

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

NetIQ Risk Service by OpenText 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.

NetIQ Risk Service provides adaptive access through the risk assessment of user access to applications or services. NetIQ 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.

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

Intersect 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. NetIQ 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 NetIQ 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.

NetIQ 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 NetIQ Risk Service using

System Requirements

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

Connect with Us
www.opentext.com



out-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 NetIQ 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**
NetIQ 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**
NetIQ Risk Service leverages Intersect to use behavioral analytics in risk computation. Intersect uses unsupervised machine learning and has hundreds of built-in algorithms that discover patterns of user access and identify threats. NetIQ 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**
NetIQ 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 NetIQ 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](#).

About NetIQ by OpenText

OpenText has completed the purchase of Micro Focus, including CyberRes. Our combined expertise expands our security offerings to help customers protect sensitive information by automating privilege and access control to ensure appropriate access to applications, data, and resources. NetIQ Identity and Access Management is part of OpenText Cybersecurity, which provides comprehensive security solutions for companies and partners of all sizes.