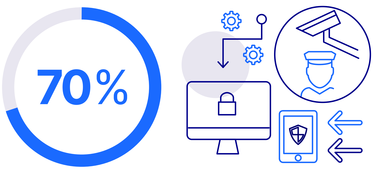
opentext™

# The Internet of Things has an Identity problem

The massive growth of Internet of Things (IoT) devices is placing significantly increased focus on identity management. Organizations need a fresh approach to managing identity that encompasses all network entities applications, systems, devices and things.

## IoT devices–The weakest link?

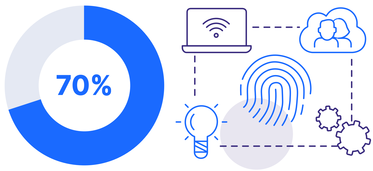



Approximately **70%** of all IoT devices have security vulnerabilities.[1]

## Can you afford a security breach?

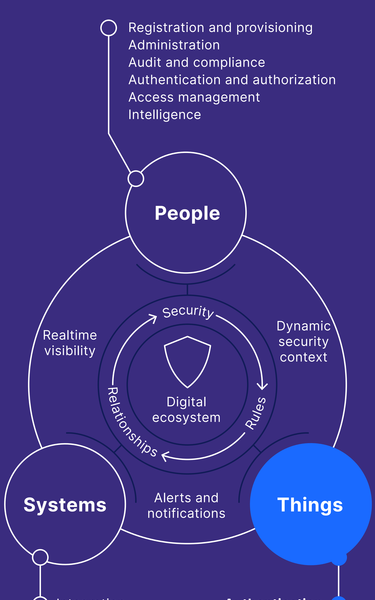

**$3.86** MM US is the average cost of a data breach.[2]

## The need for an identity-centric IoT platform




By 2023, IoT implementers will have to rearchitect their security solutions because **70%** of current providers will have rebranded, repositioned, been bought, or disappeared.[3]

## Why do IoT devices need digital identities?




75% of companies list security as their chief consideration when selecting connectivity for IoT projects.[4]

70% of IAM customers will require IDoT capabilities to support their RPA and IoT deployments up from less than 20% today.[5]

**Learn how disruptive technologies can support next-generation digital supply chain transformation today to stay ahead tomorrow.**

[1] OpenText, How IoT enables an Intelligent and Connected Supply Chain, 2018.

[2] Ponemon Institute, 2018 Cost of a Data Breach Study: Benchmark Research sponsored by IBM Security, independently conducted by Ponemon Institute, LLC, July 2018.

[3] Gartner, Predicts 2020: As IoT Use Proliferates, So Do Signs of Its Increasing Maturity and Growing Pains, December 2019

[4] Vodafone, Vodafone IoT barometer 2017/18, 2018.

[5] Gartner, The Future of IAM, 2018)