

**HID**

HID Risk Management Solution

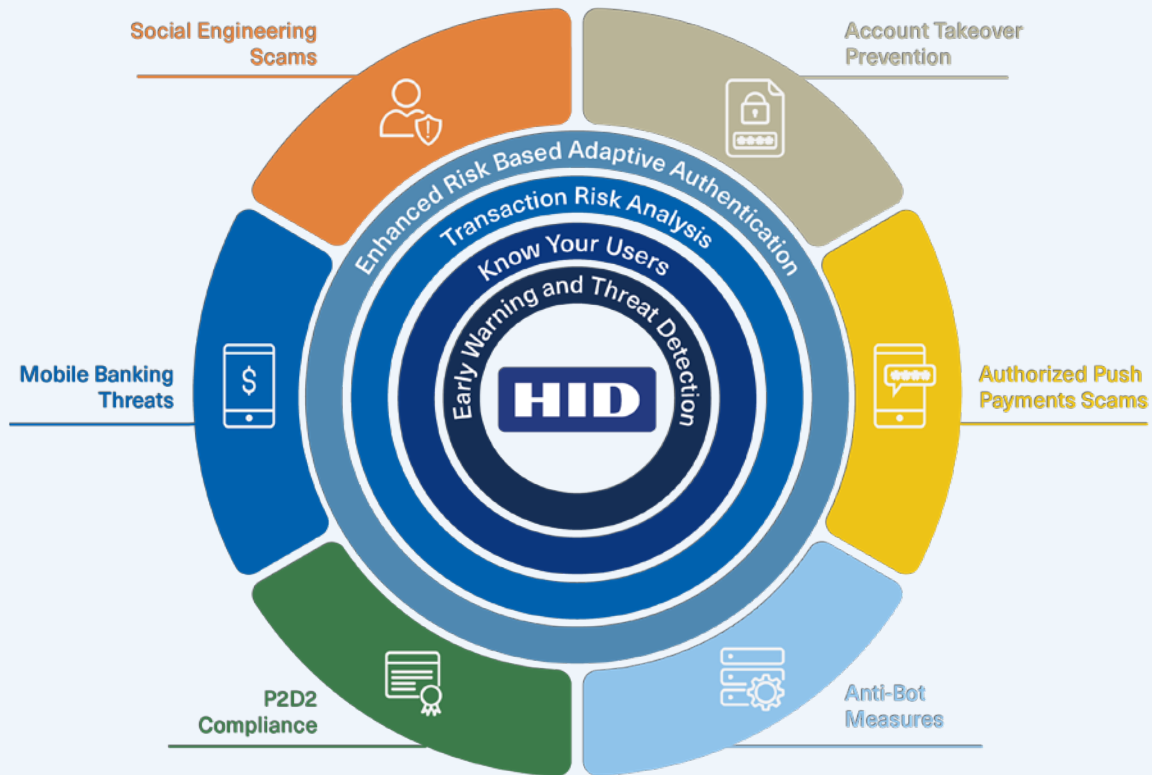
A REAL-TIME THREAT AND FRAUD DETECTION SOLUTION BASED ON DEEP BEHAVIORAL INTELLIGENCE AND MACHINE LEARNING

New-age fraudulent activities have undergone a significant evolution, demonstrating an impressive level of technological sophistication and creativity. Techniques such as phishing, vishing and malware attacks rely heavily on intricate social engineering methods for achieving their nefarious goals. As a result, many individuals become easy targets, falling victim to these innovative social engineering methods. To combat such threats, it is crucial to have a true, fraud prevention solution that helps distinguish between scam attempts and legitimate interactions.

Introducing the HID Risk Management Solution (RMS) — a comprehensive approach to safeguarding all online banking channels and empowering organizations to effectively identify, assess, mitigate and monitor risks. This powerful solution offers a holistic defence against fraud, ensuring a secure and trustworthy digital experience for banks and financial institutions. With HID RMS in place, organizations gain the tools and capabilities to build a seamless and reliable digital experience for their users. By implementing this cutting-edge solution, they can stay one step ahead of potential threats and create a safe environment, protecting both their users and their valuable assets.

HID RMS offers a unique, layered defense approach, which ensures comprehensive, multilayer protection against digital fraud. Its fast implementation, zero impact on customer infrastructure, and cost-effectiveness make it an ideal solution for businesses seeking to bolster their fraud management strategies without disrupting their existing operations.

HID Risk Management Solution's Multilayered Approach to Fraud Prevention



LAYER 1: PROACTIVE

FOCUS: EARLY WARNING AND THREAT DETECTION

This layer focuses on detecting and stopping fraud before it happens. HID RMS thoroughly examines and verifies all data displayed in a web browser, as well as the data concealed in the application code. Automatic testing is employed to compare these data sets against pre-trained models, effectively fighting against known and unknown fraud vectors. The solution is equipped to identify and flag insecure configurations, various threats, malwares, RAT scams, vishing attempts, fraudulent imitation of legitimate banking pages as well as to detect any anomalous behavior that may resemble non-human activity, indicating potential fraudulent attempts. Paired with HID's Fraud Advisory and Mitigation Services, which provides 24/7 monitoring and protection, businesses are better equipped to face modern fraudsters.

LAYER 2: PREVENTIVE

FOCUS: KNOW YOUR USERS

RMS utilizes behavioral intelligence and advanced device identification to verify user identities passively. This layer focuses on understanding if the users are legitimate or not.

Each individual's online behavior is distinct. The way people navigate through the app, their speed in clicking, tapping or swiping, and their unique usage of keyboard, mouse or tap screen all vary from person to person. RMS takes advantage of these distinctive markers and enhances them with personalized user details, including location, device, time and date, navigation patterns and transaction behavior, among other factors. By combining these elements, RMS achieves the highest level of contextual value, leading to a reduction in false rejections of legitimate users and transactions, all while enhancing risk mitigation with an unprecedented level of precision.

LAYER 3: PREDICTIVE

FOCUS: TRANSACTION RISK ANALYSIS

RMS focuses on monitoring and scoring all transactions to make informed decisions on flagging and stopping fraudulent payments and other transaction attempts.

The user's spending behavior is closely monitored and analyzed as it is compared to typical user patterns that include several parameters, such as the transaction amount, frequency, time and other user-provided data. Each transaction is evaluated using multiple models, each comprising a set of rules specific to transaction types and channels used. The fraud detection capabilities of RMS are not solely reliant on fixed rules; they leverage advanced machine learning techniques and pre-trained models to adapt to emerging fraudulent scenarios and detect anomalous behaviour by new users.

LAYER 4: PART OF A COMPLETE PORTFOLIO

FOCUS: ENHANCED RISK-BASED AUTHENTICATION

RMS is part of HID's comprehensive portfolio of robust consumer authentication solutions for a seamless end-to-end journey that includes risk-based authentication and digital identity verification all from a single vendor. HID prides itself on truly focusing on enhancing user experiences without compromising on security by offering the right security for the right user.

Learn more about
HID RMS in our [*datasheet*](#)
or download our ebook,
[*The Ultimate Guide to Risk
Management Systems.*](#)



hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 | Latin America: +52 (55) 9171-1108

For more global phone numbers click here

© 2024 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

2024-03-21-iams-hid-rms-xb-en PLT-07416

Part of ASSA ABLOY