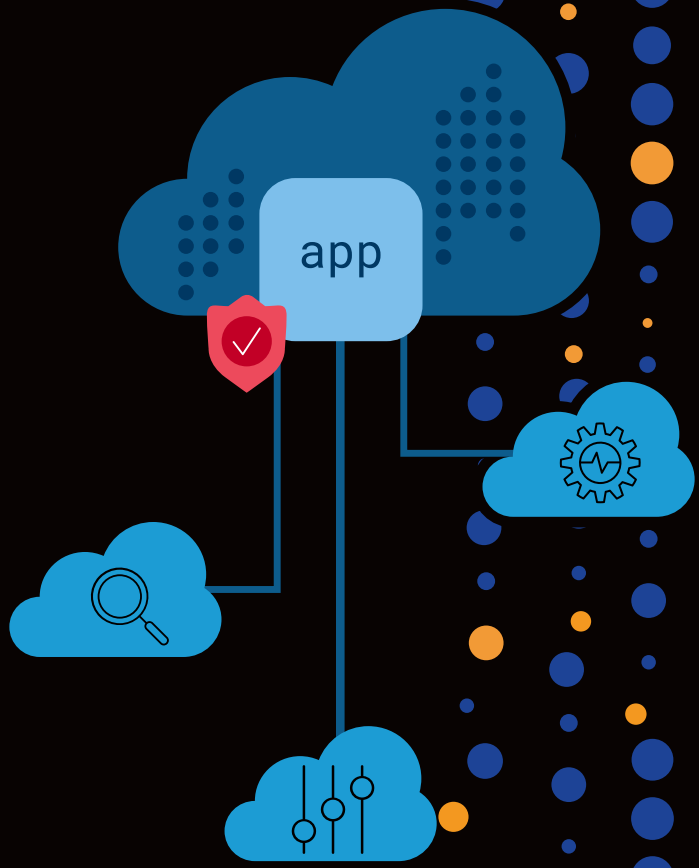
Get Frictionless App Security with F5 and Google Cloud

Learn about the impact of security friction and how to prevent it for secure apps with a better user experience.



Google Cloud

Contents

What Is Security Friction?

You know security friction when you see it—the annoying steps in an app or website that keep you from accomplishing a task. From deciphering squiggly letters to having to log in yet again, these security tools and policies frequently annoy users.

While authentication and security tools serve a clear purpose, your customers generally dislike them. People begrudgingly sign up for multi-factor authentication or identify bicycles in photos in order to securely complete a transaction. However, customers who were already on the fence may be driven away by too much friction.

Security friction can lead to:

Poor customer experiences

Abandoned transactions

Lost revenue and customers

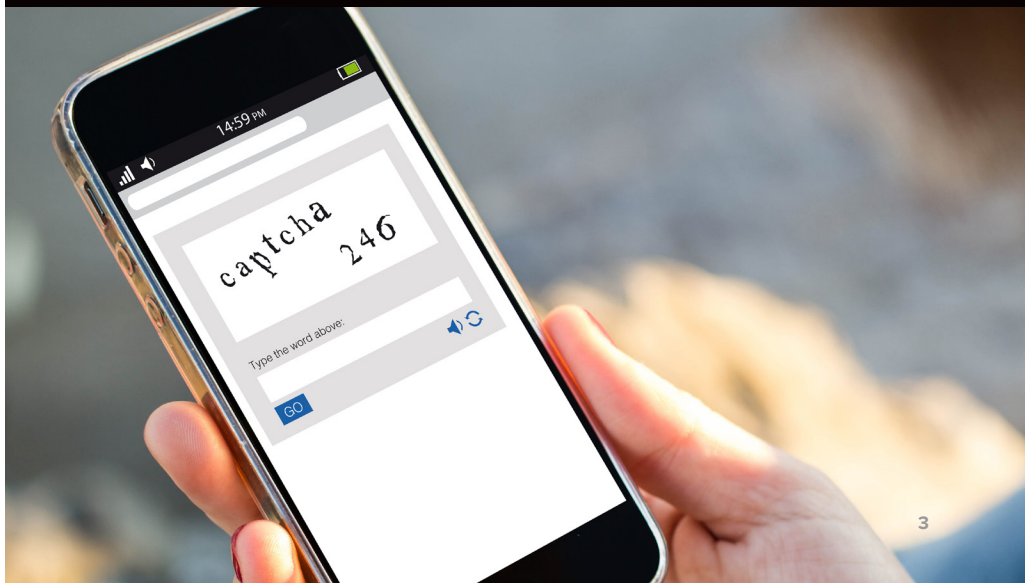
Reducing friction can lead to higher customer satisfaction, more completed transactions, and returning business. The challenge is limiting friction without compromising security.

CAPTCHA: The ultimate source of security friction

CAPTCHA is meant to stop malicious bots, but research shows that it's more effective at stopping humans.

A 2023 study found that bots solved distorted-text CAPTCHA tests correctly nearly every time. Human accuracy ranged from 50% to 84%, and humans required up to 15 seconds to solve the challenges compared to less than a second for bots.[1]

CAPTCHA is a prime example of security friction that can lead to abandonment and lost revenue.



Security Friction Impacts More than Just Customers

Friction is a problem for your own IT and security teams, too. While your SecOps team isn't solving CAPTCHAs, they may be struggling with internal friction, such as:

Multiple conflicting tools

Often each cloud environment has its own set of tools, resulting in disparate, duplicated tools for each security function, creating management headaches and inconsistencies.

Inconsistent security policies

With multiple tools, environments, and apps, security policies can easily be missed or become outdated, increasing risk.

Too many alerts

Teams may be dealing with more alerts than they can effectively triage, especially if there are false positives or duplicates due to multiple disconnected tools.

Siloed teams

When it comes to application and API security, a cross-functional effort is required. However, developer and security teams often have different priorities and struggle to work together effectively.

The Threat Landscape Contributes to Security Friction

The increasing volume and sophistication of security threats demand stricter security policies, which make reducing security friction difficult. Malicious bots are particularly troublesome, as they're becoming better at emulating humans to avoid detection.

30% of all internet traffic is bad bots[2]

Mobile APIs are more frequently targeted by bots than web apps[3]

Bots target processes like user logins and password change flows to attempt to takeover user accounts. They also cause harm by scraping inventory, pricing, and other information.

Botnets are also commonly used for distributed denial-of-service (DDoS) attacks, which have shifted to target the application layer. In 2022, there was a 165% increase in application-layer attacks, while volumetric and protocol-based attacks decreased.[4]

Other contributors to security friction

Bots aren't the only cause of security friction. Multiple environments add friction for security teams.

88%

of organizations deploy apps to multiple environments[5]

98%

of organizations use or plan to use multicloud[6]

Three Strategies to Reduce Security Friction

While it may not be possible to entirely eliminate security friction, reducing it benefits your customers, users, and employees. These three strategies can significantly reduce friction:

Employ invisible protection

- Transparent authentication
- Fast validation
- Little or no user action required

Improve detection accuracy

- Minimal false positives
- Instant access for legitimate users
- Fewer alerts

Consolidate security tools

- Unified policy management
- Single management console
- Less time spent on administration

F5 and Google Cloud have come together for secure apps and APIs in the cloud without friction. F5's portfolio of automation, security, performance, and insight capabilities empower enterprises to create, secure, and operate applications anywhere to reduce costs, improve operations, and better protect users. F5 and Google Cloud's vision for multicloud success includes frictionless security that complements performance, automation, and insight to deliver and scale the application experience.

Invisible Protection

Security that customers can't see provides them with the best experience. This requires using technology that runs behind the scenes as much as possible.

Instead of traditional CAPTCHAs, Google reCAPTCHA protects websites without friction. An advanced risk analysis engine and adaptive challenges keep malicious bots from engaging in abusive activities on your website. Legitimate users can login, make purchases, view pages, or create accounts—often without knowing reCAPTCHA is there—and fake users will be blocked.

F5 lets you add sophisticated bot and DDoS mitigation to Google Cloud that is also invisible to users. Prevent volumetric DDoS attacks or those that target the application layer before they can cause outages or slowdowns for legitimate users. Block sophisticated bots that engage in account takeover fraud, content scraping, and more, and monitor your web pages in real-time for suspicious code that could put customer accounts and data at risk—all without adding work for your uses.

Web apps and APIs are also kept secure against threats without impeding legitimate requests. Invisible protection lets you remove disruptive security tools and processes, leading to happier customers, higher conversions, and greater revenue.

Invisible solutions

Google reCAPTCHA

Seamless fraud detection for websites.

View Google Cloud best practices for security applications and APIs using Apigee.

F5® Distributed Cloud API Security

API discovery and transaction protection.

F5® Distributed Cloud Bot Defense

Real-time detection and mitigation of malicious bot attacks.

F5® Distributed Cloud Client-Side Defense

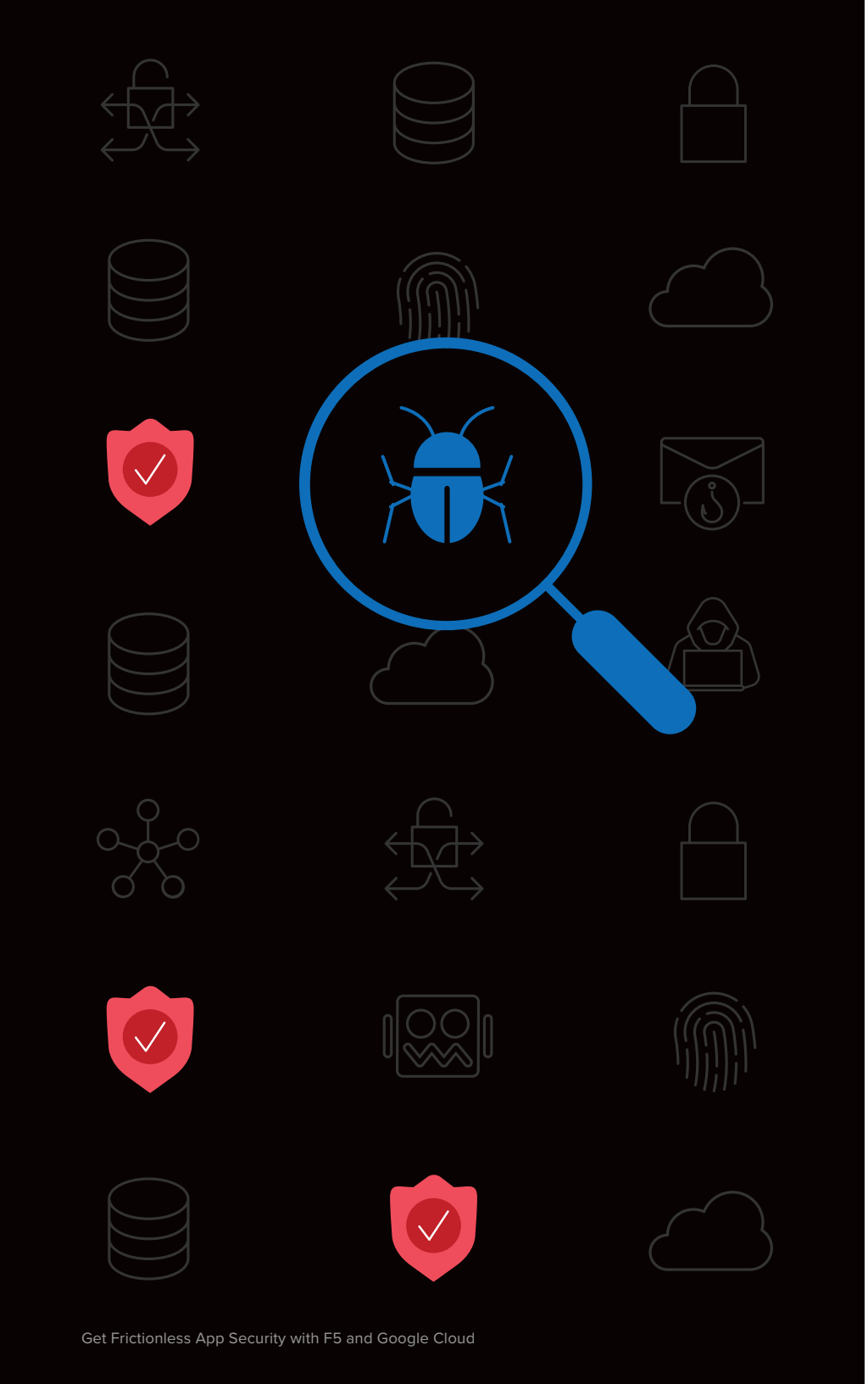
Protection for customer credentials and data against client-side supply chain attacks.

F5® Distributed Cloud DDoS Mitigation

Prevent application-based and volumetric DDoS attacks.

F5® Distributed Cloud Web Application Firewall

Advanced threat detection and AI/ML intelligence for web apps.



Accurate Detection

Being able to accurately tell legitimate users from harmful ones is vital to frictionless security. Modern bots are masters of disguise—able to emulate human behavior, solve puzzles meant to stop them, and retool quickly to avoid detection.

F5 and Google Cloud both offer adaptive algorithms using machine learning for accurate bot detection. F5 also adds rich client-side signal collection, AI, and human domain experts for accurate identification of the most sophisticated bots with a near-zero false positive rate. This ensures malicious bots are stopped while also reducing the number of alerts for security teams to investigate.

Deploy F5® Distributed Cloud Bot Defense to protect web and mobile apps, as well as APIs, against bots for accurate detection anywhere attackers may strike. Prebuilt connectors make it easy to deploy F5 protection anywhere you need it, including content delivery networks, application delivery controllers, e-commerce platforms, and clouds.

See Attackers without Being Seen

Accurate detection includes making sure bots can't evade your defenses. F5 uses advanced code obfuscation to prevent reverse engineering by attackers, having developed the first virtual machine (VM)-based obfuscation defense in JavaScript that uses telemetry encryption to prevent attackers from breaking detection methods.

Tool Consolidation

The final step to frictionless security is to smooth things out for your security teams. F5 and Google Cloud achieve that through consistent tools and policies, allowing you to reduce alerts and management consoles, even with a diverse, multicloud estate.

Bring existing app policies to the cloud with F5® BIG-IP® Virtual Edition (VE) to ensure your applications are fast, available, and secure. Traffic management, DNS, and a web application firewall provide consistency in the cloud and on-premises.

Or use the same tools for app and API security, fraud prevention, and multicloud networking in any environment with a single console. F5® Distributed Cloud Services offer SaaS-based security, networking, and application management for multicloud environments, data centers, or at the edge.

With consistent tools and policies for security and application delivery, your teams can reduce friction and multicloud complexity. As a result, IT and security teams can become more efficient, allowing them to pursue valuable tasks like innovation and threat hunting.

Provide Frictionless Security with F5 and Google Cloud

F5 and Google Cloud offer the invisible protection and accurate detection you need to reduce security friction. No matter where your apps run, you can simplify security with centralized management and consistent policies. Together, F5 and Google Cloud help you improve both security and customer experience to grow your business.

Ensure your apps and APIs are always:

Connected

Available

Secure

Learn more about F5 and Google Cloud at [f5.com/gcp](f5.com/gcp).

The F5 and Google Cloud Partnership

- **6+ years** of collaboration
- **Over 50 listings** in the Google Cloud Marketplace
- **Joint expertise** across security, networking, and industries

Sources:

[1] Andrew Searles, et al., An Empirical Study & Evaluation of Modern CAPTCHAs, UC Irvine, Jul 2023

[2] Barracuda, Threat Spotlight: How Bad Bot Traffic is Changing, Oct 2023

[3] F5 Labs, 2024 Bad Bots review, Mar 2024

[4] F5 Labs, 2023 DDoS Attack Trends, Feb 2023

[5] F5, 2024 State of Application Strategy Report, May 2024

[6] 451 Research, Multicloud in the Mainstream, Feb 2023

ABOUT F5

BRINGING A BETTER DIGITAL WORLD TO LIFE

F5 is a multi-cloud application services and security company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure and optimize apps and APIs anywhere—on premises, in the cloud, or at the edge. F5 enables organizations to provide exceptional, secure digital experiences for their customers and continuously stay ahead of threats. For more information, go to f5.com. (NASDAQ: FFIV).

Learn more about F5 and Google Cloud at f5.com/gcp