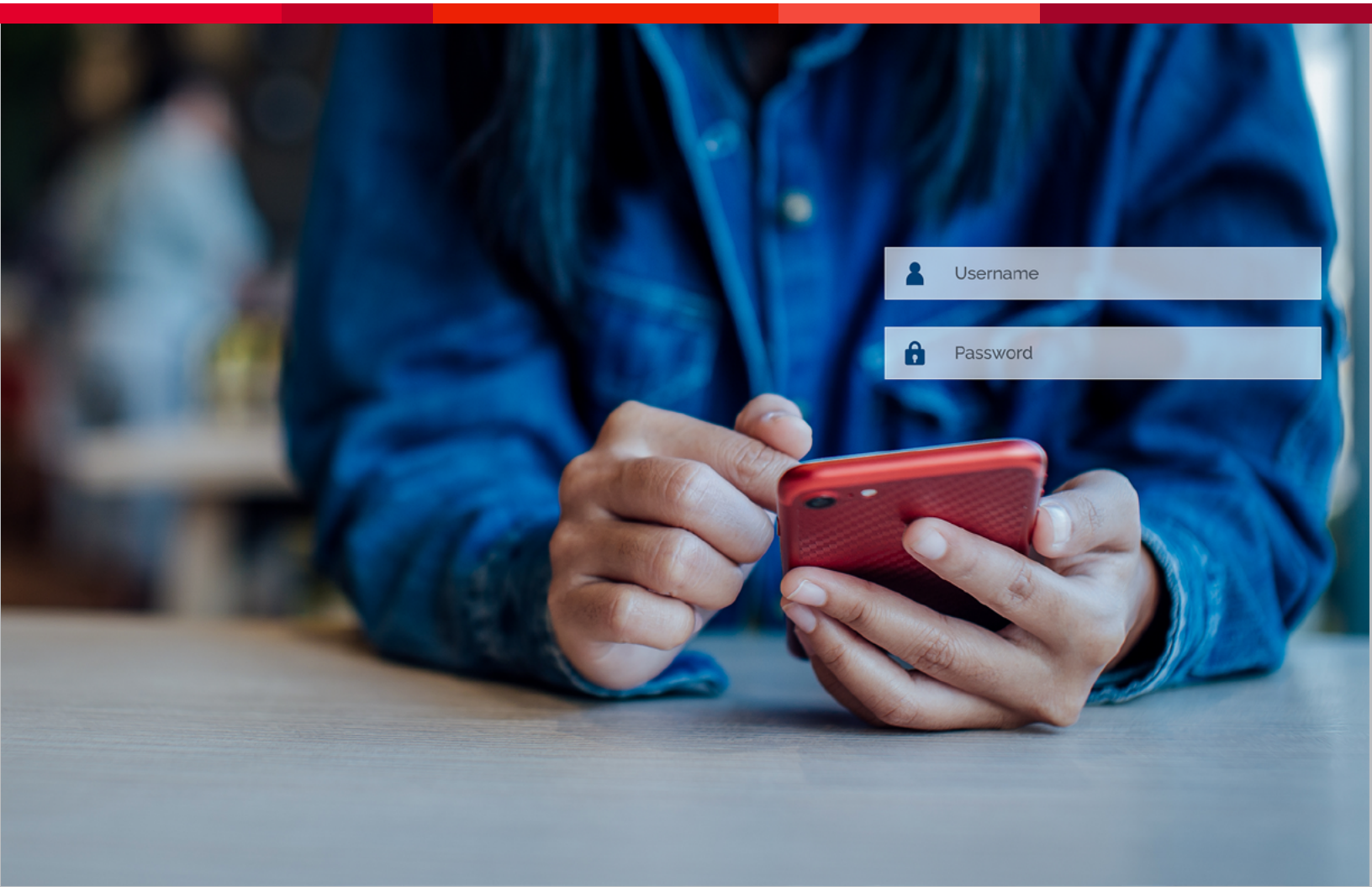
At the Intersection of Security and Revenue

F5 Distributed Cloud Authentication Intelligence and Frictionless Security



Are You Welcoming Your Customers?

In this hyper-competitive environment, not only is the competition a click away, but the largest of those competitors, the likes of Amazon, will gladly welcome your customers by name and accept orders without forcing a login. Amazon has the technology and the data to reduce security friction without risking fraud, earning them a tremendous competitive advantage. Now, with F5® Distributed Cloud Authentication Intelligence, you can level the playing field.

DISTRIBUTED CLOUD AUTHENTICATION INTELLIGENCE ALLOWS B2C ORGANIZATIONS LIKE YOURS TO PROVIDE SECURE PERSISTENT LOGIN, LIKE AMAZON, GMAIL, AND PAYPAL, A CAPABILITY THAT HAS BEEN DEMONSTRATED TO INCREASE ONLINE REVENUE FROM 1% TO 2%, ALL WITHOUT INCREASING FRAUD.

If your organization is like most, you are likely imposing strict, inflexible time durations on authentication sessions, after which users are automatically logged out. Upon return, your users must login again. In practice, this friction impedes up to 30% of customers on typical B2C web applications. These struggling customers either reset their password, contact customer support, or abandon the effort. Distributed Cloud Authentication Intelligence removes this friction by providing a recommendation on whether to extend customer sessions to durations lasting for months. In other words, known good users will be silently re-authenticated when they return to the website within the extended period.

Distributed Cloud Authentication Intelligence allows B2C organizations like yours to provide secure persistent login, like Amazon, Gmail, and Paypal, a capability that has been demonstrated to increase online revenue from 1% to 2%, all without increasing fraud.

Frictionless Security with F5

F5 Distributed Cloud Services were designed to secure enterprise customers and reduce the security friction imposed on end users.

F5 is uniquely positioned to achieve an optimal balance between security and usability. Although user friction seems like a UX issue on the surface, it is a security issue and can only be solved by someone with deep expertise in security and fraud.

F5 Distributed Cloud Bot Defense distinguishes humans from bots without forcing customers to solve those absurdly difficult CAPTCHA puzzles. In an ironic twist on Alan Turing's imitation game, it turns out that machine-learning bots are better at solving these puzzles than humans. So rather than aggravate customers with an ill-fated effort to stop bots, Distributed Cloud Bot Defense turns the tables—using machine learning to detect the bots.

In defending the world's leading financial institutions, airlines, and retailers, F5 processes over two billion HTTP transactions a day, with enriched signals collected through advanced Javascript and mobile SDKs. Utilizing the massive, rich dataset, F5 answers "Are you a human or bot?" "Are you good or bad?" and even "Are you who you say you are?" F5's AI Platform delivers less fraud, less friction, and less effort across the user journey while guarding the digital "front doors" of 40% of Fortune 500 enterprises.

The Distributed Cloud Authentication Intelligence Recommendation

With Distributed Cloud Authentication Intelligence, we're going ever further to reduce security friction and improve the experience for your customers. The product not only identifies a device, but recommends whether it should be trusted for session extension. Extending sessions provides customers with a frictionless experience as the login is performed transparently behind the scenes. Distributed Cloud Authentication Intelligence makes this recommendation by evaluating each device identifier along three dimensions: history, uniqueness, and integrity.

Each of these dimensions are evaluated with data across multiple F5-protected enterprises, encompassing approximately 40% of the B2C brands in the Fortune 500. These websites include low-frequency/high-value sites, such as telcos, and high-frequency/low-value sites, like quick-serve restaurants. And while the recommendation depends on multi-enterprise data, Distributed Cloud Authentication Intelligence at no point shares data between customers, basing recommendations exclusively on aggregate counters. The pseudonymized device identifier behind the product cannot be used to identify user information from another organization.

HISTORY

Each device is used to login into many applications. Behavioral patterns in login activities provide an important indicator of whether the device has been used for suspicious activity. Because F5 accumulates this data across many organizations, the data behind the pattern is both substantial and fresh, enabling Distributed Cloud Authentication Intelligence to produce a highly reliable legitimacy recognition model for determining its session-extension recommendation.

Moreover, Distributed Cloud Authentication Intelligence analyzes whether the device has accessed an account that F5 suspects has been compromised. F5 identifies compromised accounts as those accessed by a larger than expected number of devices, those accessed from known attack tools, and those accessed from suspicious IP addresses. Devices attempt to access multiple compromised accounts should themselves be considered suspicious and not granted extended sessions.

UNIQUENESS

Distributed Cloud Authentication Intelligence also determines whether a device is controlled by a single person or multiple users. The product determines this by analyzing whether a single device was used to log into more than one account on any enterprise's website within F5's network. When Distributed Cloud Authentication Intelligence determines that a device is shared by multiple people, it recommends against session extension so that no user on the device can take over the session belonging to another user.

INTEGRITY

In addition to login history and unique ownership, Distributed Cloud Authentication Intelligence evaluates whether the device itself is suspicious in any way. Using F5's powerful JavaScript-based device inspection technology, Distributed Cloud Authentication Intelligence can determine whether an HTTP request originates from a valid browser, whether the browser matches the HTTP agent-classifier header, and whether the browser is controlled by a scripting framework or is running within an emulator. Suspicious devices should not be trusted with session extensions.

Upon determining that the device is valid, it has a unique owner, and the login history follows a trustworthy pattern, Distributed Cloud Authentication Intelligence recommends session extension. These three dimensions have proven very powerful in granting real customers a frictionless experience while targeting security precautions at the real threats.

Proof by A/B Testing

With the F5 Distributed Cloud Authentication Intelligence recommendation, you can reduce authentication friction for your customers so dramatically that it directly impacts revenue. Without any increase in fraud, your security and identity team will deliver to your organization a measurable impact to the top line.

Don't take our word on any of this. A/B test it on your site. The revenue gain will be clearly measurable.

Distributed Cloud Authentication Intelligence supports A/B testing with little effort on your part. Or you may follow your organization's standard practices to partition traffic and evaluate A/B test results. Either way, the results you deliver to the business will be precisely measured and impressive.

Get Started

Please contact support@f5.com for more information and kick off the frictionless user journey for your customers.