NetIQ Risk Service

By evaluating the risk of an access attempt to applications or services, the NetIQ Risk Service gives you the flexibility to tailor the security and the user experience to the level of risk assessed.

Product Highlights

The Risk Service enables organizations to deploy adaptive access control without the need for complex infrastructure. Increasing security while improving the overall usability has been a significant challenge for organizations. Increasingly, organizations are turning to adaptive access to support this need.

Adaptive access is a process by which context, past behavior of a user, and the sensitivity of the application are evaluated to decide the authentication required to access the application. The goal of adaptive access is to provide the appropriate risk-mitigating assurance levels for access to sensitive resources by requiring users to further demonstrate that they are who they say they are.

Risk Service provides adaptive access through the risk assessment of user access to applications or services. Risk Service analyzes a range of indicators associated with an access activity to determine the probability that the activity is fraudulent. Factors such as the location of the user, time of access, profile and other contextual information, historic records, and behavioral data of users and entities are used to compute the risk indicator.

Risk Service is integrated with products such as NetIQ Access Manager and NetIQ Advanced Authentication to provide risk-aware adaptive authentication. Risk Service integrates with Arcsight Interset to use behavioral analytics in risk computation.

Interset uses unsupervised machine learning algorithms to discover patterns of user access and identify threats. Hundreds of built-in machine learning algorithms extract the available entities (individual users, machines, IP addresses, web servers, printers, etc.) from access information and log files and observe events that relate to these entities to determine what normal or expected behavior is. As new information comes through the analytics process, it is evaluated against previously observed behavior, as well as dynamically measured statistical peer groups, to assess potential risk.

Key Benefits

Increasingly, identity imposters are using more sophisticated tactics to defeat your digital defenses. The Risk Service protects against high-risk authentication and application access requests by initiating strong or multi-factor authentication when risk scores indicate that a higher level of identity verification is needed. Because the Risk Service offers a simple rules engine with built-in metrics, you can get started quickly with minimal investment. And beyond user access, it offers risk-based access protection for APIs used throughout your organizations, including mobile services and microservices.

The Risk Service enables your organization to evolve from static authentication and access to an adaptive environment. To be effective, it can consume contextual-related metrics from a variety of sources. In addition to its integration points, administrators can get started with the Risk Service using out-

System Requirements

- Docker Engine
- 2 GB Ram
- Optional: SQL Database for event storage
- 20 GB disk space

Contact us at **CyberRes.com**
Like what you read? Share it.

of-the-box metrics that they can configure themselves.

Key Features

- **Enables behavioral profiling**
  The best way to identify and protect against imposter-based attacks is to learn the unique normal behavior of every identity in your environment. This type of baseline enables the Risk Service to detect most anomalous and suspicious behaviors. User and entity behavior analytics (UEBA) is the next step in building an effective context-based adaptive environment.
- **Computes risk from a broad range of inputs**
  Risk Service computes risk information from a wide range of sources, including IP address and reputation, geolocation, user's identity, roles and profile information, device ID, uniquely created fingerprint of the device, cookie and browser information, header information, history, pattern of access, and information from external sources. The breadth of input range allows fine-grained risk computation and helps identify potential threats quicker.
- **Learns from past behavior and predicts potential risk**
  Risk Service leverages Interset to use behavioral analytics in risk computation. Interset uses unsupervised machine learning and has hundreds of built-in algorithms that discover patterns of user access and identify threats. Risk Service can also support a database for identifying user access patterns for risk policy evaluations.
- **Integrates with third-party services for context and risk inputs**
  Risk Service offers interfaces and APIs for integration with third-party services for contextual information and risk or behavior inputs.
- **Assesses and mitigates risk before authenticating a user**
  With Risk Service, you can assess the potential risk of a particular login attempt even before authenticating the user. Pre-authentication risk assessment allows you to fine-tune the authentication factors for user convenience and potential risk.

To learn more about NetIQ Risk Service, go to here.

760-000026-002 | M | 04/21 | © 2021 Micro Focus or one of its affiliates. Access Manager, Micro Focus, NetIQ, and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.