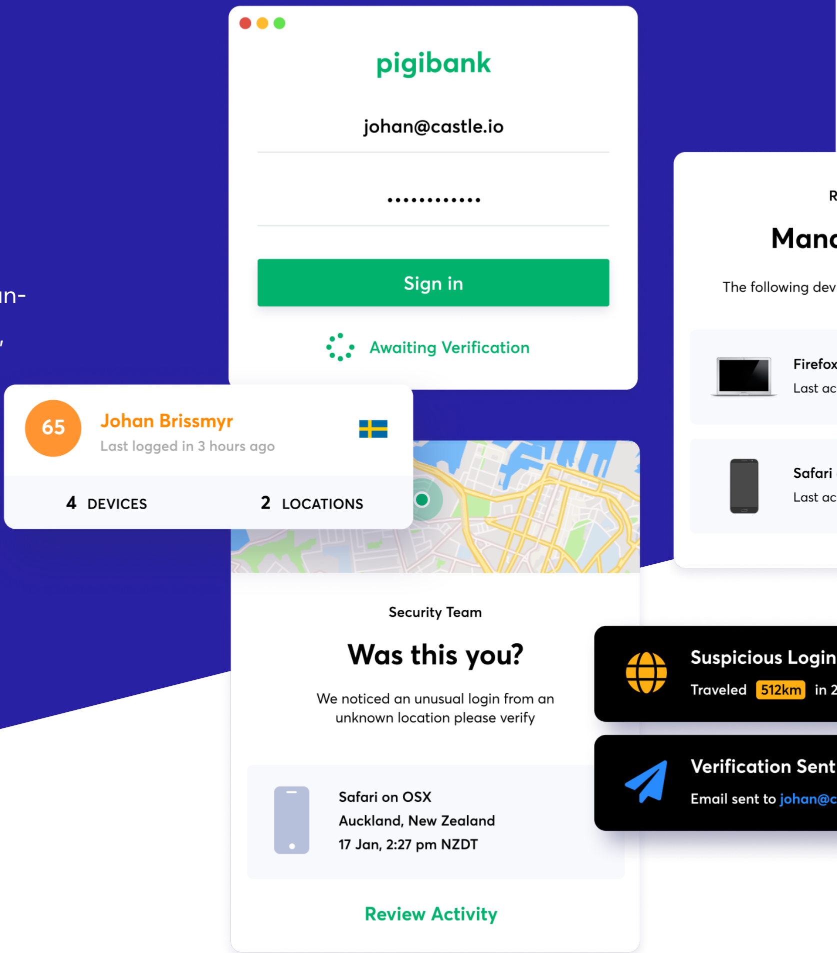
Castle

Castle for Cloudflare

A Codeless Way to Protect Customer Accounts Before and After Login

Get quick time to value in protecting your users from human-powered account takeovers, automated credential stuffing, risky user transactions and more with the Castle App for Cloudflare. With the complexity eliminated you can quickly extend threat prevention and protection for your users both before and after login. Robust insights and behavioral analytics makes it possible to respond to threats in realtime with risk based authentication as well as kick off automated workflows for full account recovery.



We noticed an unusual login from an unknown location please verify

The following dev

What is the Castle App?

The Castle App offers a codeless way to bootstrap the core of your Castle integration through Cloudflare. With the Castle App you can quickly set-up Castle user account protection on Cloudflare sites. Once it is installed, the data flow is straightforward. Cloudflare will route your traffic through the Castle App, which uses the Castle Data Store and our API to intelligently protect your end users.

Key Features

- ✓ REALTIME ANOMALY/ATTACK DETECTION
- ✓ DEVICE FINGERPRINTING
- ✓ USER AND DEVICE ANALYTICS
- ✓ USER EVENT TRACKING
- ✓ CASTLE WEBHOOKS FOR REALTIME THREAT ALERTS
- ✓ ASYNCHRONOUS WORKFLOWS

How it works

By installing the Castle Cloudflare App, Castle workers are deployed across all of Cloudflare's data centers. With powerful configurations, the Castle worker can detect key in-app events - such as successful and failed login attempts - and will automatically send notable events to Castle's API. The workers also identify requests for HTML files, and will automatically inject Castle's JS snippet, instantly enabling device fingerprinting across your web application. The Castle App adds no noticeable request latency.

This codeless integration gives you deep insights into the risks that impact each and every one of your users. The Castle Cloudflare App only sees events that match a pre-defined set of configurations. Castle can not automatically view or access any PII, Payment, or other sensitive data that isn't explicitly shared.

Benefits

Real time Insights and Analytics

Real time insights into your users and devices allow you to investigate without blinders on. APIs, Dashboards, and UIs provide transparent insights into every threat signal, risk score, and event tracked per device within a user's account.

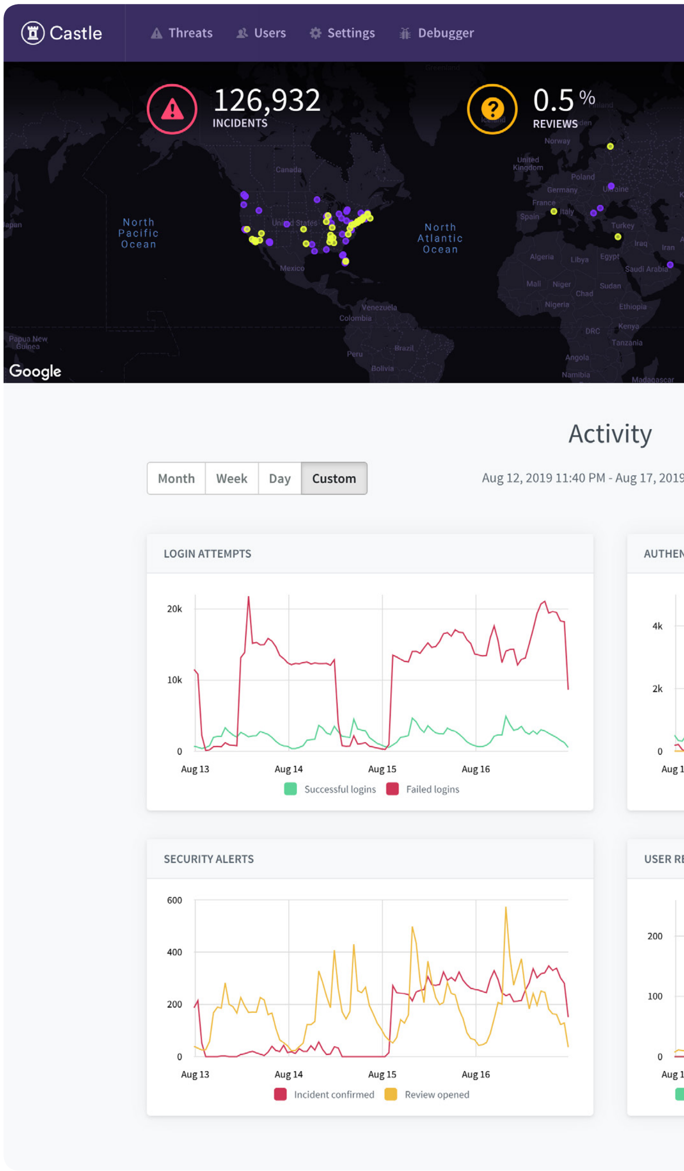
By understanding the end user and their good behaviors, devices, and transactions, it is possible to automatically respond to account threats in realtime based on risk level and policy.

Risk Based Authentication and Automated Workflows

Lose the stress and manual overhead. Account takeovers and other user attacks can be chaotic. Castle allows you to to respond to threats based on risk and formalize a process that works for your app and your users. With Castle you can easily automate intrusion alerts, step-up authentication, and account recovery workflows, but only when they're needed.

Pre and Post Login Protection

Castle isn't just focused on protecting the app and point of access. Castle is the only solution that protects the user both before and after login. Castle understands end-user behavior and can block or challenge identity when something anomalous or malicious happens at any stage.



Strong Security Should be Easy.

Protect your consumers online accounts and optimize your security investments.

Castle

castle.io