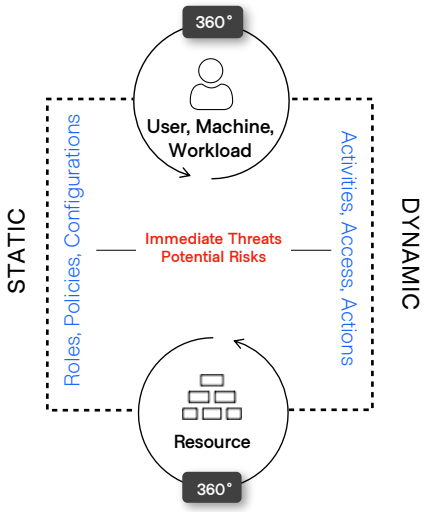
Ariksa delivers complete security management without any agents or complex, one-time onboarding efforts.

Enterprise ready - Easy Integration for Security, IT & Dev Ops

Ariksa delivers value within minutes, without any disruption to existing workflows or security processes; no weeks or days of integration efforts. Ariksa provides workflow automation and turnkey integration for ticketing and notifications with tools such JIRA, ServiceNow, Slack, Microsoft Teams, Email and SMS. Ariksa is multi-tenant and delivers completely isolated inventory and security management of cloud estate belonging to different organizations or managed by different teams across security, IT and DevOps

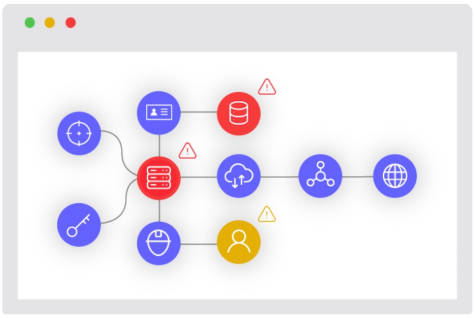
ARIKSA PROVIDES DEFENSE IN DEPTH BY IDENTIFYING THE FOLLOWING:

- RISKY IDENTITIES
- EXCESSIVE PERMISSIONS
- INACTIVE ENTITIES
- EXPOSED DATA
- UNSAFE CREDENTIALS
- NETWORK MISCONFIGURATIONS
- HIDDEN ATTACK PATHS



Cloud Explorer: Maps for 360° View On-Demand

Ariksa's cloud explorer delivers a complete 360° view for identities (user and non-user), infrastructure and platform services, by combining deep analyses and real-time correlation of underlying configurations (roles, policies, credentials etc.), and actual activity to uncover existing threats due to poor configurations or imminent threats from unauthorized actions. Ariksa's maps are available to security and IT teams on demand, without any effort, making it easy to understand problems, what's causing them, what change is needed and where, and the blast radius of change. Instead of taking hours or even days to gather and correlate data, teams have all information required for quick response or proactive assessments - dramatically eliminating errors, lowering time to resolution, and boost productivity of security/IT teams.



Context-Aware Security with Graph Explorer

Ariksa's engine builds deep context and presents a unified view of cloud fabric by combining static data and real-time insights across users (roles, privileges, memberships etc.), organizational structure (organizational units, accounts etc.), infrastructure (virtual machines, data sources, network elements etc.). Using this intelligence, Ariksa delivers distinct graphs for users and resources showing their interconnectedness, classifications and associated threats. This immediately reveals context-based risks that are critical to address and avoids hundreds of false alerts that typically overwhelm security and IT teams, and drastically reduce productivity.

- CIS BENCHMARKS
- NIST-800-53
- SOC 2
- ISO 27001
- PCI-DSS
- CCM

Turnkey Security & Compliance Standards

Ariksa provides comprehensive support for a wide range of security and compliance standards such as CIS, NIST-800, SOC 2, ISO 27001, PCI-DSS and CCM. In addition to assessing threats and risks to identities, Ariksa provides a real-time view of identity configuration and activity related issues that require remediation in order to meet corporate and organizational goals to meet specific security and compliance standards. Ariksa policies for these standards are out-of-the-box and can be easily customized, shared and tracked in distributed environments that require collaborative enforcement by security, IT and developer teams for compliance and risk management.

Get a FREE RISK ASSESSMENT of your cloud estate. No commitments.

To learn more or get started with a free trial email us at: inquiry@ariksa.com

Ariksa