

From Edge to the Core.

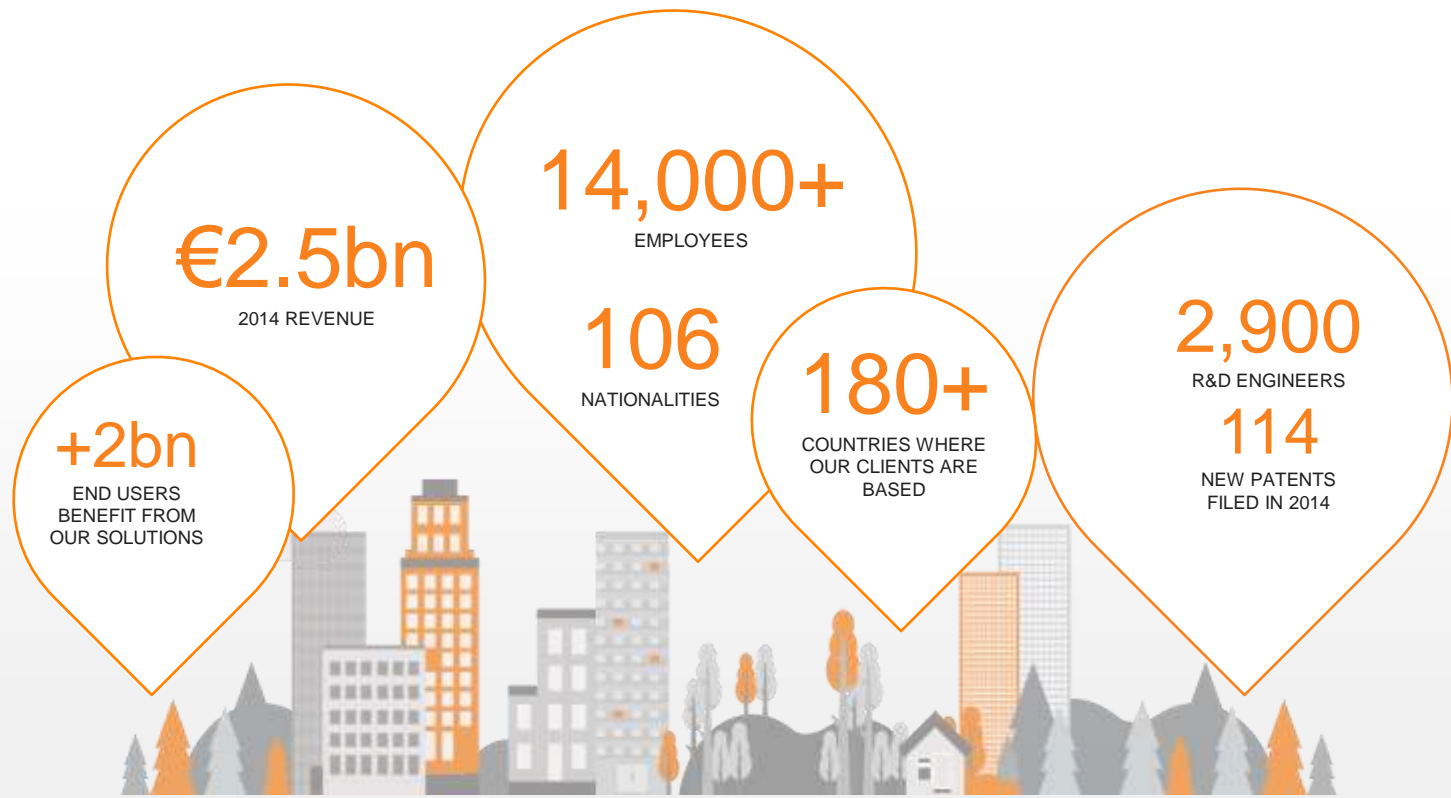
**Sicurezza dati nelle infrastrutture
condivise, virtualizzate e cloud.**



Claudio Olati
Sales Manager - Gemalto

Sergio Sironi
Regional Sales Manager - Safenet

We are the **world leader** in digital security



THE NEW GEMALTO.

WE'RE UNIQUE. **WE'RE GLOBAL.** WE'RE INNOVATIVE

We secure and manage the entire trust chain

Ensuring strong identities and securing data from the edge to the core



Our **seamless chain** of software, products, platforms and services



We enable our clients to deliver a vast range of services



Our clients are some of the world's big brands



We help people **enjoy their digital lives**

Billions of people can communicate, travel, shop, bank, work and play because they know their unique identities are secure



We bring **global expertise** to local needs



Gemalto - The Edge



Gartner Magic Quadrant: User Authentication 2014



- The **most highly ranked** vendor
- Considered the **most visionary**
- Cited for the **best execution**
- Recognized as having:
 - Very sound market understanding
 - Very strong product strategy
 - Innovation
- The competitor **others need to beat!**

Ezio Platform



Ezio Signer

The ultra-thin signing token.



- ✘ High end-user acceptance
 - ✘ Ultra-thin and compact form factor
 - ✘ Intuitive use
- ✘ Future proof
 - ✘ Scalable security
- ✘ Brand vector
 - ✘ Fully customizable to reflect the bank's image
- ✘ Easy deployment
 - ✘ No customer installation
 - ✘ Experience from worldwide fulfillments



**The Mobile Experience
Banche e Sicurezza 2015**

EZIO MOBILE

RELY ON EXISTING PROVEN SECURITY TECHNOLOGY AND “MOBILIZE” IT

Token and Readers proved to be efficient Two Factor Authentication (2FA) devices to secure eBanking operations



Use the same 2FA technology to turn mobile into a security device



Token application provides UI with keyboard and display



Token application can be integrated/extended to an mBanking application

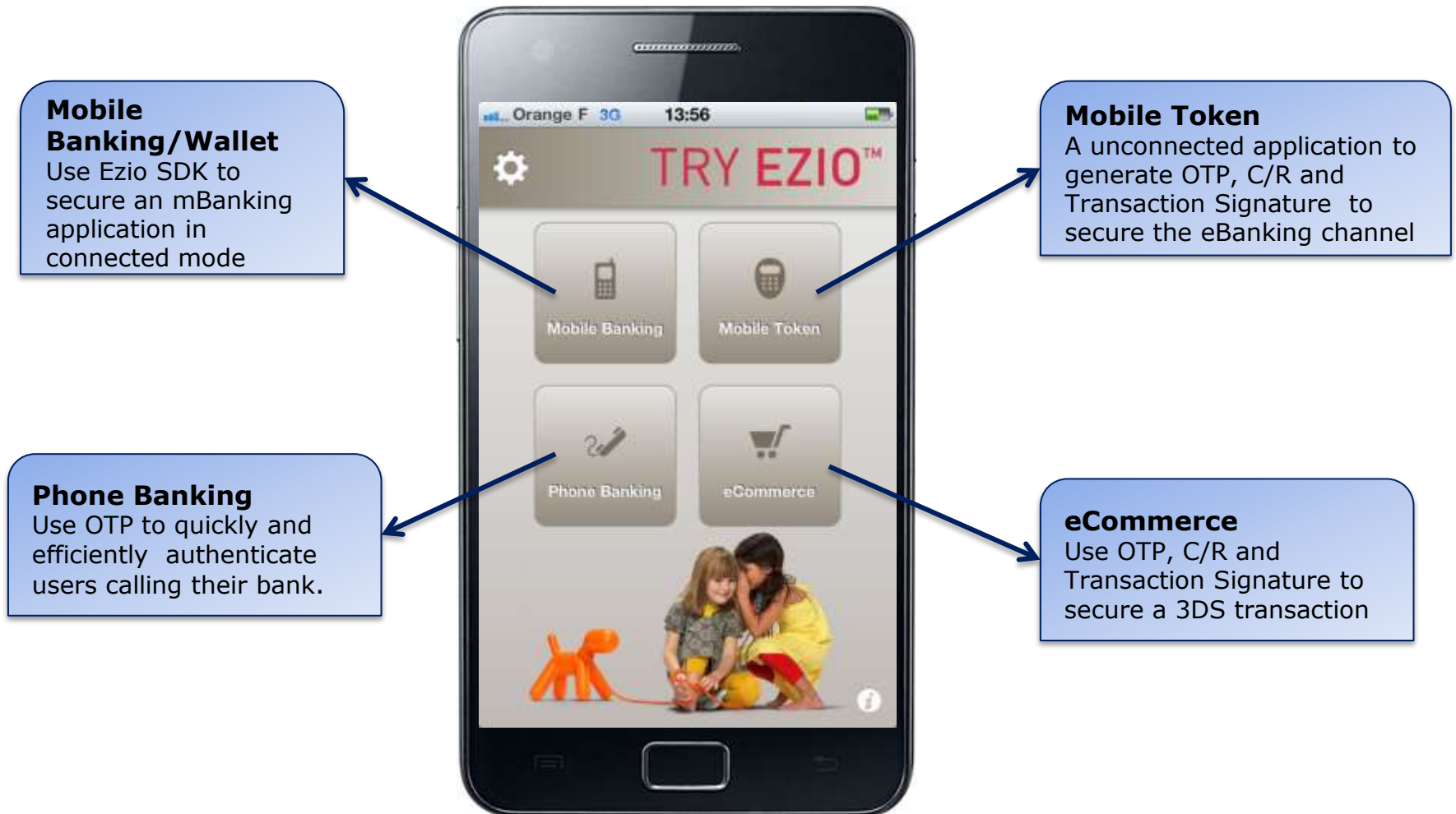


Ezio Mobile SDK

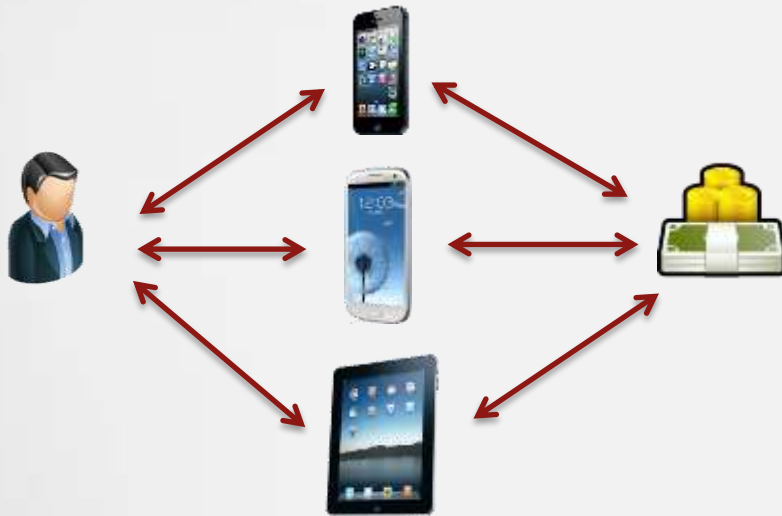


Keys and cryptographic operations are performed in a secured SW or HW container

Ezio Mobile SDK can be used to secure different channels

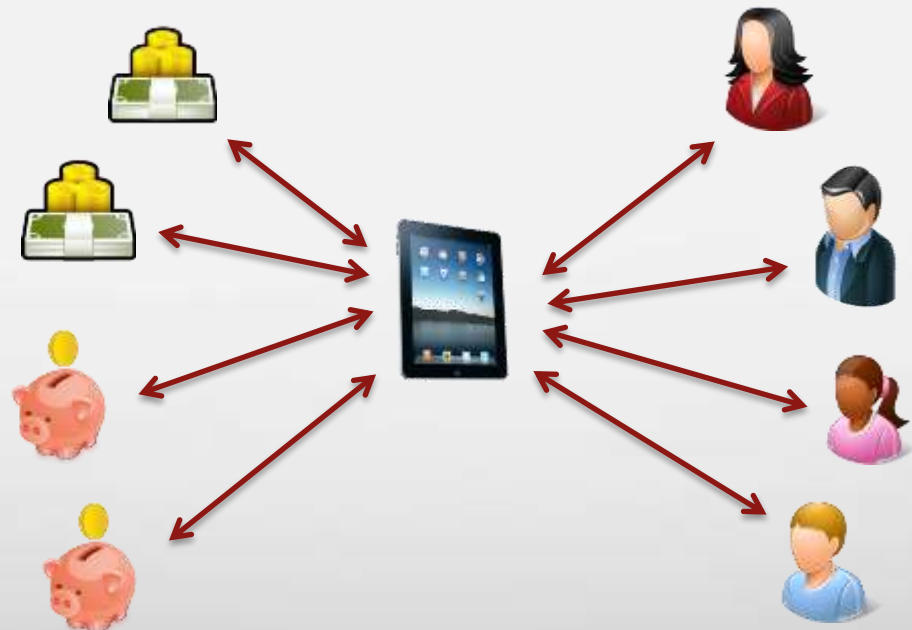


Multi Devices and multi Users



One user can hold several devices linked to the same bank account. Each device requires to go through the enrolment process to not duplicate the keys.

Each member of the family can share the same device but without sharing the credentials
Each user credential is stored in a separate secured container.

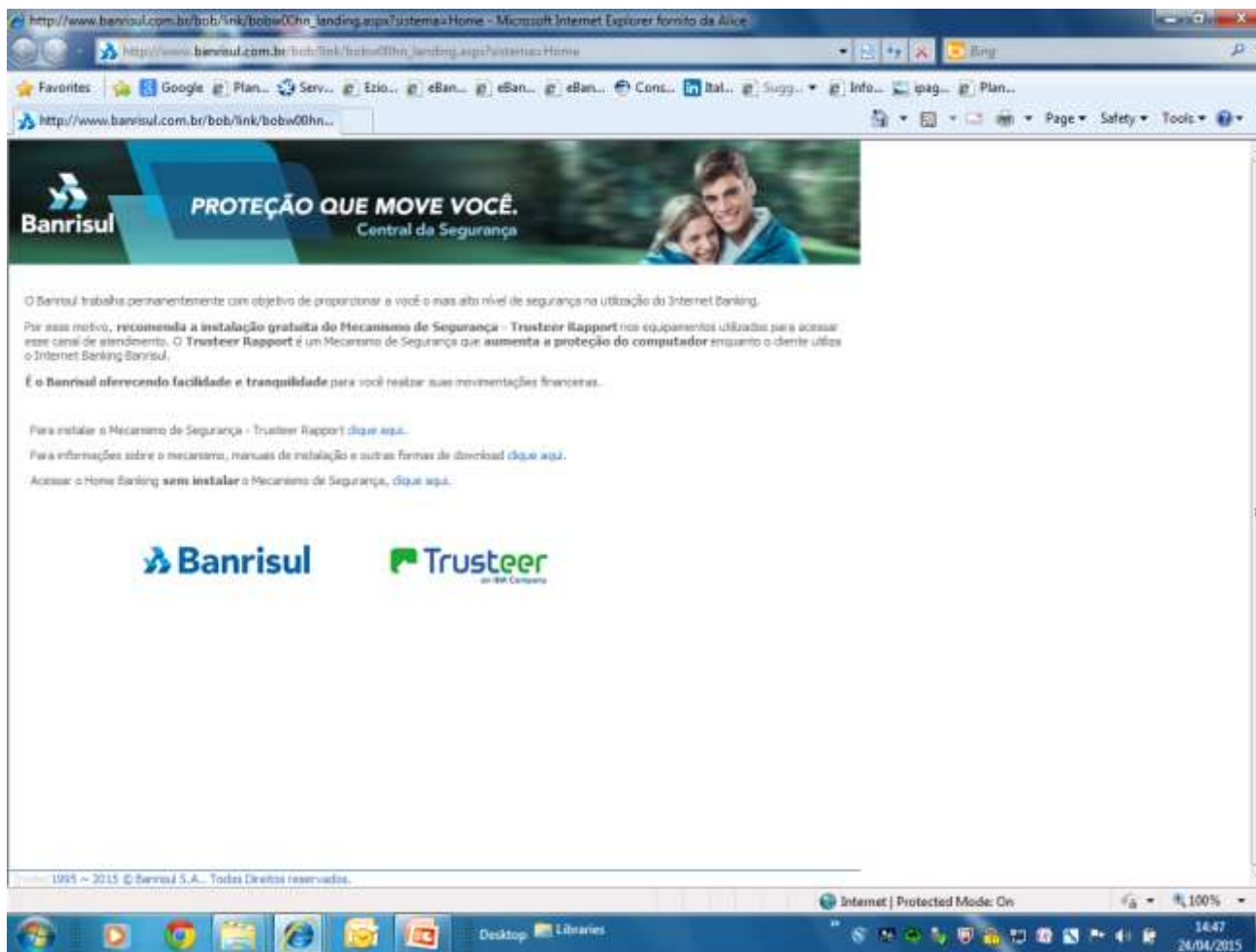


Banrisul – 3,9 M users



- ✦ Banrisul is a leading financial institution in Brazil and will enable all of its 3.9 million customers to perform secure banking transactions using their smartphone or tablet with the highly versatile Ezio platform.
- ✦ Gemalto [Ezio Authentication Server](#) provides back-end authentication to secure Banrisul's online and mobile banking operations.
- ✦ The Mobile Token app implements leading security standards and is now integrated into the Banrisul mBanking solution. It generates One-Time Passwords (OTP) and transaction signatures.
- ✦ According to the Brazilian Banking Federation, mobile banking experienced exponential growth of 184% in 2013 boosted by the wide use of smartphones in all social classes. The number of Internet and mobile banking transactions has already surpassed those facilitated in bank branches, ATMs and contact centers combined.

Banrisul- La Protezione mobile



The screenshot shows a Microsoft Internet Explorer browser window displaying the Banrisul website. The address bar shows the URL: <http://www.banrisul.com.br/bob/link/bobw00hn...>. The page features a header with the Banrisul logo and the text "PROTEÇÃO QUE MOVE VOCÊ. Central da Segurança" next to a photo of a smiling couple. Below the header, there is a paragraph of text in Portuguese:

O Banrisul trabalha permanentemente com o objetivo de proporcionar a você o mais alto nível de segurança na utilização do Internet Banking.

Por esse motivo, **recomenda a instalação gratuita do Mecanismo de Segurança - Trusteer Rapport** nos equipamentos utilizados para acessar esse canal de atendimento. O **Trusteer Rapport** é um Mecanismo de Segurança que **aumenta a proteção do computador** enquanto o cliente utiliza o Internet Banking Banrisul.

É o Banrisul oferecendo **facilidade e tranquilidade** para você realizar suas movimentações financeiras.

Para instalar o Mecanismo de Segurança - Trusteer Rapport [clique aqui](#).

Para informações sobre o mecanismo, manuais de instalação e outras formas de download [clique aqui](#).

Acessar o Home Banking **sem instalar** o Mecanismo de Segurança, [clique aqui](#).

At the bottom of the page, there are logos for Banrisul and Trusteer Rapport. The footer contains the text: "1995 ~ 2015 © Banrisul S.A.. Todos Direitos reservados." The Windows taskbar at the bottom shows the system tray with the date 26/04/2015 and time 14:47.

EZIO Dynamic Fraud Manager



What it does



- ✘ Analyzes in real-time user transaction, behavior & device ID (with 3rd party solutions)
- ✘ Defines a risk score based on bank's rules and above data
- ✘ Triggers post scoring scenario
 - ✘ Approve
 - ✘ Reject
 - ✘ Request a step up authentication
 - ✘ Transfer request to Case Management

Capabilities



- ✦ Easily configurable rules
- ✦ Real-time transaction monitoring and fraud prevention
- ✦ Transaction-level monitoring
- ✦ Easy integration with external data sources
- ✦ Open system providing user feedback on scoring decisions and analysis
- ✦ Performance metrics
- ✦ Versatile authentication server
- ✦ Adapt authentication to customer profile and risk level of the transaction
- ✦ Field-proven solution
- ✦ Large portfolio of hardware and software devices

SafeNet - The Core



What CAN happen if you go weak ...

www.theregister.co.uk/2013/02/11/bit9_hack/ bit9 hacked

Whitepapers | The Channel

The Register®

Biting the hand that feeds IT

Data Centre Software Networks Security Policy Business Hardware Science Bootnotes Columnists Video Forum Search »

SECURITY

Bit9 hacked after it forgot to install ITS OWN security product

Malware signed by stolen crypto certs then flung at big-cheese clients

By John Leyden, 11 Feb 2013

11 IT security biz Bit9's private digital certificates were copied by hackers and used to cryptographically sign malware to infect the company's customers.

RELATED STORIES

Securo-boffins link HIRED GUN hackers to Aurora, Bit9 megahacks

Infosec 2013
Video: evaluate

The software-whitelisting firm's certificates were swiped when its core systems were hacked last week. The intruders then signed malicious code and distributed it to the company's corporate clients.

A number of Bit9's customers were subsequently infected by the malware because the software was - thanks to the purloined certificates - regarded as safe by networks guarded by Bit9's technology.

MOST READ

Report: Climate change has already hit USA - and time is RUNNING OUT

Epson takes on Google Glass with wired 'augmented reality' glasses

Google buddies up with Intel for this year's big Chromebook push

How Google's Android Silver could become 'Wintel for phones'

Virtual universe in a supercomputer's pocket, spanning post-Big Bang to present day

SPOTLIGHT

64 You think this is bad, wait until you see the queues for the sandwiches

10 Web cesspit 4chan touts '\$20 bug bounty' after

Titsup UK Border IT causes CHAOS at air and seaports in



Networks are Insecure...

End Users Want Privacy!



PC NEWS / OPINIONS / FEATURES / DEALS / HOW-TO / BUSINESS / SUBSCRIBE

ALL REVIEWS ▾ LAPTOPS / TABLETS / PHONES / APPS / SOFTWARE / SECURITY /

IBM SVC - SAN

Home / Reviews / Software / Security / Obama Moves to Overhaul NSA Phone Metadata Collection

Obama Moves to Overhaul NSA Phone Metadata Collection

BY CHLOE ALBANESIU MARCH 28, 2014 06:05PM EST COMMENTS

Phone metadata would remain with the phone providers rather than in vast government data centers.



BBC News Sport Weather

NEWS BUSINESS

Home UK Africa Asia Europe Latin America Mid-East US & Canada E

Market Data Economy Entrepreneurship Business of Sport Companies

10 January 2014 Last updated at 00:05 GMT

2014: The year of encryption

By Paul Rubens
Technology reporter



theguardian

News US World Sports Comment Culture Business Money Environment

News UK news GCHQ

GCHQ taps fibre-optic cables for secret access to world's communications

Exclusive: British spy agency collects and stores vast quantities of global email messages, Facebook posts, calls, and shares them with NSA, latest documents reveal

Share 253
Tweet 198
+1 1.4k



THE WALL STREET JOURNAL. | TECH

US\$1 A WEEK

TECHNOLOGY

Tech Firms Push to Control Web's Pipes

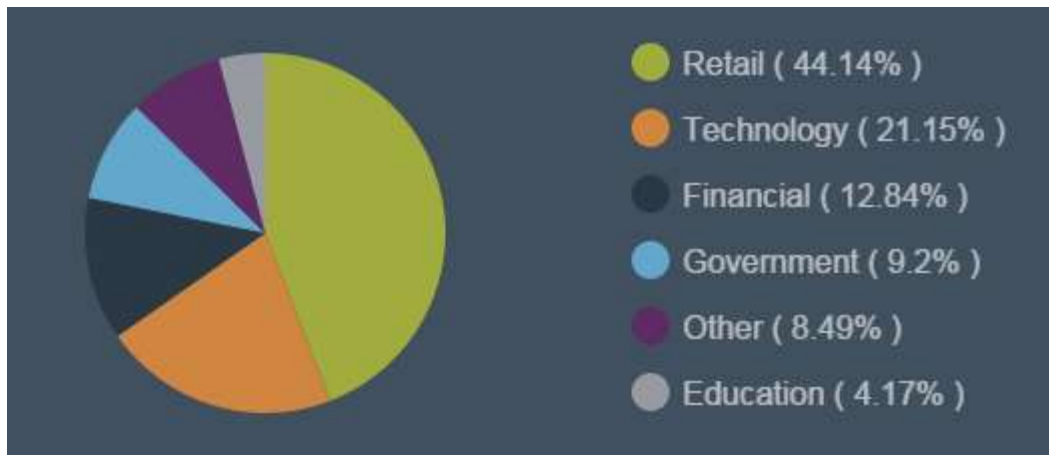
Google, Facebook Raise Tensions With Telecoms in Power Struggle for Internet's Backbone

SINCE 2013

Breach Level Index

3,023,717,864

RECORDS STOLEN



Source: <http://www.breachlevelindex.com/>

The Reality: Data Breaches

2014

1,023,108,267
RECORDS EXPOSED

... as the result of 1,541 data breaches globally

128 breaches
per month

32 breaches
per week

5 breaches
per day

>95% of all breaches involved data that was **NOT ENCRYPTED**

<http://breachlevelindex.com/>

gemalto[®]

This is driving a
fundamental **change** to the
security paradigm as we
know it today....

A New Mindset is Needed...

- 1**
Accept the Breach
Perimeter security alone is no longer enough.
- 2**
Protect What Matters, Where It Matters
Data is the new perimeter.
- 3**
Secure the Breach
Attach security to the data and applications. Insider threat is greater than ever.

Breaches will happen – we must prepare!

RBA

Biometry

Privilege management

Encryption

We must **protect**
what matters where it
matters at the edge AND at
the core

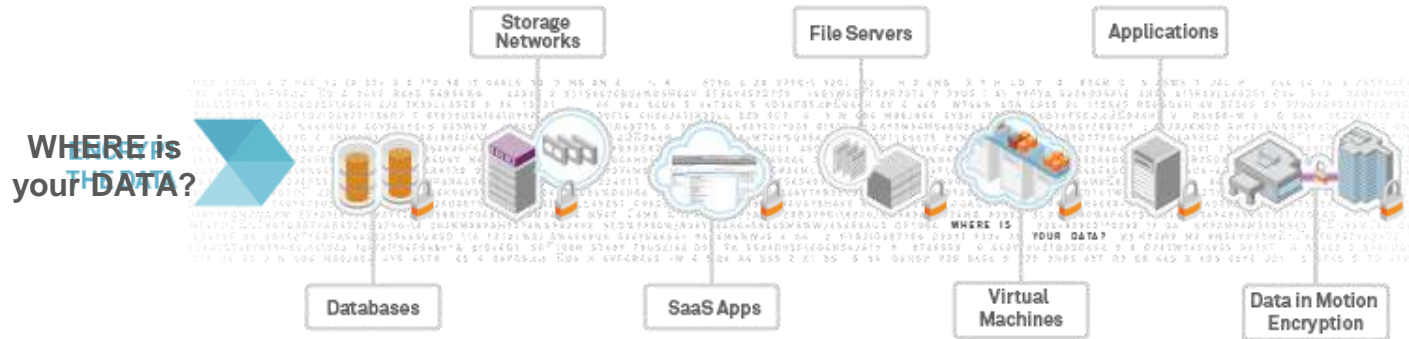
Convenience

Cloud-ready

Key Management

Contextual security

Protect What Matters, Where it Matters



Gemalto's Three Step Approach



Gemalto

3 Step Approach



Secure the Breach – Required Elements

1

Encrypt the Data

Protect the data **as it moves & where it is stored** – on-premise or in the cloud.

2

Strong Crypto Management

Manage & secure encryption keys centrally.

3

Control Access

Protect identities & ensure only authorized users have access to applications & systems.

Protecting the Data

ENCRYPT THE DATA

1

Data at Rest Encryption



Physical Data



Virtual Data



Data in the Cloud

Data in Motion Encryption



Applications

CONTROL ACCESS



SaaS Apps

3

Strong Authentication



Internal Users + Administrators

Cloud Providers Admins/Superusers

Customers + Partners

SECURE & MANAGE KEYS

2

Crypto Management



Key Manager



HSM



Crypto Provisioning System

Conclusion

- **Encryption is the essential base for protecting data and providing confidentiality**
- **Don't forget about keys: encryption is as strong and reliable as its keys are**
- **Access control assures you who can access your data**
- **Gemalto/SafeNet – The Data Protection Company**

It all starts with trust.

Thank you...

