



Security in knowledge

EVOLVING FROM BREACH PREVENTION TO BREACH ACCEPTANCE TO SECURING THE BREACH

Jason Hart CISSP CISM

VP Cloud Solutions
Safenet Inc

RSACONFERENCE
EUROPE 2013

Session ID: SP0-W10

Session Classification: General Interest



Today's issues

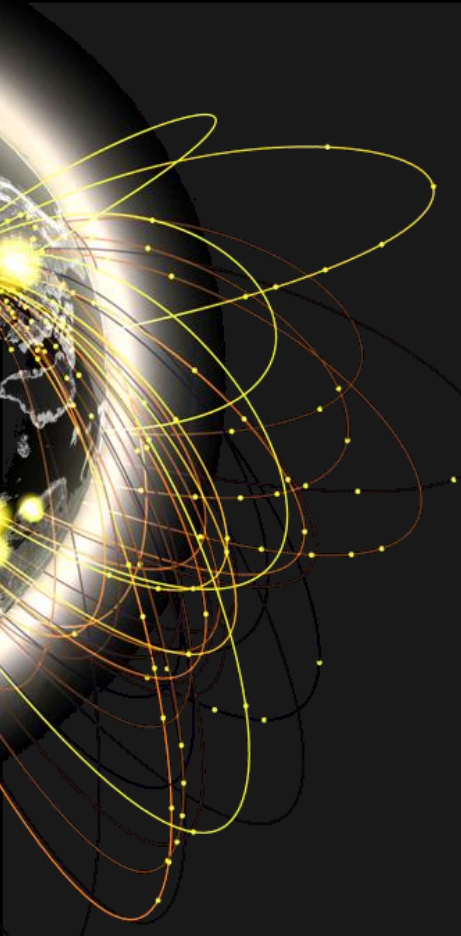
- Data breaches are rampant
- Data is moving everywhere
- The approach to protecting data must change



THE LEADING EDGE OF BIG DATA: **THEN** AND NOW



THE LEADING EDGE OF BIG DATA: THEN AND NOW



2012

IN ~~2000~~ THE WORLD GENERATED
TWO EXABYTES
OF NEW INFORMATION
EVERY DAY

Structured + Unstructured = BIG



**Structured in
Relational Databases**



**Managed, Unmanaged
& Unstructured**

Telemetry, Location-Based, etc.



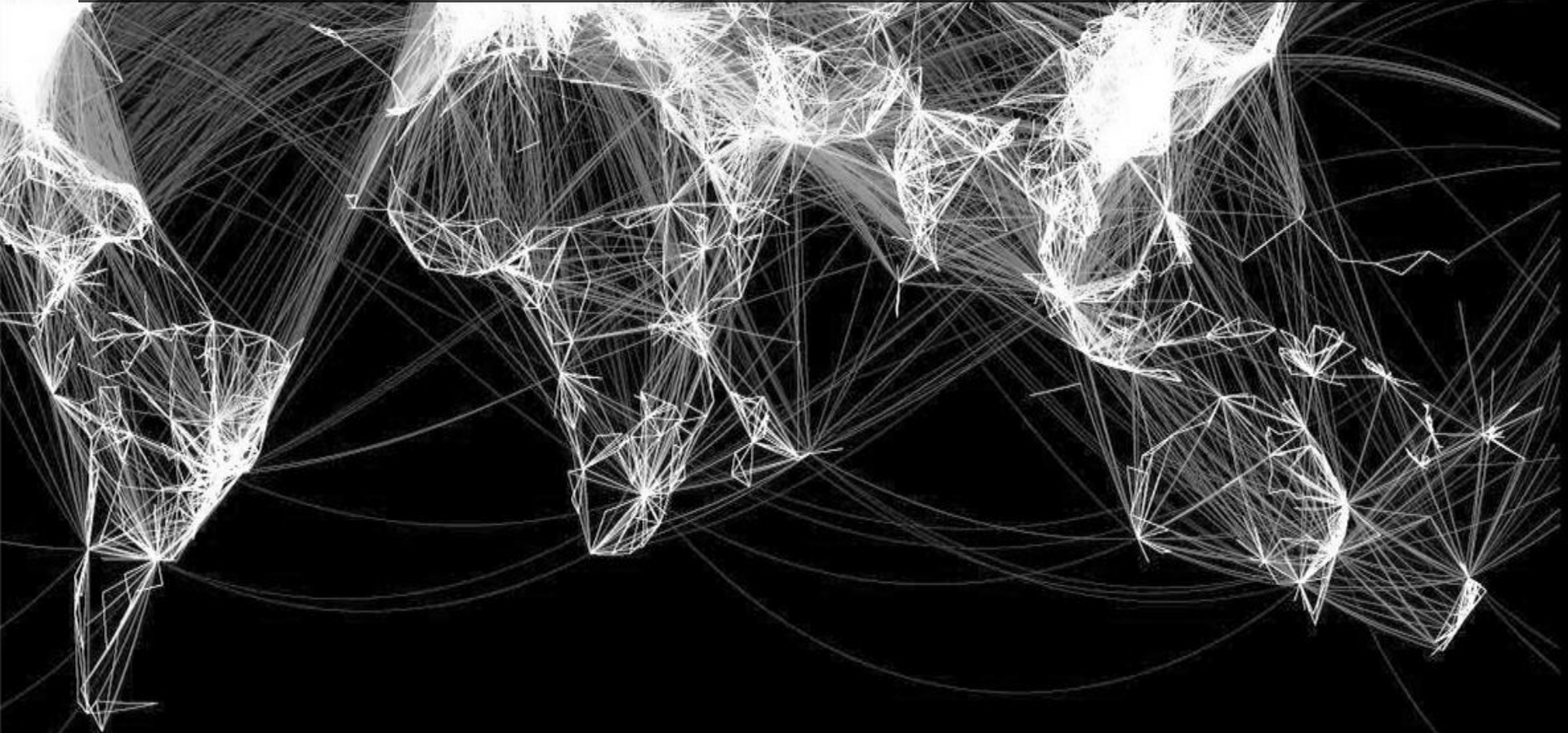
Internet of Things



Non-Enterprise

Global Flight Analysis

- 60,000 Aircraft Routes
- Sensors On Each Gas Turbine Engine = 1Tb/day



Big Data Analytics: Not New

Used Already in Many Industries

- Risk Assessment
- Price Optimization
- Monte Carlo
- Regression
- Product Recommendation



Finance



Retail



Casino



Travel



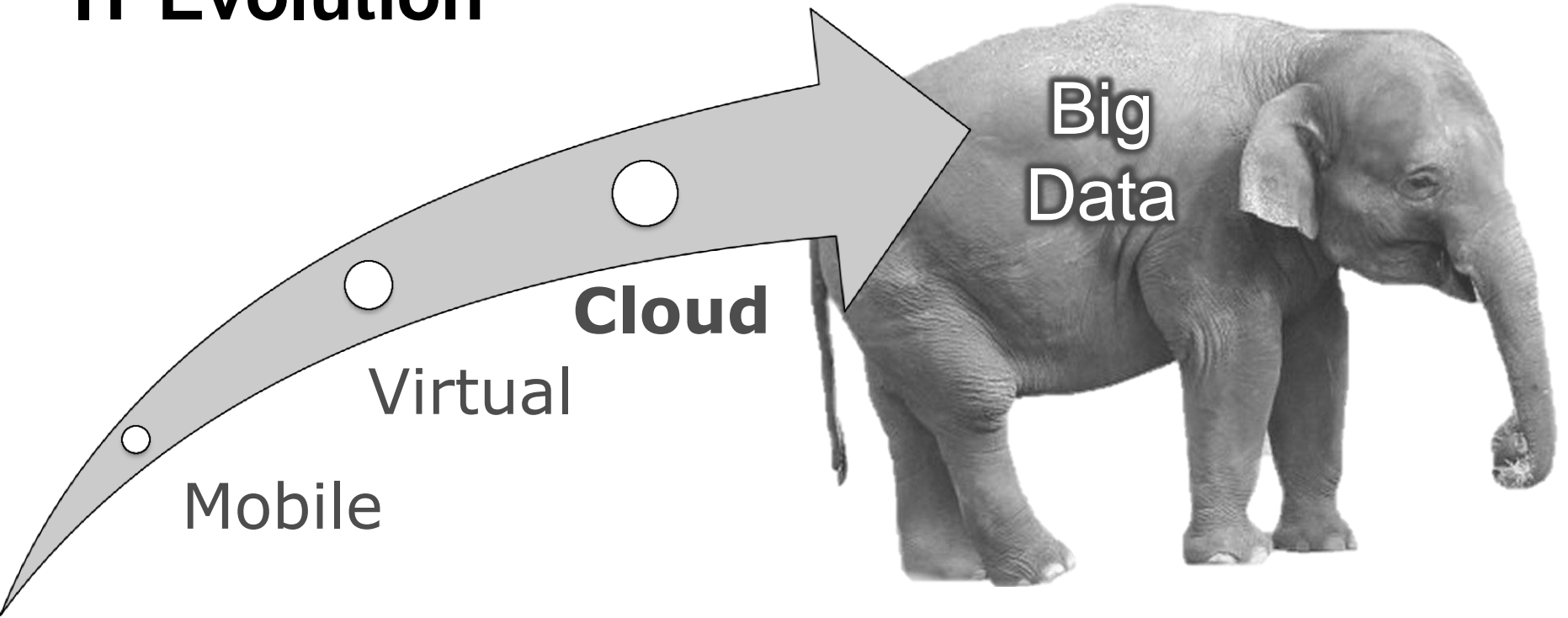
Online



Insurance

Security most keep up

IT Evolution



Your Organization's
Security Professional?



→ Protection Requires A New Approach

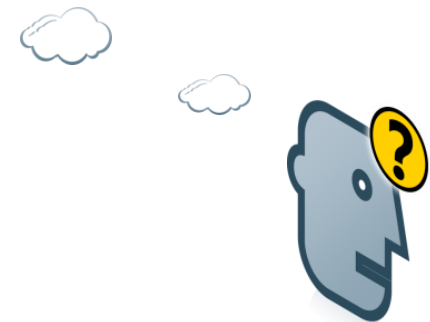


Lets Start with the Basics

- **Confidentiality**
- **Integrity**
- **Availability**
- **Accountability**
- **Auditability**



HOW DO I ACHIEVE THIS
IN A VIRTUAL WORLD?



Welcome to the next Generation

- 1st Age: Servers
 - Servers
 - FTP, Telnet, Mail, Web.
 - These were the things that consumed bytes from a bad guy
 - The hack left a foot print
- 2nd Age: Browsers:
 - Javascript, ActiveX, Java, Image Formats, DOMs
 - These are the things that are getting locked down
 - Slowly
 - Incompletely
- 3rd Age: Virtual Hacking: - **Simplest and getting easier**
 - Gaining someone's password is the skeleton key to their life and your business
 - Accessing data from the virtual world can be simple

Virtual World – With Virtual Back Doors

Welcome to the Future

- Cloud Computing
- Virtual Environment
- With Virtual Security holes

During the past 15 years with learnt nothing



Evolution of Threats

Criminals

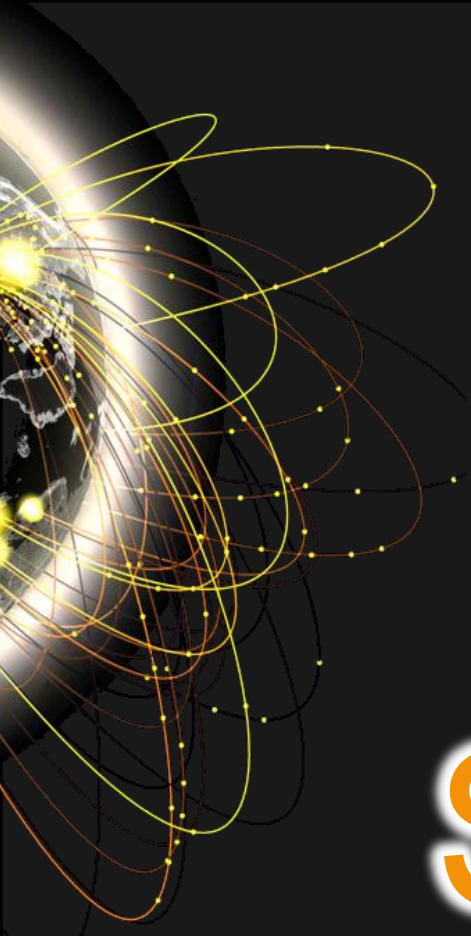


Activists



Spies





2013

SOME FACTS

**Will your organization,
or your partner, suffer
a security breach this
year?**

**Nobody's immune, no
target is too small,
or too large.**

The methods used by hackers to gain access to data are numerous, wide-reaching and ever-growing.

However Nothing Has Changed

IT'S BEST TO STICK WITH WHAT YOU KNOW

AS LONG AS WE LOCK DOWN THE
NETWORK WE'LL BE SAFE, WON'T WE?

IT'S OBVIOUS WHEN YOU'VE BEEN HACKED

IT'S EASY TO SPOT WHEN SYSTEMS
HAVE BEEN BREACHED, ISN'T IT?

The Facts



69%

69% of breaches were spotted by an external party — 9% were spotted by customers.



29%

Social tactics — using email, phone calls and social networks to gain information on individuals — are often ignored, but contributed to 29% of attacks.



76%

76% of network intrusions exploited weak or stolen credentials. Strict policies are required to reduce this easily preventable risk.

Verizon 2013 Data Breach Investigations Report

RSAC CONFERENCE
EUROPE 2013

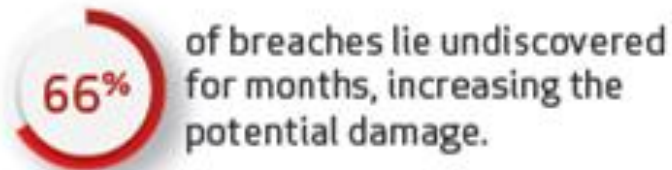


THE
DATA
PROTECTION
COMPANY

The Facts

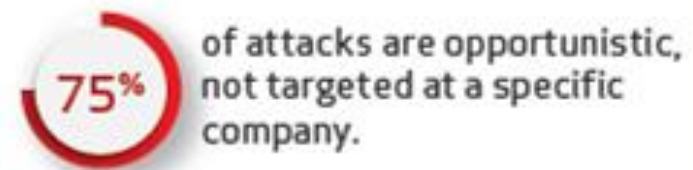
Most breaches lie undiscovered for months...

It's not really surprising that many breaches happen quickly — perpetrators driven by financial gain will often quickly move on if not successful. What's alarming is how long breaches take to spot, and how long they take to fix — during which time sensitive data remains exposed.



Hackers are interested in companies just like yours...

All kinds of organizations — from government agencies to iconic consumer brands, internet startups to trusted financial institutions — have reported major data breaches in the last year. Nobody's immune, no target is too small, or too large. It could be you next.



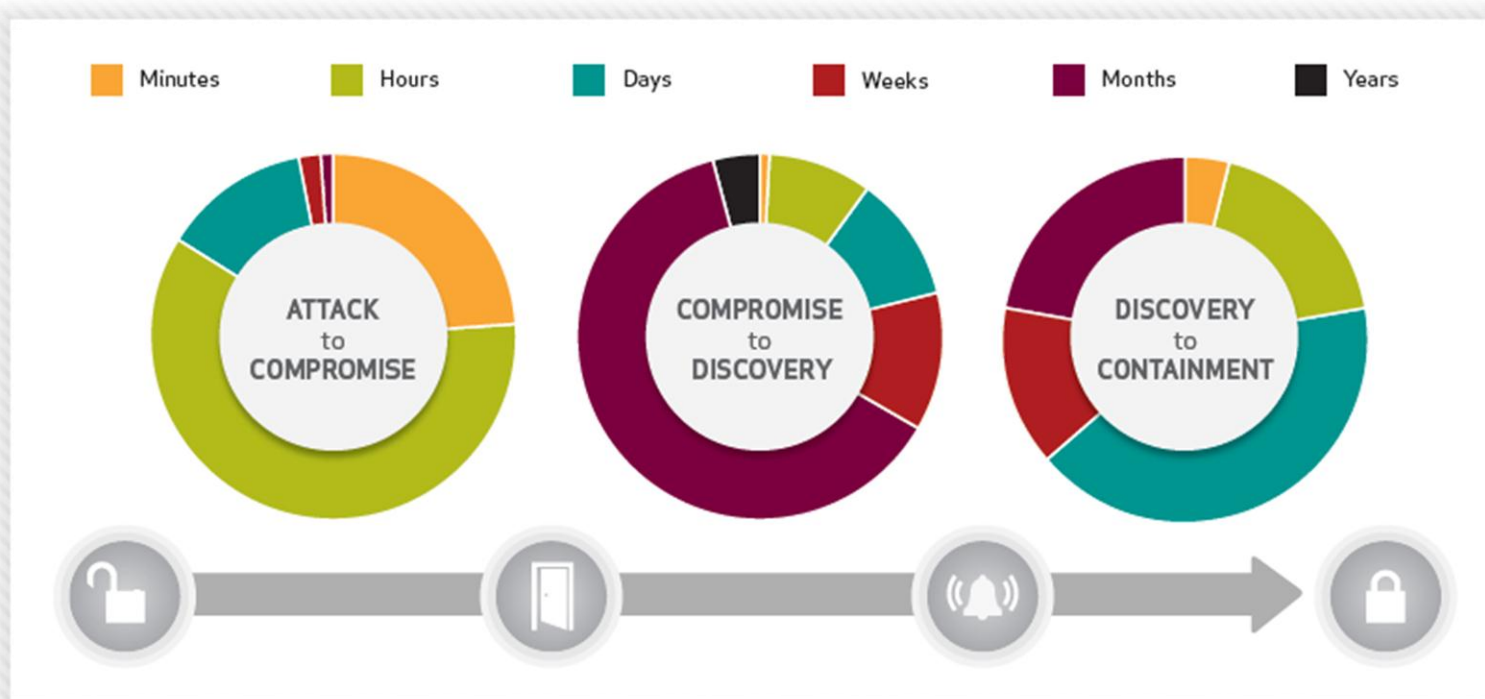
Verizon 2013 Data Breach Investigations Report

RSAC CONFERENCE
EUROPE 2013



THE
DATA
PROTECTION
COMPANY

The Facts



- In 84% of cases, the initial compromise took hours — or even less.
- In 66% of cases, the breach wasn't discovered for months — or even years.
- In 22% of cases, it took months to contain the breach.

Verizon 2013 Data Breach Investigations Report

RSACONFERENCE
EUROPE 2013

 #RSAC

 SafeNet.

THE
DATA
PROTECTION
COMPANY

The Facts



66% of the breaches in our 2013 report took months or even years to discover (62% months, 4% years).



The problem is getting worse. In the 2012 DBIR, just 56% of breaches took a month or more to be discovered.

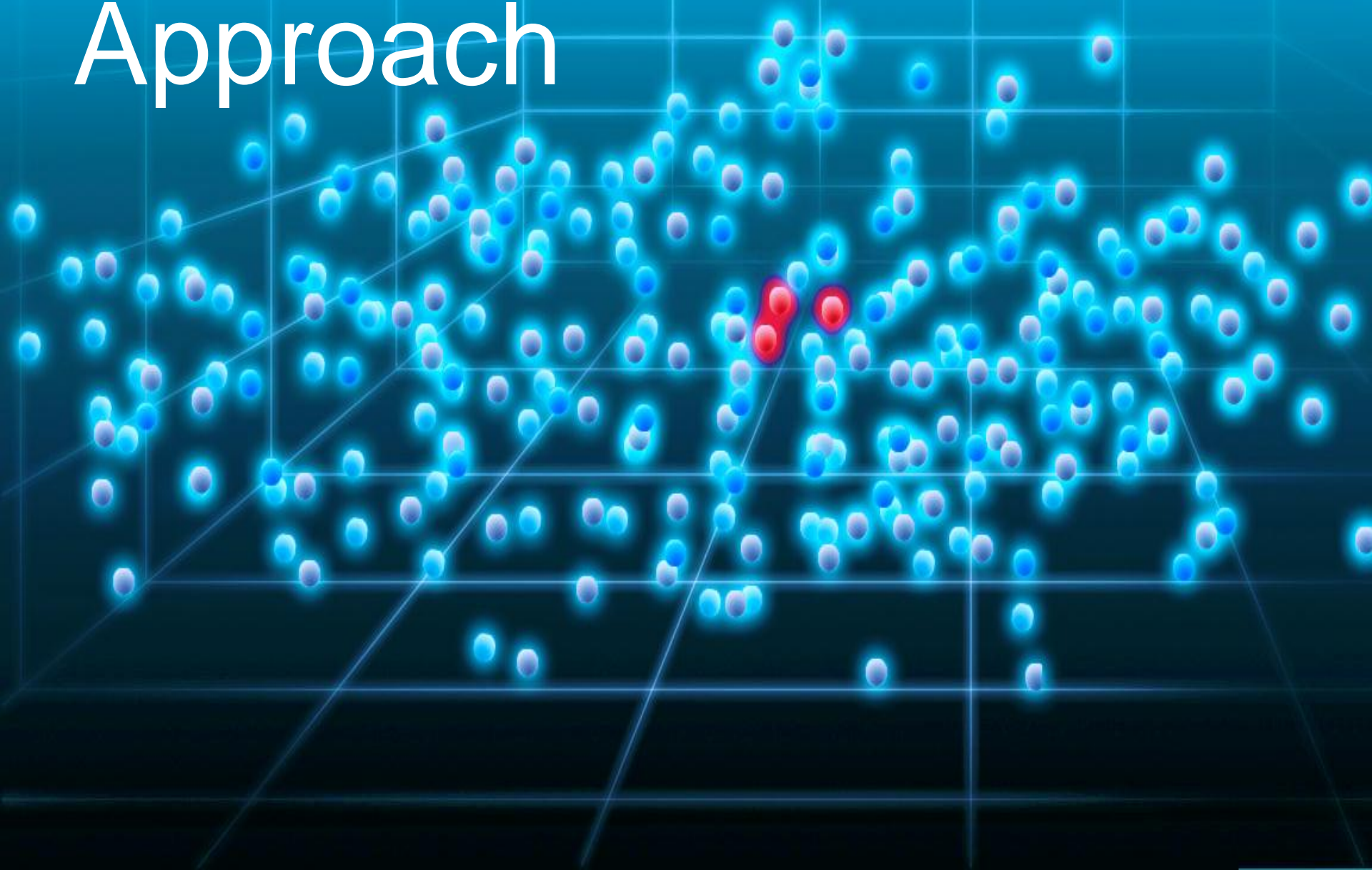
Verizon 2013 Data Breach Investigations Report

RSAC CONFERENCE
EUROPE 2013

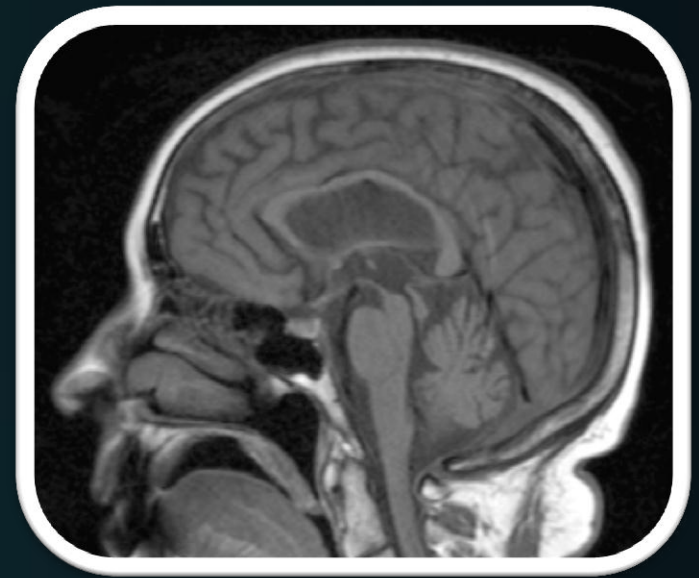


THE
DATA
PROTECTION
COMPANY

Threats Require A New Approach



**This is about you forgetting
what you know
about InfoSec**



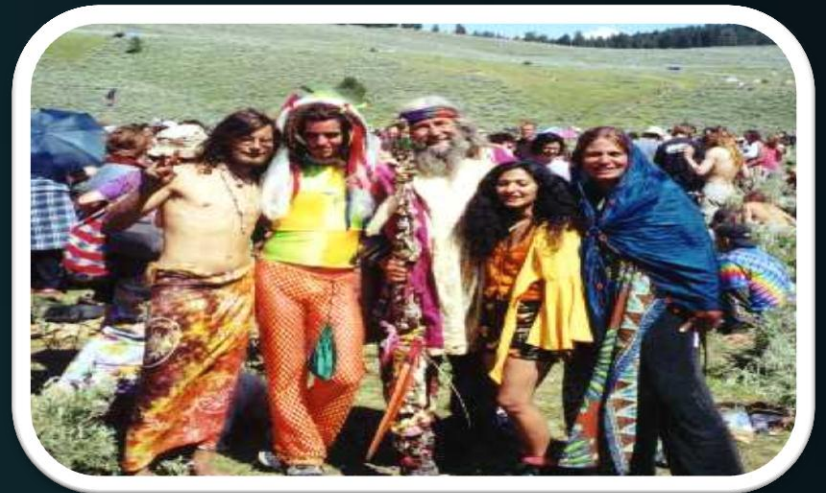
**You are still investing ~ 90% of
your budget with the same mind
set Into Network / Perimeter
defense...**



**While everything around
you has changed?**



**Just like my mother in the
60's data was born to be free
(or at least shared)**



**And the most scary
part....**

**That The Problem and the
'Solution' are out of sync...**



The new mindset ?

**Transform your mind from
Breach Prevention
To
Breach Acceptance**

Google

password ext:xls site:s3.amazonaws.com

Search

About 175 results

Finding XLS files with "password" on Amazon S3 cloud storage drives

Web

Images

Maps

Videos

News

Shopping

Blogs

More

[XLS] september links - An

<https://s3.amazonaws.com/file>

File Format: Microsoft Excel -

3, nazikilan@gmail.com, ilang

12-Sep, 18-Sep, 22-Sep, Plea

[XLS] Copy of user.xls - A

<springpad-user-data.s3.amazonaws.com>

File Format: Microsoft Excel -

1, Username, Password, Pin/

Cox, mic [redacted]@cox

[XLS] Social Networking -

<s3-media.s3.amazonaws.com>

Copy_of_user.xls [Compatibility Mode] - Microsoft Excel

File Home Insert Page L Formu Data Review View Add-It Load T Charts Ac

Arial 10 B I U A A

Font Alignment

Clipboard

C23 fx

A B C D

1 Username Password Pin/Notes

2 MUD st [redacted]@gmail.com mu [redacted]

3 Cox mi [redacted]@cox.net cox [redacted]

4 OPPD op [redacted] opp [redacted]

5 USAA ms [redacted] ms [redacted]

6 FAFSA 12c [redacted] 6 [redacted]

7 Metro mg [redacted] UIO [redacted]

8 US Bank ust [redacted] usb [redacted] 990 [redacted]

9 Black Hills gas bla [redacted] bla [redacted]

10 phone mich [redacted] spr [redacted]

11

12

13

14

Bills Forums Web Mail Reg Codes and Product Info

Username and passwords for bank accounts, email, and everything else

**Which means, assume
a breach will happen....**

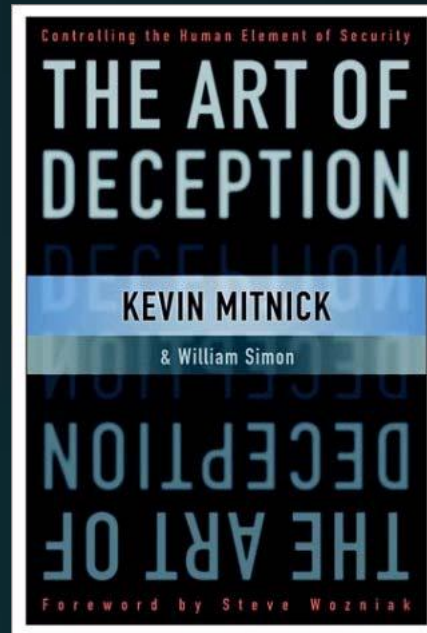


Think like a bad guy...

What is he after?



Used by Hackers as a standard tool



**That your perimeter
(aka network) Might not
have died but
its not really
doing well....**



Ok, now what should
I do?



**How about
Kill the Data....**

Kill the Data – >
Crypto

**Is it really that
simple?**

SafeNet 'Secure Breach' Survey....

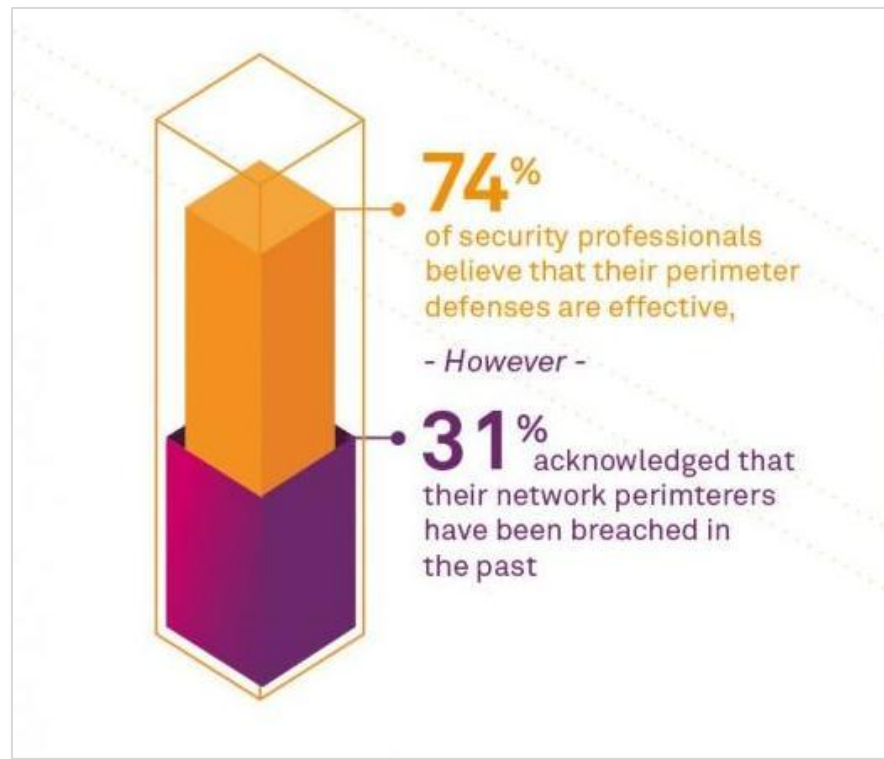


- **31%** admitted that their perimeter has been breached
- **20%** were not sure if they'd been breached.
- **38%** believe unauthorized users currently have access to their networks.
- **65%** think they will suffer a data breach within 3 years
- **59%** believe if their perimeter is breached, their data would not be safe.
- **20%** wouldn't trust their own company with their personal data....

State of Data Security

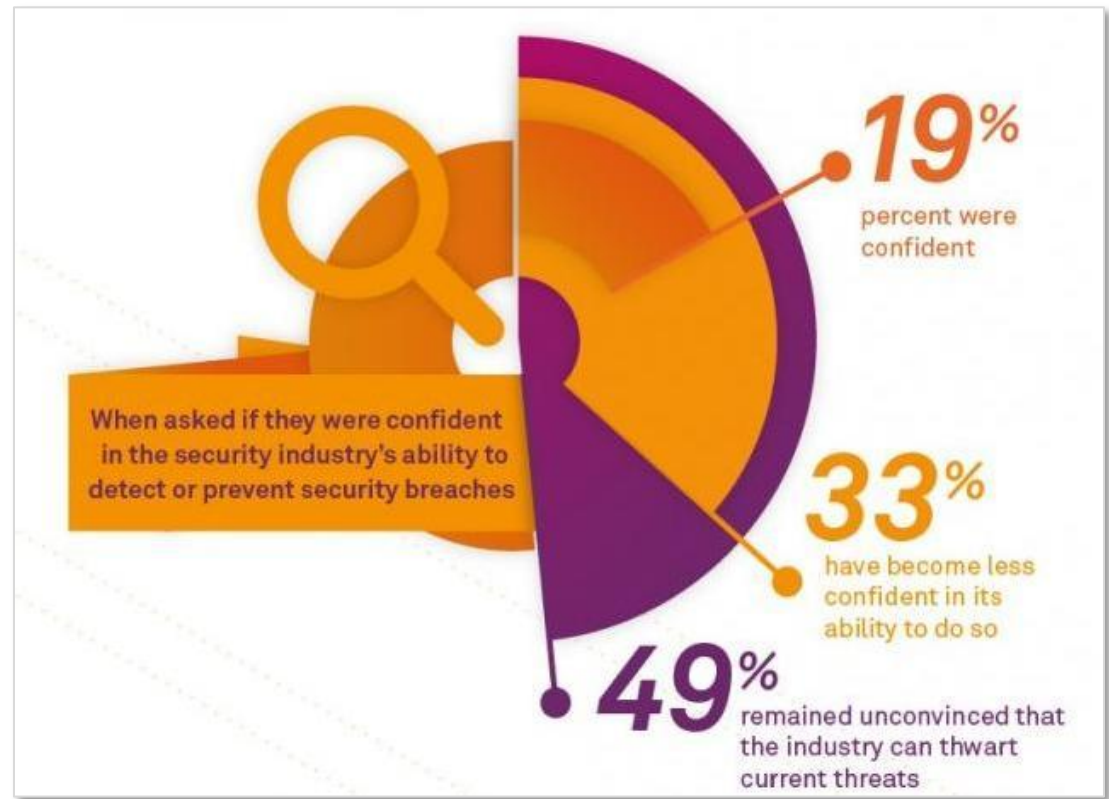
Persistent **belief that perimeter defenses are effective.**

Significant **acknowledgement of past breaches.**



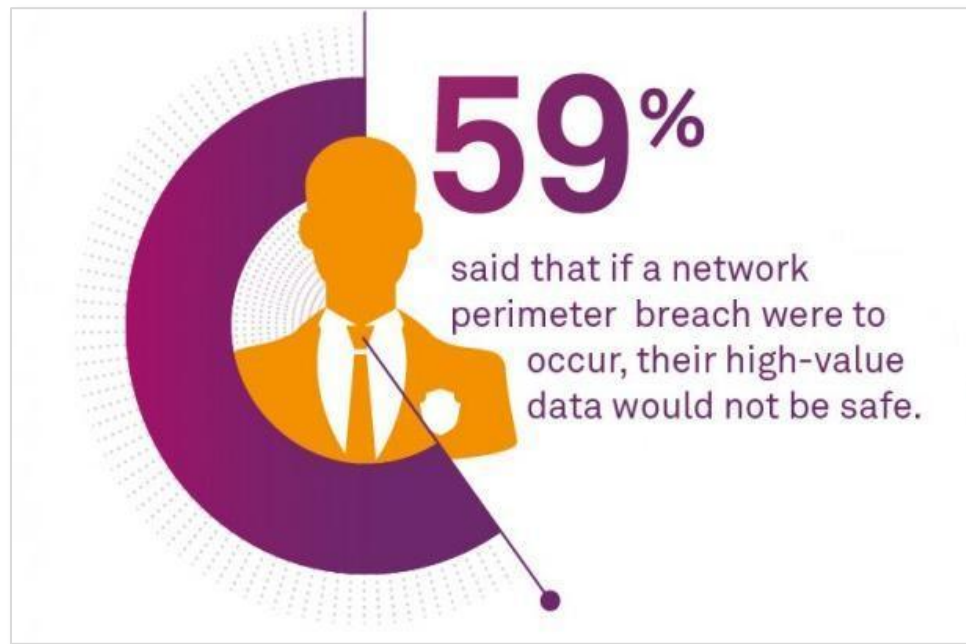
State of Data Security

Doubt in security industry's **ability to detect and prevent breaches.**



State of Data Security

Recognition that if perimeters failed, high value data **would not be safe.**



A new prescription for the “Secure Breach” era

MEDICAL CENTER

NAME _____ AGE _____
ADDRESS _____ DATE _____

Rx

SIGNATURE

LABEL

REFILL 0 1 2 3 4 5 PRN NR

Introspection

- Its time to try something new...

Acceptance

- You can't prevent a perimeter breach...

Understanding

- Know your enemies and what they are after...

Action

- Protect What Matters...THE DATA!

Control Access To Data?

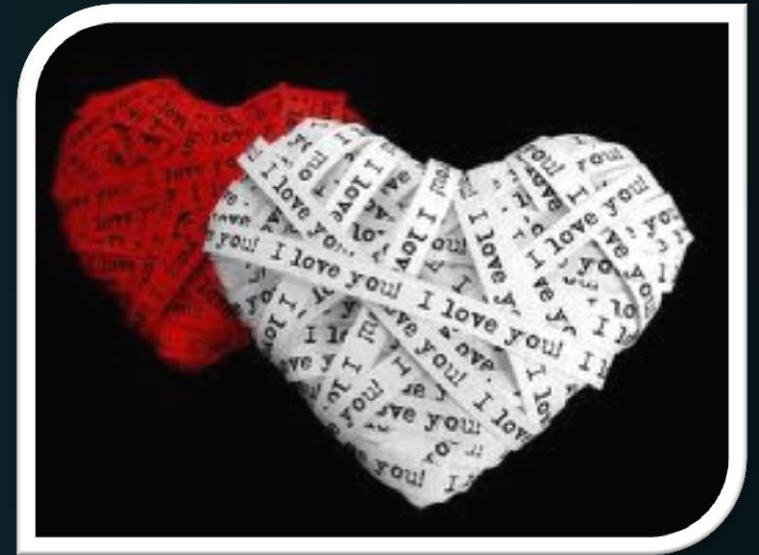
Cloud/Virtualization Loves Crypto....



Compliance Loves Crypto



High Value Data loves crypto



Hackers?

They HATE Crypto



Think breach acceptance
Data is the new perimeter

Kill The data
Kill it The Right Way

A photograph of the back of a person's head with dark hair, covered in numerous yellow sticky notes. The person is wearing a white collared shirt and a dark jacket. The background is a solid green color. A semi-transparent grey horizontal band is overlaid across the middle of the image, containing the text.

Forget Everything

InfoSec has (to) Changed

A black and white photograph of two people in conversation. The person on the left is seen in profile, looking towards the right. The person on the right is facing them, with their hands raised in a gesturing motion. The background is a textured, light-colored wall. A semi-transparent grey rectangular box is overlaid across the middle of the image, containing white text.

Breach Prevention?

How is that working for you?

A white dove is shown in profile, facing left. A small, dark-furred monkey is perched on its back, looking towards the camera. The background is a blurred outdoor setting with some dry leaves on the ground. A semi-transparent grey banner is overlaid across the middle of the image, containing the text.

Breach Acceptance

Accept a breach will happen




**Protect What Matters
Where it matters**



Breaches

Don't like Encrypted Data

Its everywhere...

A person is skydiving over a vast, hazy landscape. The person is wearing a black jumpsuit, a yellow helmet, and goggles. They are in a stable, horizontal position with arms and legs spread out. The background is a clear blue sky with some light clouds. A semi-transparent black banner with white text is overlaid on the center of the image.

We can help
And We've done it before



Security in knowledge

Thank you!

Jason Hart CISSP CISM

Safnet Inc

Jason.Hart@Safenet-inc.com

www.safenet-inc.com