

SECURITY 2013



21. ročník konference o bezpečnosti v ICT

How Easy Passwords can be Hacked and the Virtual World

Jason Hart CISSP CISM
VP, Cloud Solutions
Safenet Inc



About Me





Legal Disclaimer

ALWAYS GET PERMISSION IN WRITING.

- Performing “scans” against networked systems without permission is illegal. Password cracking too
- You are responsible for your own actions!
- If you go to jail because of this material it's not my fault, although I would appreciate it if you dropped me a postcard.
- This presentation references tools and URLs - use them at your own risk and with permission

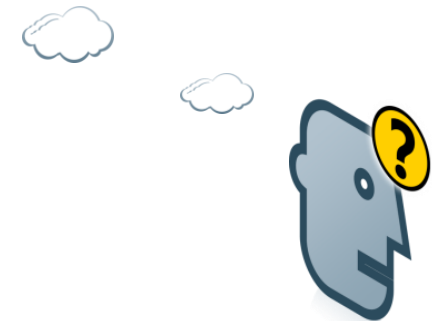


Accepted Security Principles

- Confidentiality
- Integrity
- Availability
- Accountability
- Auditability



However we have forgotten about it
in a virtual world





What a great 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 and there Data
 - Accessing data from the virtual world can be simple

Virtual Word – With Virtual Holes

- Welcome to the Future
- Cloud Computing
- Virtual Environment
- With Virtual Security holes
- During the past 15 years with learnt nothing





Password Attack via Device

Welcome to the Future of Hacking

- Attack channels: web, mail, open services
- Targeted attacks against users and business and or premium resources
- Totally invisible to the mobile users
- Mobile devices are becoming an easy target for **Advanced persistent threats (APT)**

In return for flooding /b/ this morning, have 62,000 passwords and emails. The top half is "password | email", and the bottom half is "email | password"; these are random assortments from a collection, so don't ask which site they're from or how old they are, because we have no idea. We also can't confirm what percentage still work, but be creative or something.

Enjoy, and [REDACTED] delivers.
twitter.co[REDACTED]

[REDACTED] cecup | debra@writerspacemail.com |
[REDACTED] am1 | cissy.hartley@gmail.com |
[REDACTED] 64 | rdndrgnfly@gmail.com |
[REDACTED] eesa | poohwine@yahoo.com |
[REDACTED] 76 | debby236@comcast.net |
[REDACTED] read | kathyvalenzi@gmail.com |
[REDACTED] en | p2000n@yahoo.com |
[REDACTED] boy | donna.errelat@ctv.ca |
[REDACTED] pe | conniequadel@comcast.net |
[REDACTED] ie | tamjeang1@msn.com |
[REDACTED] y12n | nueman@hotmail.com |
[REDACTED] n06 | drac_n_roll@yahoo.com |
[REDACTED] an | jennylynn1216@yahoo.com |
[REDACTED] woman | deborah625@aol.com |
[REDACTED] er | horseunicornkey@aol.com |
[REDACTED] ell | dizzheart@aol.com |
[REDACTED] ee | dschenk@carolina.rr.com |
[REDACTED] e12 | amdragonetti@cox.net |
[REDACTED] in311 | evitap5@cox.net |
[REDACTED] in311 | evitap4@cox.net |
[REDACTED] mi23 | irishchelle@cox.net |
[REDACTED] rney | serafya@yahoo.com |
[REDACTED] le | junettearnold@yahoo.com |

SLICKHACKERS GROUP
FASTEST ON THE WEB

[Testimonials](#) [F.A.Q.'s](#) [News](#)

[Cart](#)

TOOLS

SERVICES

SH

ORDER

CONTACTS

SPECIALIST IN...

HOTMAIL, YAHOO, GMAIL, AOL & MYSPACE

ONLY \$100 USD!

SlickHackers@Live.com



SLICK HACKERS GROUP

Email Hacking

We hack hotmail password and crack passwords of all web based email accounts. Our task is to provide excellent customer support and help

Hack Passwords

We are professionals interested in helping serious people for whom an email password would mean saving their marriage, knowing the truth, preventing a fraud, protecting their family/job/interests only when conventional ways and normal procedures do not work.



CloudCracker

A password cracking service for penetration testers and network auditors who need to check the security of WPA2-PSK protected wireless networks, crack password hashes, or break document encryption.

Start Cracking

File Type WPA/WPA2

Handshake File

ESSID

Next

Handshake

Delivery

Options

Confirm

Big. Fast. Cheap.
Run your network
handshake against
300,000,000 words
in 20 minutes
for \$17.

"Welcome to the
future: cloud-based
WPA cracking is
here!" --
TechRepublic

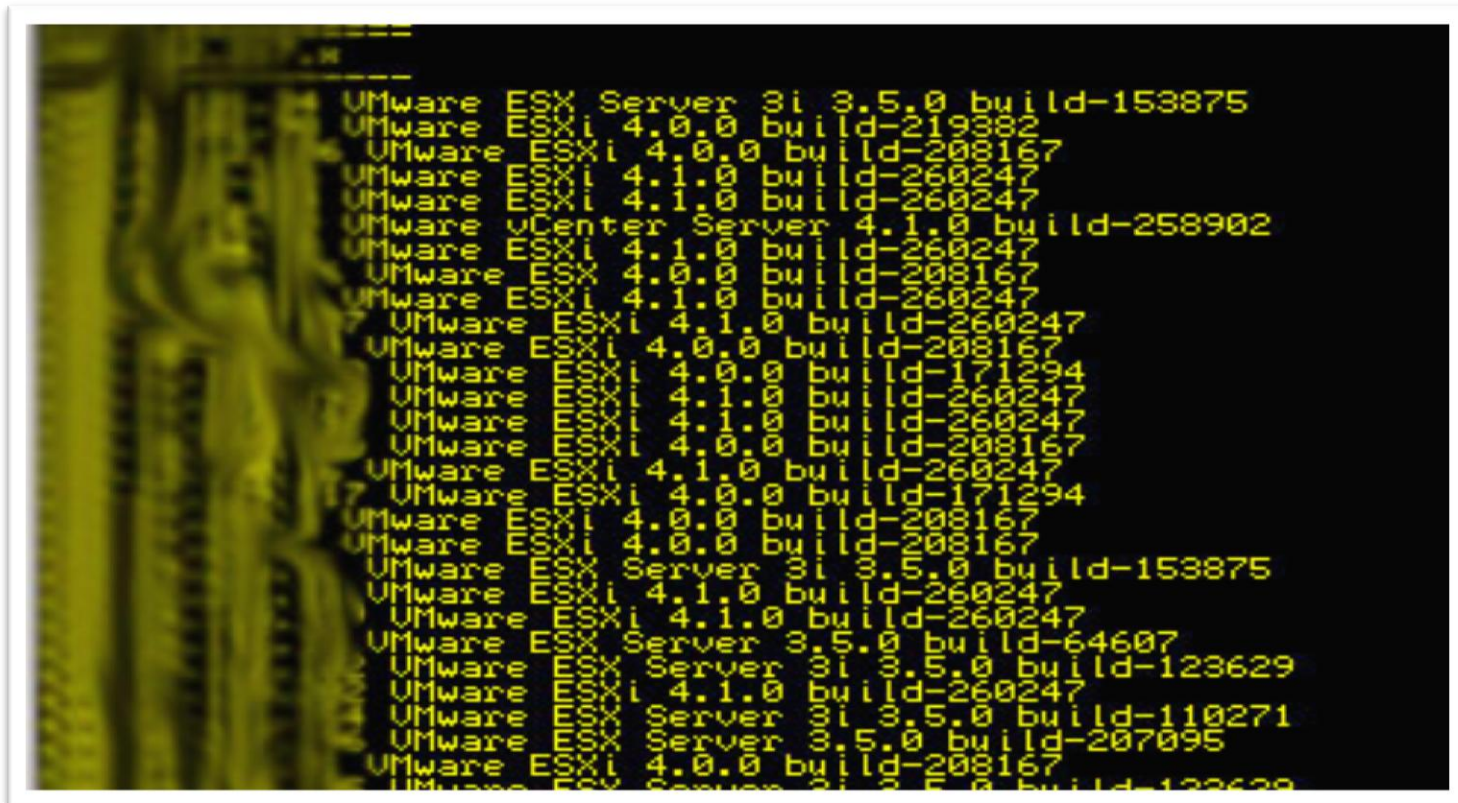
"Low cost service
cracks wireless
passwords from the
cloud..." --
TheRegister

"This really is a great
idea." -- Hacker News



Lets Start

vCenter servers directly connected to the web. . . .WOW

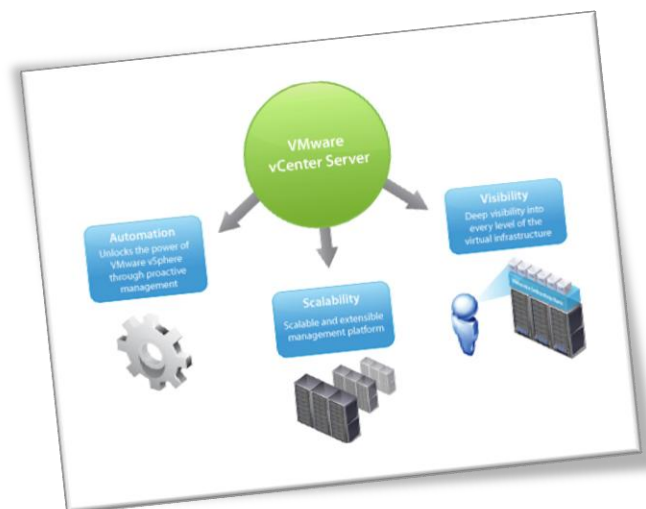


The Target

Vmware vCenter Version 4.1 update 1

- Services running:

- Update Manager
- vCenter Orchestrator
- Chargeback



- Each Service has a web server running

Web Attack 101History repeating

••• The Attack

vCenter Orchestrator attack vector 1.....

Installed by default within vCenter is an very interesting file:

C:\Programfiles\VMware\Infrastructure\Orchestrator\configuration\jetty\etc\passwd.properties



This file contains md5 passwords and can easily be bruteforced using rainbow tables



Point & Click



Any one can do

```
$ msfconsole
```

```
##
```

```
###
```

```
##
```

```
##
```

```
$ msfconsole
```

```
##
```

```
###
```

```
##
```

```
##
```

```
## ## #### ##### ##### ##### ## #### ##  
##### ## ## ## ## ## ## ## ## ## ##  
##### ##### ## ##### #### ## ## ## ##  
## # ## ## ## ## ## ## ## ## ## ##  
## ## #### ## ##### ##### ## #### #### ##  
##
```

```
msf > use auxiliary/scanner/vmware/vmware_enum_sessions  
msf auxiliary(vmware_enum_sessions) > set RHOSTS [TARGET HOST RANGE]  
msf auxiliary(vmware_enum_sessions) > run
```

This module will log into the Web API of VMWare and try to enumerate all the login sessions

SECURITY 2013 



A Live Security Experiment Was Conducted Today



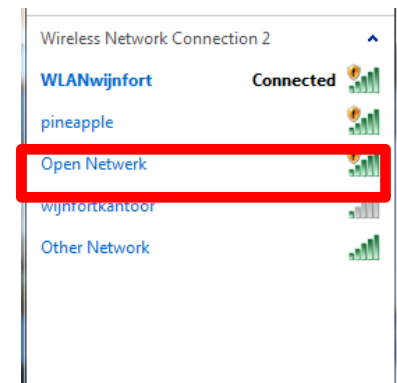
Background

- Wireless Networks are part of our life and are convenient.
- However Wireless Hotspots are the single most dangerous technology for mobile and smart phone users
- Whether you're connecting to a public Hotspot or a ROUGE AP – a Hackers Access Point
- Welcome to the increasing unseen security threat facing you and your users



Experiment

- At 10:30hrs today a Rouge Wireless Access Point was activated, with the objective of seeing how many people would try to use the access point
- The Name of the Wireless Access Point is
 - “Open Network” (Have you tried 😊)





Overview





The results

- During a period of 2 Hours a total of 43 people accessed the rouge wireless access point
- All users could have been compromised



**For the ones who did
Not use the
Rouge AP**



WEAPONIZING THE WEB

MORE ATTACKS ON USER GENERATED CONTENT

Next Generation Password Hacking



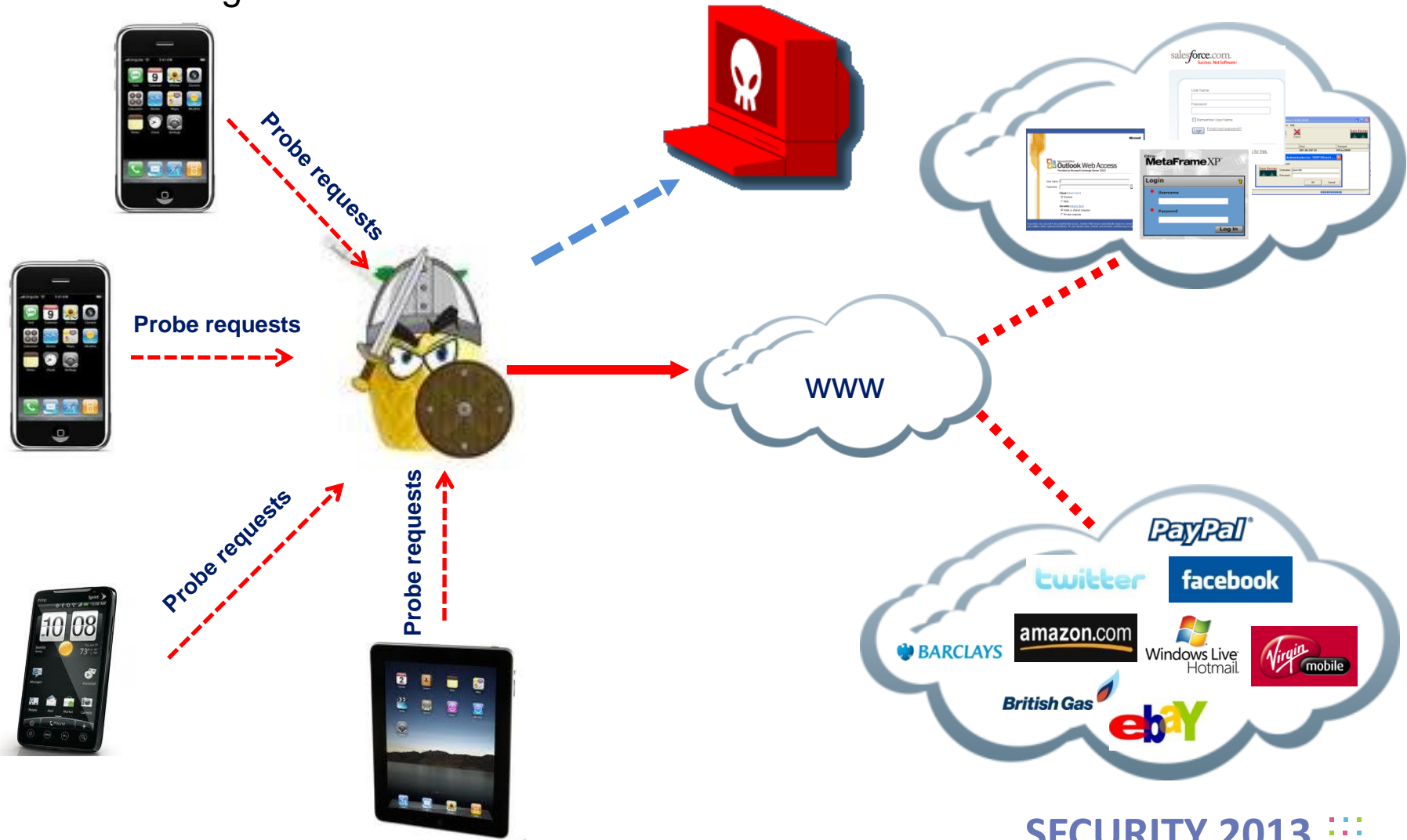
43823	50:ea:d6:91:bc:93	172.16.42.103	isiks-iPhone	01:50:ea:d6:91:bc:93
43799	c8:bc:c8:ea:59:13	172.16.42.215	GhostMAC	01:c8:bc:c8:ea:59:13
43735	a8:6a:6f:ca:c8:c0	172.16.42.163	BLACKBERRY-E7B4	01:a8:6a:6f:ca:c8:c0
43663	28:6a:ba:1a:6d:fc	172.16.42.224	Mr-Macs-ipad	01:28:6a:ba:1a:6d:fc
43647	d0:23:db:41:de:8a	172.16.42.100	Martins-iPhone	01:d0:23:db:41:de:8a
43642	00:16:e3:8f:75:a1	172.16.42.177	swlpt	01:00:16:e3:8f:75:a1
43634	00:1d:fe:dc:e1:85	172.16.42.117	* *	
43634	0c:60:76:65:d5:a8	172.16.42.112	FLDLP114B	01:0c:60:76:65:d5:a8
43661	14:8f:c6:c4:ba:06	172.16.42.107	Scotts-Phone	01:14:8f:c6:c4:ba:06
43626	f0:cb:a1:5e:ed:93	172.16.42.127	* 01:f0:cb:a1:5e:ed:93	
43619	90:21:55:b7:a0:b0	172.16.42.170	Android_352212047584847	*
43602	78:a3:e4:e9:ac:f0	172.16.42.138	* 01:78:a3:e4:e9:ac:f0	
43602	18:20:32:a8:e4:c7	172.16.42.219	iPad	01:18:20:32:a8:e4:c7
43562	24:ab:81:4d:56:5f	172.16.42.237	* 01:24:ab:81:4d:56:5f	
43585	d0:23:db:2f:74:79	172.16.42.111	Jasonhs-iPhone	01:d0:23:db:2f:74:79
43444	38:e7:d8:78:f3:c1	172.16.42.225	android_20014688ba37b875	*
43407	a0:88:b4:c5:d3:fc	172.16.42.162	20141-lap	01:a0:88:b4:c5:d3:fc
43371	40:6a:ab:fd:54:59	172.16.42.227	BLACKBERRY-393E	01:40:6a:ab:fd:54:59
43697	00:26:ff:74:88:9e	172.16.42.232	BLACKBERRY-305B	01:00:26:ff:74:88:9e
43360	00:1e:65:18:e1:98	172.16.42.166	uk812211	01:00:1e:65:18:e1:98
43346	0c:74:c2:d5:05:c2	172.16.42.178	* 01:0c:74:c2:d5:05:c2	
43342	90:84:0d:ae:36:ef	172.16.42.115	Nicole	01:90:84:0d:ae:36:ef
43319	00:21:6a:7f:a1:fc	172.16.42.190	UK813411	01:00:21:6a:7f:a1:fc
43673	cc:08:e0:be:d7:99	172.16.42.147	BurzuJ	01:cc:08:e0:be:d7:99
43283	00:21:6a:83:ba:e0	172.16.42.128	UK813682	01:00:21:6a:83:ba:e0
43452	30:7c:30:5e:28:09	172.16.42.181	BLACKBERRY-C9B6	01:30:7c:30:5e:28:09
43652	00:23:14:2d:17:a0	172.16.42.202	uk783613	01:00:23:14:2d:17:a0
43550	4c:ed:de:60:33:c6	172.16.42.106	Jason-TOSH	01:4c:ed:de:60:33:c6
43697	18:3d:a2:1c:a9:68	172.16.42.156	uk827790	01:18:3d:a2:1c:a9:68
43270	00:1e:65:42:6b:8e	172.16.42.124	uk814617	01:00:1e:65:42:6b:8e
43665	a0:88:b4:06:e7:68	172.16.42.150	UK833187	01:a0:88:b4:06:e7:68
43264	00:21:6a:0b:c3:72	172.16.42.114	uk816008	01:00:21:6a:0b:c3:72



Live Attack

Against a the Cloud .

... ARP Attack







Virtual World

With Virtual access by any one With only a click





Google™ Hacking

Yes Google as Hacking Tool....



Google

intext:"name" intext:"address" intext:"taxpayer" site:dl.dropbox.com

Search 7 results (0.23 seconds)

Everything

[PDF] W-9

https://dl.dropbox.com/s/.../CTMUN_W9_Request_For_TaxID.pdf?...

File Format: PDF/Adobe Acrobat - Quick View

Request for **Taxpayer** ... Fiequester's **name** and **address** (optional) ... The number shown on this form is my correct **taxpayer** identification number (or I am waiting ...

[PDF] PG933-17 Page 1 of 16 05/2010 Mailing Address: PO Box 9394 ...

<https://dl.dropbox.com/.../Burke%20-...>


File Format: PDF/Adobe Acrobat

Aug 24, 2011 – titled in the **name** of the deceased participant as well as your **name** – for Mailing **Address** of Financial Institution (Street or PO Box). **Name** of ...

Looking for sensitive data leaks in Dropbox cloud storage



site:dropbox.com/gallery



site:dropbox.com/gallery

Search

About 164,000 results (0.33 seconds)

Web

www.dropbox.com/gallery/

Images

[Sommerblut 2011 - Dropbox - Photos - Simplify your](https://www.dropbox.com/gallery/16453785/1/Sommerblut_2011_COPYRIGHT-HINWEISE)
https://www.dropbox.com/gallery/16453785/1/Sommerblut_2011_COPYRIGHT-HINWEISE 1 image. Last modified 5/18/2011.

Maps

Videos

18 images. Last modified 5/23/2011. ALFONS_Fotos_wg 12 images .

News


[GracerHopper112011 - Dropbox - Photos - Simplify your](https://www.dropbox.com/gallery/9183906/.../GracerHopper112011)
[https://www.dropbox.com/gallery/9183906/.../GracerHopper112011...](https://www.dropbox.com/gallery/9183906/.../GracerHopper112011)

Shopping

More

Dropbox is a free service that lets you bring your photos, docs, and videos share them easily. Never email yourself a file again!

Cancel Camera Upload Enable



Save Your Photos to Dropbox
Your photos and videos can be automatically uploaded to Dropbox.



SkyDrive®

site:live.com "skydrive" ext:dmp

Google site:live.com "skydrive" ext:dmp

Search About 2,700 results (0.41 seconds)

Database dump files on Microsoft SkyDrive

<https://cid-8847e773b11eec31.skydrive.live.com/emb...>

Windows Live SkyDrive
<https://skydrive.live.com/embedicon.aspx/.../060510-38688-01.dmp>
Open 060510-38688-01.dmp 060510-38688-01.dmp.

Windows Live SkyDrive
<https://skydrive.live.com/embedicon.../122509-26520-01.dmp?cid...>
Open 122509-26520-01.dmp 122509-26520-01.dmp.

Google site:live.com "skydrive" ext:dmp

Search About 1,470 results

Web <https://skydrive.live.com/emb...>

Images <https://skydrive.live.com/emb...>

Maps <https://skydrive.live.com/emb...>

Videos <https://skydrive.live.com/emb...>

News <https://skydrive.live.com/embedicon.aspx/.Public/0...>

Shopping <https://skydrive.live.com/embedicon.aspx/Minidump/...>

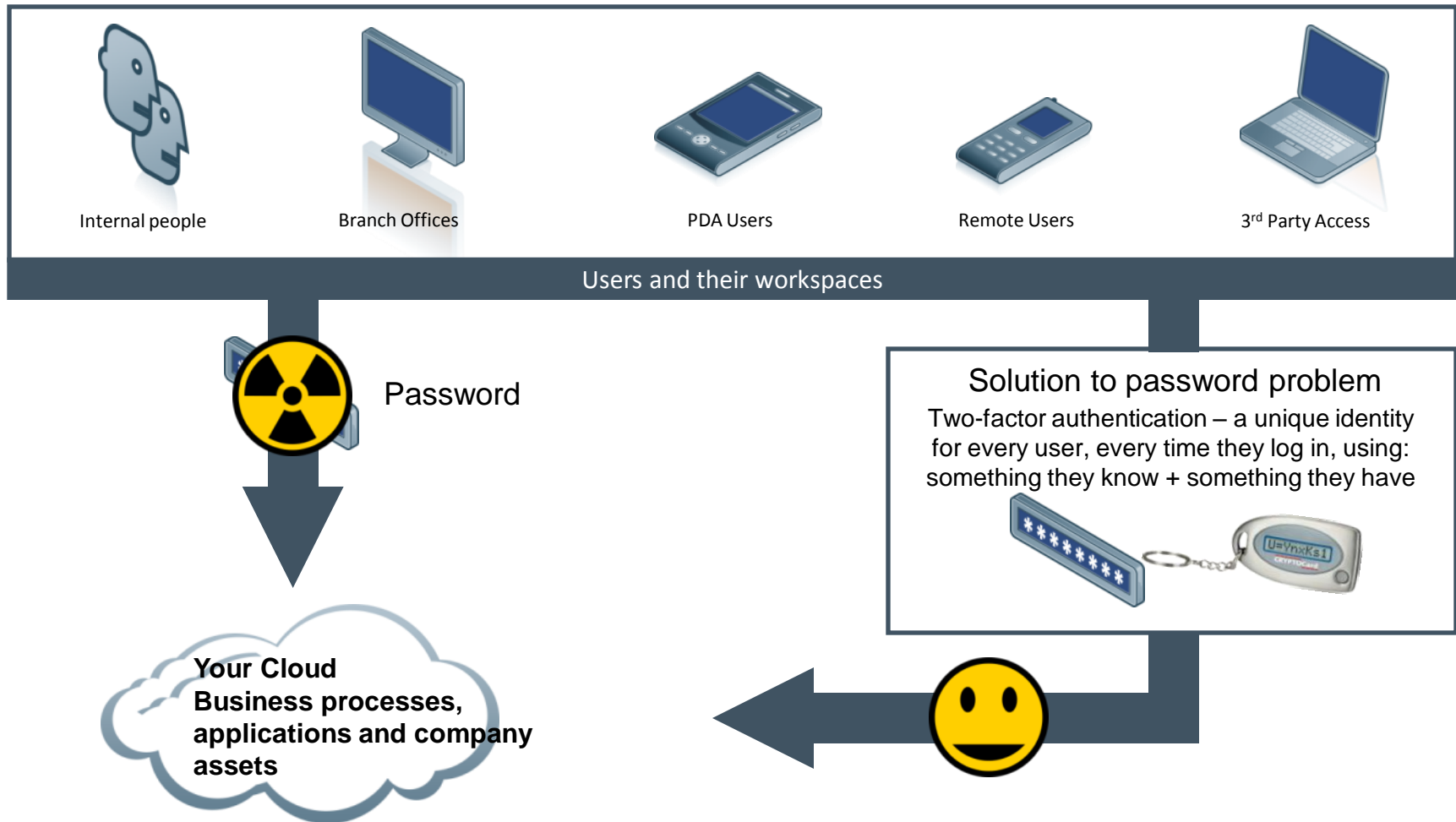
More

**The Battle
For the Virtual
World Has
Begun**





The Solution



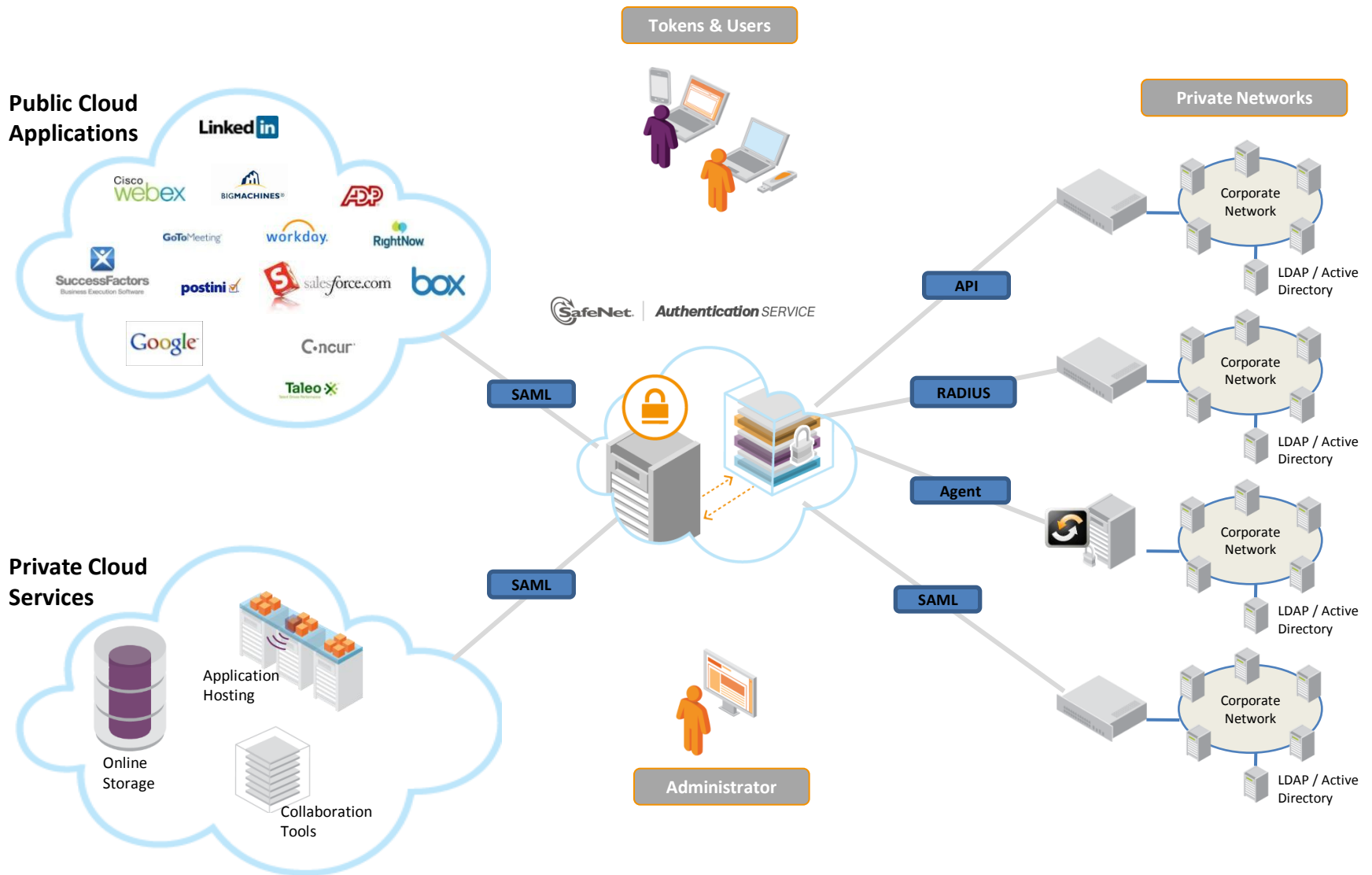


SafeNet Authentication - SAS

- Provides the ability to rapidly scale, deploy authentication
- Simple, easy and low-cost, driving strong authentication into all markets
- Offer a multi-tenant, multi-tier authentication platform that allows an almost infinite number of “virtual” authentication servers for Citi

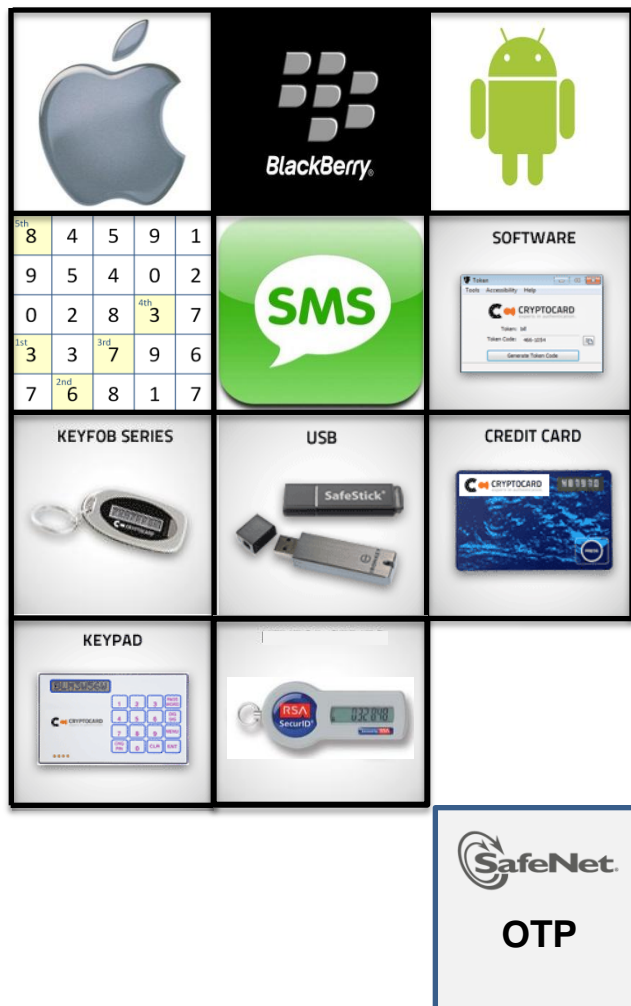


Overview





Token Choice



Choose the right token type for each user:

- ✓ Phone based
- ✓ Software
- ✓ Multiple hard tokens
- ✓ 'Tokenless' either SMS or Grid based

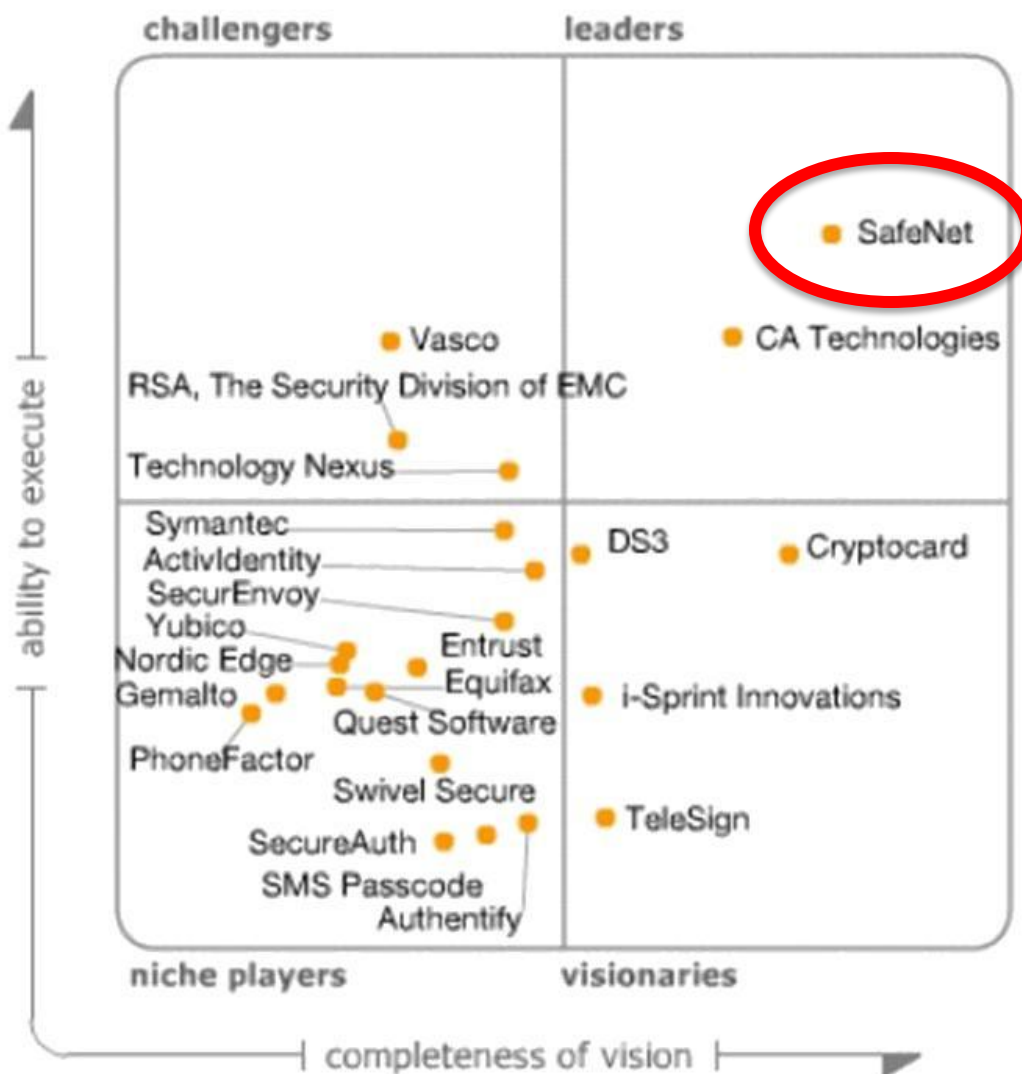
Our Authenticators:

- ✓ Don't expire
- ✓ Can be included in the service charge
- ✓ Seed keys can be generated by the customer
- ✓ Can be re-assigned to new users
- ✓ Self enrollment options reduces administration
- ✓ OTP & PIN complexity defined by the customer

Provides the lowest overall total cost of ownership
Supporting 3rd party tokens enables an orderly and
cost effective migration

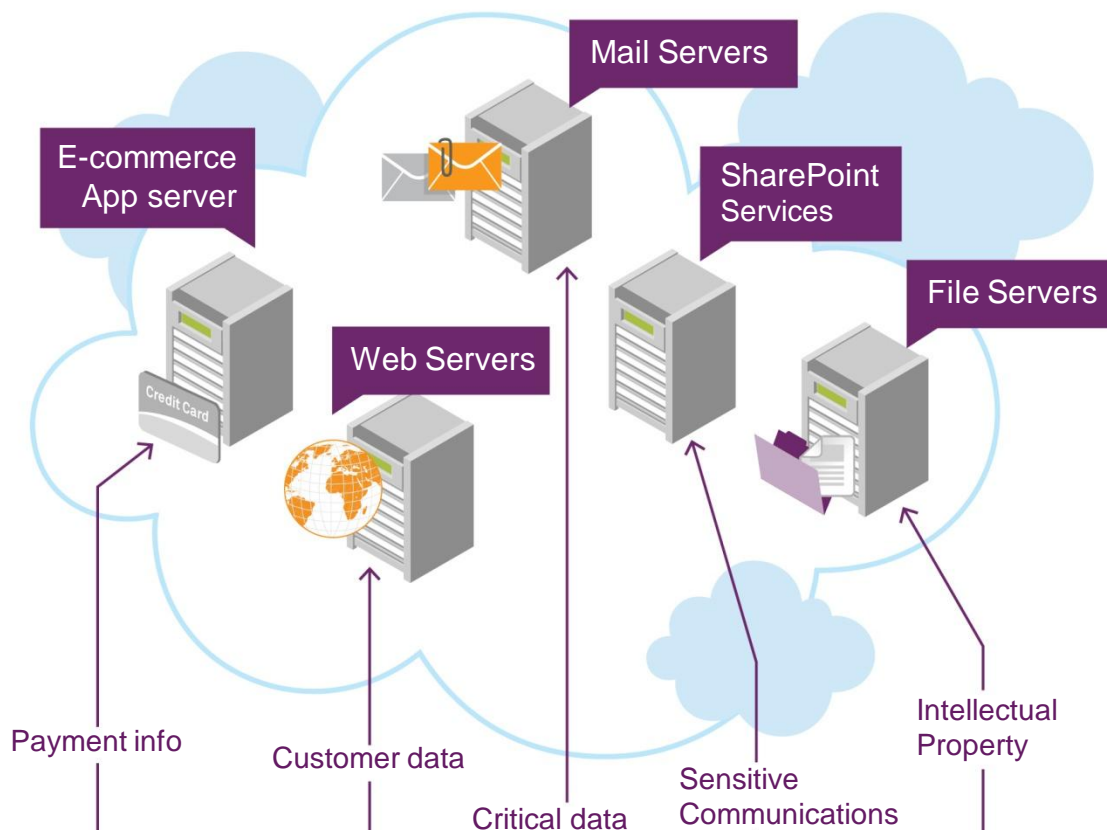


Leader Meets Visionary





Moving Your Data to the Cloud

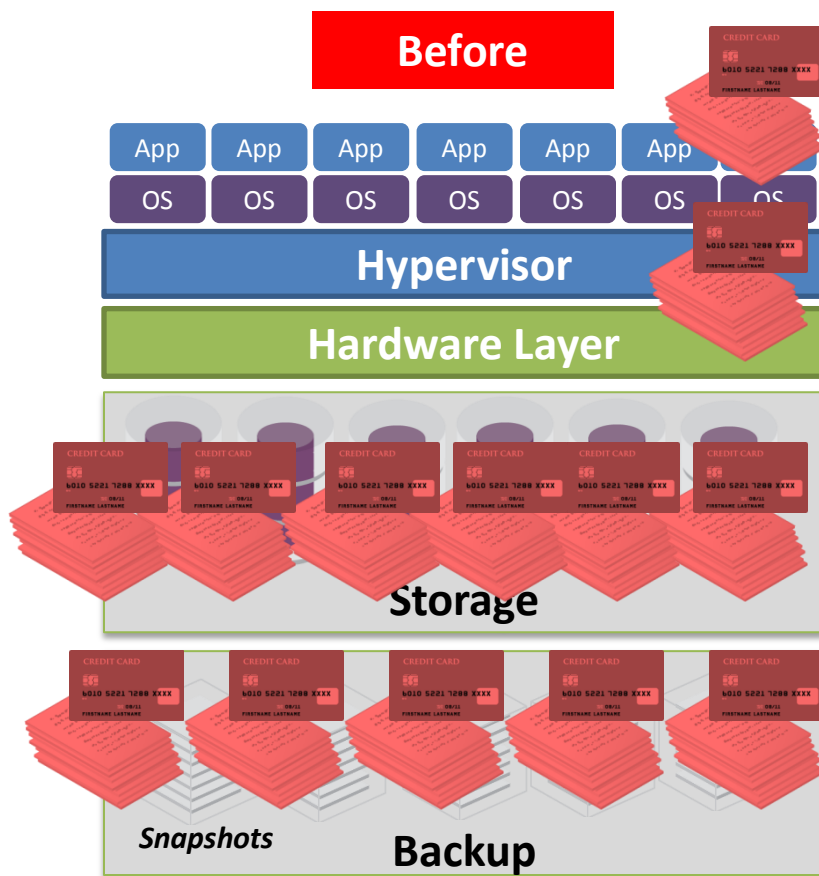


- **Sample Customer Goal:**
 - Move e-commerce, internal apps and customer services to virtual environment
 - Increase performance and lower costs
- **Some Concerns:**
 - How do I know when my data moves?
 - Who is accessing my data?

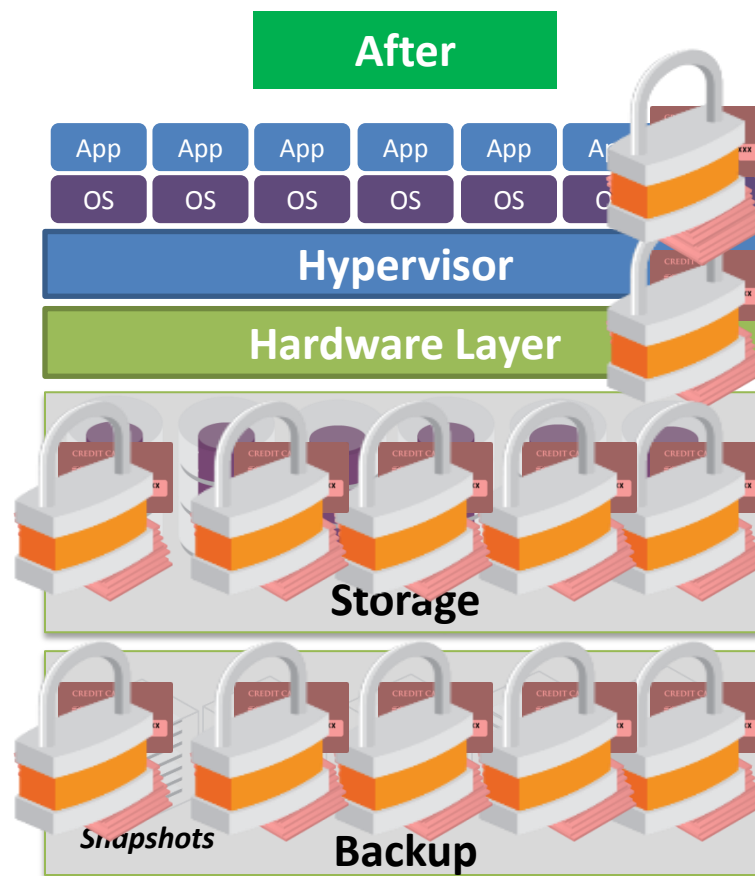
4A!6W4Z01 5 *158R7 T68Y87 2P{66! 46Z64A!6 64Z555446E65D\$66A55S4096 9 Q1 5 *158R7 T68Y87 2P{66! 46Z64A!6
66A55 879U54164\099P7A65S2679G6+6Q1W\$66A55S46D6+6Q1W5F*158R75T6PY 7879U54164\099P7A65S2679G6+6Q1W\$66A55
65Y43F4 654G312TY6GFAS6432346S5X46G5445Y43U21B35D6F45Y\$87D161W134F4 654G312TY6GFAS6432346S5X46G5465Y43
5F4D34R6046%Q65A44S35Z24X11Y5H66T84R65F4D3B6F55::..: W44H36VF4RR658+4S3546%Q65A44S35Z24X11Y5H66T84R65F4D3
32DF19 2 *03988!93048LSK93M{%WJ6565S4U32DF16JDU687?S46D939{8933+809 9 2 *03988!93048LSK93M{%WJ6565S4U32DF1
9P7A6LG5Z51 C96X65V33N34B6655U54164\099P7A65S26D35F\6G4H56J41JK33 4\ LX6Z51 C96X65V33N34B6655U54164\099P7A6



Example



Data Security
OR
Virtualization/Cloud



Data Security
AND
Virtualization/Cloud

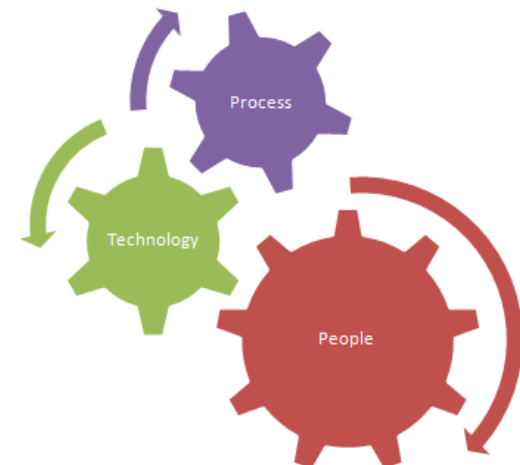
SECURITY 2013



Secure Breach

Protect the Data by applying Confidentiality and Integrity

We need to replace people with Data



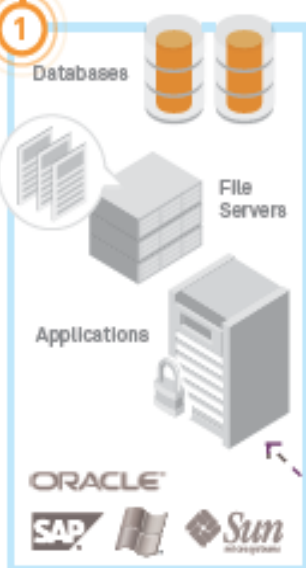
Protecting the Lifecycle of Sensitive Data

Sensitive Data is Everywhere And So Are We

WHERE IS YOUR DATA?

WHERE ARE YOUR KEYS?

Live Data



Stored Data



Virtualized Data



Key Management and Root of Trust



Access



WHO AND WHAT IS ACCESSING YOUR DATA?



Warning

- Pockets of Encryption
- Operational Inefficiencies
- Audit Deficiencies & Failures
- Sensitive Data Exposure



SafeNet - Who We Are:

Trusted to protect the world's most sensitive data
for the world's most trusted brands.



We protect the most
money that moves in the
world, \$1 trillion daily.



We protect the most digital
identities in the world.



We protect the most
classified information
in the world.

FOUNDED

1983

REVENUE

~500m

EMPLOYEES

+1,500

In 25 countries

OWNERSHIP

Private

GLOBAL FOOTPRINT

+25,000

Customers in
100 countries

ACCREDITED

Products certified
to the highest
security standard



The Data Protection Company

SafeNet delivers **comprehensive** data protection solutions for **persistent protection** of high value information.

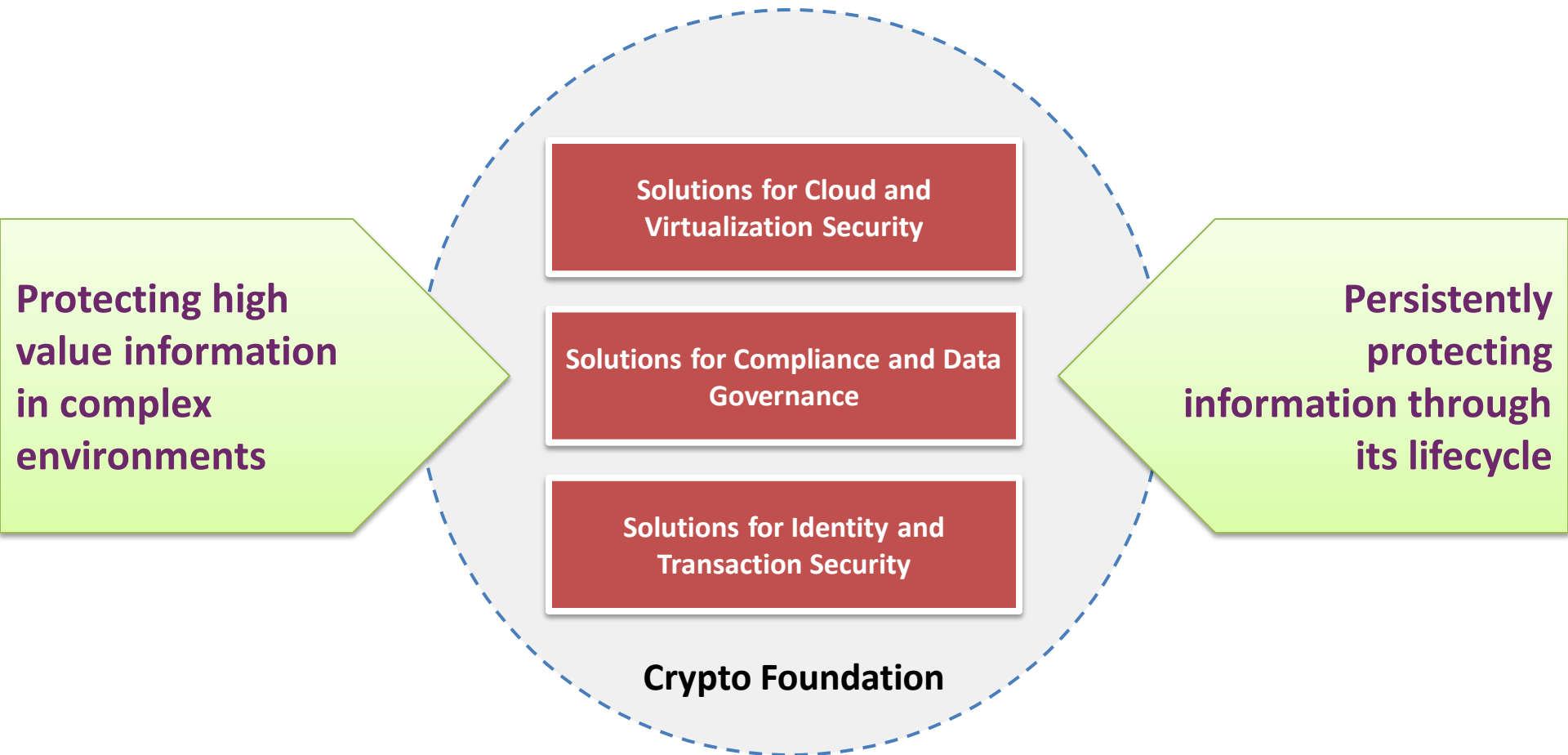
Over \$1 Trillion a Day | #1 in Classified Data | #1 in Digital Identities



PCI | HIPAA | GLBA | SOX | FISMA | EU Data Privacy | Japan PIP | German GDPdU | Etc.



The Data Protection Company



From the Datacenter to the Cloud



Comprehensive Storage Security

StorageSecure

Complete VM Encryption



vmware
READY

High-Assurance Virtualization

Hardware Security
Modules *and* KeySecure

Authentication



Authentication SERVICE



Thank you

Jason Hart CISSP CISM
VP Cloud Solutions

Jason.Hart@Safenet-inc.com

SafeNet delivers **comprehensive** data protection solutions
for **persistent protection** of high value information.