Verizon Bot Management

Prevent sophisticated fraud and cyberattacks on web and mobile applications.

Solution brief

Your goal is to deliver excellent service and value to your customers. But too frequently, cyberattackers using bots try to take advantage of the applications you've built for customers and use them to perpetrate large-scale fraud or other unauthorized activity.

Defend yourself with Bot Management. Part of Verizon's Web Security, Bot Management can protect web and mobile applications and application programming interface (API) endpoints from sophisticated attacks that could otherwise result in lost money, time and brand loyalty.

The problem with bots: Attackers simulate humans to defraud websites and mobile applications.

Web and mobile applications face an onslaught of sophisticated attacks with one commonality: Instead of exploiting application vulnerabilities, attackers abuse an application's functionality. Imitation attacks simulate human behavior using highly sophisticated automated tools. The most prevalent threats include:

Credential stuffing

Attackers test lists of stolen credentials on the login application. Because end users often reuse passwords across different online accounts, any list of stolen credentials typically has a 0.5% to 2% login success rate on a large website or mobile application,[1] leading to account takeover and online fraud.

Unauthorized aggregation

Attackers scrape valuable information from an enterprise website or mobile application and sell the data to competitors or use it for unauthorized purposes. This process presents an infrastructure burden and numerous security challenges.

Fake account creation

Attackers create fake user accounts in high volumes in order to perform various types of fraud. We have seen fake accounts used to exploit online reward promotions, conduct money laundering and further disguise credential stuffing.

These types of attacks defeat traditional security controls, including next-generation firewalls, web application firewalls (WAFs) and other common defense techniques, such as IP-based blocklisting, rate limiting and CAPTCHA.

Prevent fraud and deflect automated attacks with Bot Management.

Bot Management can help protect your web and mobile applications and API endpoints by determining in real time if an application request is from a fraudulent source and then taking an enterprise-specified action, such as blocking, redirecting or flagging the request.

Any list of stolen credentials typically has a 0.5% to 2.0% login success rate on a large website or mobile application.[1]

Bot Management goes beyond traditional bot mitigation. By defending the world's largest companies for many years, we have developed expertise in identifying not just whether the request was made by a bot or human, but whether the request was made with malicious or benign intent. This provides enterprises full context into the user's transaction flow, enabling real-time fraud prevention.

verizon

How it works

Bot Management is flexible enough to fit within your unique environment. It can be deployed inline as a reverse proxy (see part 1 of illustration) on-premises or consumed via API (see part 2 of illustration).

Client signals

Verizon collects advanced telemetry to enhance the ability of the defense engine to detect attacks. These signals are collected via JavaScript® on web applications and a software development kit (SDK) on native mobile applications.

Bot Management Defense Engine

The Bot Management Defense Engine is the decision component of Verizon Bot Management that detects and mitigates automated transactions aimed at the enterprise's protected applications. It relies on hundreds of signals to deflect fraudulent requests by detecting automation at the network, browser and user levels. The reverse proxy can be deployed on-premises, hosted within Verizon's data centers or in a Verizon-managed public cloud.

AI-based cloud

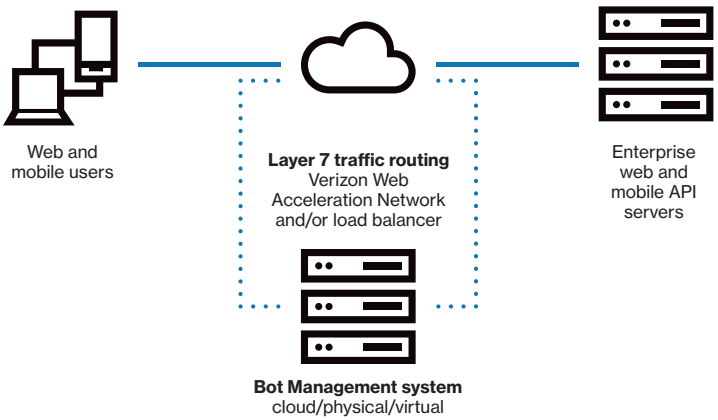
Verizon's artificial intelligence (AI) analyzes all transactions to deploy new countermeasures to mitigate attacks.

API-based

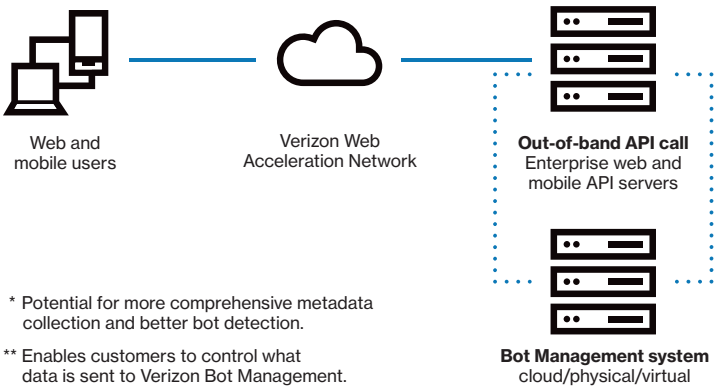
Once the client signals have been submitted, an API responds regarding whether the transaction was generated by an automated or human source and passes that information along to the origin server. The enterprise uses this API response to decide whether to allow or deny the traffic.

Common Bot detection deployment models

Inline reverse proxy model*



Non-inline API model**



* Potential for more comprehensive metadata collection and better bot detection.

** Enables customers to control what data is sent to Verizon Bot Management.

Key benefits of Bot Management

Detection of advanced attackers that retool

As soon as new countermeasures are deployed, 5% to 10% of attackers will typically attempt to retool.[2] Bot Management is designed to adapt and maintain full efficacy even as attackers evolve.

We use supervised and unsupervised deep learning methods to detect attackers' techniques and then autonomously deploy appropriate countermeasures. Because our AI is trained on years of attack data from Fortune 500 companies, we are able to uniquely provide long-term, persistent efficacy, giving your enterprise more complete protection.

Omnichannel protection: Web, mobile and APIs

Once an enterprise introduces a strong defense for one application, attackers quickly begin targeting a different application, often shifting to other channels beyond web. Verizon has solutions for websites, native mobile applications and API endpoints, helping provide full enterprise protection.

Zero effort to operate

Bot Management is provided as a fully managed service so that attacks are deflected with virtually no effort from enterprise employees. The professional services team configures installations, monitors deployments and maintains the technology on behalf of customers.

Once deployed, the Security Operations Center monitors traffic 24/7 and provides incident response. Additionally, threat experts deliver regular briefings on attacks and industry intelligence collected across our customer network, acting as an extension of an enterprise's security and fraud teams.

Collective customer defense

As soon as a new attack technique is observed on one customer, all other Verizon customers are immediately protected from it. Customers leveraging this platform include the largest companies in the world, including three of the top five U.S. banks, five of the top 10 global airlines and three of the top five global hotels. Because the most sophisticated attackers tend to target the largest B2C companies first, all customers benefit greatly from the aggregate attack dataset.

Flexible deployment options

Bot Management is architecture agnostic, designed to provide a unified security posture across all channels. The service can be deployed inline as a reverse proxy on-premises, hosted within a data center or in a managed public cloud, or consumed via an API, giving you maximum flexibility.

Reduced user friction

Using Bot Management allows customers to remove the burden of security from the end user. First, this unique technology surgically identifies attackers without impacting legitimate users. Second, by preventing automated traffic from reaching the origin server, it also reduces server latency, improving performance. Lastly, because of our efficacy, many companies are able to reduce or remove high-friction mechanisms, including CAPTCHA and multifactor authentication, thereby improving the overall user experience.

Why Verizon

Bot Management is part of Verizon's comprehensive Web Security solution with rich features, operations and support. Verizon offers industry-leading service and support; comprehensive, multilayered solutions; and Agile- and DevOps-friendly interfaces. We can help you continually evolve your security approach as you work to keep pace with innovation.

Learn more:

Contact your Verizon Business Account Manager to find out more about strengthening your web and mobile security with Bot Management.

verizon

1 https://www.shapesecurity.com/attacks/credential-stuffing

2 https://www.shapesecurity.com/solutions