iovation®

SOLUTION BRIEF

Achieving End-to-End Authentication

From low-risk to high-risk actions, be prepared to dynamically adapt

Layered Authentication That Adjusts to Your Most Complex Needs

Authentication has traditionally been cybersecurity's first line of defense. For online businesses, it answers important questions like "Is the person visiting my website or mobile app the person they say they are?" or "Are they a fraudster, hacker, or digital combatant?"

Authentication can also be a frustrating obstacle businesses put in front of good customers. Dated, cumbersome authentication methods often get in the way of purchases, slow mobile transactions, drive up session abandonment rates, and drive down customer satisfaction scores.

To solve these challenges, iovation's *Dynamic Authentication Suite* provides two stand-alone authentication products that work in tandem to address two critical authentication needs:

- **Customer Authentication:** Provides contextual, device-based authentication for low-risk transactions that transparently provides identification and deep contextual insights.
- **LaunchKey MFA:** Offers robust, multifactor user authentication designed for a broad range of risk scenarios, while adding authorization to the mix.

THE RIGHT LEVEL OF AUTHENTICATION FOR VARYING LEVELS OF RISK

AUTHORIZATION	Highest risk, needs dynamic, real-time authorization with multi-party options	LAUNCHKEY MFA
MULTIFACTOR AUTHENTICATION	Increased rigor, heightened risk, but still an excellent experience	LAUNCHKEY MFA
DEVICE-BASED AUTHENTICATION	Low risk, low friction, high usability	CUSTOMER AUTHENTICATION

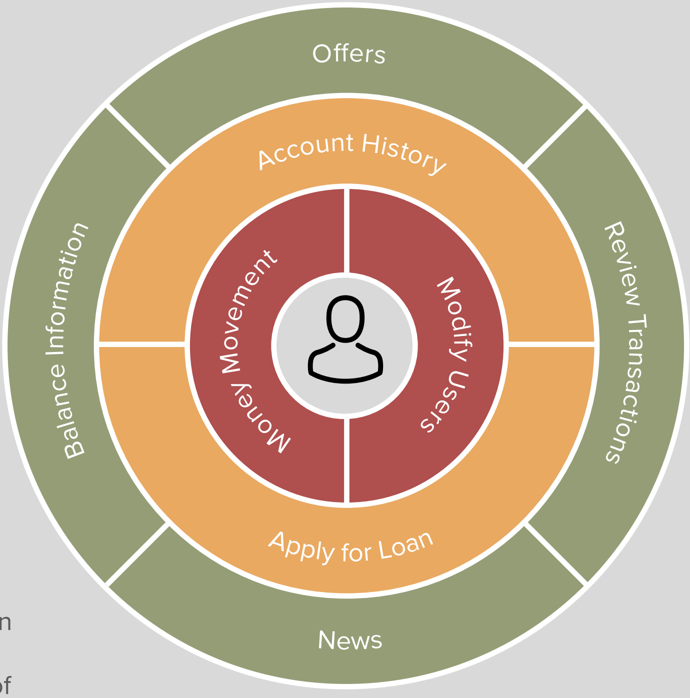
LAYERED AUTHENTICATION

Adapting Tools for Varying Risk

Uses Customer Authentication service

Uses LaunchKey MFA solutions

Uses LaunchKey MFA Interactive Authorization



By combining iovation's Customer Authentication service and LaunchKey MFA, the Dynamic Authentication Suite addresses a full spectrum of authentication requirements for varying levels of risk.

Context: Setting Criteria Against Which Risks Will Be Assessed

Every authentication or authorization request brings at least two kinds of risk context:

- **Risk in what the user is asking to do:** The user may ask to view balance information, which is a low-risk task, or create a new user account, which carries greater risk. At a retail site, the user may log in to browse and make a purchase, or create a new shipping address, which is very often a primary vector for fraud.

- **Risk in how the user is doing it:** Is the customer logging in from a known and registered device? Are there indications of anonymizers, emulators, or spoofing at work? Is the person trying to disguise their identity, location, or IP information? Answers to these questions can help assess risk.

Unfortunately, most authentication and authorization systems are blind to these nuances of context. They're designed to accept or reject the credentials or certificates offered, and not question variations in “what” those credentials unlocked or “how” they were employed.

Bob's username and password combination would be good enough to authenticate an end user as 'Bob' in most classic authentication schemes.

However, a smarter authentication scheme would also check to see if those credentials came from a risky source like a TOR browser exit node, a proxy, or a spoofed IP address. With iovation's *Dynamic Authentication Suite,* this deeper layer of additional context is both visible and actionable.

Context and the Power of “if”

The *Dynamic Authentication Suite* allows iovation's device-based *Customer Authentication* service to provide valuable insight and context to iovation's *LaunchKey MFA* platform, automatically and in real time. *Customer Authentication* serves as a real-time input to the multifactor authentication decisioning engine.

Imagine the following scenarios:

- If the user's credentials are good, but the device has been rooted or jailbroken: **Deny the request or ask for two factors of authentication.**

- If the language and country of the device are logically consistent: **Use the standard authentication process. But if not consistent, add an additional factor.**

- Not all proxied traffic is bad, but if a user's device is coming across on a proxy service: **Request that at least one knowledge factor, rather than just possession or inherence, be presented.**

This integration enables the transparent *Customer Authentication* service to act as the first line of authentication defense and provide intelligence that drives subsequent authentication requests for *LaunchKey MFA*. Not only that, it can align those requests with risk, even as risk conditions continue to change.

SaaS-based Interoperability

As authentication expands beyond the enterprise and deep into prospect and customer environments, IT security professionals are finding that traditional models simply don't fit. Identity stores and on-premise servers were rarely designed to scale to hundreds of thousands or millions of identities. Even where these integrations could happen with authentication servers, they've proven to be complex and time-consuming.

SaaS-based authentication systems address much of these problems by their very design. Their capabilities are abstracted away from the physical hardware that supports them and they can be easily scaled up as demand grows.

LaunchKey MFA and the *Customer Authentication* service, the core products comprising iovation's *Dynamic Authentication Suite*, are delivered through scalable, responsive SaaS infrastructures. Both have comprehensive software development kits (SDKs) that allow your teams to build the unique capabilities for device-based and multifactor authentication into your own products and services.

- Both services come with detailed SDKs to integrate key functions into Apple and Android applications.
- *LaunchKey MFA* provides a white-label SDK that allows you to completely brand your mobile authenticator with your organization's look and feel.
- Both products support MacOS and Windows applications, as well as JavaScript integrations.
- *LaunchKey MFA* supports the standard authentication protocols your InfoSec team already relies upon, like OAuth 2 and OpenID.

Your developers need not use all of the robust capabilities in *Customer Authentication* or *LaunchKey MFA* right away. Both SDKs allow specific features or capabilities to be delivered within your own apps without having to integrate the entire solution.

Continuous Authentication Today

Security experts have long recognized that authenticating users at one point in their session—typically at login—is insufficient for protecting against modern threats. Session hijacking, session fixation, and other kinds of man-in-the-middle attacks rely on the fact that communications are best intercepted during authentication, and that additional authentication events are rare once a session has begun.

Continuous Authentication suggests that sessions are continually monitored to ensure the user is still who they claimed to be when the session began. Numerous checks look for anomalies that may not have been present when the session started, such as a change in the device's IP address. Or, the system can look for odd velocities, like an abnormal number of checkouts or a high number of new account creations from one device.

Even simple mismatches can be identified, like older browser versions working with brand-new OS versions. When detected, the APIs can either issue additional authentication requests or deny the current transaction.

It will take some time to refine and perfect the vision of continuous, always-assured authentication. And it will likely involve the integration of not only risk and context, but also behavioral and biometric authentication methods.

Without question, iovation's *Dynamic Authentication Suite* is a solid foundation for anyone looking down the road towards a continuous authentication strategy that encompasses real-time risk, authentication, and authorization.

iovation®

To learn more about iovation's Dynamic Authentication Suite and schedule a demo, please contact us or visit www.iovation.com.