CyberRes

White Paper

Is Your Environment Adaptive Enough for Zero Trust?

Raising your access security to a zero-trust level requires continuous analysis and control.

Although most organizations still use firewalls as their first line of defense and they remain a key component of their security strategy, changes in where services are located, who controls them, and how they are used continue to challenge that paradigm. The trend towards cloud-based services is as strong as ever. The amount of business being conducted remotely is at an unprecedented level and workers are using their own devices to do it. At the very least, cloud-based services have put a serious dent into IT's practices of creating layers of security protection for their sensitive or regulated data.

For the foreseeable future, organizations with zero trust roadmaps don't typically include plans to eliminate firewalls or any other type of perimeter-based security boundary, especially those with complicated hybrid environments. Instead, the shift in network security is to move away from the traditional approach where resources inside the firewall are delivered simplified access than those on the outside. Zero trust's initial focus was to apply tighter controls for each network segment and resource endpoints. Or, to compare it to the physical building metaphor, putting a security guard at every door, hallway, and elevator—and even at each office entry. But despite zero trust's network origins, it's important to point out that today these same concepts have moved up the stack to the services and applications layer.
This approach means that IT can use zero trust methodologies to control responses to access of their protected resources directly. While it does provide far more flexibility than the network approach for cloud-based services, this granular level of control will likely create scenarios where static authentication policies degrade the user's experience. Referring back to the security guard at every door metaphor, imagine having to authenticate before entering every room in the office building. Instead, zero trust security needs a dynamic authentication model that is far more flexible and less intrusive than today's static implementations.

At the application and services level, organizations will not be able to achieve zero trust without developing an adaptive access management model.

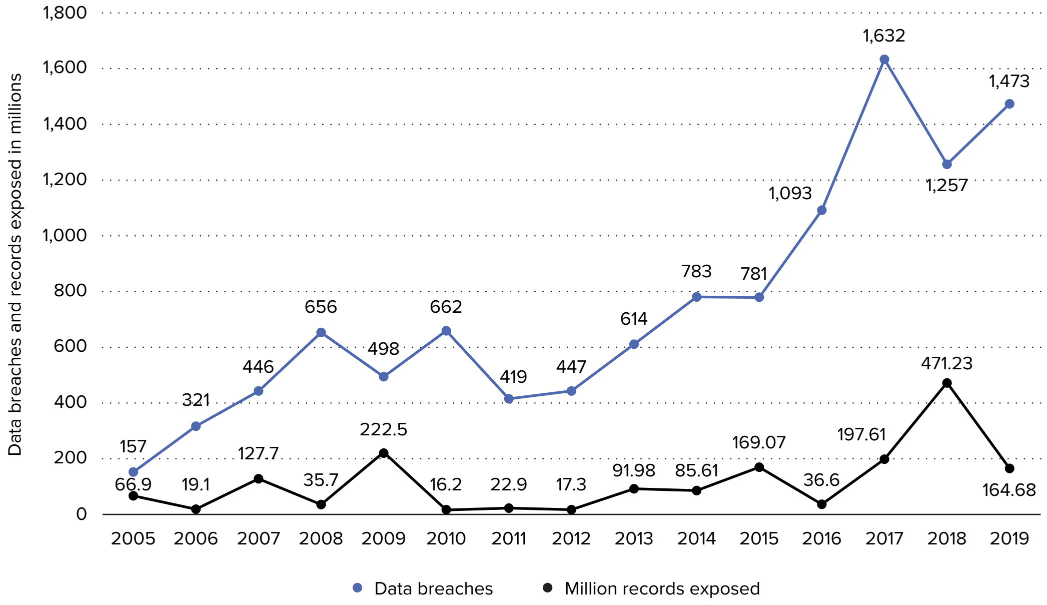


Figure 1. Breaches and exposed records

Because of its control across each session, continuous authentication enables adaptive access management and helps to achieve zero trust security.

Still No Meaningful Headway Protecting Against Breaches

Even before the digital world's mass migration to cloud-based services, it was clear that status quo security strategies weren't up to the task of securing its resources. A good source of data breach trends is the Verizon Data Breach Investigations Report (DBIR). Each year, the DBIR offers the most comprehensive snapshot of the worldwide data breach landscape. This report is built from a worldwide survey and numerous interviews. These annual reports (which go back to 2008) reveal that in spite of countless security projects and billions of dollars of investment, outsiders are just as likely to breach an organization's defenses today as they were a decade ago. Consider these situations where users' credentials can be compromised and organizations still aren't effectively protecting against them:

- Spear phishing or a datastore hack of someone holding a common credential
- Visiting a website that has been corrupted with cross-site scripting code to dupe the user into handing over his credentials
- A user's mobile device or some other type of BYOD that has been compromised, stolen, or is running a vulnerable unpatched operating system

With this lack of progress, it's clear that a significant security paradigm shift is needed. Enter zero trust.

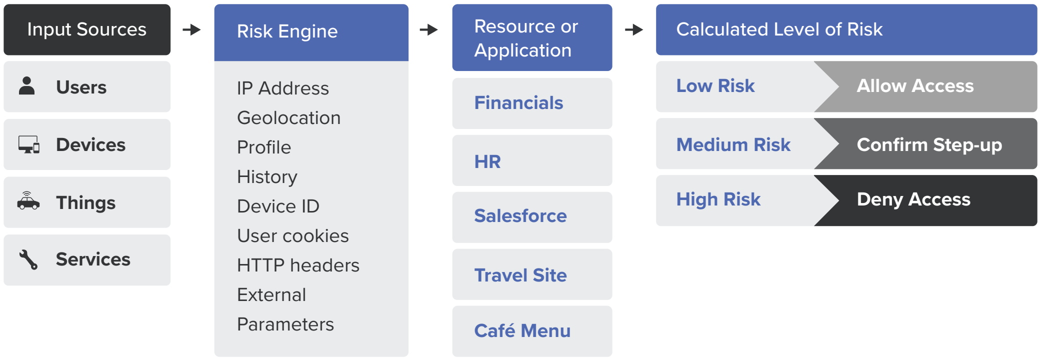


Figure 2. Traditional Risk Based Authentication

Beyond just policies, risk events triggered through behavior analytics work with continuous authentication to reduce or block high-risk access.

The Role of Continuous Authentication in Adaptive Access Management

Zero trust is a welcome addition to the access security model, but it requires an underlying shift to the way access is delivered. With zero trust, neither the user's device nor the origin of the request automatically grants access to services. However, it requires a greater understanding of the context of the question, as well as a higher level of verification of the identity requesting it. It's a rigorous and adaptive level of security.

From the early days of the computer age, digital information has been protected by some type of key, typically a username and password, always at the beginning of a session. Where warranted, a higher security level is established using tokens or two- factor authentication, again, at the beginning of the session. Typically, these configurations are static. The rules are usually simple, meaning that when a step-up authentication is invoked, it is typically based on simple criteria such as whether the user is remote, or the device is known. The defining pattern in these scenarios is that an original level of risk is assessed and adjusted for at the time of the request for access and isn't recalculated for the rest of the session.

With continuous authentication, the system's assessment of whether access to a service should continue is repeatedly reassessed. Access metrics are continuously gathered, and the risk is frequently being recalculated. As IT security groups define the risk models that fit their business, the zero trust paradigm is a closed-loop representation, not an open one. Not only is closed-loop monitoring and control a higher security approach, but the model is conducive to behavioral analytics, which provides a level of identity-centric metrics far beyond standard risk metrics commonly used today. Grant and forget model of access control has its place in enforcing corporate policies but continue to fall short in today's connected world.

As noted earlier, in addition to the security advantages of retaining access control of each session, continuous user tracking does more than just enhance the ability to protect assets—it enables you to build a far greater library of user context. This repository of contextual information provides a foundation from which user and entity behavioral analytics (UEBA) can be applied to build a deeper level of risk intelligence that extends far beyond typical risk-based authentication.

The NetIQ product line provides the most comprehensive components needed for an organization to achieve adaptive access management.

In review, continuous authentication provides immediate security benefits as well as more sophisticated protection as time progresses, such as:

- Measuring actions to determine whether the authorization level should be changed offers better protection immediately.
- Gathering contextual information each time protected data is accessed builds a more complete profile of the user's normal behavior.
- Leveraging UEBA technology, executing analytics on contextual data on a regular basis provides a more accurate picture of expected behavior, improving the ability to identify risky situations.

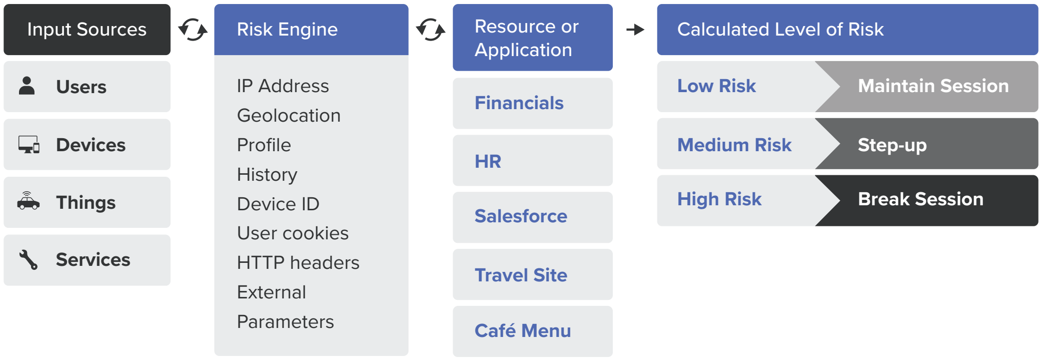


Figure 3. Continuous Authentication and Authorization

- Now, more than ever, monitoring all the different types of **Input Sources** for risk is essential. For example, API interactions such as microservices account for the bulk of todays data movement. If your organization relies solely on API security checks for programmatic security, you're vulnerable.
- Most metrics fed to the **Risk Engine** are prescriptive, but **External Parameters** include more sophisticated contextual information such as UEBA based metrics. Continuous authentication allows continual scoring and active session control.
- Not all your **Resource or Applications** or other digital resources require the expense of zero trust security or even risk-based protection. To reduce costs, limit zero trust security models to only the resources that need it.
- Expanding your ability to measure user context improves your ability to identify risk behavior and invoke the right action (honor request, invoke additional authentication(s), or terminate session) based on the **Calculated Levels of Risk**.

Adaptive Access Management for Your Security Infrastructure

As we've discussed, traditional defenses such as firewalls and static access policies and configurations aren't very effective against today's advanced bad actors, who simply bypass them. Instead, upgrading to continuous authentication provides the foundational level of intelligence (advanced user context) and controls needed to power adaptive access management. Continuous authentication applies the same types of risk assessment as basic risk-based authentication but remains active throughout the session. This holistic approach to access management defends against both outsiders, whose favorite tools are compromised credentials (phished or hacked) and man-in-the-middle attacks, as well as insiders who abuse their granted rights or who take advantage of a shared credential to gain unapproved access.

For an adaptive security infrastructure to be effective, security needs to move beyond prescriptive risk policies and lean more on deeper user context and behavior analysis. Security groups may very well find that using a hybrid approach where prescriptive access policies are enforced by default but are given less weight individually as behavioral information is accumulated to high confidence levels for a specific user. To accommodate diverse scenarios, organizations may need a mix of strong and passive authentication methods to apply the best fit based on the situation and risk, i.e., how sensitive the information is and the context of access.

Adaptive Access Management for Your Business

One of the key challenges of expanding user access with continuous authentication is usability. Invariably, there will be policies or behavioral security events that will interrupt legitimate users. So, while a higher level of contextual intelligence is the lifeblood of adaptive access management, no-friction authentication is what makes it valuable. Reducing requests for strong authentication when a risk event is triggered will keep users productive and help eliminate undesirable workarounds.

The most common approach to removing or minimizing these interruptions is to verify the user's identity through passive authentication. Passive authentication can be a biometric (think of Windows Hello), a behavioral characteristic (for example, the unique way people type), or something the user has (such as a Bluetooth-enabled mobile device that is close to the device being used for the request). The larger the library of passive authentication methods available for use, the more flexibility you will have to match the right method to the situation, or the flexibility to invoke multiple types to increase your verification confidence. Another way to use mobile devices to passively verify a user is through the Global System for Mobile Communications (GSM), which is surprisingly accurate Some FIDO devices are completely passive as well.

Each method has strengths and weaknesses, and no single method will meet your needs. If you require frictionless authentication or if you need a mix of no- and low-friction methods for different situations, risk scores, or behavioral events, here are some options for consideration:

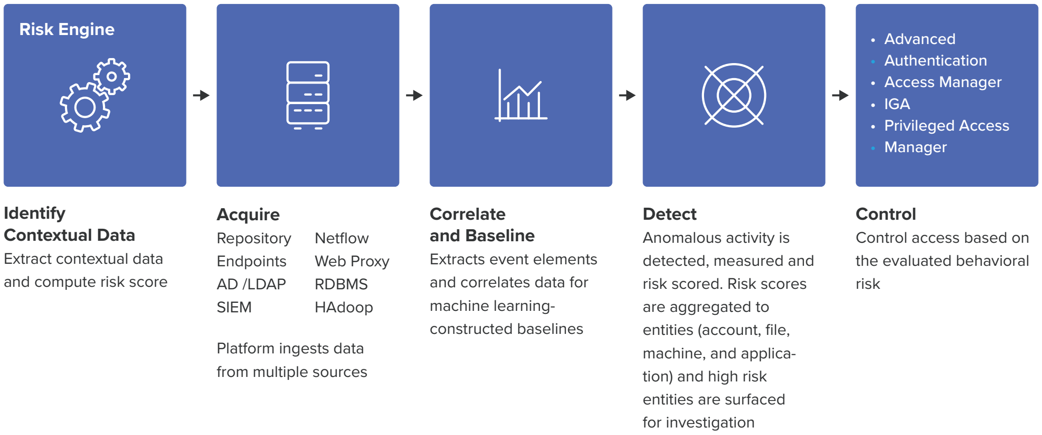
- Good quality, wide-touch fingerprint readers
- Voice print
- Low-friction devices provided by FIDO that require only a simple touch or a wave on your smart phone
- Mobile facial recognition using the smart phone's selfie camera

Each method has strengths and weaknesses, and no single method will meet your needs. There are also other options, but many have higher friction than those listed above. Having options that keep adaptive access invisible to legitimate users is paramount to successful adaptive access management.

Adaptive Access Management Is Core to Zero Trust

In summary, organizations need new access management approaches in order to reach a zero trust level of security—one where the default security behavior assumes a hostile environment. This continuous authentication creates true adaptive access by:

- Extending monitoring and control throughout the session
- Detecting when the risk level has changed since the start of the session and then initiating an authentication request
- Tuning (reducing or increasing) the authorization level based on the identified risk and available identity verification



Risk Engine

- Advanced Authentication
- Access Manager
- IGA
- Privileged Access Manager

Identify Contextual Data
Extract contextual data and compute risk score

Acquire

Repository	Netflow
Endpoints	Web Proxy
AD /LDAP	RDBMS
SIEM	HAdoop

Platform ingests data from multiple sources

Correlate and Baseline
Extracts event elements and correlates data for machine learning-constructed baselines

Detect
Anomalous activity is detected, measured and risk scored. Risk scores are aggregated to entities (account, file, machine, and application) and high risk entities are surfaced for investigation

Control
Control access based on the evaluated behavioral risk

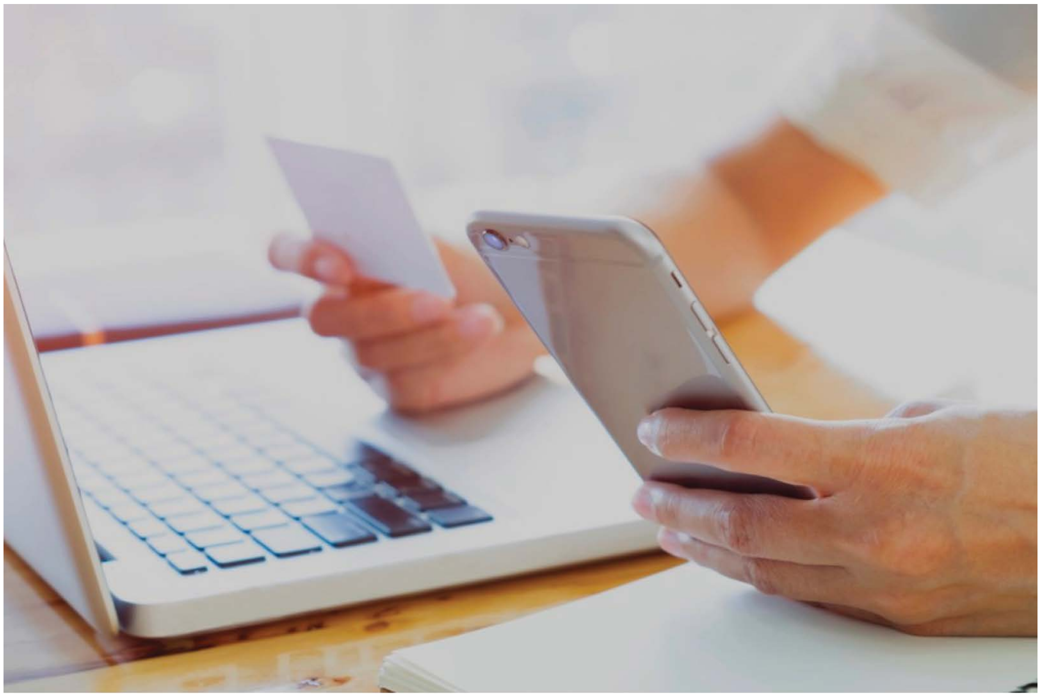
Figure 4. Raising the intelligence of access control through automated learning

Today's organizations need risk detection that goes beyond defined policies to include behavioral analytics. The only way to achieve metrics with the needed depth is to gather richer context metrics and apply machine learning to them.

No-friction or low-friction authentication is essential to adaptive access. If user disruption isn't minimized, then continuous authentication isn't viable to the business. While the level of acceptable user disruption varies with each organization, the closer it is to zero, the more flexibility you will have to safely deliver access to sensitive information.

Using the NetIQ Product Line to Build Adaptive Access Management

As organizations modernize their identity and access management architecture, they recognize that NetIQ offers the richest set of solutions to enforce least privilege, manage identity and access, and build a zero trust environment. Read on to learn about the NetIQ products that IT security teams are using to achieve adaptive access management.



NetIQ Access Manager

Whether it's through the Connector Catalog of prebuilt connectors, or through the self-configuration tool Connector Studio, NetIQ Access Manager is noted for its simplicity in supporting SSO and federation. You also have access to the Connector Factory team for public-facing websites if you need help plugging in the right meta-data.

Access Manager also comes with its own reverse proxy, which serves as an application and services gateway. The gateway makes applications accessible across multiple resources and can be configured to simplify the user experience. And although it is often used to add a security layer to legacy applications, you can also use it in conjunction with federated single sign-on to deliver the best user experience.

Based on measure risk, Access Manager can dynamically change a user's authorization to services and make it possible to respond immediately to a threat. Access Manager's ability to enforce an immediate authentication or cut off access makes it an essential element to creating an adaptive access environment.

NetIQ Risk Service

NetIQ Risk Service is a next-generation risk engine designed to integrate across entire NetIQ product line. Risk Service currently supports integration with NetIQ Advanced Authentication and NetIQ Access Manager, with more integrations on the way. In addition to offering prescriptive policy-based risk scoring, the Risk Service also supports integration with User and Entity Behavior Analytics (UEBA) solutions such as Micro Focus Interset. These integrations offer real-time risk scoring across all protected resources, as well as risk analysis that can be drilled down to each user.

Micro Focus Interset

While Interset isn't part of the NetIQ product line, it is the Micro Focus solution for applying state-of-the-art machine learning to create the advanced user behavior analysis. Interset gathers user metrics during the entire session, from which it develops fine-grained risk assessment criteria at the user level. Used in conjunction with the Risk Service's built-in engine, Interest offers the unique ability to increase usability while raising security.

NetIQ Advanced Authentication

The NetIQ Advanced Authentication is a standards-based, open architecture framework designed to be the single point of integration for the entire organization. It offers dozens of native authentication types, including passive ones. In addition to the security advantage it provides by having all authentication policies in a central location, Advanced Authentication's framework is the perfect infrastructure to build a library of methods (passive and otherwise) as needed. It provides several opportunities for users to verify their identity before being blocked from access. Adaptive Authentication also provides zero trust in conjunction with its multiple authentication types.

To learn more about how NetIQ can help you build an adaptive access environment, please visit **www.microfocus.com/en-us/cyberres/identity-access-management**.

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.

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes

A Micro Focus Line of Business