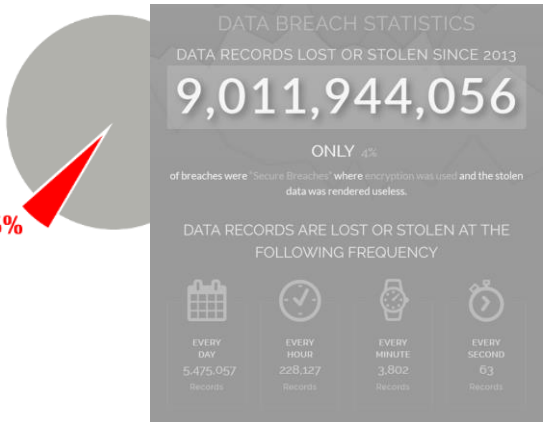
Preventing Fraud in SAP® ERP

SAP ERP Security Status

- Fraud is common, despite use of GRC, SoD, SSO & Identity Management, due to reliance on knowledge-based security (passwords).
- According to ACFE, globally 5% of gross revenues are lost to fraud. www.acfe.com
- According to Ponemon Institute, the average 2017 cost of a data breach is $3.6 million.
- According to Gemalto, more than 9 billion data records have been breached since 2013.



http://breachlevelindex.com/
http://www.ponemon.org/

The Root Cause of Fraud

- Without use of **biometrics**, "identity management" and SoD in SAP ERP are easily circumvented with "borrowed" passwords.
- Why do governments rely on biometrics for border control, elections, financial benefits and more? It is effective!

With **Biometric** Access & Identity Management…

- SAP activities can be absolutely prevented, **or** permitted with restrictions, while creating a tamper-proof log, user by user.
- Granular control checkpoints could include:

  Log-on, opening specific menus or tables … editing specific fields … exceeding a threshold financial value … viewing, exporting, printing sensitive data and much more.

PalmSecure

Some Business Use Cases

- Diverse areas of SAP activity can be controlled, such as:

Log-on access, physical access … data privacy in HR, healthcare, customer service … prevent unauthorized access to Intellectual Property assets/BOM… regulatory compliance such as GDPR, SOX … prevent Time & Attendance, Retail POS fraud at shared devices … eliminate unauthorized financial / procurement activities … enforce Segregation of Duties and GRC policies… and more…

valantic SAP Gold Partner FUJITSU SAP Global Partner