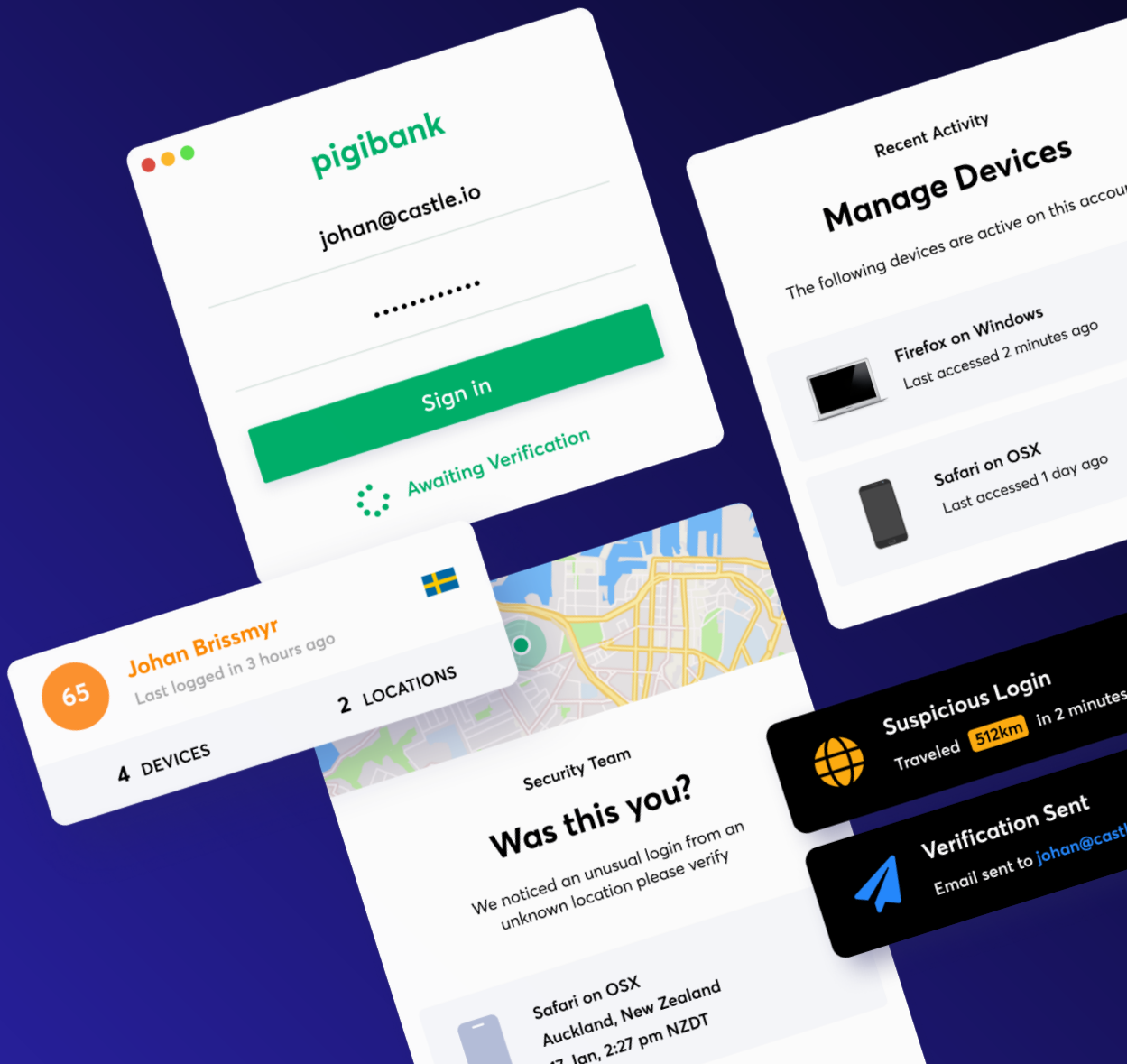
Castle

BROCHURE

Castle's Customer Identity Protection Platform

A identity-centric approach that enables the good while stopping the bad



Castle allows you to get quick time to value in protecting your users from account takeovers, automated credential stuffing, fake account creations, risky user transactions and virtually any attack that relies on humans or bots impersonating your valid users.

Security threats don't just stop at login, they can happen at any step: from phishing attacks at login to bots performing carding attacks in accounts to account takeover attacks during a password reset. Castle redefines customer security by protecting a user's identity through their entire journey with your digital business from registration to recovery with automated, custom workflows for account response and recovery. Instead of focusing exclusively on the threat, Castle puts user experience at the center of the security model that enables the good in addition to stopping the bad, whether it is on mobile or web.

Key Features

- ANOMALY/ATTACK DETECTION
- DEVICE FINGERPRINTING
- USER BEHAVIOR ANALYTICS
- ADVANCED BOT DETECTION
- REAL-TIME THREAT ALERTS
- AUTOMATED REMEDIATION WORKFLOWS
- GRANULAR RISK POLICIES
- CUSTOMER LIFECYCLE PROTECTION

Castle's Key Features

User Behavior Analytics

Real-time insights into users and devices allow you to investigate without blinders on. Castle provides insights into every threat signal, risk score, and event tracked per device within a user's account and reasons for those users' risk scores.

By understanding end-users and their good behaviors, devices, and transactions, it's possible to automatically respond to account threats in real-time based on risk level and policy.

Risk-Based Authentication

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, that align with your risk tolerance. You can deny the riskiest logins and in-app transactions (such as profile changes or abnormal transactions) outright while still ensuring legitimate users can use your application without any friction.

Identity-Aware Bot Detection

Preventing advanced bot attacks requires more than traditional approaches such as parsing through web traffic and trying to understand attack tools and traffic origins. Castle offers higher fidelity bot detection by layering on the context of a user's identity to traditional bot detection risk signals.

By analyzing Identity behavioral analytics in addition to traditional risk patterns, Castle can stop automated attacks such as fake account creations, credit card stuffing, and account takeovers by tying a user to their device and application activity.

Security Automation

With custom policies and automated workflows, organizations can now streamline response and recovery tailored to your organization's needs without involving the support team. Organizations can challenge compromised users through inline workflows or trigger an out-of-band notification that requires a password reset. When behavioral anomalies are detected that may or may not be malicious (i.e. a new device or location), you can push notifications to the end-user alerting them of the activity and asking them to validate.

Putting the User First

User-Trained Machine Learning

When you put security directly in the flow of a user interacting with your application or service, you gain valuable context that allows for better decision making. Security teams can customize policies to decide when and how they want user feedback. Triggering a custom response or challenge allows you to tune responses based on tolerance for both risk and user friction. This could be a simple verification email to the user, an authentication challenge, or any other mechanism the organization supports.

The results of challenges feedback into Castle's machine learning for additional context allowing the engine to be trained on approved or "good" behavior directly from your users. Over time this allows the machine learning to be tightly customized to the user and reduce the need for future friction or verifications.

User Device Management

Users who want to review their device activity can do so through a "review page" built on our APIs. The Device Management API can also be called at any point in your app to either ingest raw data about a user device or display a list of devices Castle recognizes to the user. If you show a user their list of devices, you can also build in feedback mechanisms so the true user can report and revoke access from unknown devices, allowing them to participate in their account security

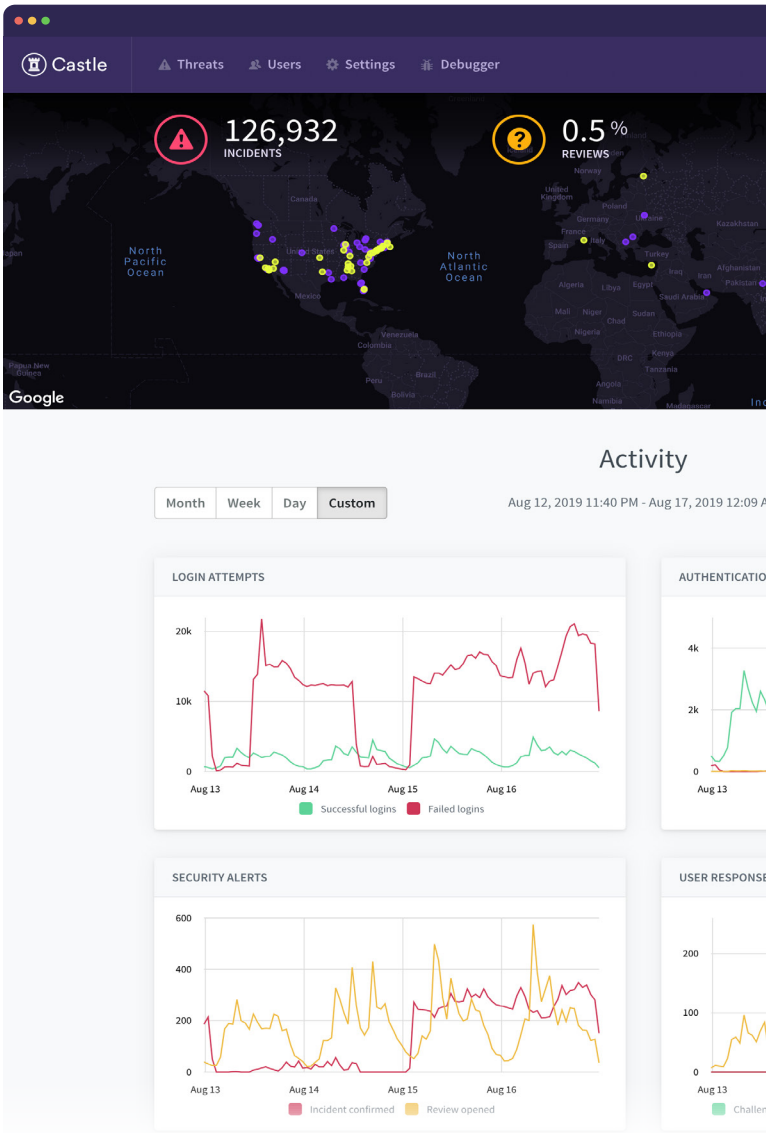
User Session Protection

Castle isn't just focused on protecting a single point of access; Castle protects users both before and after login. With dynamic behavioral profiles of users, Castle can block or challenge identity when something anomalous or malicious happens at any stage.

Analyzing risk before a user account is created, ensuring all devices are healthy at login, and challenging a user based on risk throughout their entire session helps protect every stage of the customer's digital account lifecycle.

Benefits of Automated Workflows

- FEWER HELPDESK/SERVICE TICKETS
- LESS MANUAL SECURITY INVESTIGATION TIME
- REDUCTION OF ADMINISTRATIVE COSTS
- SMALLER ATTACK SURFACE AND TIME
- MINIMIZE FINANCIAL LOSS AND FRAUDULENT ACTIVITY
- STRONGER CUSTOMER ENGAGEMENT AND TRUST



Customers

Every day, Castle is protecting millions of consumer and online accounts for our customers. Leading brands choose Castle to protect and engage their users in security. Some of our customers include: Gilt, Chime, Touch of Modern, Optimizely, Rue La La and many more.

"The benefit of Castle is that account takeover is a total non-issue now."

Steven Ou

CHIEF TECHNOLOGY OFFICER, TOUCH OF MODERN

"A successful integration is one that I don't have to sit on to use and that can alert us with a minimal amount of false positives. That's what we have with Castle."

Ken Pickering

VP OF ENGINEERING, RUE LA LA

"Working with Castle has been a breeze, docs were very easy to navigate, and the integration was fast and painless, allowing us to protect against bot attacks on both web and mobile."

Marcus Brito

DIRECTOR OF ENGINEERING, YIELDSTREET