# F5 Distributed Cloud Authentication Intelligence

## Elevate trust for legitimate customers and improve their experience

Identify and authenticate known customers and support modern, seamless, and secure experiences by taking an analytics-first approach. F5® Distributed Cloud Authentication Intelligence identifies customers based on a blend of network, hardware, and software telemetry collected via lightweight JavaScript code injection.

The solution makes intelligent authentication recommendations using risk and recognition signals, based on behavioral biometrics and machine learning, to determine historical associations (such as prior successful authentications), the uniqueness of the transacting end-user entity, identity spoofing, and anomalous behavior.

You benefit from a collective defense network that tracks billions of legitimate and suspicious daily events that are connected across devices, identities, and enterprises. To avoid reverse engineering, our client-side JavaScript code is highly obfuscated with an industry-leading JavaScript virtual machine and randomized opcodes—ensuring attackers can't learn how they're being observed.

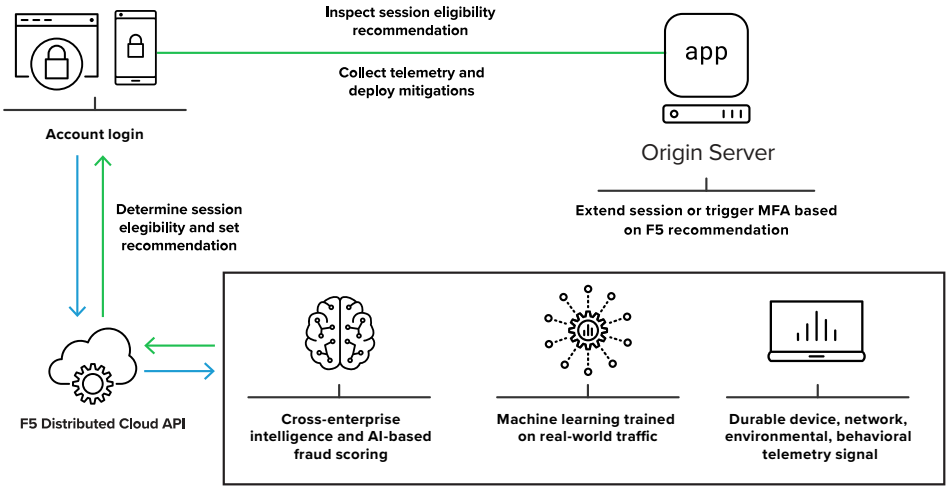


**Figure 1:** Highly obfuscated JavaScript code collects telemetry that is analyzed by machine learning. A recommendation is returned that tells the origin server that a known, good user is attempting to log in.

# Key Benefits

**Reduce friction for revenue-impacting events**

Authentication Intelligence supports authentication flows that are continuous and adaptive, with trust baked into the customer journey. You can impact topline revenue using high-quality risk and recognition signals to safely extend login windows or re-authenticate known customers.

**Dramatically improve existing multi-factor authentication experiences**

Rather than knowledge-based verification questions, navigating email verification processes or performing repeated out-of-band (OOB) one-time password (OTP) authentication requests, Authentication Intelligence performs transparent multi-factor authentication (MFA) by verifying a transacting end-user with device identification information (such as mobile, laptop, or PC) in the context of a physical location (home, office, or datacenter) as an additional factor.

**Reduce false negatives by adaptively applying friction**

Authentication Intelligence assesses end-user intent based on telemetry, behavioral biometrics, and machine learning—enabling you to lower friction for customers and increase friction for fraudsters. You get enhanced detection with a globalized defense network processing billions of daily transactions. Adversaries can't see how they're being detected because of our innovative JavaScript virtualization obfuscation.

**Increase ROI through lower support costs**

Improve the customer experience and reduce the number of support calls and tickets for failed authentication challenges. Not only does re-authentication and MFA reduction improve conversions, but it also reduces the total number of support hours.

# Features

Support risk-based authentication journeys with the ability to correlate insights across disparate security and fraud ecosystems, and remove the need to fine-tune authentication rules. Improve topline revenue by extending login windows, automatically re-authenticate known good users, and lower MFA friction.

**Advanced behavioral biometrics**

- App familiarity
- Keyboard shortcuts
- Copy/paste
- Mouse movements
- Typing patterns
- Autofill usage
- Screen utilization

**Behavioral based decisions**

- Device activity
- Purchase behavior
- User journey profiling
- Login activity
- Payment activity
- Account changes

**Globalized signal detection**

- Attack signatures
- Anomalous behavior
- Improbable time zone switching
- Environment spoofing
- Conflicting user agents
- Browser/JavaScript emulation frameworks

**Telemetry based identity**

- Device ID
- OS
- Browser
- VPN usage
- Hosting ASN usage
- WebGL Renderer cycling
- Webgl VM usage

# More Information

Contact us to learn more about how Authentication Intelligence can help improve your customer security and reduce friction.

**White papers**

Impact of Fraud Detection & Prevention Report by Aite

At the Intersection of Security and Revenue

**Customer story**

Global Multinational Retailer Grows Revenue

**On-demand webinar**

Cybersecurity Myths That Are Harming Your Business

**Solution overview**

F5 Distributed Cloud Security Solutions for
PSD2-Compliant Strong Customer Authentication