

Solving Authentication Challenges

Whether its to protect against long time security threats, desire to speed up business processes, or making engagement more convenient for their consumers, there are plenty of reasons why organizations want to transition as much of their environment as viable to passwordless.

Multi-factor authentication: governments have established policies and issued mandates requiring that access to sensitive information be protected by 2 factor authentication. Additionally, organizations commonly provide multiple types of authentication to accommodate user and situation diversity.

Strong authentication: although passwordless solutions have been around for decades, recent shifts in the market have pushed this type of technology to the forefront. Passwordless technologies are highly resistant to the most common ways they are hacked, phishing. They also are key to making authentication easier for users.

Convenient access: while security teams are primarily focused on protecting their resources, business owners and especially the users themselves place speed and convenience on the top of their list of priorities.

- Smartphones have moved passwordless authentication, such as fingerprint and eye scan, to mainstream.
- New technology and a fast-growing market has made passwordless devices far more affordable to purchase, enroll, and manage than historically possible.

NetIQ Advanced Authentication Framework

Consolidate Siloes

Bring all your authentication islands into a single framework for central point of administration and policies



Flexible



Platform

Every Platform

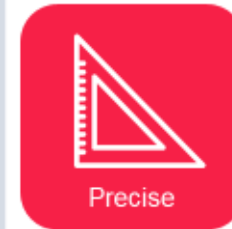
Through multiple clients and SDKs, deliver secure access to all your services and resources

Integrations

The framework's pluggable architecture allows you to control your standards-based devices from a central console for virtually every application



Open



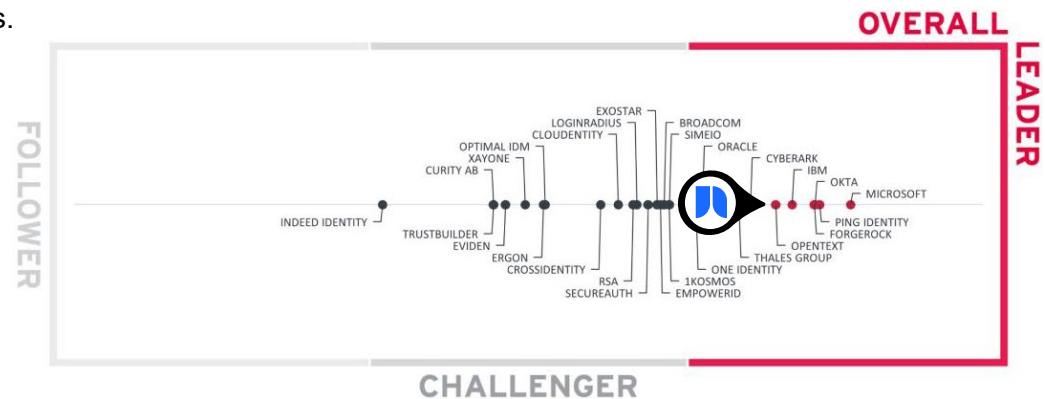
Precise

Match Context

Take advantage of the rich set of authentication options to deliver the right experience and security

Authentication – core component of Access Management

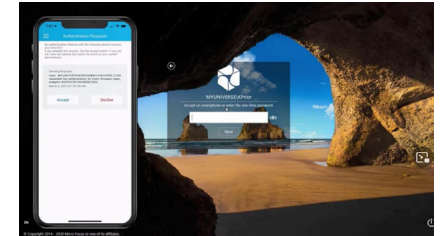
KuppingerCole rates NetIQ by OpenText with a strong positive for Security, Functionality, Deployment, and Usability. OpenText has completed the purchase of Micro Focus, including CyberRes.



NetIQ Advanced Authentication

METHODS				FEATURES					CLIENTS			RISK
Smart Phone	Geo-Fencing	Bluetooth	FIDO 2	Docker	Kubernetes	Multi Tenant	Air Gap Updates	FIPS 140-2	Windows CP	Mac OSX Auth Agent	Linux PAM	IP Address
Windows Hello	WH for Business	Emergency Password	FIDO U2F	ADFS Plug-In	OAuth2	SAML	RADIUS	REST	Win Device Services	Mac Device Services	Linux Device Services	User Cookies
NetIQ App	Microsoft Live	Google Auth	SMS OTP	Kerberos	Microsoft NPS	IIS Auth Plug-In	Citrix/RDP FlexSSO	DB Safety Net	Windows Tap-n-Go	Mac OSX Tap-n-Go	FIDO Extension	HTTP Headers
Voice OTP	Hard Token	3 rd Party Soft Token	Email OTP	Shared Authenticator	Account Linking	2 nd Factor Caching	Repository Sync Agnt	DB Migration	Windows OTP Tool	Mac OTP Tool	Offline Login	User Last Login
Face Biometric	Fingerprint	TouchID	Windows OTP Tool	Auto Enrollment	LDAP Repo	SQL Repo	SCIM Repo	DB Bridge	Windows Custom Logo	Mac Custom Logo	Cached Credentials	Time of Login
SAML	OAuth2	RADIUS Client	Mac OSX OTP Tool	Multiple Enrollment	Custom Enrollment	Localization	Custom UI Text	Backup Scheduler	Authentication Agent	NIST Biometric	Endpoint Security	Historical
PKI PKCS-11	PKI PKCS-7	Device Authentication	Voice Call	FlexOTP	HTTP Proxy	Mobile App Policies	Mobile App SDK	Token Admin Portal	Workstation Pswd Snyc	BYOD	RDP/TS Redirect	
RFID	NFC	Swisscom Mobile ID	BankID	WCAG 2 Compliance	Password Filter	Support Assist Login	RADIUS Rules	Dashboard Widgets	PLAP	Search Card Portal	VMWare Redirect	
PIN Code	LDAP Password	Challenge Response		ReCaptcha	U2F Facets	Connectwise Integration	IPv6	Private Cloud	VDI Auth Agnt	Local Acct Mapping	Citrix Redirect	
				CEF Log Forwarding								

More Info



- NetIQ Unplugged YouTube Channel: <https://www.youtube.com/c/NetIQUnplugged>
- Advanced Authentication [for your business](#) flyer
- [NetIQ Advanced Authentication website](#)

Key Benefits

Increased security – when organizations have the ability to consolidate all their authentication siloes down to a single architecture, they're able manage their entire organizations with one set of policies, ensuring consistent access across their entire environment.

Lower TCO (total cost of ownership) – aside from the inherent vulnerability of authentication silos, having to touch multiple authentication administration points to add, remove, modify user authentication creates expensive overhead and headache.

Flexibility – the Advanced Authentication framework offers the most method integrations available on the market. It's part of NetIQ's platform that delivers advanced risk management which offers custom rules, behavioral analytics, and resource risk calculations. Available as an appliance, Docker containers, or SaaS.

Trusted

by some of the largest deployments in the world for Workforce, B2B, and B2C.

