

A Smarter Approach to Fraud Prevention

Without the Friction



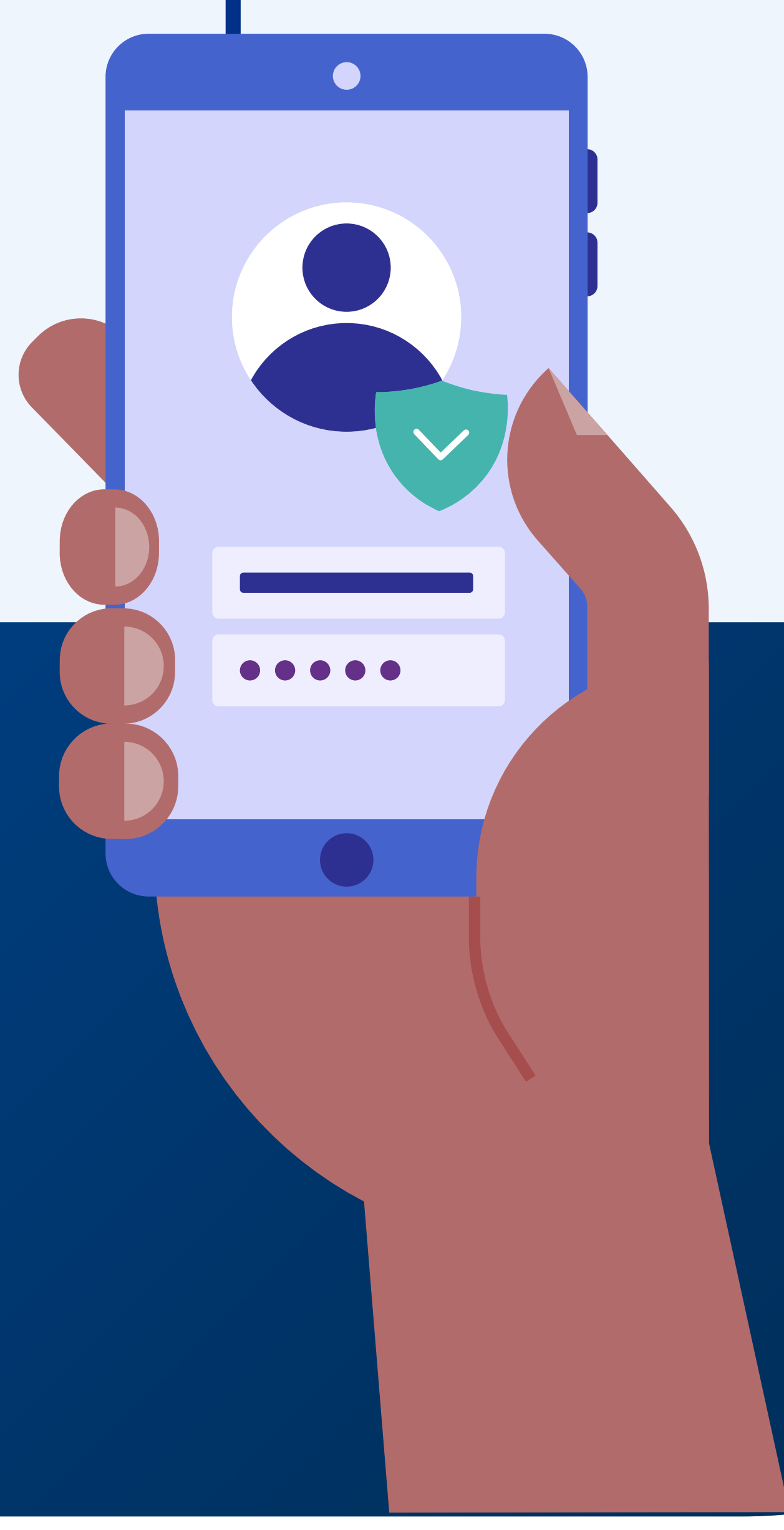
Outsmart fraudsters using a powerful combination of threat detection engines that work behind the scenes to deliver a smoother, safer experience for your customers as they bank online.

The Three Engines of Real-Time Threat Detection

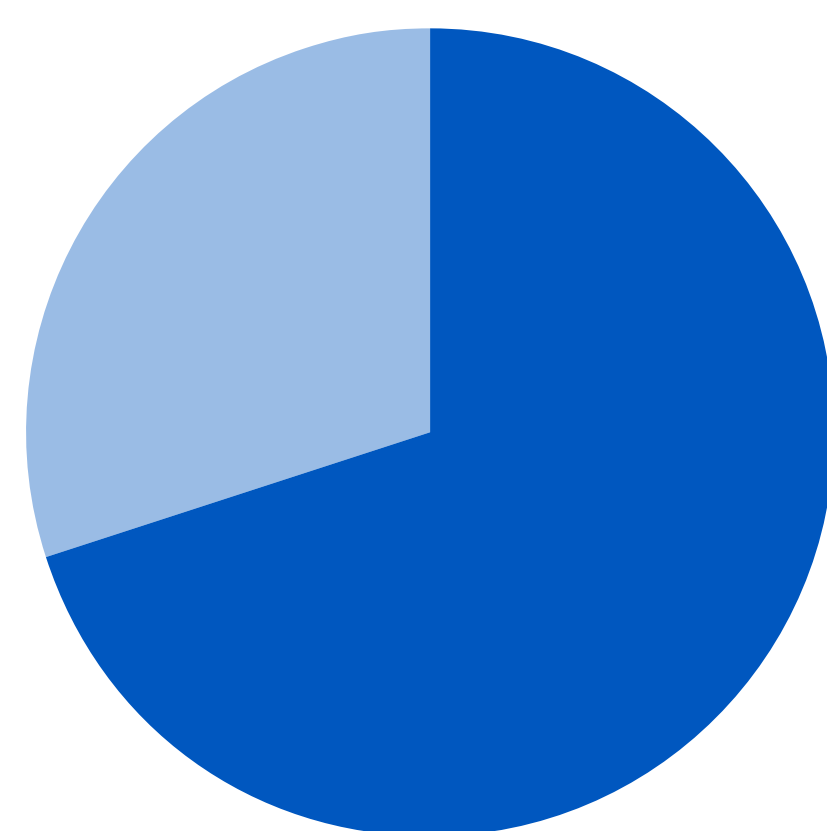


1	2	3
Behavior Engine	Anomaly Engine	Threat Engine
<p>Safeguard your customers by knowing them better.</p> <p>Collect and analyze behavioral biometrics to help pinpoint fraud — undetectably.</p>	<p>Harness the power of pattern recognition.</p> <p>Machine-learning algorithms help the system understand when a transaction isn't normal.</p>	<p>Combat known and unknown cyber threats.</p> <p>Zero-day detection capabilities catch malware, bots and phishing attacks sooner.</p>
<ul style="list-style-type: none"> Date/time behavior Device usage and interaction Navigation behavior Application interaction behavior Transaction/log-in behavior 	<ul style="list-style-type: none"> Payment behaviors/anomalies Suspicious/trusted accounts Known fraud schemes Suspicious sequence 	<ul style="list-style-type: none"> Phishing Malware Bots Application/device protection

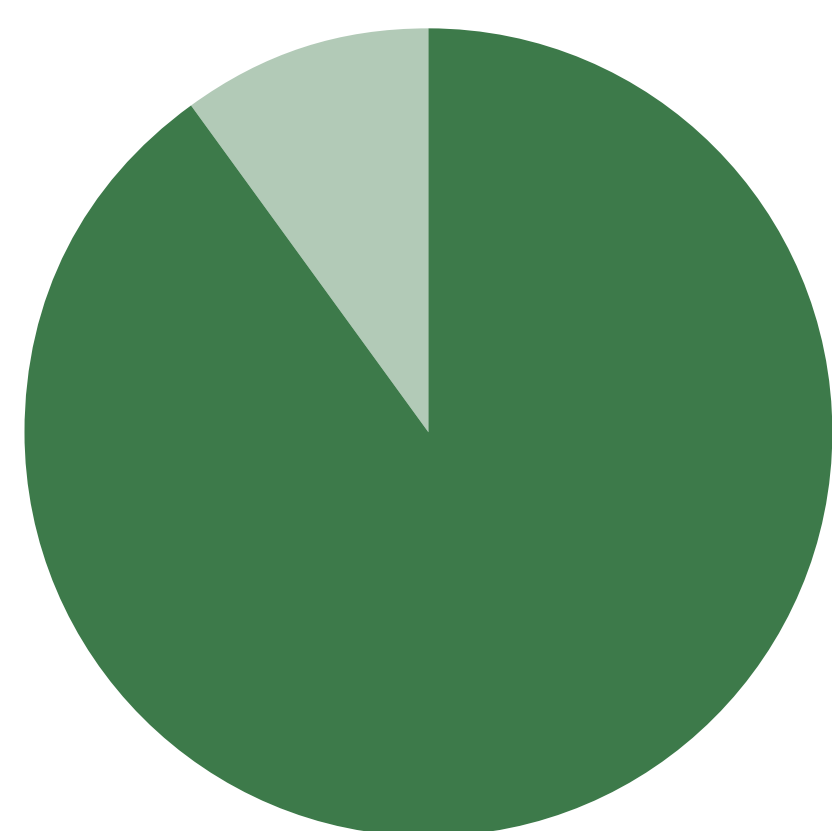
Working together, these AI-driven engines calculate a real time that tells the system whether to step up authentication — without creating frustration for legitimate users.



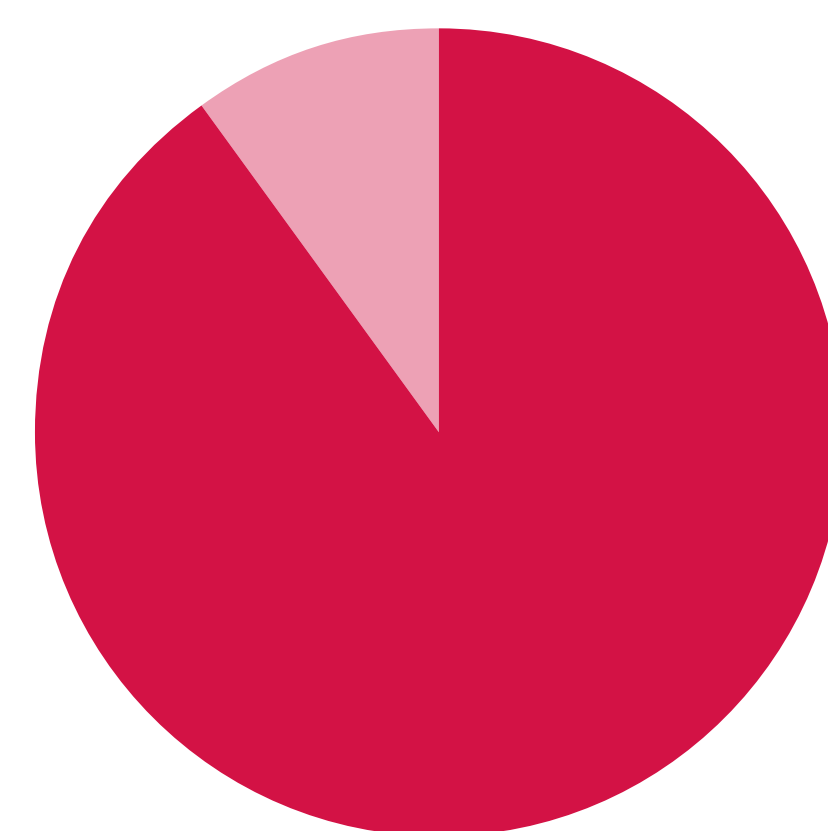
Improve Fraud and Risk Detection, Reduce Costs



70% Better detection than traditional fraud detection. Stop cyber attacks like phishing and zero-day malware before they happen



90% Fewer false positives to save time and money investigating non-threats, while giving users a trusted and seamless experience



90% Reduction in authentication costs without reliance on SMS-based verification. Machine learning and AI support risk-based, adaptive authentication