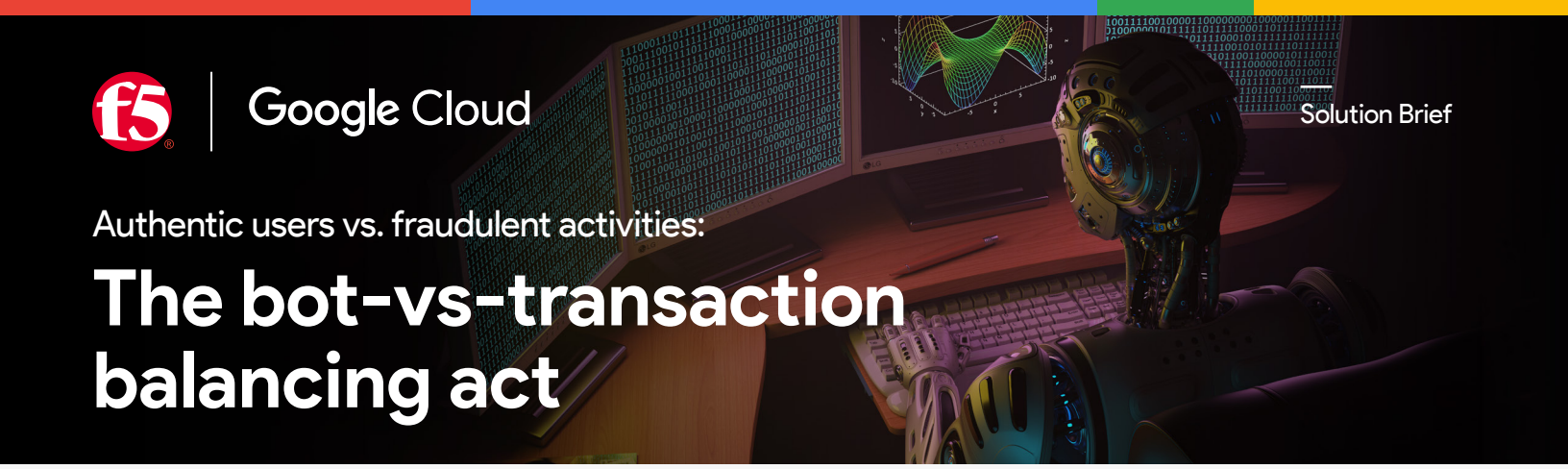

Google Cloud

Solution Brief

Authentic users vs. fraudulent activities:

The bot-vs-transaction balancing act

Whether it's lost transactions, customer departures, diminished revenue, or an ill-informed company forced to make less-than-optimal business decisions, each of these scenarios is the result of the situations organizations routinely encounter when bots attack business systems, workflows, and transactions:

- System/application downtime and poor site performance kills transactions
- Stolen accounts and credentials lead to loss of personal/private information
- Adverse impacts on SEO campaigns crumbles advertising ROI
- A poor experience and apparent lack of cyber hygiene can deteriorate customer trust

Fraud is increasing in sophistication and is often carried out by organized groups using technologies and techniques that are difficult to thwart. These fraud teams, their attack methods, and their tools constantly change, dynamically evolving to bypass the toughest security measures. This puts security teams on the defensive, strains precious business and operating resources, and still exposes the organization to significant financial and brand reputation harm.

Business leaders face a tough choice: A) implement countless layers of security to verify human behavior, potentially frustrating users, or B) accept the fraud losses. It's a tricky balancing act.

Attacker Advantage

In the Business of Fraud

Fraudsters employ bots and automated attacks looking for any opportunity to hijack business logic, take over customer accounts, and steal money. Fraud typically costs businesses 1% or more of their annual revenue.

Limitless Targets

Rapidly shifting business models create more web-facing and mobile access points for fraudsters to target. While historically focused on B2C, bots are increasingly hitting B2B applications too.

Bots are Running Rampant

Growth in global web traffic has led to a growth in bot traffic and other automated activities and transactions. Bots make up over 1/2 of all automated web traffic.

Funded for Sophistication

Fraud targets business process weaknesses including but also beyond software vulnerabilities using ongoing reconnaissance to identify, retool, and circumvent security countermeasures. Sophisticated arsenals of bot automation and evasion techniques increases the attacker effectiveness as they launch attacks exploiting weaknesses such as those found in the OWASP Top 10.

Responder Disadvantage

Not in the Business of Anti-Fraud

IT, security, lines-of-business, fraud, and compliance teams tend to only look at issues related to their own piece of the puzzle – access to relevant data is tough to acquire, analyze, decipher, and act upon.

Modern Apps Increasing Exposure

The response to Covid was swift, leading to new partner portals and e-commerce. Modern app architectures and cloud-enabled infrastructures expand the threat surface and introduce added complexity.

Hard to Scale Defense

Rapidly adapting cyberattack tactics are difficult to track at scale. Threat pace and volume have a direct impact on system and infrastructure performance making it even more difficult for teams to keep up; shortage of resources/skills exacerbates the problem.

Built for Customers, Not Bots

Constant struggle to balance secure apps with a positive user experience. Most organizations leave critical teams out of the bot management decision process, rarely sharing information in an automated, cohesive way that centralizes intelligence and approach making it much more difficult to separate the good behavior from the bad.

Responding to the challenge

Security must adapt to attackers that retool their methods to bypass countermeasures—this must be accomplished without frustrating users. This ability to react as apps and attackers adapt can dramatically improve business outcomes by slashing fraud losses, providing better customer experiences, and maximizing operational efficiencies and business intelligence.

More than just revenue protection

Organizations can discourage and thwart attackers whose methods increase in sophistication, volume, and damage by fighting fraudsters at their own bot automation game. F5 and Google Cloud help you mitigate bot attacks and system/network/application abuse at scale using resilient, cloud-powered protection that adapts as attackers retool. This includes delivering extraordinary digital experiences to end-users through adaptive applications with frictionless security that complements performance, automation, and insight to provide and protect the value offered to customers at scale.

75% of surveyed decision-makers plan to increase their organization's investment in bot management.

Gartner, "State Of Online Fraud And Bot Management," Jan 2021, commissioned by Google

Stay ahead of threats

Safely embrace the transformation of architectures, cloud, and third-party integrations by proactively protecting the increasing threat surface. Significant application vulnerabilities are released daily, and attackers quickly weaponize them in automation frameworks to find and exploit them for monetary gain. We're out-front defending against these threats with you.

Integrate security into the business

Effective application security is automated and integrated. Intelligent automation improves effectiveness by launching and stabilizing security controls earlier in the development lifecycle. This leads to higher AppDev, DevOps, and SecOps effectiveness with less manual effort and reduced strain on precious engineering, operations, and IT resources.

Modernize infrastructure and applications

Google Cloud is a more flexible, secure cloud provider that embraces open-source, making it the best platform to reduce infrastructure complexity while modernizing applications, allowing for multi-tier and distributed architectures over cloud- or container-native services.

Delight customers faster

Organizations need consistent and automated security to effectively manage the growing complexity of securing applications across architectures, clouds, and developer frameworks—all at the speed of application development. Dynamically and contextually enable stepped-up security controls and countermeasures to mitigate customer frustration.

The value of the Google/F5 partnership

Sometimes it's necessary to combine two perspectives and capabilities to overcome some more difficult challenges. F5 and Google join forces to defend their customers against existing and emerging threats by deploying comprehensive security solutions that protect critical applications from bot attacks, web fraud, unauthorized access, DDoS attacks, DNS attacks, and attacks against APIs. F5 and Google Cloud help you mitigate bots and abuse with resilient, cloud-powered protection that adapts as attackers retool.

Google Cloud has always prioritized security; the platform's robust security and cutting-edge encryption allow companies to store and analyze sensitive and personally identifiable information safely. Google and F5 combine to ensure policy compliance across the entire application portfolio—no matter how apps are built or where they are deployed.

The complete portfolio of automation, security, performance, and insight capabilities—all powered by Google Cloud—empowers you to create, secure, and operate adaptive applications that reduce costs, improve operations, and better protect users.

- Outcome-driven defense that adapts to ever evolving threats
- Prevent bots from scraping sensitive data
- Prevent malicious automation and API abuse
- Reduce strain on network resources
- Enable contextual deployment of features like MFA

How it works

As a trusted Google Cloud technology partner, F5 has become the AI-based, real-time fraud prevention leader. F5 leverages the Google Cloud BigQuery data analytics platform, TensorFlow machine learning platform, Google Cloud Dataflow, and Pub/Sub data processing pipelines, along with Google Cloud Kubernetes platform, compute, Cloud Storage, and networking.

Keep the network running smoothly: Common use cases

Advanced technologies and data analytics provide the dynamic insights needed to address the ever-changing threat landscape and attack techniques. The most battle-tested AI/ML engine collects proprietary signals that can't be faked and classifies them by learning from billions of attacks per day. This results in comprehensive, advanced mitigation that protects the network from being overrun by harmful traffic while ensuring legitimate traffic and the resulting transactions continue without delay.

Bot Protection

Proactive, multi-layered security that blocks and drops bad bot traffic before it can hit your network, mitigating bots that perform account takeovers, vulnerability reconnaissance, and denial-of-service attacks targeted at your network or app layer.

Application Security

Security must be integrated into the app development lifecycle across architectures, clouds, and frameworks. Security must also adapt to attackers that retool to bypass countermeasures—without frustrating users.

Online Fraud Prevention

A closed-loop AI system trained on verified human data that evaluates truth and intent to help stop fraud in real-time by distinguishing good from bad actors, invisibly protecting every app from attack, fraud, and abuse.

It's time to control the bots

Stop accepting the loss and don't settle for bot management technologies that fail to deter cybercriminals or frustrate customers with unacceptable workflow friction that leads to transaction abandonment and lost revenue.

Learn how the F5 and Google solution provides customers with best-in-class bot mitigation, anti-fraud, DDoS, and additional protection from malicious and unwanted automated web traffic for web and mobile applications.

F5 | Google Cloud