VERTICAL | HEALTHCARE

SENETAS

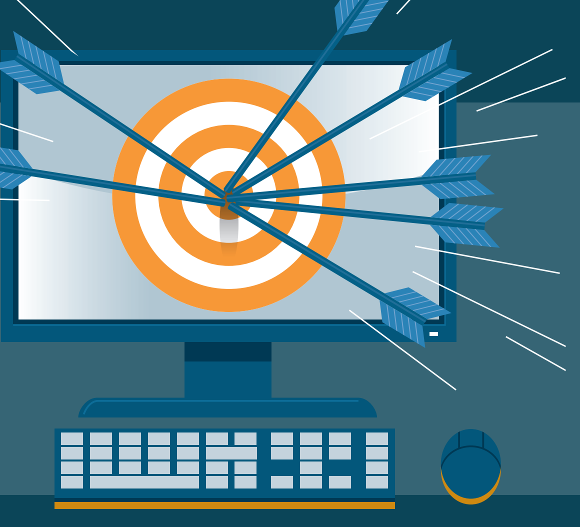
HIGH-ASSURANCE ENCRYPTION FOR HEALTHCARE NETWORK DATA

The high-speed networks used by modern healthcare organisations are becoming increasingly complex. Multiple devices and links feature across a variety of network technologies, protocols and topologies. With this complexity comes risk.

DATA BREACH LANDSCAPE

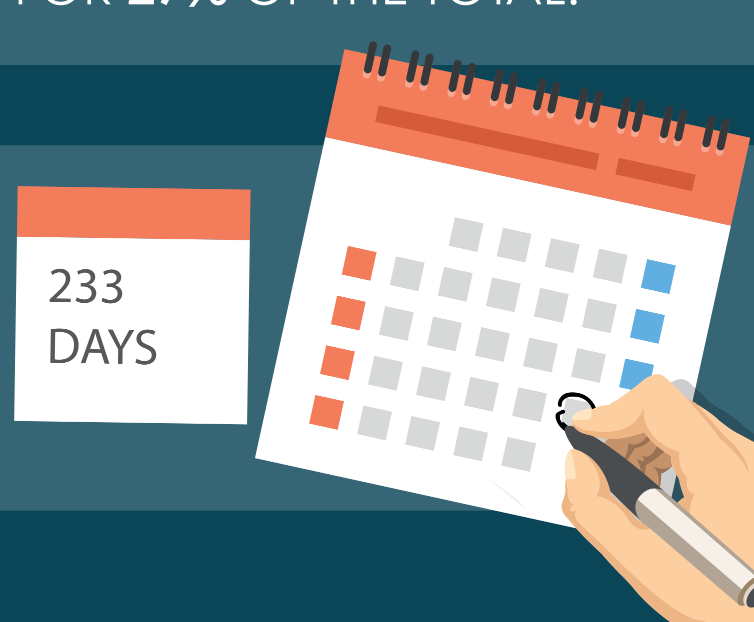
SINCE 2013, **245,233,384** HEALTHCARE RECORDS HAVE BEEN LOST OR STOLEN

KEY STATISTICS



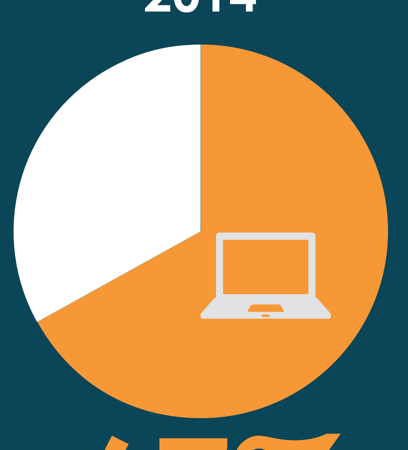
IN **2016**, HEALTHCARE LED ALL INDUSTRIES WITH A TOTAL OF **263 DATA BREACHES** ACCOUNTING FOR **27%** OF THE TOTAL.

233 DAYS
THE NUMBER OF DAYS FOR A HEALTHCARE BREACH TO BE DISCOVERED.



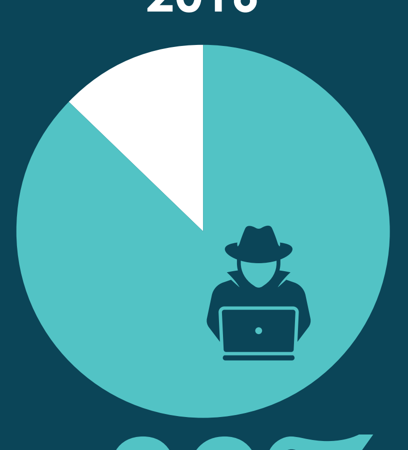
THE PRIMARY SOURCES OF A DATA BREACH?

2014



67%
WERE LOST OR STOLEN DEVICES

2016



82%
WERE LARGE-SCALE DATA HACKS

SCOPE OF THE PROBLEM

- According to the Ponemon Institute, **90%** of healthcare organisations have suffered a data breach in the last two years. The average cost of a data breach is **US$2.2m**.
- At least **1 data breach per day** was averaged during 2016.

THE COST OF A DATA BREACH

THE AVERAGE COST PER LOST OR STOLEN HEALTHCARE RECORD (GLOBALLY) IS **US$355**.

The costs associated with a data breach could be felt directly, or indirectly by the breached organisation and include:

- BUSINESS DISRUPTION
- FINANCIAL PENALTIES
- LOSS OF PRIVACY
- RISK TO PATIENT WELLBEING
- LOSS OF REPUTATION
- COMPLIANCE FAILURE
- CRIMINAL PROSECUTION

NOTABLE HEALTHCARE BREACHES

2016 was a notable year for healthcare data breaches. Although the US was the victim of most attacks, the UK, Australia and India were hit multiple times.

ANTHEM
State-sponsored attack in which **80m** records were stolen

PREMERA
US healthcare provider loses **11m** patient records that could include DOB, social security, bank account and clinical records

MUTUELLE GÉNÉRALE DE LA POLICE
112k health insurance records stolen

BANNER HEALTH
3.7m customers' payment card details compromised via food outlets

RED CROSS BLOOD SERVICE
550k records leaked which showed details of "at risk sexual behaviour"

QUEST DIAGNOSTICS
A data breach resulting in **34 000** records stolen, including names, telephone numbers, DOBs and test results.

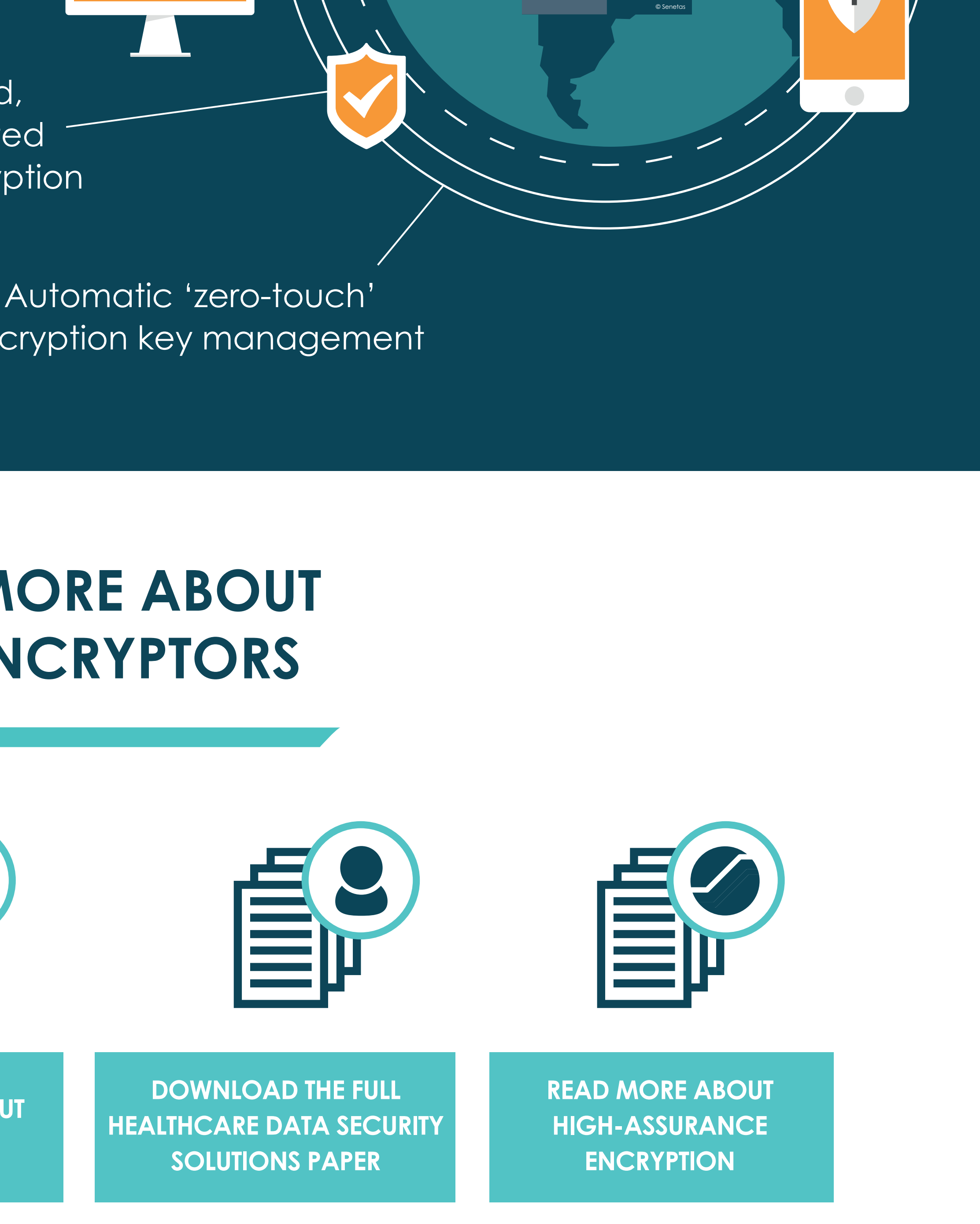
NHS
239 data security incidents reported between June – October 2016.

BLUE CROSS / BLUE SHIELD
US medical insurer has **1.1m** policy holder records hacked

WHAT IS HIGH-ASSURANCE?

Not all encryption solutions are the same. The critical nature of healthcare networks (and the data they carry) requires a robust encryption solution that provides certified, high-assurance network security and maximum network and application performance; without compromise.

Senetas high-assurance Metro Area and Carrier Ethernet encryptors include the security assurance of certification by leading independent testing authorities and feature the following essential attributes:



DISCOVER MORE ABOUT CN SERIES ENCRYPTORS

DISCOVER MORE ABOUT CN ENCRYPTORS | DOWNLOAD THE FULL HEALTHCARE DATA SECURITY SOLUTIONS PAPER | READ MORE ABOUT HIGH-ASSURANCE ENCRYPTION

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.

Europe, Middle East & Africa	T: +44 (0)1256 345 599	E: info@senetas-europe.com
Australia and New Zealand	T: +61(03) 9868 4555	E: infoanz@senetas.com
North and Central America	T: +1 949 436 0509	E: infousa@senetas.com
Asia Pacific Region	T: +65 8307 3540	E: infoasia@senetas.com

SENETAS

HEALTH-GR0718