Three Real-World Scenarios That Impact PCI Compliance

Presenters:

Rob Chapman

Director, Information Security - Cybera

CONEXXUS

solve forward

Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

Housekeeping

This webinar is being recorded and will be made available in approximately 7 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions
- Our webinars may be used toward PCI continuing education credits. Please contact arussell@conexxus.org for questions regarding a certificate of webinar attendance.

Email: **info@conexxus.org**

CONEXXUS
solve forward

Presenters

Conexxus Host

Allie Russell
Standards Coordinator
Conexxus
arussell@conexxus.org

Moderator

Kara Gunderson
Chair, Data Security Committee
POS Manager, CITGO Petroleum
kgunder@citgo.com

Speakers

Rob Chapman
Director, Information Security
Cybera
rob.chapman@cybera.net

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy

CONEXXUS
solve forward

2020 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
January 23, 2020	How to elevate your business through digital transformation	Dean Marier	Cybera
February 27, 2020	Progress in the “API Sprint”	Gray Taylor David Ezell	Conexxus Conexxus
March 18, 2020	Data Security Beyond PCI: Securing the Enterprise	Ed Adams Marc Punzirudu Kara Gunderson Sam Pfanstiel	Security Innovation ControlScan CITGO Petroleum ControlScan
April 2, 2020	Presentation by GS1	Liz Sertl	GS1
May 7, 2020	Breach response considerations for the convenience store and petroleum market	Todd McClelland	McDermott Will & Emery
July 16, 2020	How PCI Security Council Is Responding to COVID-19	Troy Leach	PCI SSC
July 30, 2020	Managed Network Service Providers: What you need to know		Joint MNSP’s

CONEXXUS
solve forward

2020 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
August 27, 2020	How an Attacker Bypasses Network, Software & Physical Controls	Jeff Gibson Geoffrey Vaughan	ControlScan Security Innovation
September 24, 2020	Lessons Learned with IoT API Integration	Scott Cheek	SageNet
October 22, 2020	Ransomware Protection and how a Managed Security Service Provider can help Oil & Gas Retailers from being the next target	Ajith Edakandi	Hughes Network
November 12, 2020	Three Real-World Scenarios That Impact PCI Compliance	Rob Chapman	Cybera
December 3, 2020	EMV: A Focus on 3rd Party Retrofit Kits	Dan Harrell Bill Pittman Dan Witkemper	Invenco Sound Payments Gilbarco
January 2021	Securely Connecting Third-Party Vendors	Simon Gamble	Mako Networks
February 2021	A Step-by-Step approach to Automating Security Response in a Multi-Vendor Environment	Ash Swamy Robert Hicks	Omega

CONEXXUS
solve forward

Thank you to our 2020 Diamond Sponsors

Three Real-World Scenarios That Impact PCI Compliance

Presenters:

Rob Chapman

Director, Information Security - Cybera

CONEXXUS

solve forward

First Things First

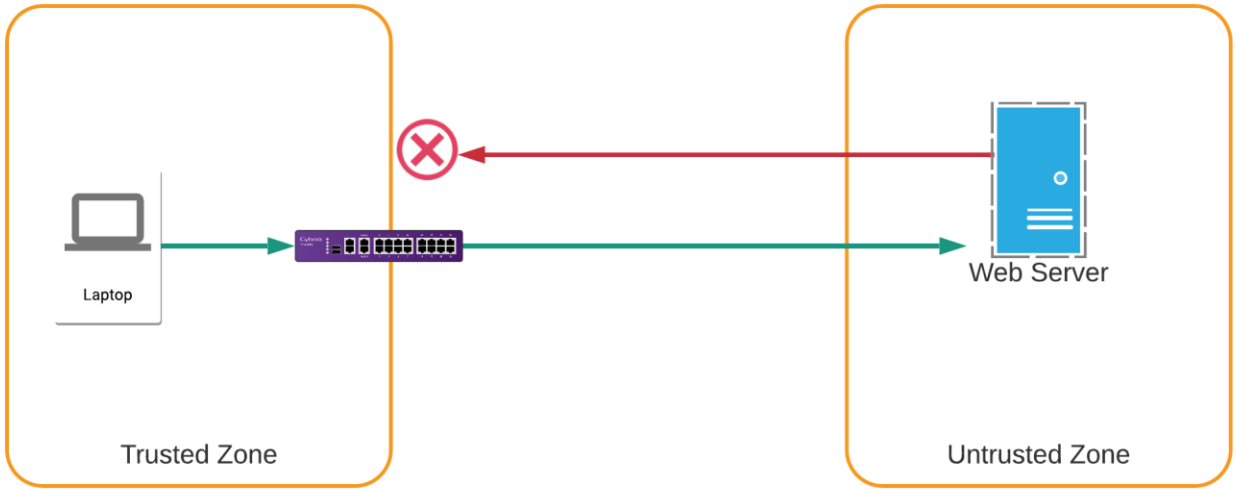
PRIORS AND OPINIONS

EXPECTATIONS AND CONCERNS

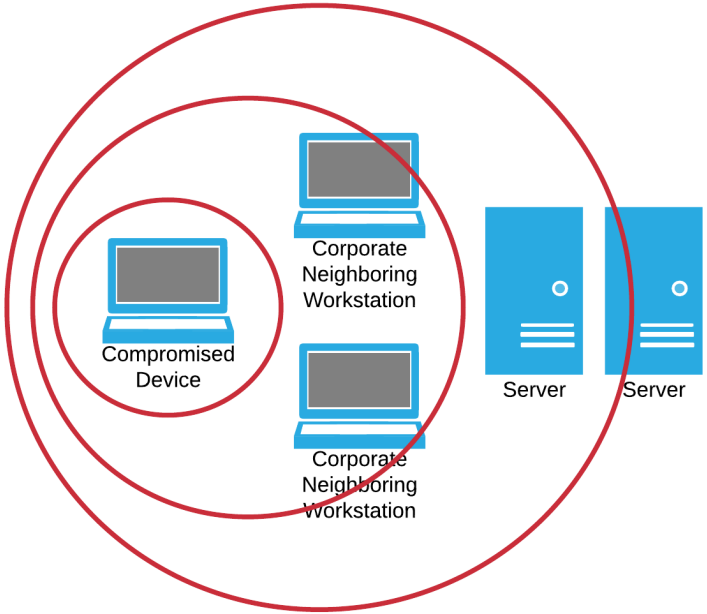
IMPORTANT MENTAL MODELS

CONEXXUS solve forward

Trust and Untrust Zone



Blast Radius



Three Scenarios

- The Value of Penetration Testing
- The Impact of IoT on PCI Scoping
- Better Security with ATG monitoring

Validating What We Know

"Just because a system is not in scope for PCI DSS, it doesn't mean the entity should leave that system unprotected, as it could still pose a risk to the entity's network and business. A common pattern seen in data breaches is where the attacker targets systems deemed by the entity to be out-of-scope for PCI DSS, then leverages those systems to gain access to more systems, which eventually provide a path to systems where CHD data can be found."

- Guidance for PCI DSS Scoping and Network Segmentation

Validating What We Know

A FRIEND GETS OWNED (STORY)

Validating What We Know

- Outcomes-Based Approach
- Penetration Testing vs. Vulnerability Scanning
- Real-World Modeling
- Modern Threats and Attacks

When it comes to scoping for PCI DSS, the best-practice approach is to start with the assumption that everything is in scope until verified otherwise.

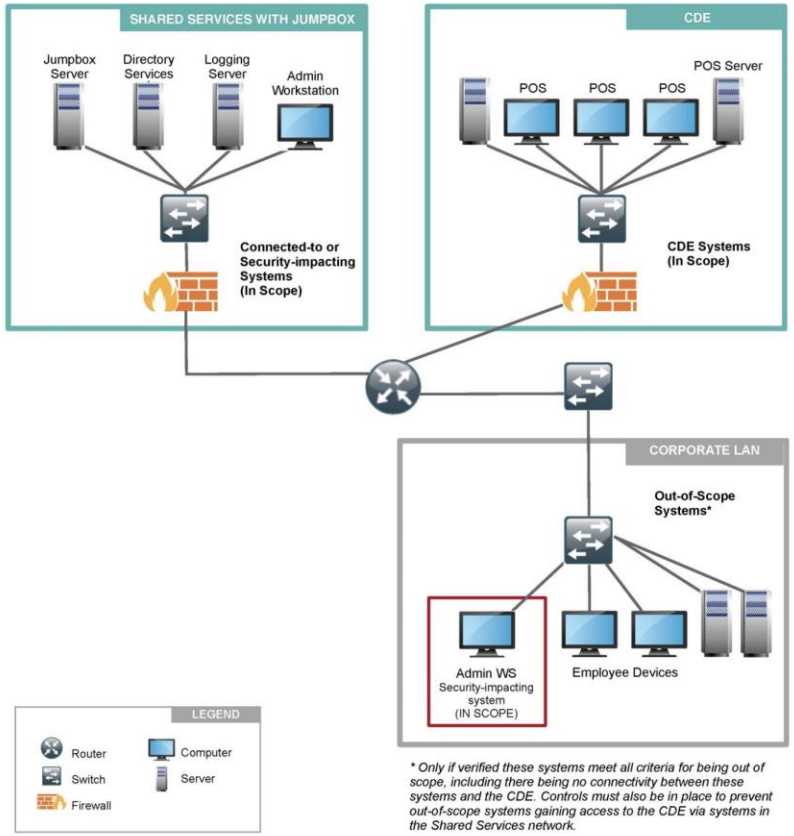
IoT in the Card Data Environment

SCOPING (STORY)

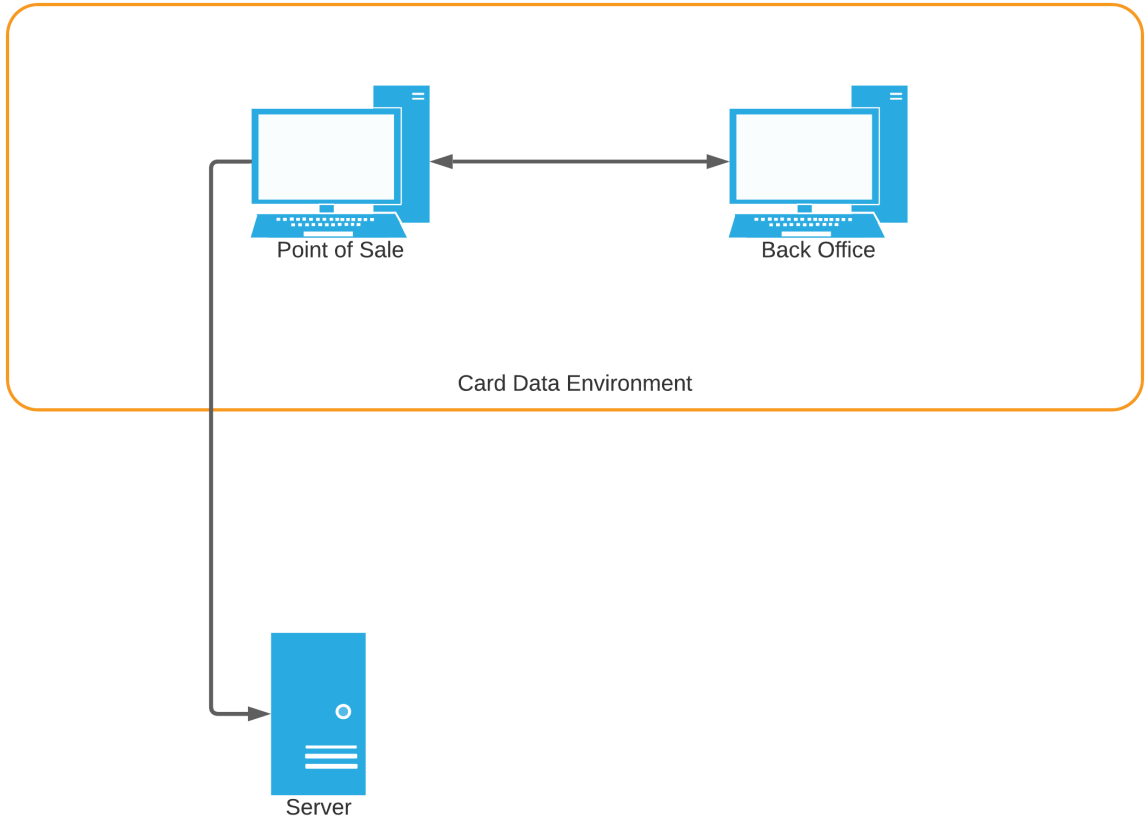
Systems with connectivity or access to or from the CDE are considered “connected-to” systems. These systems have a communication path to one or more system components in the CDE. Connectivity may occur over physical, wireless, and virtualized technologies.

Physical connectivity may be via a traditional network (for example, Ethernet or power-line communication) or direct system-to-system connection (for example, USB, component, etc.).

Scenario 2

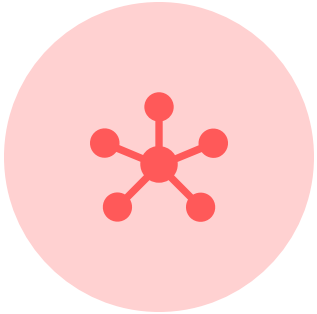


** Only if verified these systems meet all criteria for being out of scope, including there being no connectivity between these systems and the CDE. Controls must also be in place to prevent out-of-scope systems gaining access to the CDE via systems in the Shared Services network.*


Point of Sale
Back Office
Card Data Environment
Server

What Can We Do

BETTER COMMUNICATION AND DOCUMENTATION



BETTER PLATFORM UNDERSTANDING

BETTER DESIGN

CONEXXUS solve forward

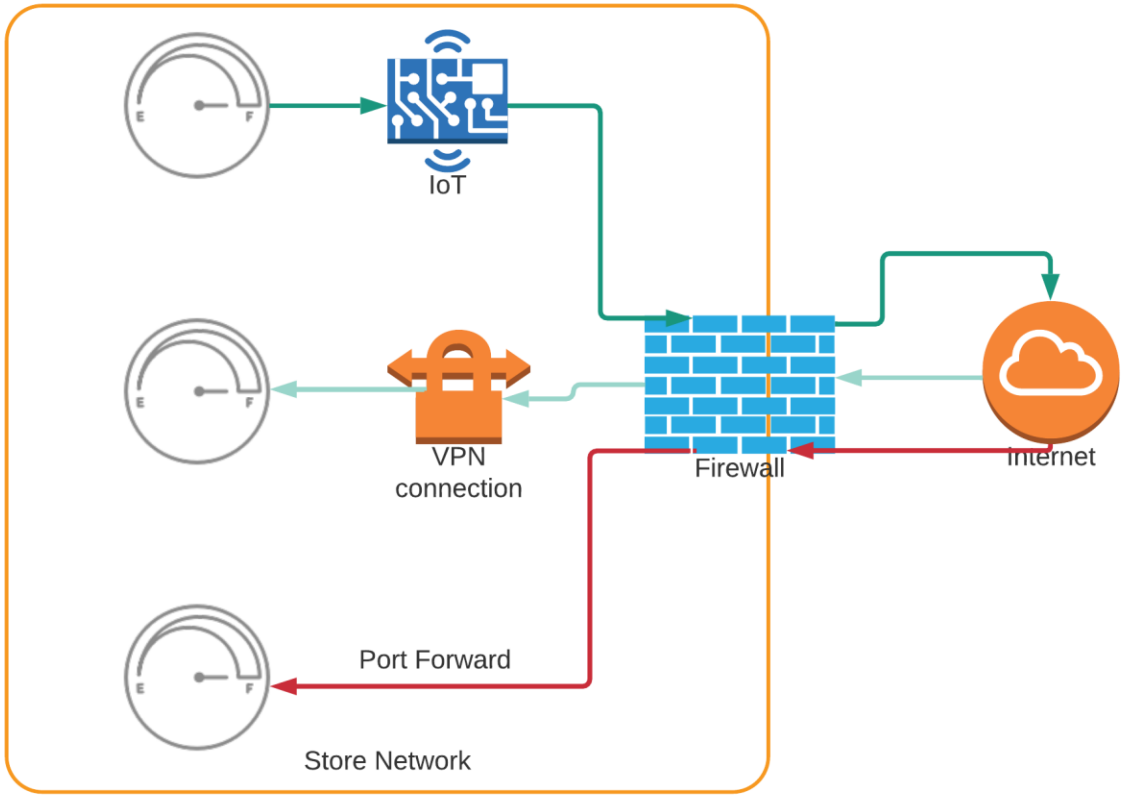
Securing ATGs on the Edge

ATG MONITORING

I20100
10/29/20 10:12 AM

IN-TANK INVENTORY

TANK	PRODUCT	VOLUME	TC-VOLUME	ULLAGE	HEIGHT	WATER	TEMP
1	REGULAR	15850	0	4101	87.78	0.00	53.54
2	PRMIUM	2794	0	3314	55.68	0.00	52.94
3	E-85	2500	0	3608	51.12		58.93
4	DIESEL	1852	0	4256	40.84	0.00	60.31


IoT
VPN
connection
Firewall
Internet
Port Forward
Store Network

How Do We Improve

- Move Away from Firewall Port-Forwards
- Design for Trust-to-Untrust Data Flow
- Validate What We Know

CONEXXUS
solve forward

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Profile: Conexxus.org
- Follow us on Twitter: @Conexxusonline

DISCLAIMER: Conexxus does not endorse any products or services that may be described or mentioned in this presentation. The views and opinions expressed in this presentation are solely those of the speakers and not of Conexxus. By hosting this webinar, Conexxus is not providing any legal advice; if you have any questions about legal issues raised or discussed, you should seek the assistance of attorneys who are competent in that area.