NetIQ Risk Service: Your Source of Risk Intelligence and Control

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

NetIQ Risk Service at a Glance

Intuitive Rules Engine

Use the graphical UI to create risk policies from built-in context metrics.

Out-of-the-Box Integration with Micro Focus Interset

Drive down user friction while maintaining security through machine learning that offers advanced behavioral analytics (UEBA).

Centralized Risk Service for the NetIQ Portfolio

Create the best adaptive access experience for both user- and API-based access.

The Risk Service is the next generation of contextual security designed for the NetIQ product portfolio. It retains the best of what the previous risk engine offered in that it enables security teams to adapt their user's authentication and authorization based on risk. Administrators can configure these policies on their own without specialized expertise.

In addition to the built-in rules engine, the Risk Service now offers out-of-the-box integrations with ArcSight Interset. Interset applies advanced unattended machine learning technology to establish a behavioral baseline for each individual accessing resources. The longer Interset runs, the more effective it is in driving down friction for each user. The Risk Service is wholly self-contained: enforce corporate access security policies, consume six out-of-the-box data UEBA templates from Interset, or both.

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 more effective approach to secure access than what was possible with past practices. Not only is virtually all information now digital, but it's also 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 situations where their security policies lock down their environment to the point where usability is compromised, productivity is hindered, and people are frustrated.

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, they need a new security model. One of those models is zero trust (ZT). ZT is based on the premise that no access request should be trusted by default, regardless of the user's location—even if 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 ZT 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,

“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
Large Regional Credit Union

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

such as private customer and patient information, financial records, intellectual property, or other types of sensitive or regulated data.

The key point is that before ZT can be 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 isn’t providing enough protection.

Putting Intelligence into Access Management

What makes the Risk Service different? It can build a powerfully adaptive environment without custom coding or hiring expensive specialists. The NetIQ approach not only makes the most of your current architecture but also makes it easy to add adaptive access management to it. Even across the most complex environments, NetIQ enables you to personalize what is relevant and secure all of your sensitive information. There are five capabilities that make the Risk Service and the NetIQ portfolio unique:

- Simple GUI-based rules engine to enforce corporate policies designed to control risk or comply with government mandates
- Rules engine contains built-in metrics that can be incorporated out of the box and an integration interface to consume whatever user analytics you are collecting.
- Prebuilt out-of-the-box Interset templates that feed UEBA level heuristics enable you to maintain security levels as your drive down friction.
- Advanced analytics and risk policies applied to API-based access (microservices- and application-based mobile access).
- The central risk service for the NetIQ portfolio.

The Risk Service is NetIQ’s next step in helping organizations 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 homegrown or customized implementations.

Learn more about NetIQ Risk Service.

About NetIQ

NetIQ provides security solutions that help organizations with workforce and consumer identity and access management at enterprise-scale. By providing secure access, effective governance, scalable automation, and actionable insight, NetIQ customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the NetIQ homepage at **www.cyberres.com/netiq** to learn more. Watch video demos on our NetIQ Unplugged YouTube channel at **www.youtube.com/c/NetIQUnplugged**.

NetIQ is part of CyberRes, a Micro Focus line of business.

CyberRes
A Micro Focus Line of Business