



Decentralized Authentication

06 February 2019 By: Kyle Marchini, Al Pascual

This original research report, sponsored by HYPR, was independently produced by Javelin Strategy & Research. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

For most consumers, interactions with businesses, whether in finance, commerce, health care or beyond, are moderated through digital channels. The wide-ranging nature of consumers' digital profiles has offered ample opportunities to fraudsters for access and misuse — a challenge that has been exacerbated by reliance on outmoded authentication methods.

Moreover, the expansion of consumer devices in the Internet of things challenges conventional authentication schemes, which have remained largely unchanged for 40 years. Today, the Internet of things encompasses nearly 870 million consumer devices, many of which already provide access to financial or payment information. Not only are emerging devices such as virtual home assistants poorly suited to the use of passwords or security questions, they frequently lack robust safeguards to ensure that data stored on the device cannot be accessed by malicious actors, making it all the more challenging to minimize risk of compromise.

Download Whitepaper

Please fill out the form below with a valid email address and we will email you a link to the whitepaper.

This research report was sponsored by:



It was independently produced by:



Copyright ©2018 GA Javelin LLC, (dba as Javelin Strategy & Research). Javelin Strategy & Research is a division of Greenwich Associates. All rights reserved. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of GA Javelin LLC.

javelinstrategy.com

inquiry@javelinstrategy.com

925.225.9100