No Compromise Behavioral Analytics

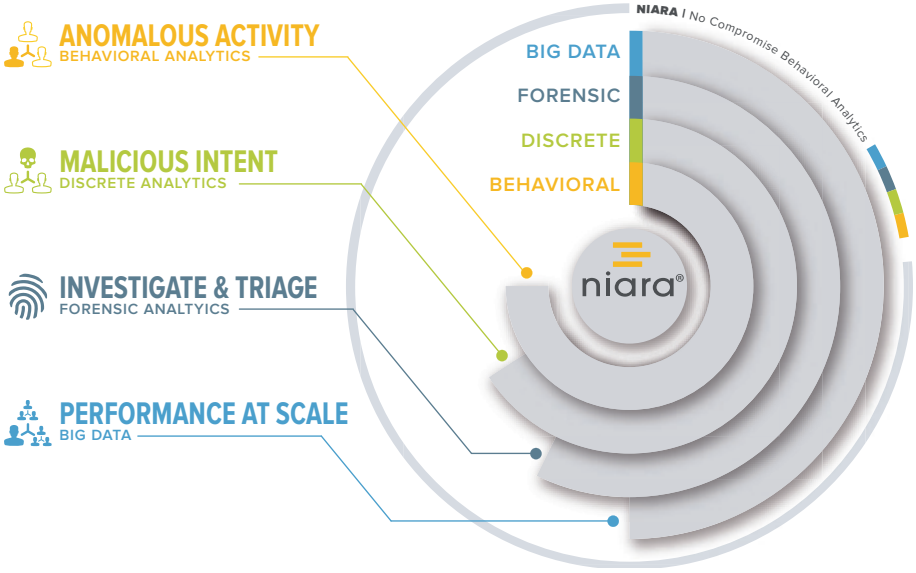
KEY FEATURES

- User and Entity Behavior Analytics (UEBA)
- Comprehensive data sources for analytics – logs, flows, packets, files, alerts and threat feeds
- Leverages supervised, semi-supervised and unsupervised machine learning
- Monitors entities for deviations against self-learnt historical and peer baselines
- No rules, signatures or configuration
- Integrated analytics and forensics
- Advanced visualizations
- Works standalone or in conjunction with SIEM/log management
- Deploys on premise or in the cloud

BENEFITS

- Compromised user and malicious insider detection, alert prioritization, incident investigation and threat hunting
- More reliably links anomalies to malicious intent
- Improves analyst productivity through analytics driven visibility
- Accelerates incident investigations through high fidelity Entity360 views
- Amplifies threat hunting via intelligent machine learning driven tagging

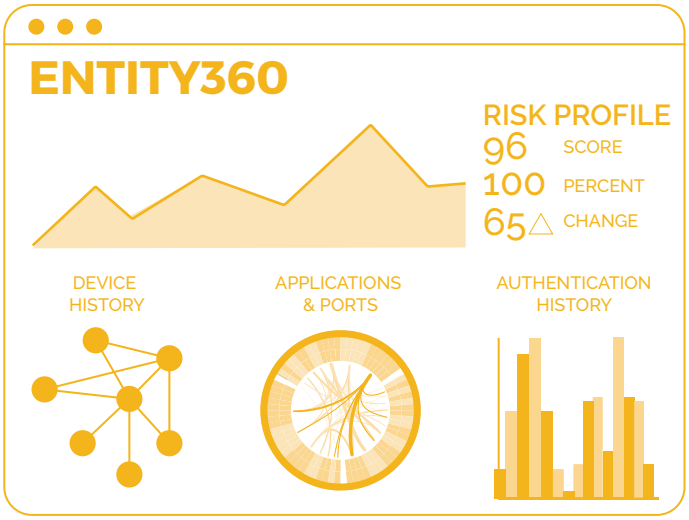
Niara's security analytics platform automates the detection of attacks that have evaded an organization's perimeter defenses (compromised users & hosts, malicious insiders), and empowers security teams with analytics driven visibility for accelerated incident investigation, efficient alert prioritization and amplified threat hunting capabilities.



Niara Solution

Niara applies behavioral analytics on a combination of network and security data and provides the following capabilities

- Comprehensive Entity360 risk profiles for users, hosts and IP addresses
- Stateful record of events across data sources over time to surface high fidelity anomalies
- Multi-dimensional analytics combined innovatively to link anomalous events to malicious intent.
- Enables historical views into Entity360 risk profiles
- Calibrates alerts by severity and classifies them by attack stage
- Detection of anomalies such as privilege escalation, credential violations, internal reconnaissance, lateral movement, abnormal access to high value resources, command and control, exfiltration



Entity360® Risk Profiles

Niara Entity360 is a consolidated representation of an entity's activity regardless of data source, devices used or activity type. Entity360 includes a risk score (0 to 100) that represents the likelihood that an entity has been compromised. Entity360 profiles can be accessed by existing consoles and workflows through an open API.

- Risk score calculated using a multi- variate model
- Trend line of risk scores for the entity over time
- Timeline views of analytics driven security events
- Detailed analytics results backed by forensics
- Distilled summaries of fused data, including authentication, internal and internet activity, device history

Alert360®

Niara Alert360 provides in depth information about an alert and simplifies its prioritization and investigation

- Alert summaries and recommended mitigation actions
- Primary IOC that triggered the alert
- Canned and custom querying to aid in the investigation of the alert
- Forensic evidence relevant to the alert
- Automatic detection of other entities also impacted by the same IOC

Incident Investigation and Threat Hunting

Niara has built in capabilities to help simplify incident investigation and threat hunting

- Search historical activity data using IOCs from STIX and custom threat feeds
- Retroactive analytics on data to detect anomalies
- Monitor and tag activity data to assist in historical user or host investigations
- Advanced visualizations to spot anomalous patterns

Data Sources

The Niara platform supports the following data sources

- VPN, FW, IPS/IDS, Web proxy, Email logs
- NetFlow, Bro logs
- EndPoint protection logs
- DLP logs
- Packets
- DNS logs
- Active Directory logs
- DHCP logs
- External threat feeds
- Alerts from 3rd party security infrastructure

Deployment Options

- On-premise software or appliance
- On-premise Hadoop application
- AWS Virtual Private Cloud (VPC)

About Niara

Niara's security analytics platform automates the detection of attacks that have bypassed an organization's perimeter defenses and dramatically reduces the time and skill needed to investigate and respond to security events. The solution applies machine learning algorithms and forensics to data from the network and security infrastructure to detect compromised users, entities, and malicious insiders, speed threat hunting efforts, and reduce the time for incident investigation and response by focusing security teams on the threats that matter. For more information, visit www.niara.com or contact info@niara.com