

# PROTECTING BIG DATA IN MOTION

Big Data describes the exponential growth in the collection, sharing, analytics and storage of multi-source information. In essence, it gives meaning to the seemingly random.

The richness of Big Data makes it appealing to cyber criminals, who are using ever-more sophisticated techniques to breach organisations and either manipulate this information or steal it, often for fraudulent use.



## BIG DATA IN NUMBERS

### 1.7MB

THE AMOUNT OF DATA CREATED BY EACH PERSON, EVERY SECOND, BY 2020<sup>2</sup>.

### 3m GB

THE AMOUNT OF DATA THE INTERNET RECEIVES EVERY MINUTE<sup>1</sup>.

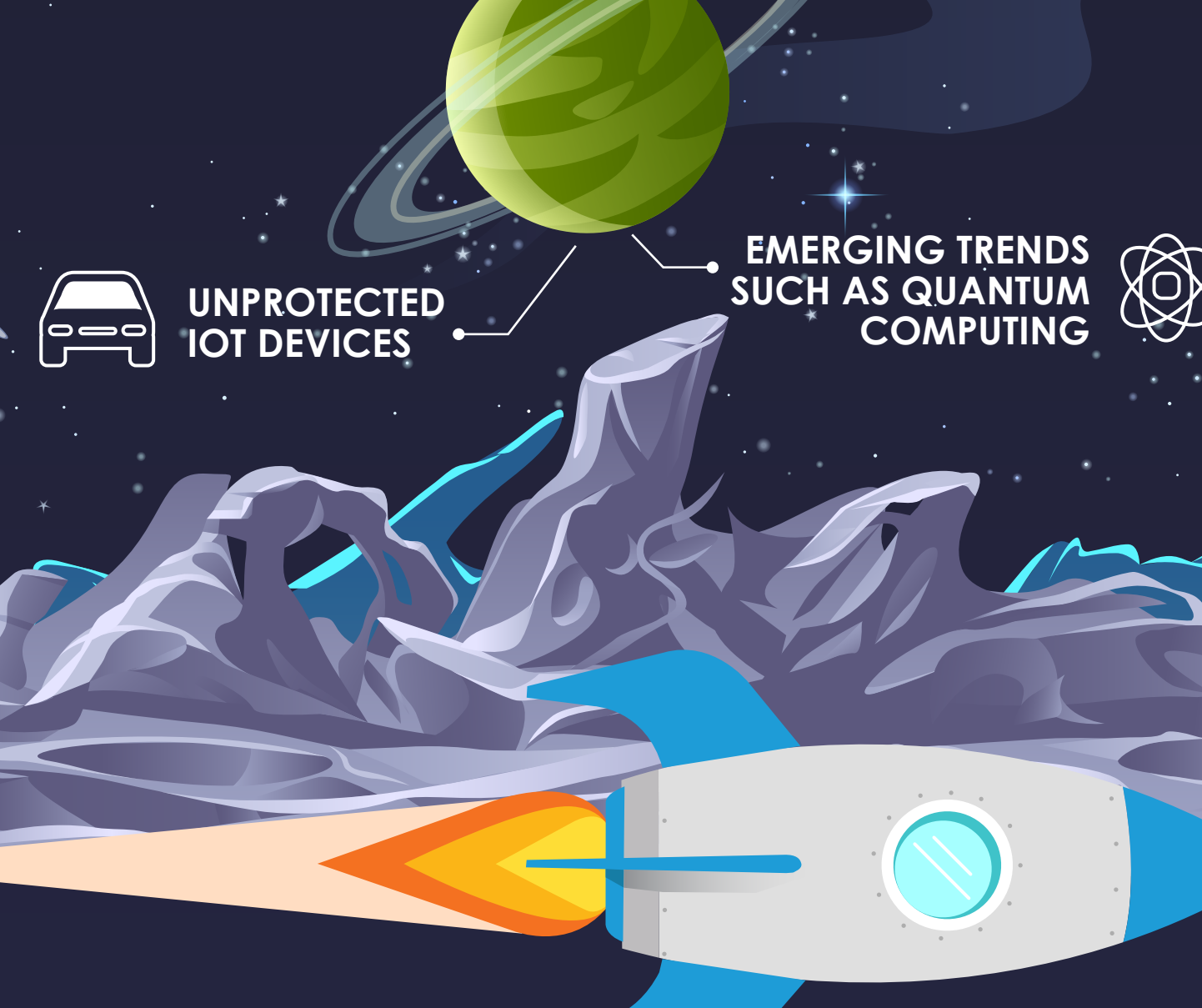
### > 20bn

THE NUMBER OF DEVICES CONNECTED BY THE IOT BY 2020<sup>4</sup>.

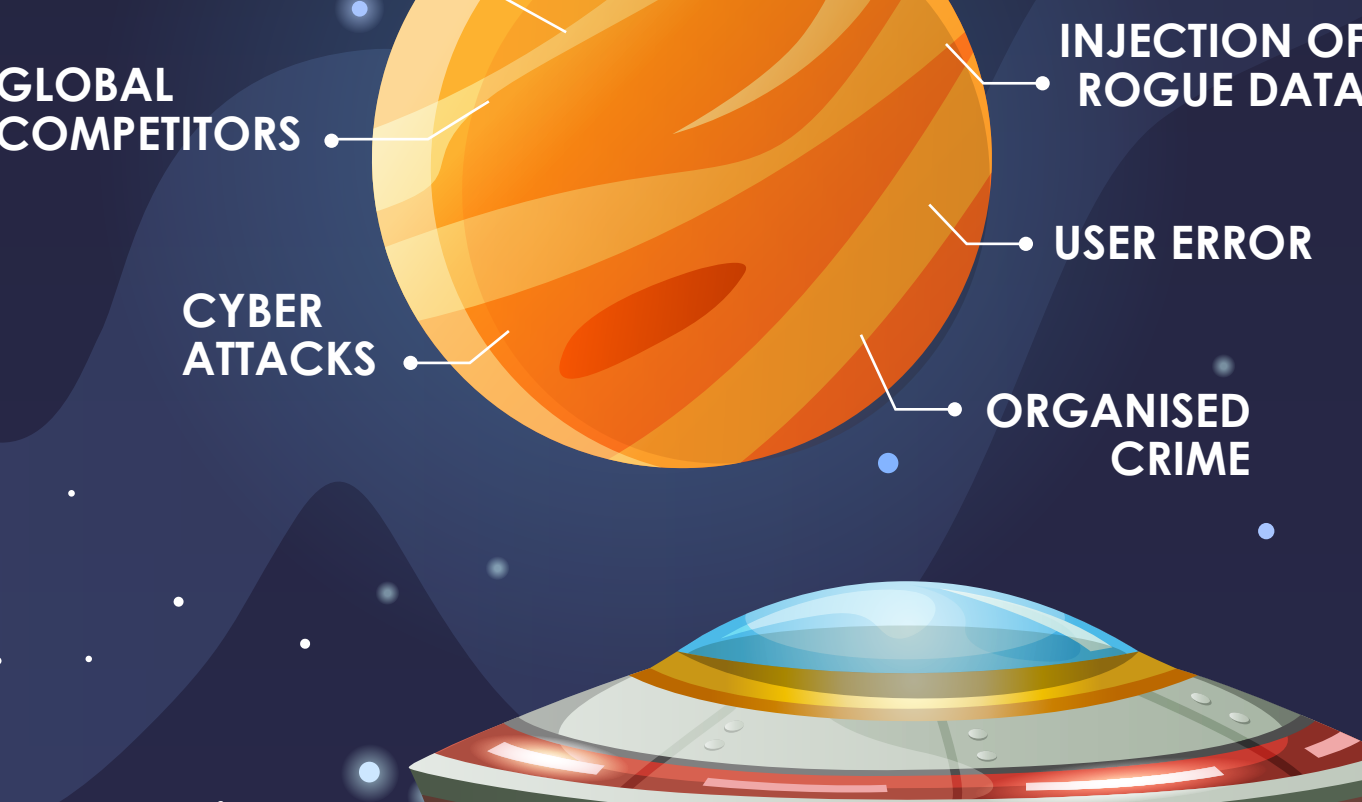
### 175ZB

THE PREDICTED GLOBAL VOLUME OF DATA BY 2025<sup>3</sup>.

## RISK FACTORS

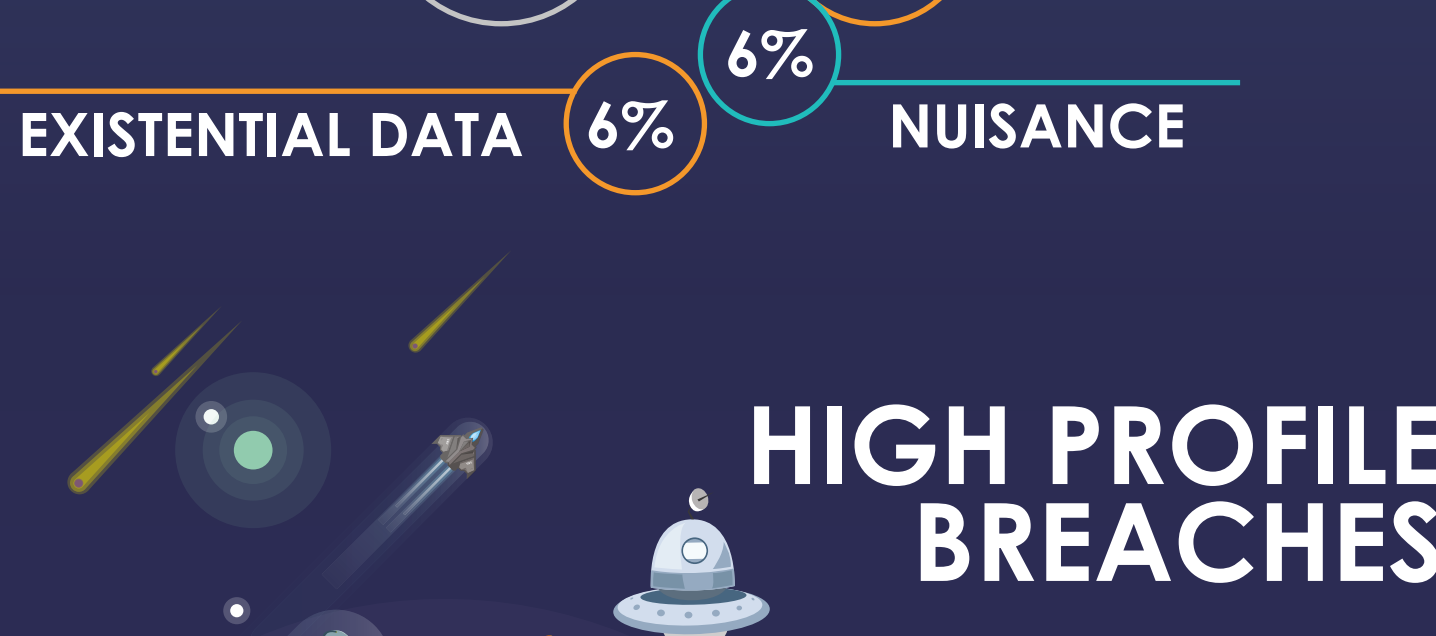


## THE THREAT LANDSCAPE



## TYPES OF BREACH

Over **13bn** records have been lost or stolen since 2013, with data encrypted & rendered useless in just **4%** of breaches<sup>5</sup>.



## HIGH PROFILE BREACHES

### MARRIOTT HOTELS

The personal information, including credit card details & passport information, of all Starwood Hotels customers dating back to 2014 was stolen.

### 500M

### LOCALBOX

Data from multiple sources – including data scraped from social media platforms – was stolen after a cloud storage repository was left publicly available.

### 48M

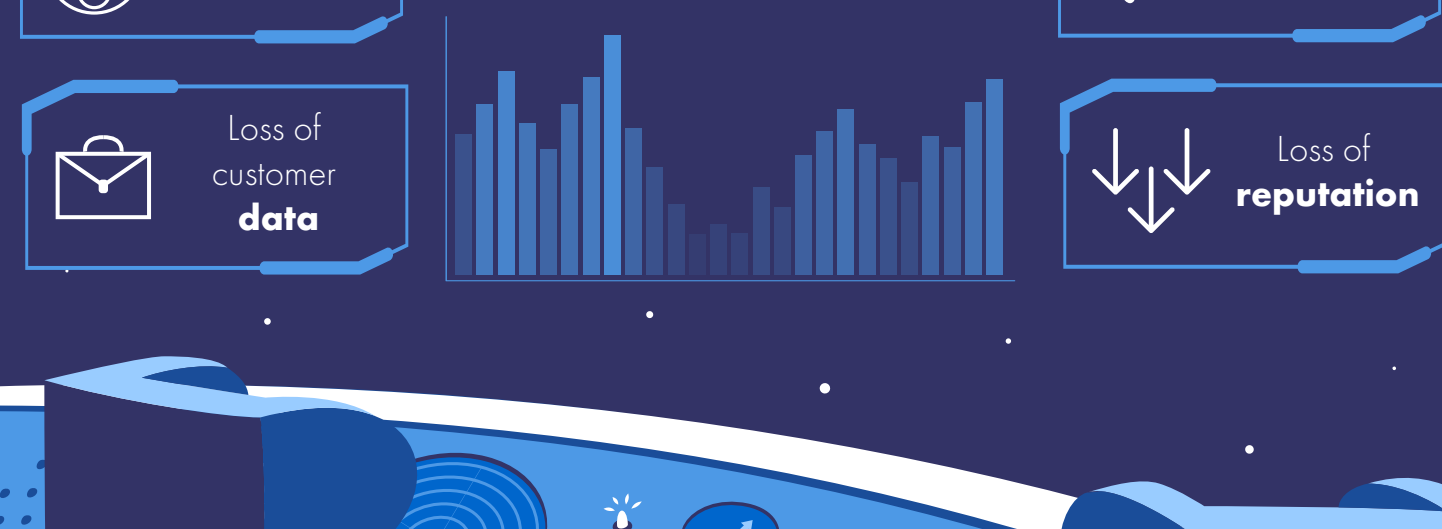
### EQUIFAX

Sensitive information from a number of sources, including names, social security numbers & driver's license details, was stolen from one of America's most prominent credit rating agencies.

### 143M

## CONSEQUENCES OF A BREACH

On average, it takes **197 days** to identify a breach and a further **69 days** to contain it<sup>6</sup>.



## SOLUTIONS



CN SERIES

### HARDWARE ENCRYPTION

FOR CORE NETWORK & IT INFRASTRUCTURE

Multi-certified high-assurance encryption

Maximum performance without compromise

Near-zero latency and network overhead

Crypto-agile and quantum-ready

State-of-the-art encryption key management



CV SERIES

### VIRTUALISED ENCRYPTION

FOR VIRTUAL CPE & VIRTUALISED WAN

Strong & effective WAN encryption

Rapid scalability across '000s of links

Flexible pricing and licensing

Transport independent multi-layer encryption

Seamless integration with SafeNet KeySecure



SUREDROP

### ENCRYPTED FILE-SHARING

AVAILABLE ON-PREMISES OR FROM THE CLOUD

100% control over data sovereignty

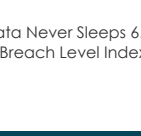
Unlimited file size and type

Standards-based encryption

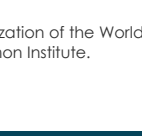
Effortless management & control

Votiro Content Disarm & Reconstruction technology

## DISCOVER MORE ABOUT SENETAS ENCRYPTION SOLUTIONS



PROTECTING BIG DATA IN MOTION



BIG DATA SOLUTION PAPER



INTRODUCING SENETAS E-BOOK

<sup>1</sup>. Domo, Data Never Sleeps 4.0. <sup>2</sup>. Domo, Data Never Sleeps 4.0. <sup>3</sup>. The Digitization of the World from Edge to Core - IDC. <sup>4</sup>. Gartner. <sup>5</sup>. Gemalto Breach Level Index. <sup>6</sup>. 2018 Cost of a Data Breach Study - Ponemon Institute.

Senetas CN Series hardware encryptors and CV Series virtual encryptors are distributed and supported internationally by Gemalto under its SafeNet brand; within the US Federal Government by SafeNet Assured Technologies, and throughout Australia and New Zealand by Senetas and accredited partners.

Senetas is a leading developer of encryption security solutions; trusted to protect enterprise, government, defence, cloud and service provider data in over 35 countries. From certified high-assurance hardware, and virtualized encryption, to secure file sharing with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.