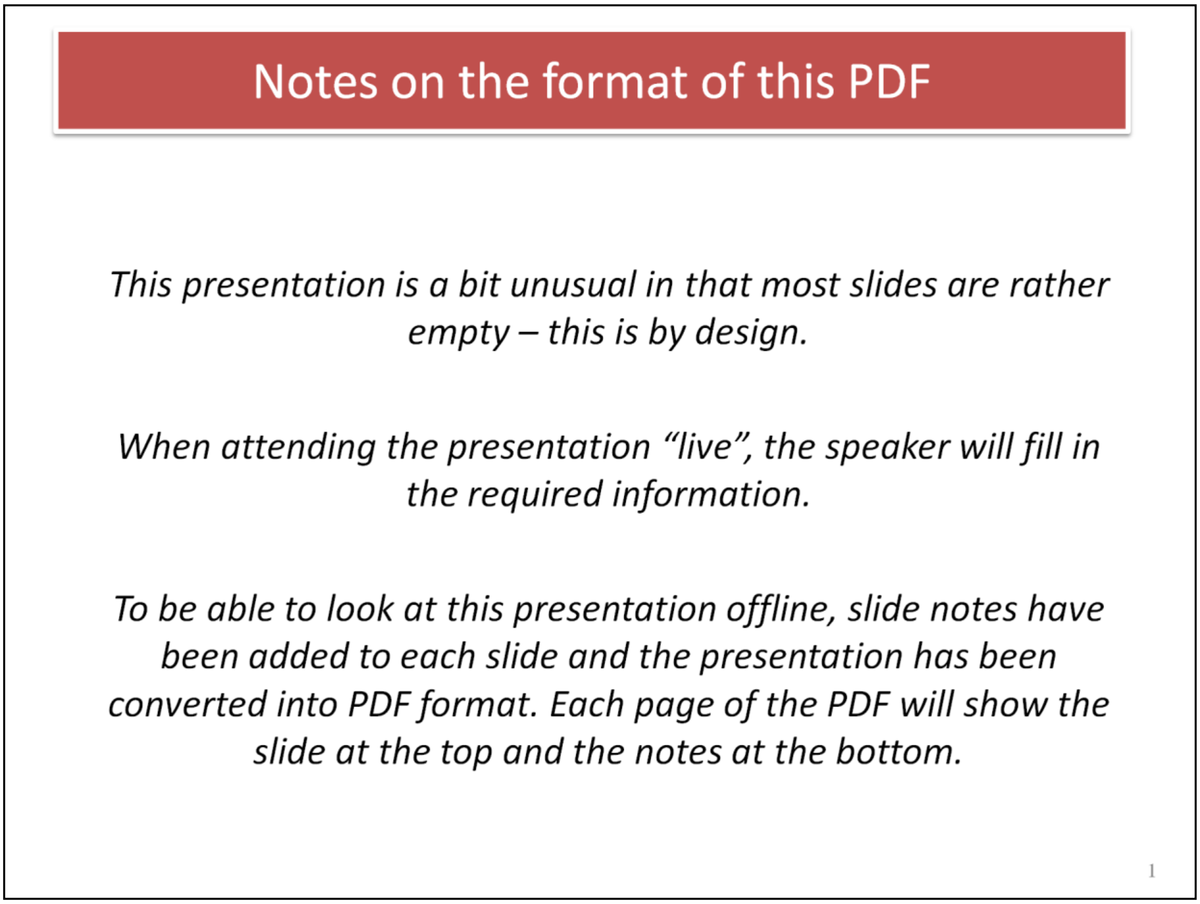


Notes on the format of this PDF

This presentation is a bit unusual in that most slides are rather empty – this is by design.

When attending the presentation “live”, the speaker will fill in the required information.

To be able to look at this presentation offline, slide notes have been added to each slide and the presentation has been converted into PDF format. Each page of the PDF will show the slide at the top and the notes at the bottom.

Make yourself comfortable.
Play it safe.

ussales@comforte.com
www.comforte.com

Where in the World is my credit card data?

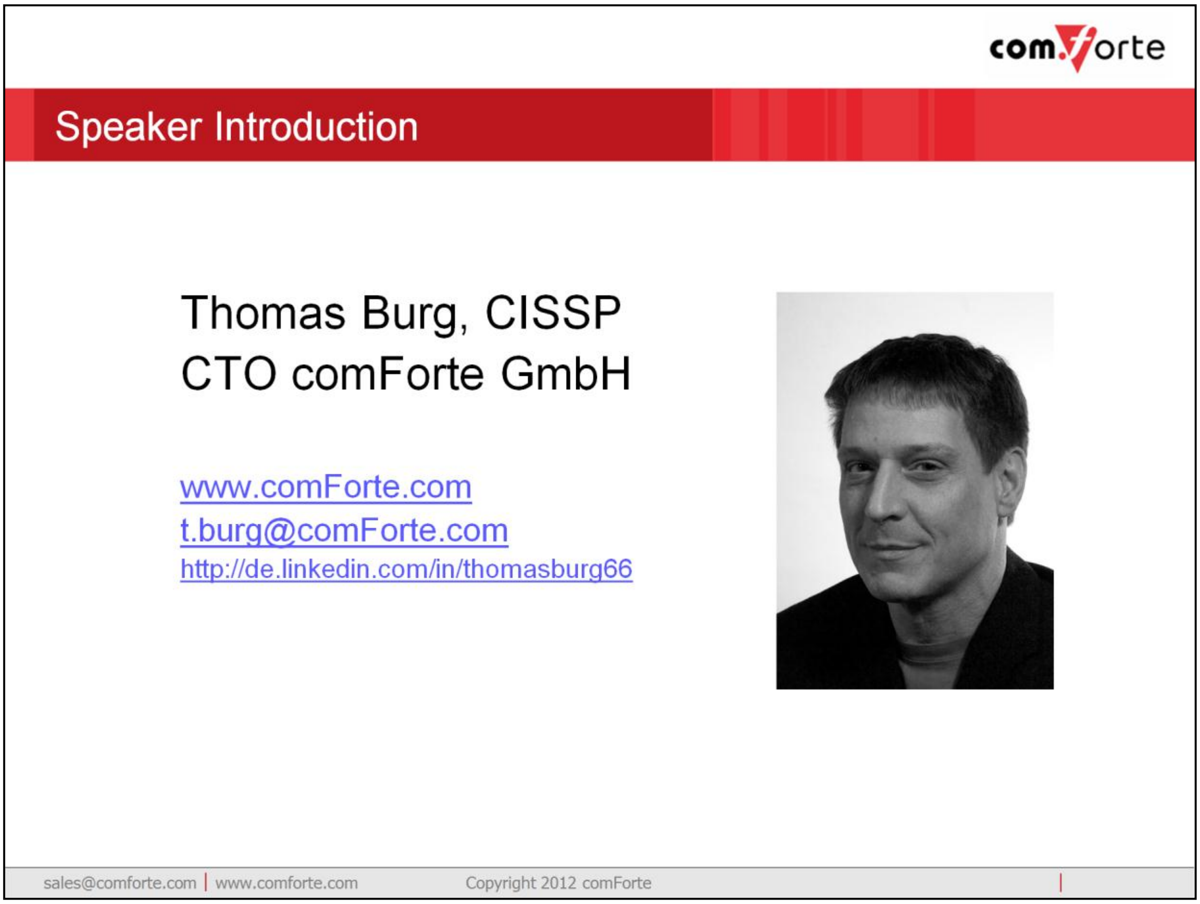
(and why should I care ?)

September 2012

Thomas Burg, CISSP
comForte 21 GmbH
t.burg@comforte.com
http://de.linkedin.com/in/thomasburg66

The presentation breaks into the following pieces:

- we start with a Poll to get audience participation but also to see where the audience stands
- We then discuss that it is non-trivial to exactly know where “my credit card data” is – after all files get FUP DUPed easily…
    - We also mention that using production data for test is Verboten, however creating good test data is not easy – unless you use SecurData for it
- Next, we discuss “My auditor wants proof where my credit card data is”
    - We start with a quick side-track about PCI (“love it” / “hate it”?) in which we also hand out the “nightmare on PCI street blog” and discuss why PCI might not be a bad thing after all
    - We show the actual verbage of the PCI standard which makes pretty clear that the auditor indeed cares
- Finally, we introduce PANfinder
- and end with a Summary



comForte

Speaker Introduction

Thomas Burg, CISSP
CTO comForte GmbH

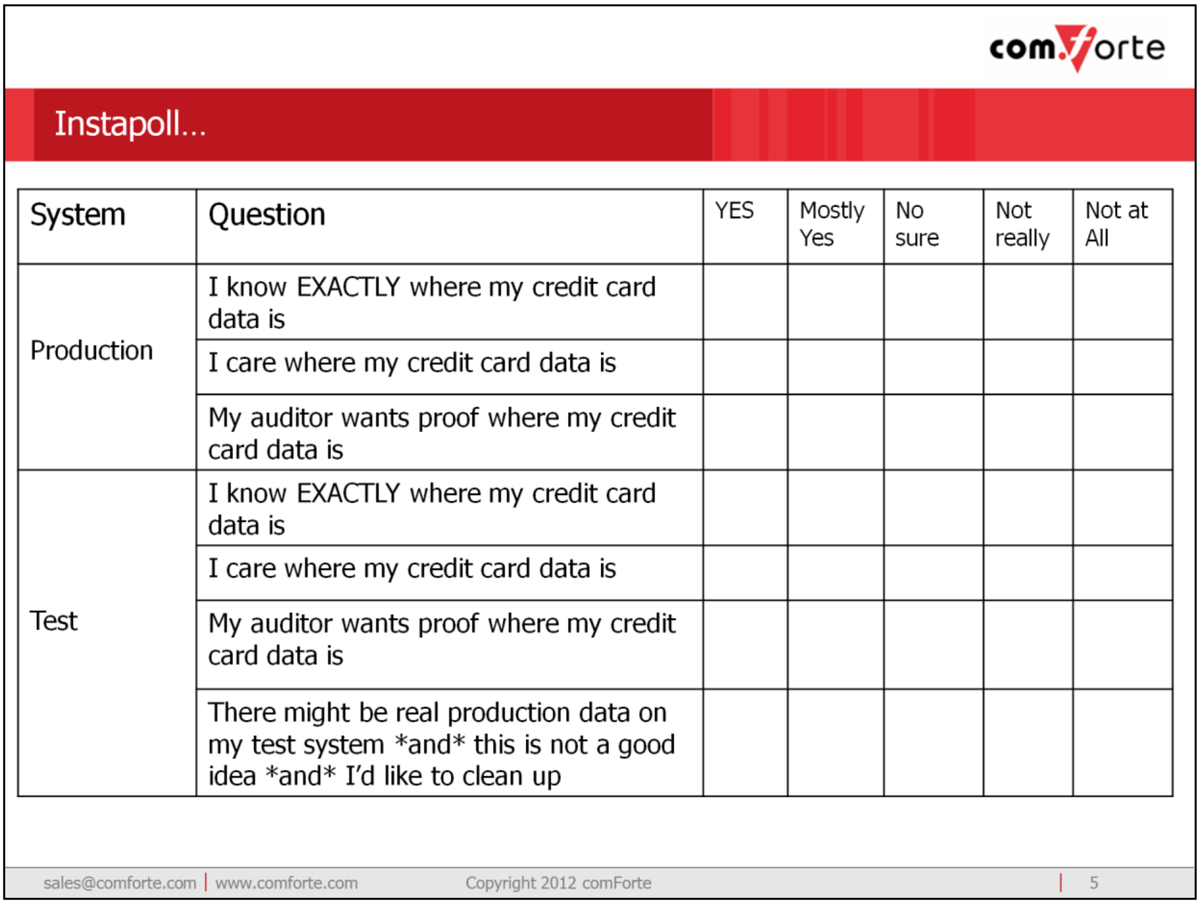
www.comForte.com
t.burg@comForte.com
http://de.linkedin.com/in/thomasburg66

Thomas Burg is CTO of comForte 21 GmbH. He was a ‘computer kid’ at the age of 13 and wrote his first COBOL programs on

Tandem Computers at the age of 20 while studying physics. Thomas received a Masters in Physics from the University of Mainz and

spent a year as visiting graduate at the University of Washington, Seattle. His work focus is Computer Security as well as integrating

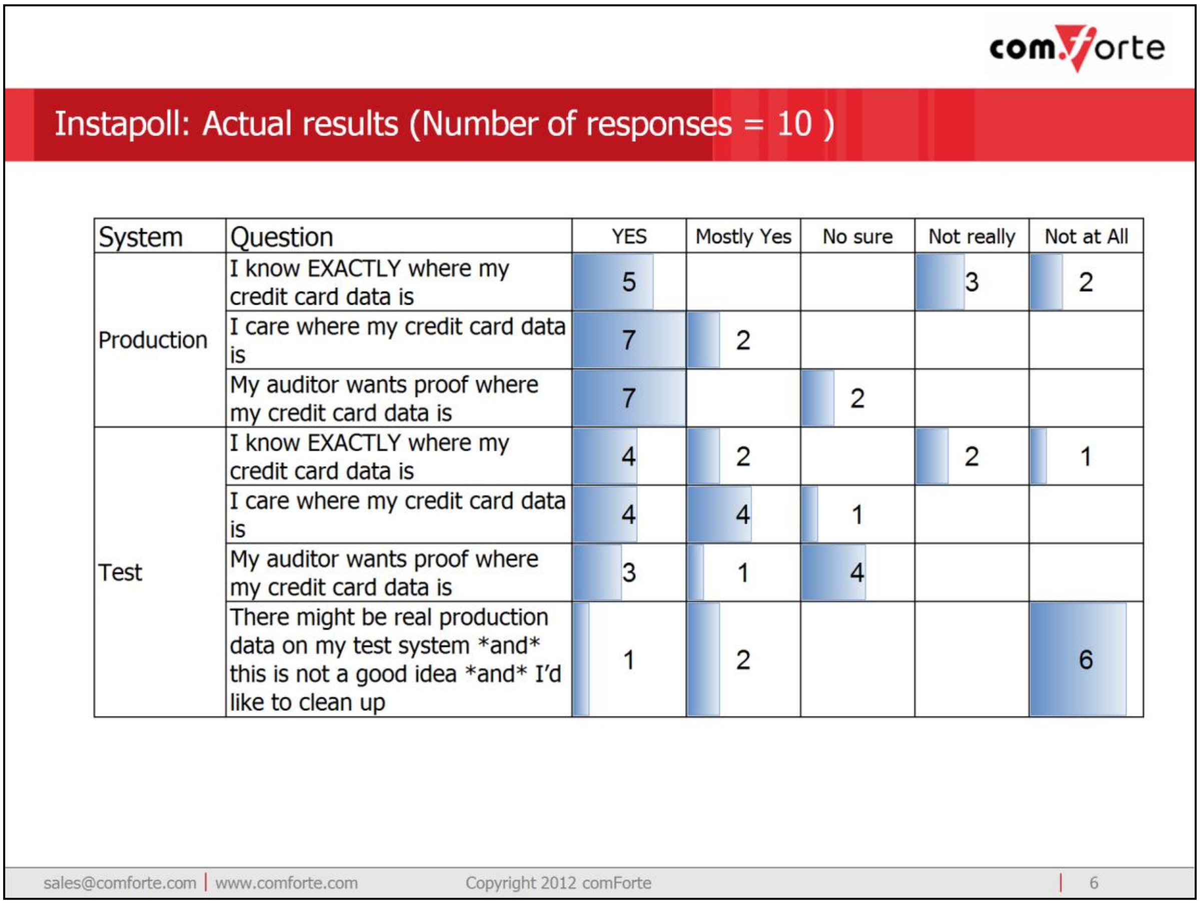
HP NonStop systems into an Enterprise architecture.



Instapoll…

System	Question	YES	Mostly Yes	No sure	Not really	Not at All
Production	I know EXACTLY where my credit card data is					
	I care where my credit card data is					
	My auditor wants proof where my credit card data is					
Test	I know EXACTLY where my credit card data is					
	I care where my credit card data is					
	My auditor wants proof where my credit card data is					
	There might be real production data on my test system *and* this is not a good idea *and* I'd like to clean up					

Before we go into the presentation I'd like to do a quick poll … So I kindly ask each participant to take 2 min to fill out the form which my colleague is just passing around. It should take no longer than 2 minutes and we'll use the collected results to jump-start the presentation.



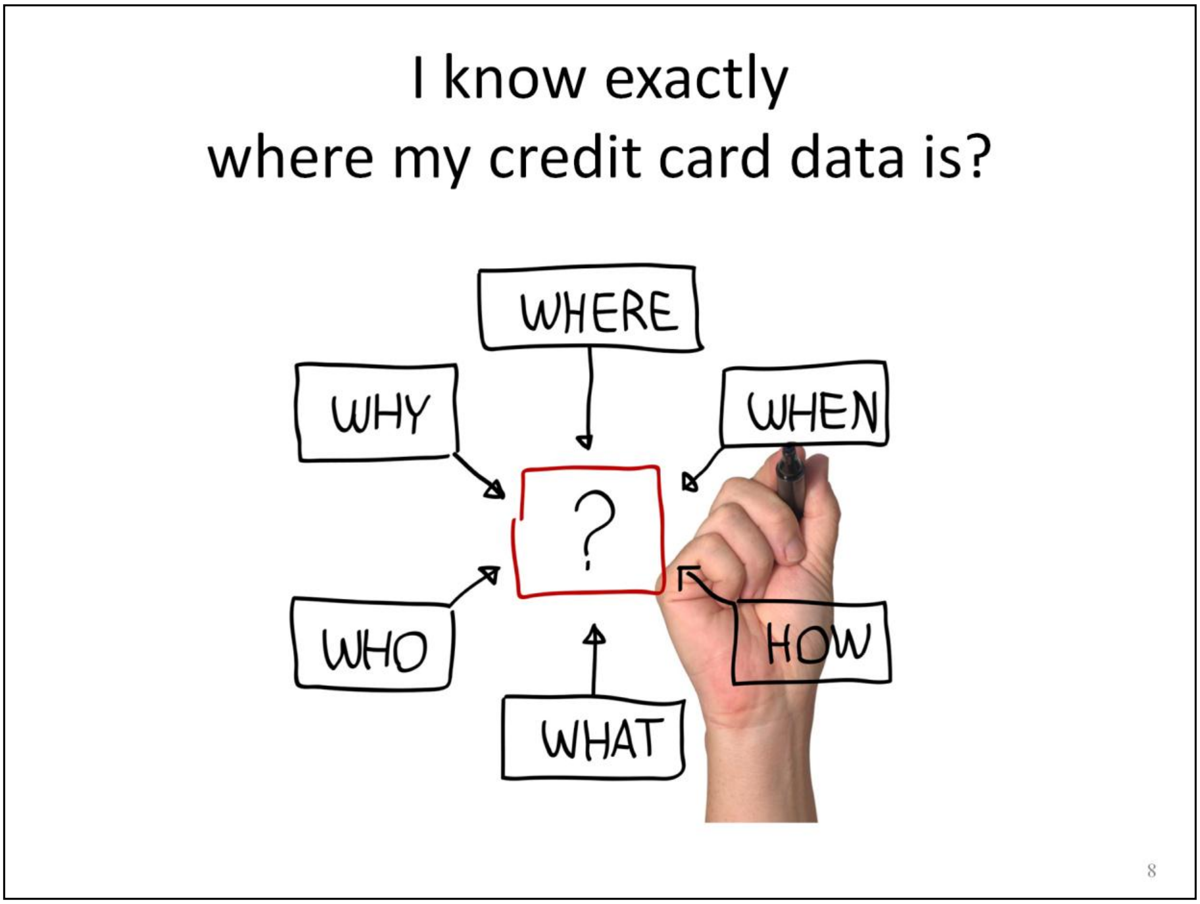
Instapoll: Actual results (Number of responses = 10)

System	Question	YES	Mostly Yes	No sure	Not really	Not at All
Production	I know EXACTLY where my credit card data is	5			3	2
	I care where my credit card data is	7	2			
	My auditor wants proof where my credit card data is	7		2		
Test	I know EXACTLY where my credit card data is	4	2		2	1
	I care where my credit card data is	4	4	1		
	My auditor wants proof where my credit card data is	3	1	4		
	There might be real production data on my test system *and* this is not a good idea *and* I'd like to clean up	1	2			6

sales@comforte.com | www.comforte.com Copyright 2012 comForte | 6

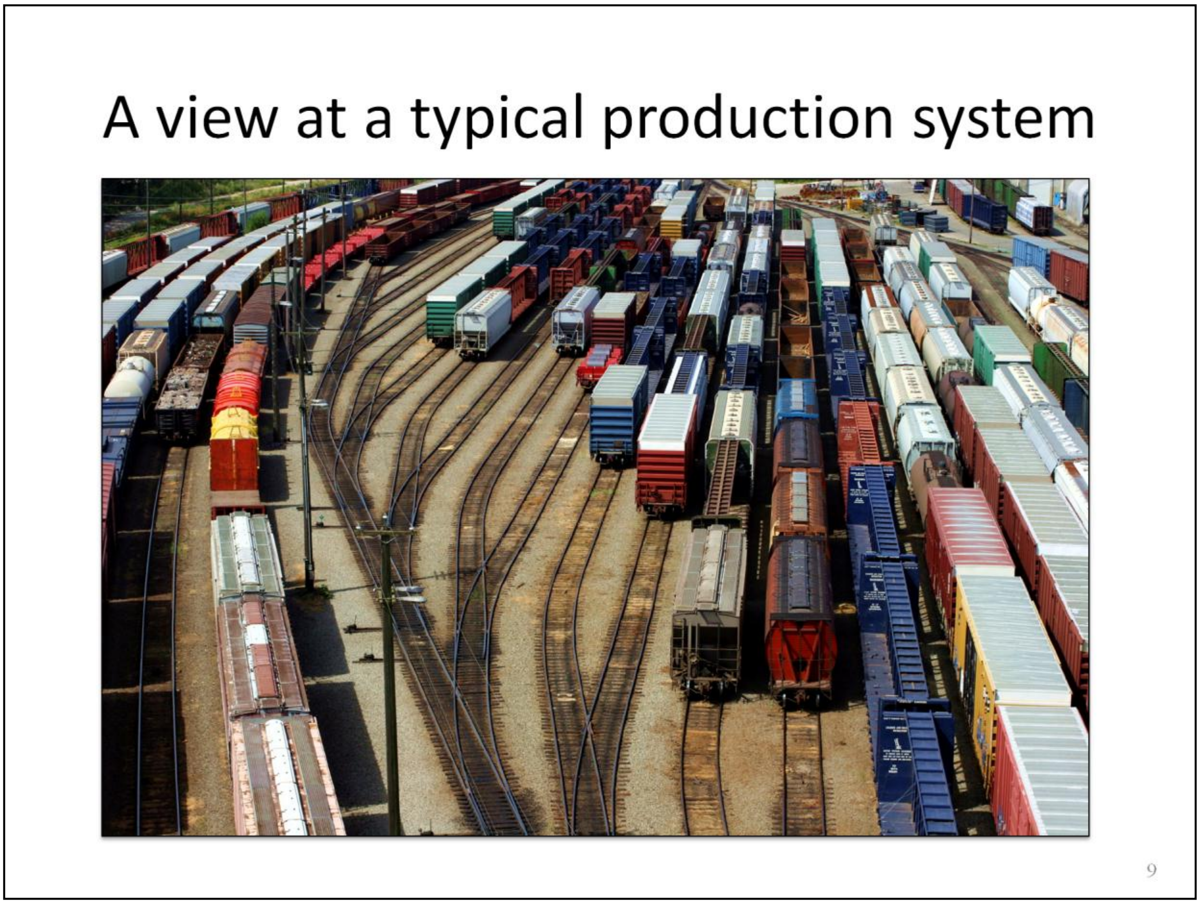
Let's discuss the results… While there were only 10 participants in the survey, the survey results do show:

- people DO care about where their credit card data is
- About half of the audience admit to *not* knowing exactly where their credit card data is on their production system; even more don't know on their test system
- Most of the auditors indeed require proof where the credit card data is on both test and production system
- all in all it seems like PANfinder is the right product for most of them…



I know exactly where my credit card data is?

Let’s discuss some questions of the poll in more depth… Knowing where the data is can be tricky, especially in large institutions where systems are complex and handled by multiple people. Also, systems change over time.



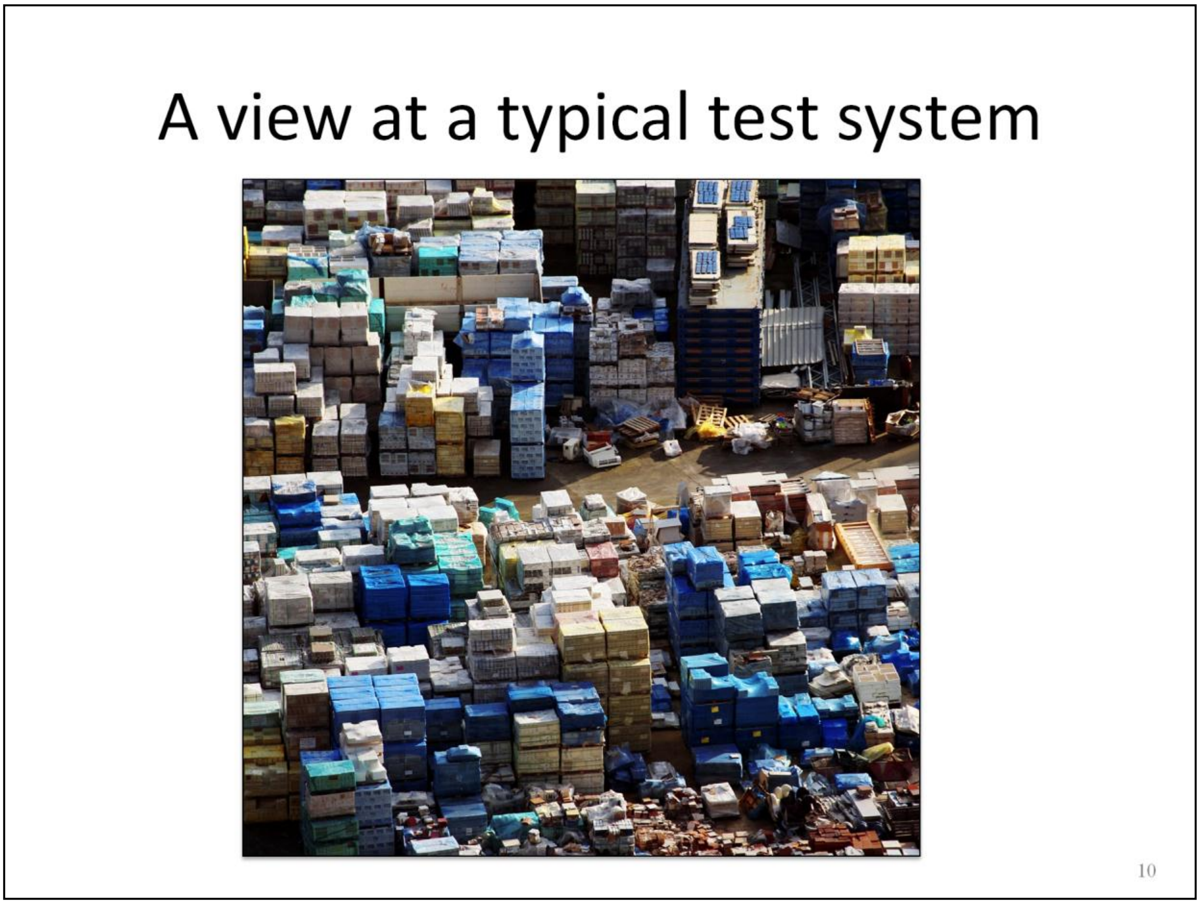
A view at a typical production system

This picture shows a typical large railway system. I chose this image as a metaphor for a typical production system: Things are well organized, well documented, everything goes according to plan (hey, at least in Swiss railway). However, even in Swiss railway things every now and then do NOT go according to plan. A train gets diverted, an engine fails. So, processes are broken for “quick fixes”. Trains end up in unexpected places.

Translate this to a typical credit card processing system: You have some of the following files (at minimum):

- transaction log file
- if you process “on-us”: cardholder file
- if you settle to another system: daily settlement (intermediate) files
- if you synchronize to other systems: possible files to be transferred in batch mode

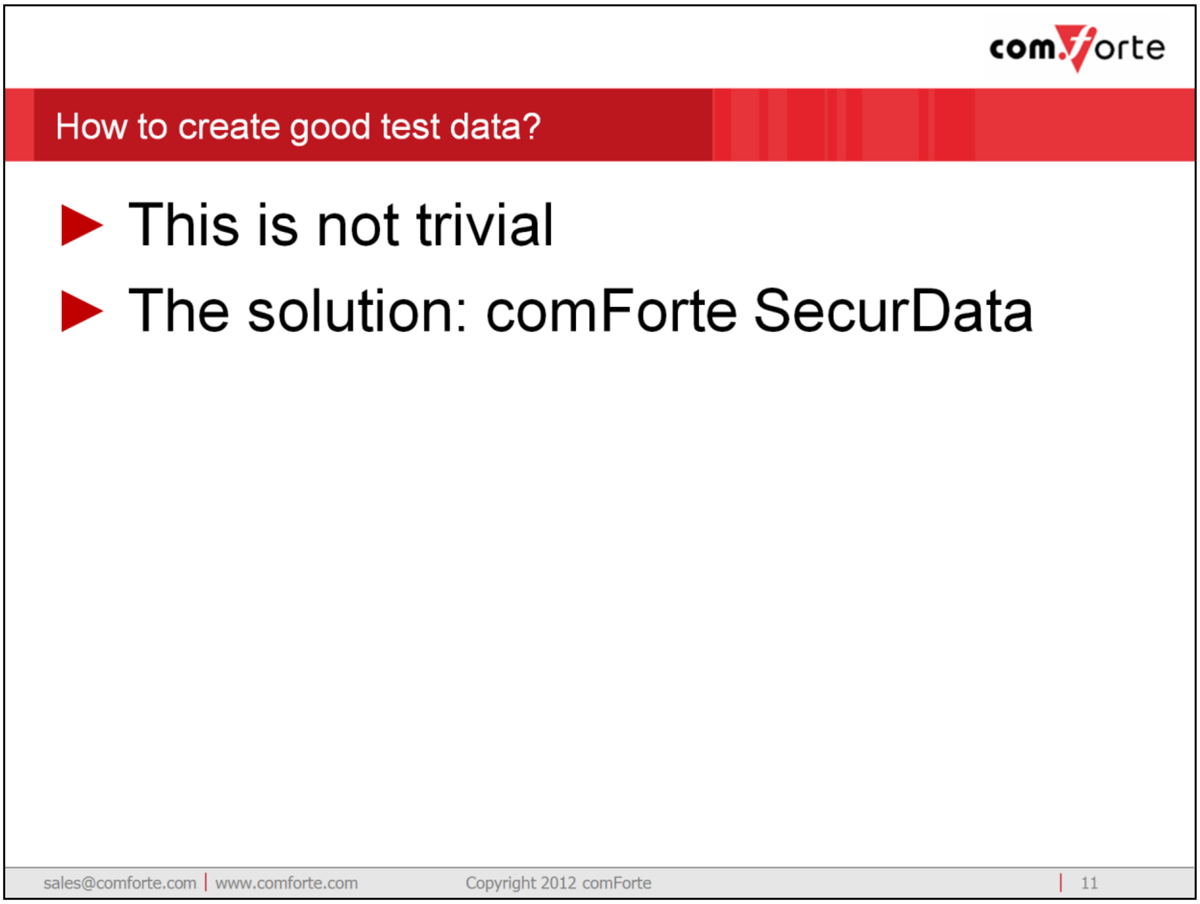
This is a subset of the “planned for” situation. The more complex your system is, the harder it is to get a full grip…. So why not automate the search? Most probably, you *will* have a rather good grip but to ‘double-check’, a computer program is the right tool – searching is easy for computers.



A view at a typical test system

Applying the prior metaphor to a test system, things get much more complex:

- you may be testing various releases of various applications
- very often on test systems data is created on the fly, but never purged
- of course it is Verboten to use production data in test, but if time pressure mounts …



How to create good test data?

- This is not trivial
- The solution: comForte SecurData

This is not trivial

Cannot copy production data

Needs to be “close to” production data, otherwise worthless

The solution: comForte SecurData

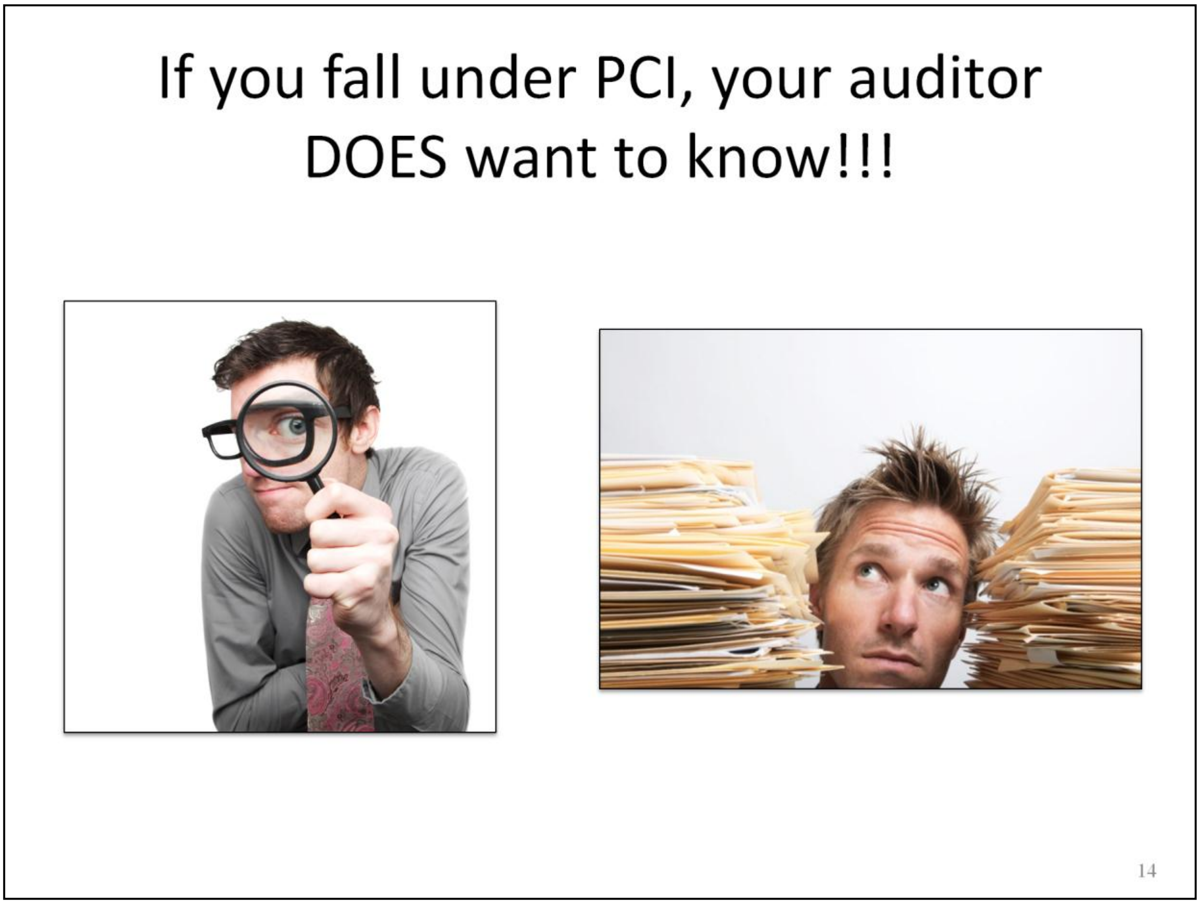
Can tokenize data “in place”

Can also replicate data from production system to test system, leave it unchanged in production but tokenize at test system

Creates high quality test data with no security risk whatsoever

My auditor wants proof where my credit card data is ??

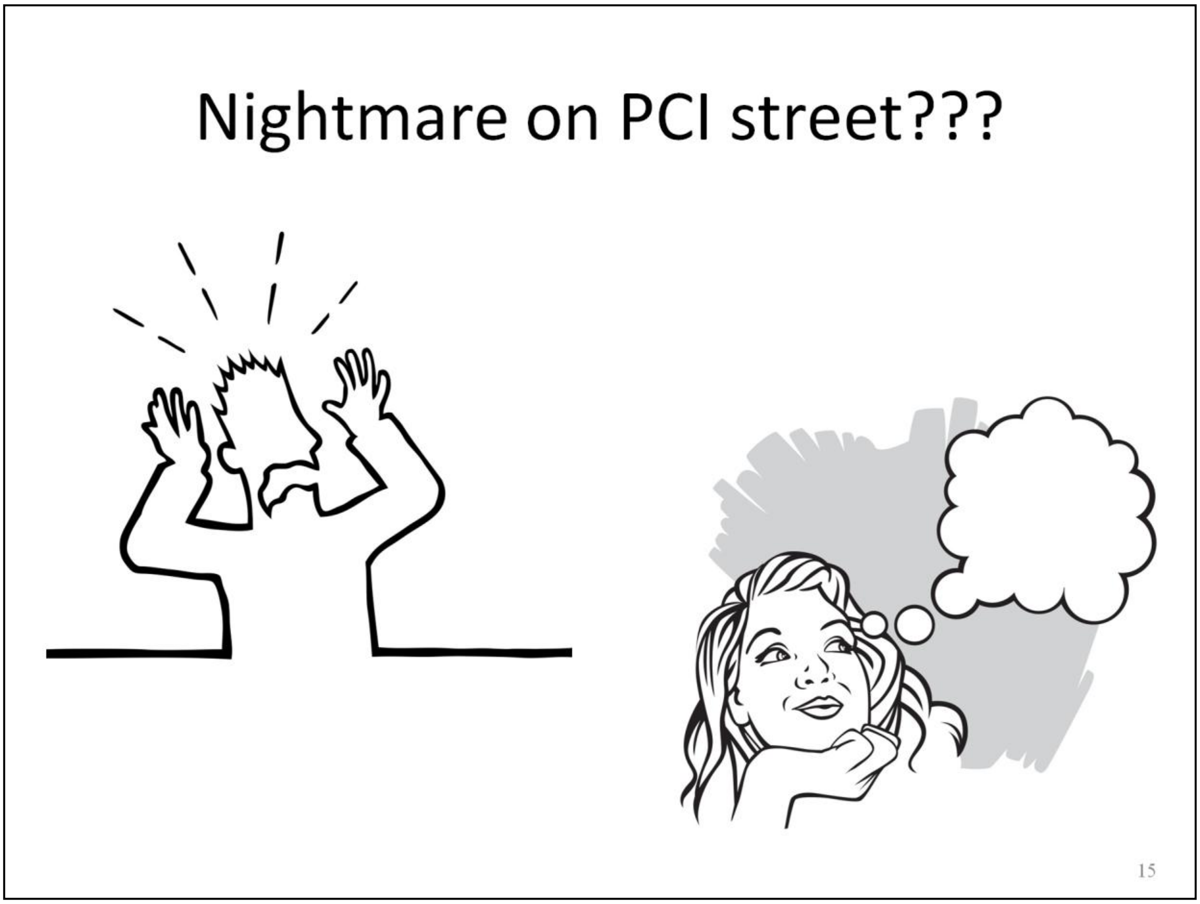
PCI verbiage aside, it’s kind of a “Duh” question: if you don’t know where the data is, you cannot properly protect it.



If you fall under PCI, your auditor DOES want to know!!!

We'll show in a second that PCI in fact requires EXACT and PROVEN knowledge of where credit card data is.

However, before we look at the actual PCI requirements, let's talk a bit about PCI… (or internal audits)…

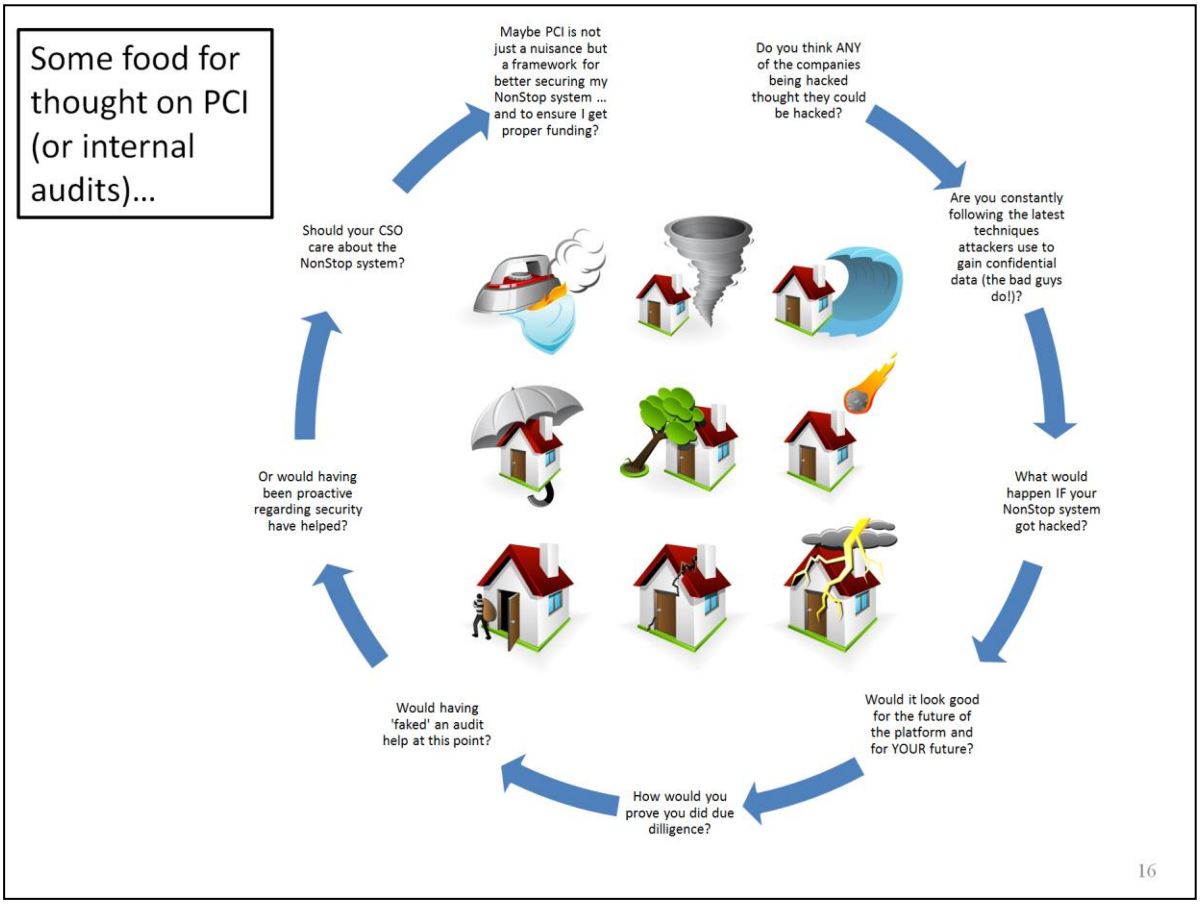


Nightmare on PCI street???

15

How do you view PCI – left or right?

Thomas Burg has written a ‘short story’ called “Nightmare on PCI street” about this which is appearing in the current issue of The Connection – we’ll hand it out now so you can read it afterwards. Point in case: do get your CSO involved. From a risk management perspective, the NonStop systems should certainly NOT be overlooked…



Some food for thought on PCI (or internal audits)…

Maybe PCI is not just a nuisance but a framework for better securing my NonStop system … and to ensure I get proper funding?

Do you think ANY of the companies being hacked thought they could be hacked?

Are you constantly following the latest techniques attackers use to gain confidential data (the bad guys do!)?

What would happen IF your NonStop system got hacked?

Would it look good for the future of the platform and for YOUR future?

How would you prove you did due dilligence?

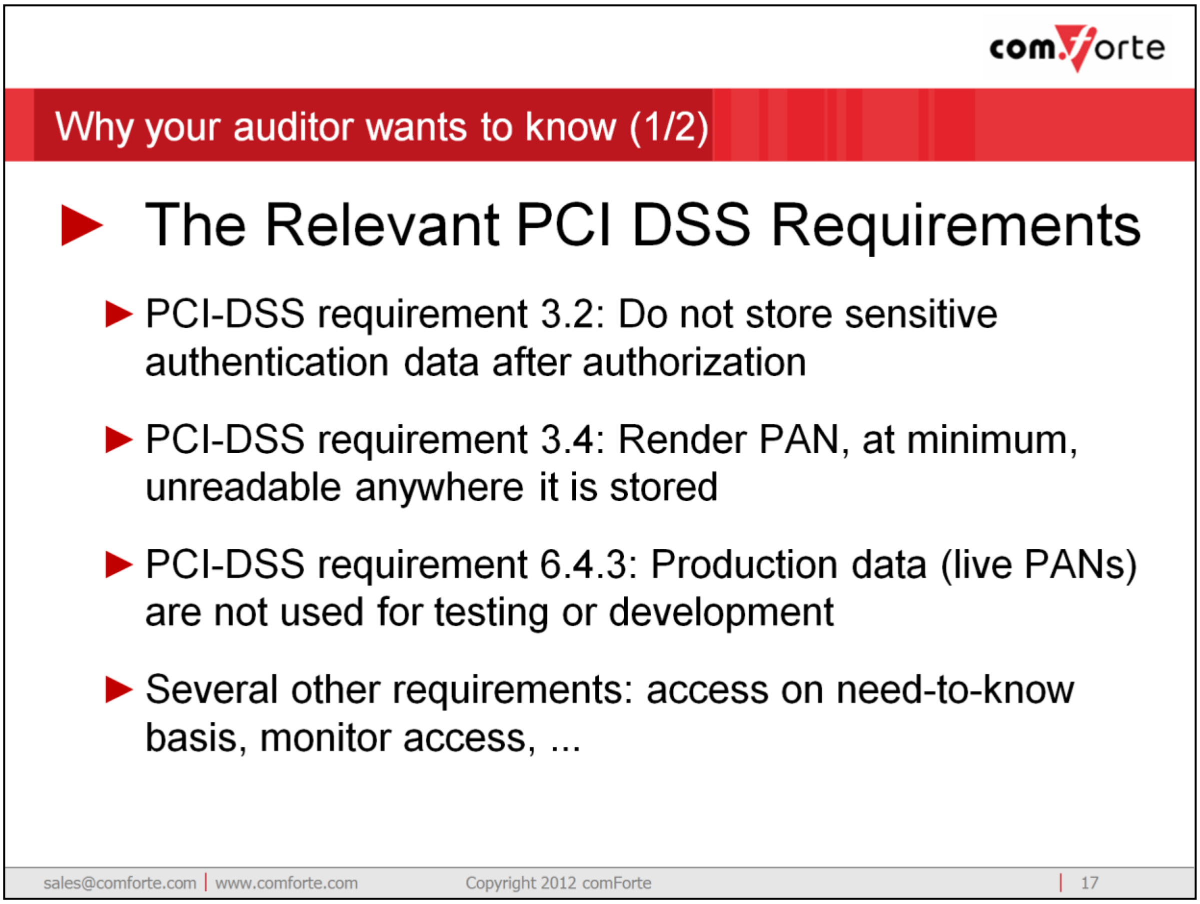
Would having 'faked' an audit help at this point?

Or would having been proactive regarding security have helped?

Should your CSO care about the NonStop system?

The icons in the center depict a couple of insurances each and every one of us most probably has for his house. How likely is a tornado destroying your house? Or lightning striking it?

But: Do you have a fire insurance?



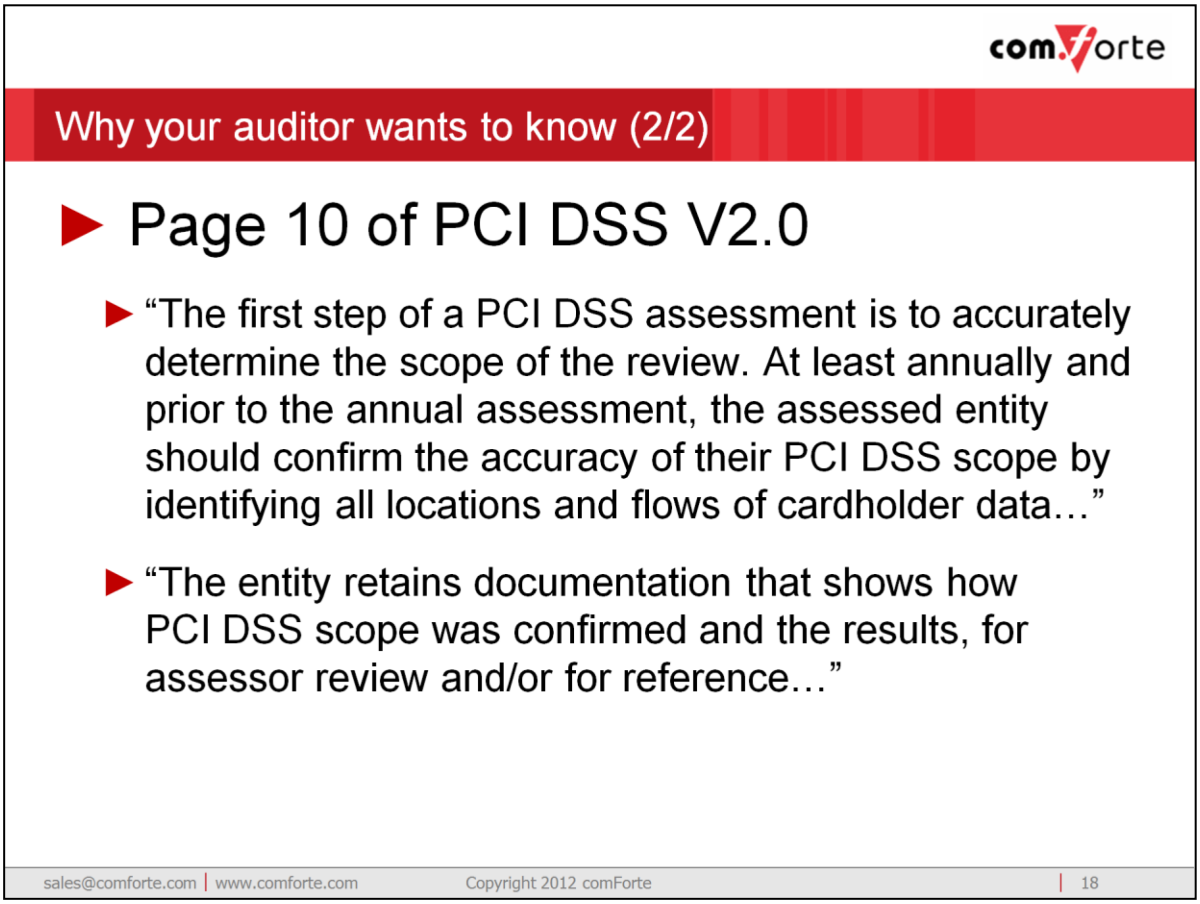
Why your auditor wants to know (1/2)

The Relevant PCI DSS Requirements

- PCI-DSS requirement 3.2: Do not store sensitive authentication data after authorization
- PCI-DSS requirement 3.4: Render PAN, at minimum, unreadable anywhere it is stored
- PCI-DSS requirement 6.4.3: Production data (live PANs) are not used for testing or development
- Several other requirements: access on need-to-know basis, monitor access, ...

sales@comforte.com | www.comforte.com Copyright 2012 comForte | 17

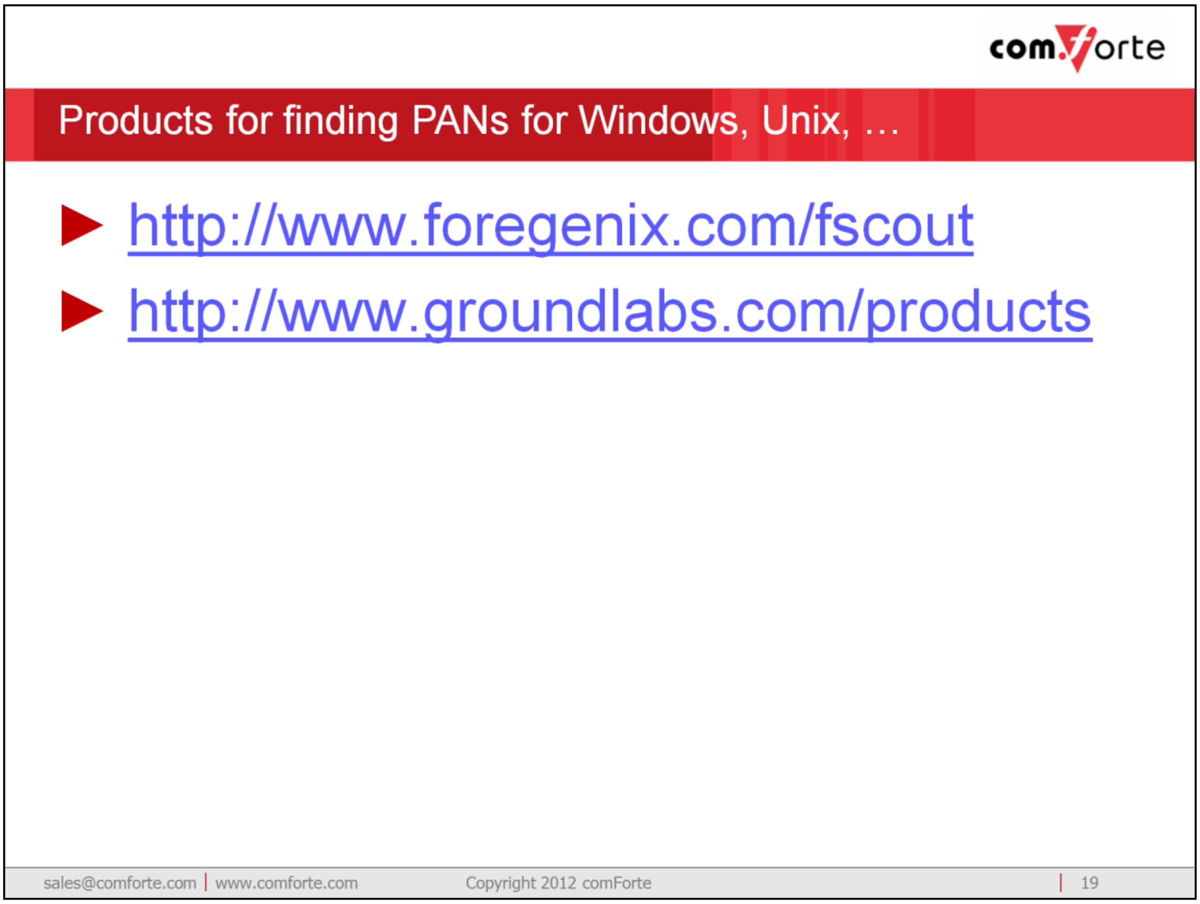
Having discussed PCI a bit and –maybe- having established that it is there to protect your NonStop system from the unlikely; here is some verbiage in the standard which makes it clear that you need to have a good grip where exactly your credit card data is: Unless you know, how can you implement the action items above?



Why your auditor wants to know (2/2)

- Page 10 of PCI DSS V2.0
  - “The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data…”
  - “The entity retains documentation that shows how PCI DSS scope was confirmed and the results, for assessor review and/or for reference…”

Before even talking about specific “line items”, the PCI standard provides guidance about how to properly identify files containing critical data.



Products for finding PANs for Windows, Unix, …

- http://www.foregenix.com/fscout
- http://www.groundlabs.com/products

There are a couple of products for non-NonStop platforms which support ‘searching for PANs’. However, NonStop is not supported by any of these products…

What would an ideal tool to "find all files containing credit card numbers on NonStop systems" be characterized by?

does not impact CPU usage

provides meaningful results

is FAST

can be configured for my specific needs

is powerful

does not create a PCI violation itself

Introducing PANfinder!

does not impact CPU usage

- can be configured to use all available CPU or to always stay at a low CPU usage
- several parameters for fine-tuning

provides meaningful results

- minimizes "false positives" (file not containing real PANs is marked as containing PANs)
- minimizes "false negatives" (file containing real PANs is not found)

is FAST

- Summary scans stop after 'X' PANs found
- Use of change detection monitoring
- Configurable Include/Exclude wild carded file sets
- Re-run file list

can be configured for my specific needs

- i.e. credit card prefixes I actually use

is powerful

- Searches multiple file formats (Enscribe, SQL/MP)
- Searching of open and locked files
- Configurable resource utilisation (maximum scan speed v minimum system impact)
- Scheduled searches (Netbatch)
- Syslog output, SIEM/enterprise logging solution integration (Arcsight, RSA enVision etc.)

does not create a PCI violation itself

- PCI-DSS compliant reports (suspected PANs are appropriately masked)

➡ PANfinder was build against all these specs

➡ See http://www.comforte.com/products/protect/panfinder/ for details

Real-life story …

… this morning I presented PANfinder to …. In short, it went really well. First off I did a short overview presentation and answered a few questions from …, then I installed the software on one of their development machines and ran a demo for them i.e. Initial PANfinder run against the sample files we ship.

I then suggested we run it against some of their application logs which we know contain unprotected PAN data, just to see what we would find. … included her personal subvol as well as one of the log subvols. It couldn't have been planned any better. In her personal subvol was a Connex log file from 2009 that contained PAN data!!!

Highlighted perfectly that PANs could be located anywhere, not just where you would expect to find them. The scan also returned zero false positives so it was good all round.

Summary

▶ I know exactly where my credit card data is?	▶ *Are you sure???*
▶ My auditor wants proof where my credit card data is?	▶ *We think so!*
▶ SecurData can provide secure yet realistic test data based on production data	▶ *Absolutely yes*
▶ PANfinder assists in finding credit card data ➡ Giving correct and complete results ➡ Satisfying your auditor	▶ *Absolutely yes*

End of slides

Thank you for your interest,
any questions please send sales@comforte.com or
t.burg@comforte.com