Powering Adaptive Security through the NetIQ Risk Service

If you want to elevate security while still delivering the best user experience, you need an adaptive infrastructure. The NetIQ® Risk Service enables you to adapt security levels based on measured risk, optimizing both security and usability.

NetIQ Risk Service at a Glance:

- **Intuitive rules engine:**
  Build risk policies from the built-in context metrics using the graphical UI.
- **Integration with Micro Focus Interset (UEBA engine):**
  Mature your risk policies by leveraging perceptive behavioral analytics.
- **Tight integration with the NetIQ portfolio:**
  Create the best adaptive access experience for users and APIs.

The NetIQ Risk Service is the next generation of contextual security, evolved from Access Manager's risk engine. It retains the best of what the engine has to offer—a simple way for organizations to establish an adaptive authentication experience without the need to involve the engineering team or other departments. The Risk Service extends that same simple implementation beyond Access Manager to other NetIQ solutions. The first completed integration is NetIQ Advanced Authentication. New out-of-the-box NetIQ integrations will be announced as they are finalized. It's important to note that the Risk Service is wholly self-contained; it doesn't require supplementary modules to set up rules, configure policies, or integrate with other contextual input sources.

Why a Risk Service?

Growing security requirements—Organizations that still rely on a static authentication and access infrastructure might not recognize the merits of investing in an adaptive environment. Simply stated, today's universally connected world requires a different level of security than what past practices delivered. Not only is virtually all information now digital, but it's connected and accessible far beyond the protection of secure buildings or robust firewalls. Access is no longer limited to secured corporate devices; it's available to a variety of personal devices as well. To protect against outsiders, organizations often find themselves in a situation where their security policies have locked down their environment to the point where usability is compromised and productivity hindered. Conversely, when you have a security paradigm that adapts identity verification and security controls to match current risk, you are working from a foundation that minimizes disruption of services while optimizing usability—especially if you combine adaptive authentication with single sign-on.

A requirement for Zero Trust—Now that organizations are managing digital resources that can potentially reside almost anywhere, we've arrived at a place where a new security model is needed. One of those models is Zero Trust. Zero Trust is based on the premise that no access request should be trusted by default, regardless of the user's location—even they are inside the corporate firewall. The business imperative becomes developing a strategy that minimizes the friction on users who are accessing secured information while still maintaining a Zero Trust posture. Of course, someone accessing a cafeteria menu or general corporate operational information doesn't pose the same level of risk to the organization as someone accessing vulnerable resources such as private customer/patient information, financial records, intellectual property, or other types of sensitive or regulated data. The key

> **"Pulling in metrics from a variety of sources allows us to build an effective context needed to measure the level of risk of a customer's interaction. By using a risk service, we're able to empower our mobile app customers with more services and a better experience without raising exposure to our business."**
>
> **CHIEF MARKETING OFFICER**
> for a large regional credit union

point is that before Zero Trust can be pervasive or ubiquitous across your organization's digital landscape, there must be some level of intelligence controlling its applicability. While imposing a myriad of authentication requests breaks usability, the vast number of credential-related breaches demonstrates that relying on a static, single sign-on layer policy across the entire environment simply isn't providing enough protection.

Using the Risk Service to Build Context

The NetIQ Risk Service enables administrators to set up and customize policies that effectively measure risk for their environment. The criteria might vary from simple information available about the user's location or device to leveraging Micro Focus® Interset for more powerful behavior heuristics. These context metrics enable you to start out simple and increase context richness where needed. The business measurement of well-designed policies provides optimized usability for legitimate users engaging in digital interactions, whereas requests for additional information or identity verification are reserved for high-risk access situations.

Increasing Your Ability to Adapt to Risk

As identity verification and access control requirements continue to evolve, it's important to note that the broad set of technologies in NetIQ Risk Service make it a leading solution for implementing an adaptive access management environment because it offers:

- A simple rules engine and built-in metrics that enable organizations to get started quickly with minimal investment
- Risk-based access protection for APIs
- Integration with Micro Focus Interset and other behavior analytics engines
- Tight integration with the NetIQ portfolio, which offers an industry-leading identity and access management solution

The NetIQ Risk Service is Micro Focus's next step in helping organizations to expand their risk-based access management infrastructure. It provides more ways to create adaptive security policies, which were previously reserved for those who invested in home-grown or customized implementations.

To learn more about NetIQ Risk Service or to start a trial, go to: **www.microfocus.com/netiq-risk-service**