WHITE PAPER

Attack Vectors Threatening Your Customer Trust

Security and brand trust have never been more interdependent. With applications and APIs driving how brands show up in the world — and the volume of cyberattacks skyrocketing globally — securing digital applications without stifling customer experience has become job one for security teams around the world.

Strong customer experiences build brand trust, which has a measurable impact on business performance. From website performance to data protection and everything in between, the security choices that organizations make affect customer experience too often for the worse. Cumbersome controls that protect the business can introduce areas of friction for the customer, resulting in loss of trust and, ultimately, revenue.

Security choices also affect growth and innovation. As businesses continue to expand digitally and migrate data and applications to the cloud, countless threat actors are focused on attack vectors opened up by those moves. Security solutions now must aim to evolve ahead of their changing tactics and sophisticated multi-vector attacks (different types of attacks at the same time or in quick succession) by selecting solutions that work together to secure your company and the trust your customers have placed in your brand.

Which attack vectors should top your list?

The newest big target on the block: APIs

Applications drive nearly every aspect of your business, and application programming interfaces (APIs), which connect pieces of software and allow communication among various applications, have become a new favorite target for threat actors. Why? Too often, applications and business processes involving APIs are initiated and deployed faster than security teams can evaluate them, leading to misconfigurations and vulnerabilities. Those flaws are what threat actors look for — using business logic abuse, successful API attacks allow them to gain access to your environment, where they can steal data and even launch additional attacks. And they're not just targeting APIs that go through your web application firewall. Even when authenticated by your WAF, APIs can still become vulnerable to attack, indicating that attackers are now regularly performing reconnaissance to identify specific APIs to exploit.

It's important to remember that any API can potentially be targeted. In industries such as healthcare, the interoperability of IoT devices, for example, has made APIs a huge target for criminals looking to steal personally identifiable information (PII) or to launch ransomware attacks. Securing APIs thus starts with gaining a view to every API associated with your organization, also known as your API estate.

Akamai API Security actually helps you inventory your estate, then provides visibility into the historical behavior of every API, so you can learn what normal versus abusive API behavior looks like. With this knowledge, you can hunt for active threats so you can stop abuse quickly — before threat actors achieve their goals.

More sophisticated and easier to deploy than ever: Bad bots

Bots are moving through your website all the time. In fact, all your search engine optimization efforts are geared to gain their favor. Mixed among the good ones are malicious bots that undertake a range of cyberattacks. Bad bots are perhaps best known for monopolizing limited inventory — such as buying up limited-edition athletic footwear or huge quantities of concert tickets or hotel reservations — but bots use roughly the same method when overwhelming your business with an excessive number of requests in a distributed denial-of-service, or DDoS, attack, which is designed to take your business offline.

What many people do not know is that DDoS has become a relatively easy and inexpensive attack form that is being used by a new crop of attackers to bring down multibillion-dollar corporations and critical public infrastructure, including schools, hospitals, airports, and utility providers. These attacks create massive service interruptions that cost their victims enormous amounts of revenue per minute. In a marked departure from traditional attackers of the past, these attacks are almost always carried out by sophisticated nation-state actors, political hacktivists, and professional cybercriminals with the help of botnets — large networks of connected devices (which could be user devices or simple IoT devices) infected and controlled by bots.

Bots are also used to launch credential stuffing attacks that lead to account takeover attacks. Credential stuffing occurs when an attacker uses a list of usernames and passwords gained during a large data breach, then submits those credentials in massive attempts to log into other institutions. Bots are deployed to undertake millions of account takeover attempts, and because many people tend to reuse usernames and passwords, a small fraction will work. Once the attacker gains access to an account, it becomes an account takeover attack.

Credential stuffing is just one of many methods threat actors use to take over legitimate accounts. Once they control an account, they can siphon off loyalty points and transfer digital assets, drain gift card balances, and make fraudulent purchases using stored credit card information. They may even sell the entire account to another threat actor. If this happens to your customers, trust is almost always irrevocably broken. But even unsuccessful credential stuffing attacks can be harmful to your brand, because the bot traffic flooding your site during these attempts can significantly reduce resource availability and slow response times — creating frustrating experiences for your customers and site visitors.

Finally, scraper bots are used for both good and malicious purposes, but what's less obvious is that their presence can slow site performance and pollute the metrics businesses need to make important decisions, making their side effects potentially worse for your brand than what they scrape.

Akamai has a suite of solutions designed specifically to mitigate the threats introduced by bad bots:

Akamai App & API Protector with Malware Protection is the foundation for protecting against theft of your data, PII, and other account information — and for blocking bot-driven DDoS attacks, as well as ransomware, malware, and more. It allows your customers to have constant access to your web properties and ensures that site performance isn't slowed when you do experience an attack.

Akamai Bot Manager detects all bot traffic and mitigates malicious bots at the edge. It uses AI models to analyze bot behavior, and deploys browser fingerprinting and machine learning (ML) algorithms to make detection increasingly accurate, reducing friction for users while protecting them from fraudulent activity.

Akamai Content Protector mitigates scrapers from stealing your web content that can be used for malicious purposes while also mitigating site performance degradation. With ML-driven detection, potentially malicious bot scraper activity is classified by risk to inform the appropriate response.

Another foundational solution for protecting your customers is to enhance secure account access. Akamai Account Protector thwarts human-driven fraud that is often coordinated by bots, while allowing trusted users frictionless, secure access to your site that encourages them to remain logged in longer and return often.

The cost of malicious scripts: Client-side threats

Similar to bots, third-party scripts largely do good things. They enable functionality, marketing tools, analytics, and more to generally enhance your overall user experience (UX). But they also turn the web browser into a critical client-side threat surface.

Client-side threats aim to trick your customers into accessing malicious content. They take advantage of weaknesses in applications that are running on the computer being operated directly by the user (usually your customer), referred to here as the client. Client-side security thus encompasses the technologies and policies used to protect customers from malicious activity occurring on web pages.

Script attacks can cause significant financial harm to organizations and diminish trust with customers, partners, and payment processors. Not surprisingly, client-side security is a key focus of the new requirements of the Payment Card Industry Data Security Standard (PCI DSS v4.0). To comply, any organization processing payment cards online must know what scripts are running on their site, when they change, and when they stop running.

Defending against these attacks is not easy. Third-party scripts are numerous and continuously changing, making them extremely difficult to monitor. Script attacks themselves also take various forms, such as web skimming and formjacking. Entire criminal syndicates (most notoriously, Magecart) have organized themselves around these kinds of techniques to steal payment card data and PII.

In our world of digital payments and online shopping and researching, client-side security is more critical than ever — especially on checkout and payment pages where personal and financial data is being collected. You need to have visibility into all scripts running on your site, the ability to detect suspicious behavior, and mitigation measures in place to defend against attacks. Akamai offers a specific solution to cover these threats:

Client-Side Protection & Compliance maintains customer privacy and trust within the browser by protecting all of your users against client-side attacks like web skimming, formjacking, and Magecart.

Protect infrastructure to protect customer experience

At the core of the customer experience is the underlying digital infrastructure that powers everything about your brand. DNS security, reliability, and performance is what ensures that your customers can access your services whenever they need them. DNS systems essentially equal your online presence. When they go down, so does your entire digital presence. That is why threat actors constantly attack the DNS systems of their targets with DDoS attacks. Considering the super-competitive playing field all industries face, you need nothing short of nonstop DNS availability and 100% uptime to ensure customers, and potential customers, experience the best your brand has to offer.

Akamai offers a gold standard portfolio of solutions to protect your digital infrastructure from various DDoS attacks:

For the most powerful DDoS defense, Akamai Prolexic offers multiple options for protection, including scrubbing centers in more than 32 global locations, and a staggering 20 Tbps of dedicated defense capacity.

Akamai Edge DNS offers a comprehensive, purpose-built, authoritative DNS solution that uses the scale, security, and capacity of Akamai Connected Cloud to manage your DNS zones.

Akamai Shield NS53, a bidirectional DNS proxy solution with dynamic security policy enforcement, can be used to protect key components of your origin DNS infrastructure — whether on-prem, in the cloud, or hybrid — from resource exhaustion attacks.

We're your partner in ensuring customer trust

At Akamai, we've been focused on how brands show up for more than 25 years. Starting out as a content delivery network pioneer, we solved speed issues for the very first digital storefronts. Over the past decade, we've used the traffic visibility afforded by our content delivery network — one of the largest in the world — to monitor and analyze threats daily, research that organically allows us to evolve our security solutions as attack vectors continue to grow and change. As a key security partner to our customers, we share a commitment to keeping their businesses up and running and to protecting their customer experience, while affording them the confidence to experiment with new digital experiences that lead their industries.

Next steps

Here are some resources to help you consider the next best step for protecting your brand:

A Walk on the Client Side

JavaScript is essential for delivering powerful user experiences, but it leaves your website vulnerable to client-side threats and end-user data theft.

Web skimming, Magecart, and formjacking attacks can result in harmful consequences for brands — from fines to trust erosion and revenue loss.

Where the infection starts

Exploiting first-party vulnerabilities
Security misconfiguration, framework vulnerabilities, etc.

Third-party supply chain attacks
Injection of malicious code via authorized third-party provider

How web skimming attacks steal end-user data

End user browsing online
Web application
End user enters sensitive info into
Data skimmed by malicious script
Compromised JavaScript

Strengthen your web page integrity with client-side protection.

Simplify Your Web Application Security

Get one-stop, zero-compromise security for websites, applications, and APIs.

The Top 10 Considerations for Bot Management

Learn the top considerations for a bot management strategy.

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn. Published 06/24.