Inside the Standard

John Elliott
PAYMENTS, SECURITY, PRIVACY AND RISK SPECIALIST

@withoutfire www.withoutfire.com

And Those Requirements Are

Security Standards Council

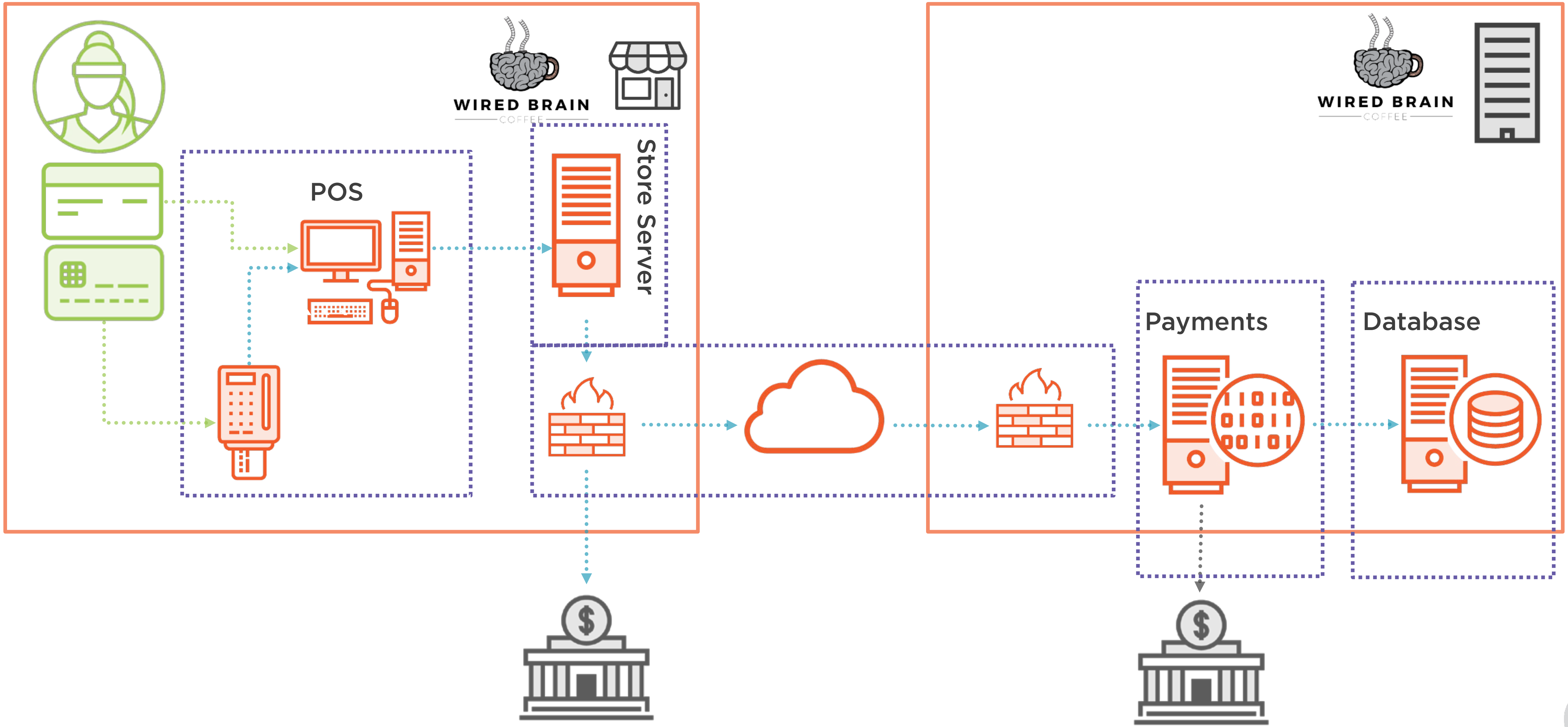
Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures

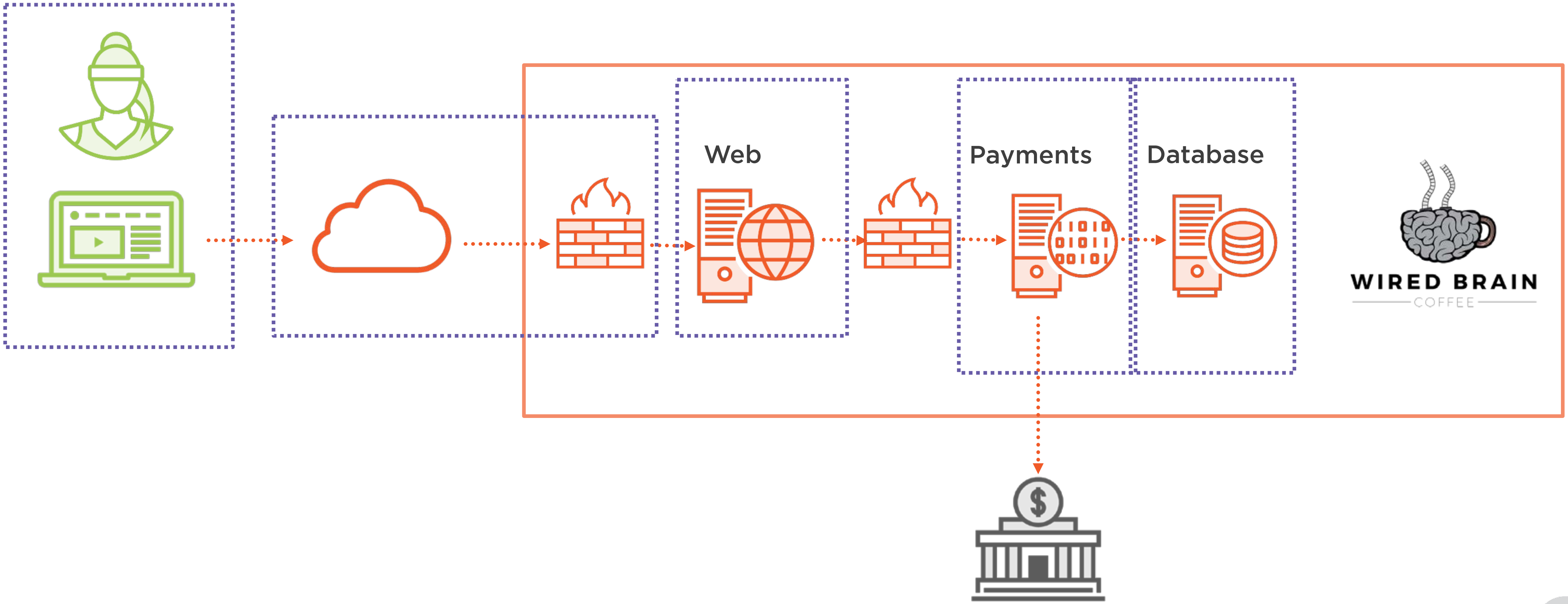
Version 3.2
April 2016

1. Have firewalls
2. No defaults
3. Protect stored data
4. Encrypt transmissions
5. Use anti-virus
6. Secure apps and OSes
7. Restrict access
8. Identify and authenticate
9. Physical protection
10. Log and monitor
11. Test security
12. Have policies

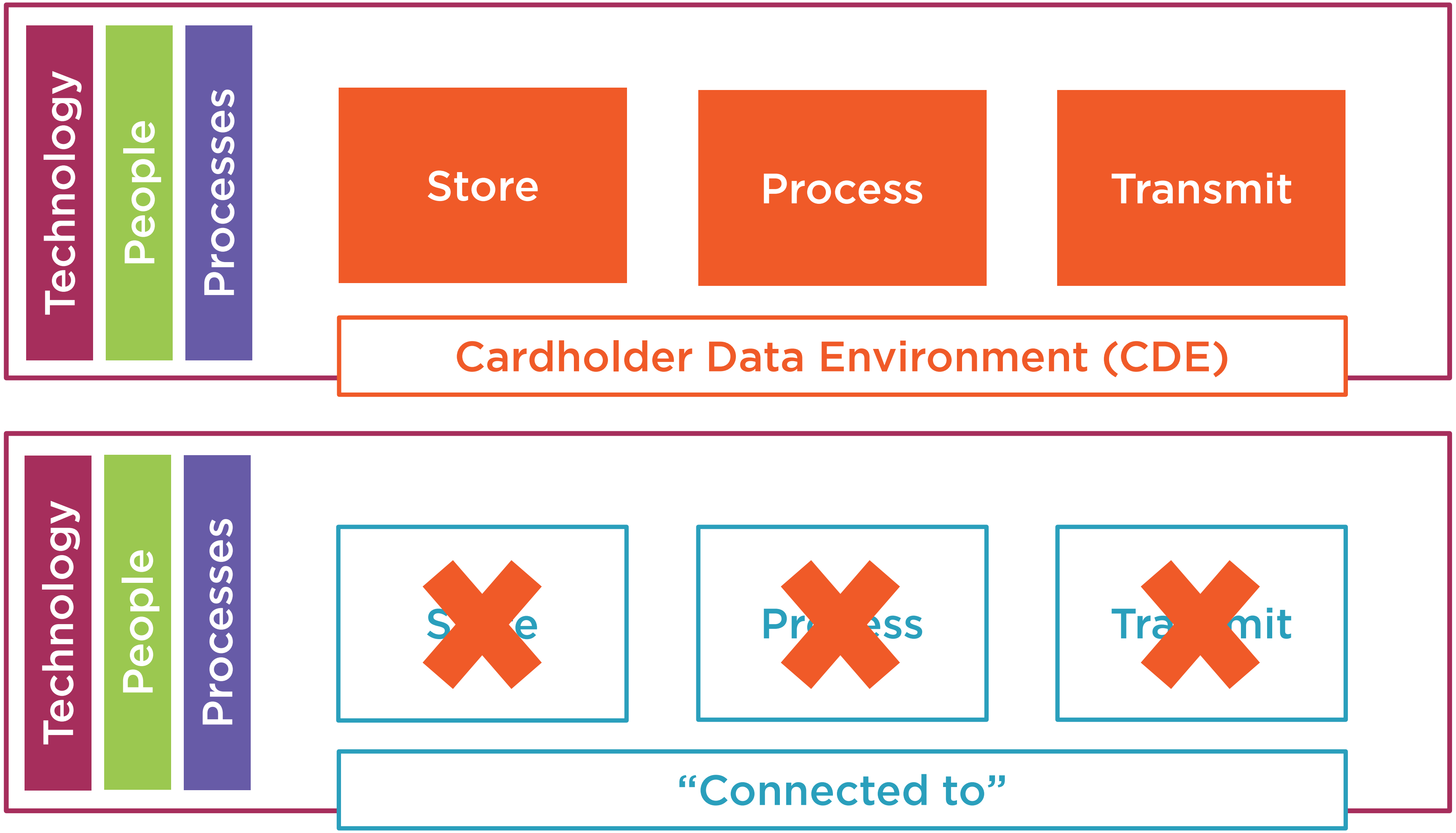
Face to Face Example



E-commerce Example



Scope of Requirements



Technology

People

Processes

Store

Process

Transmit

Cardholder Data Environment (CDE)

Technology

People

Processes

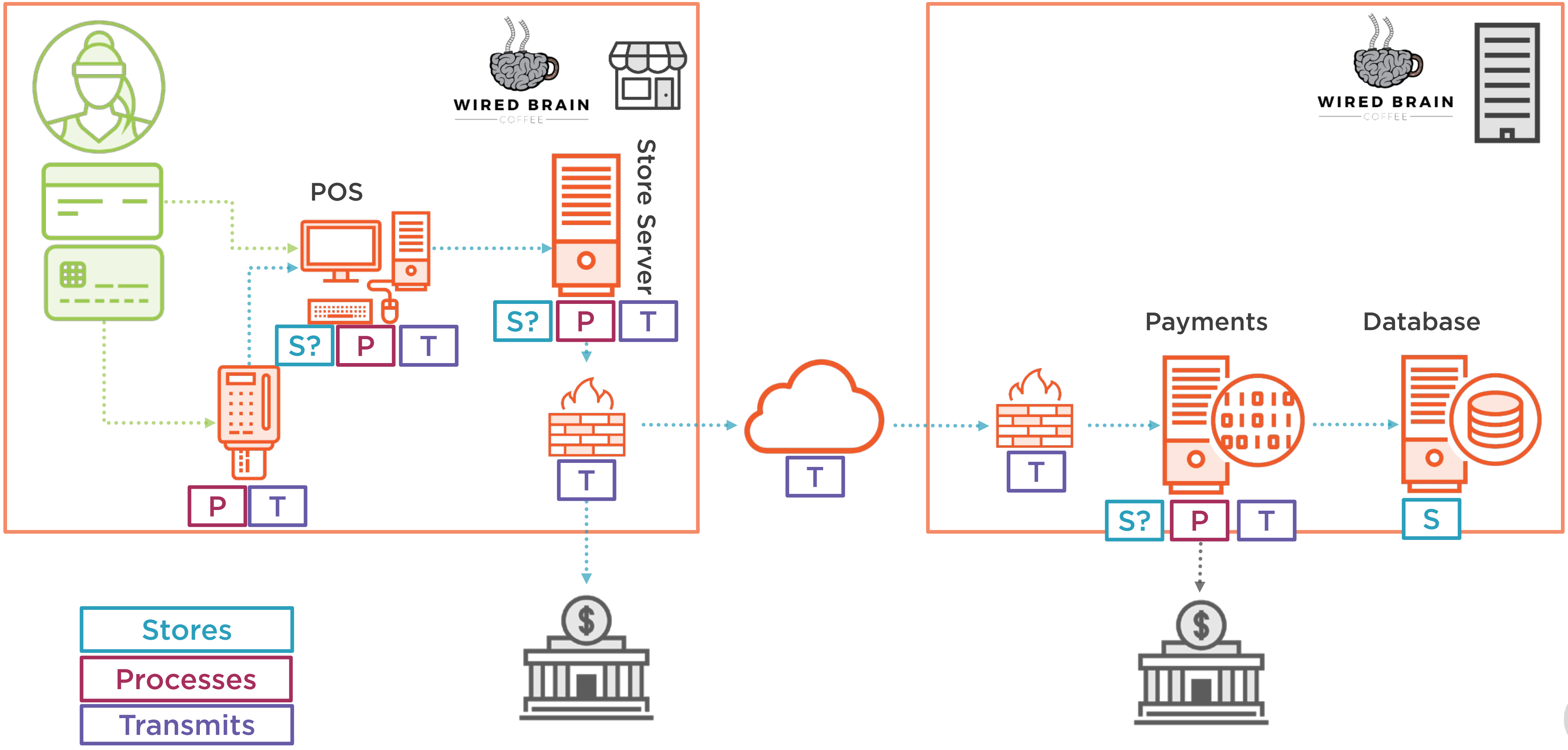
~~Store~~

~~Process~~

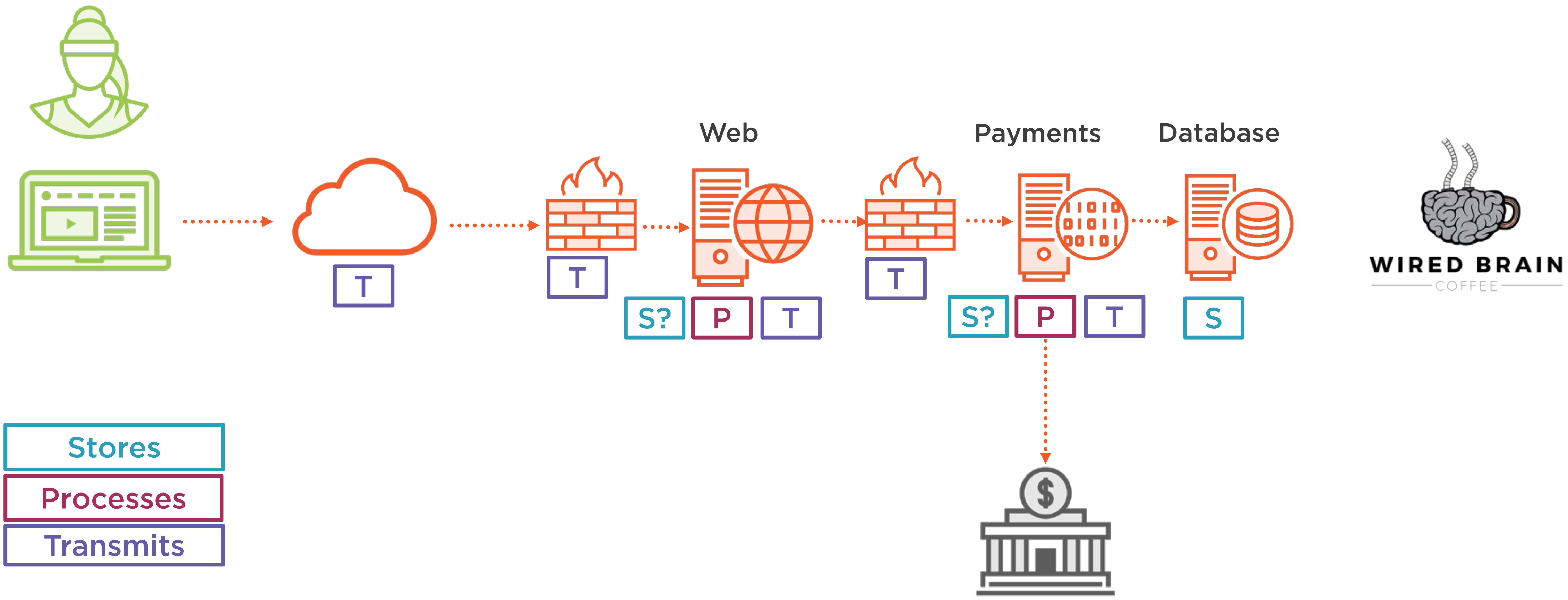
~~Transmit~~

"Connected to"

What's in Scope of the Requirements?



What’s in Scope of the Requirements?

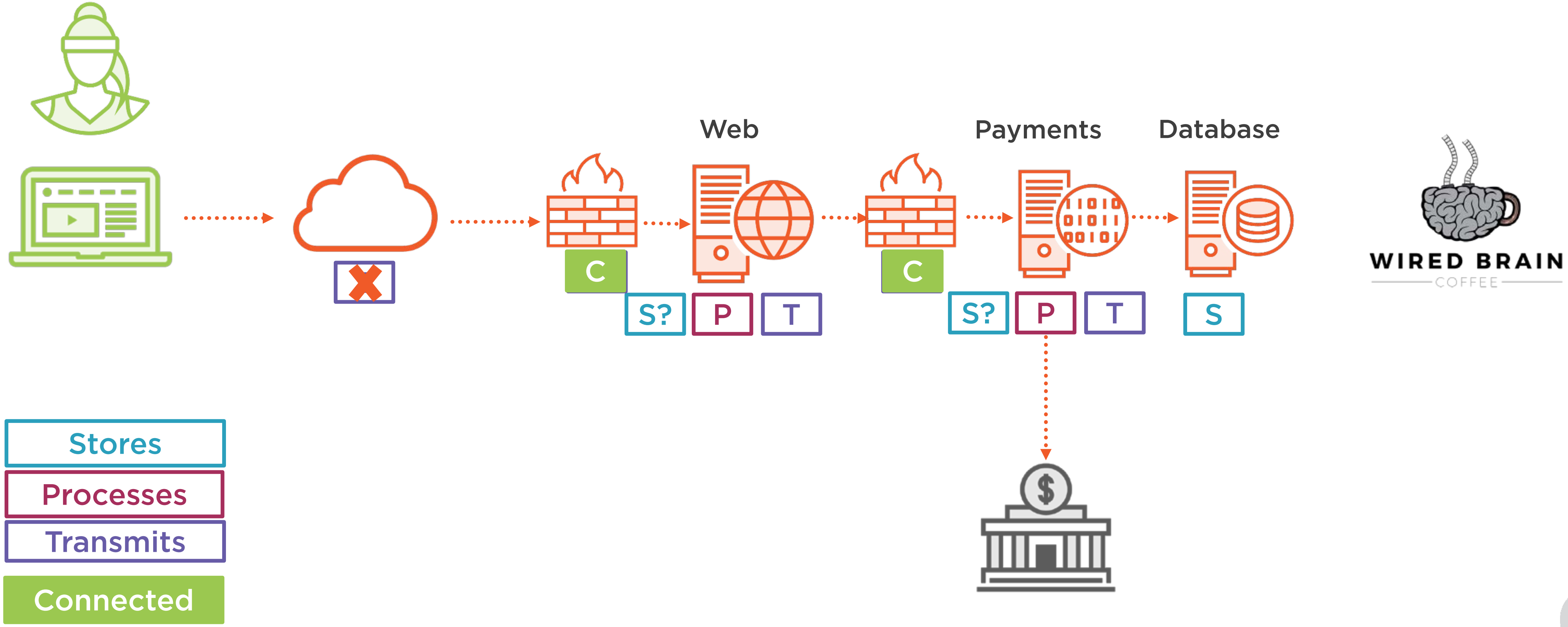


Stores

Processes

Transmits

But Encryption



Quick Look at All Twelve

Security Standards Council

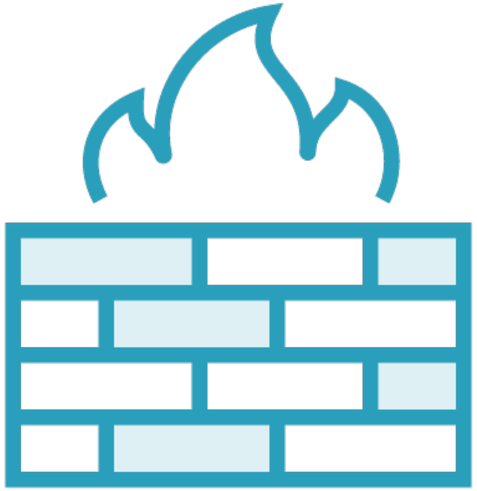
Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures

Version 3.2
April 2016

1. Have firewalls
2. No defaults
3. Protect stored data
4. Encrypt transmissions
5. Use anti-virus
6. Secure apps and OSes
7. Restrict access
8. Identify and authenticate
9. Physical protection
10. Log and monitor
11. Test security
12. Have policies

1. Install and Maintain a Firewall Configuration to Protect Cardholder Data



Have configuration standards for firewalls

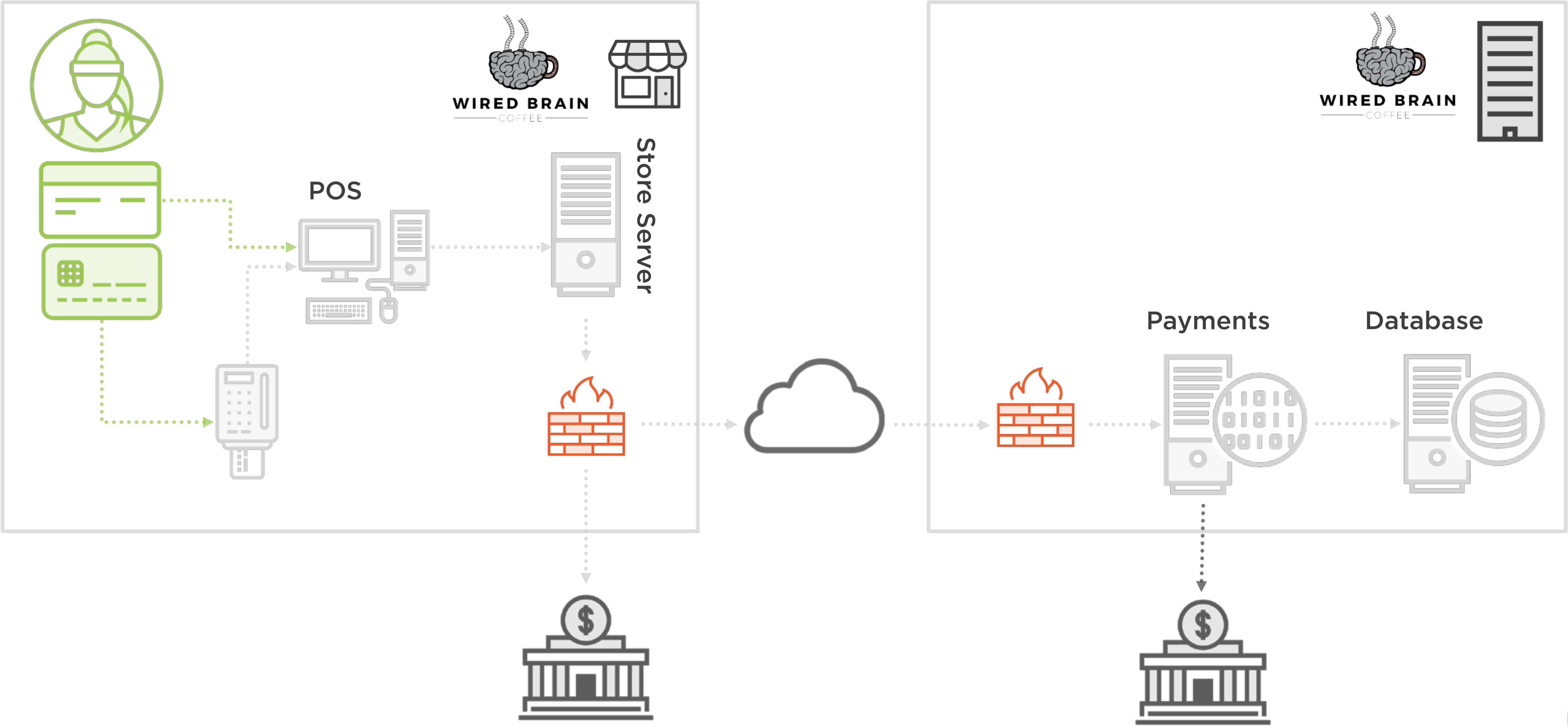
Build and configure firewalls properly

Make all traffic go through a firewall (ie not a direct connection to the internet)

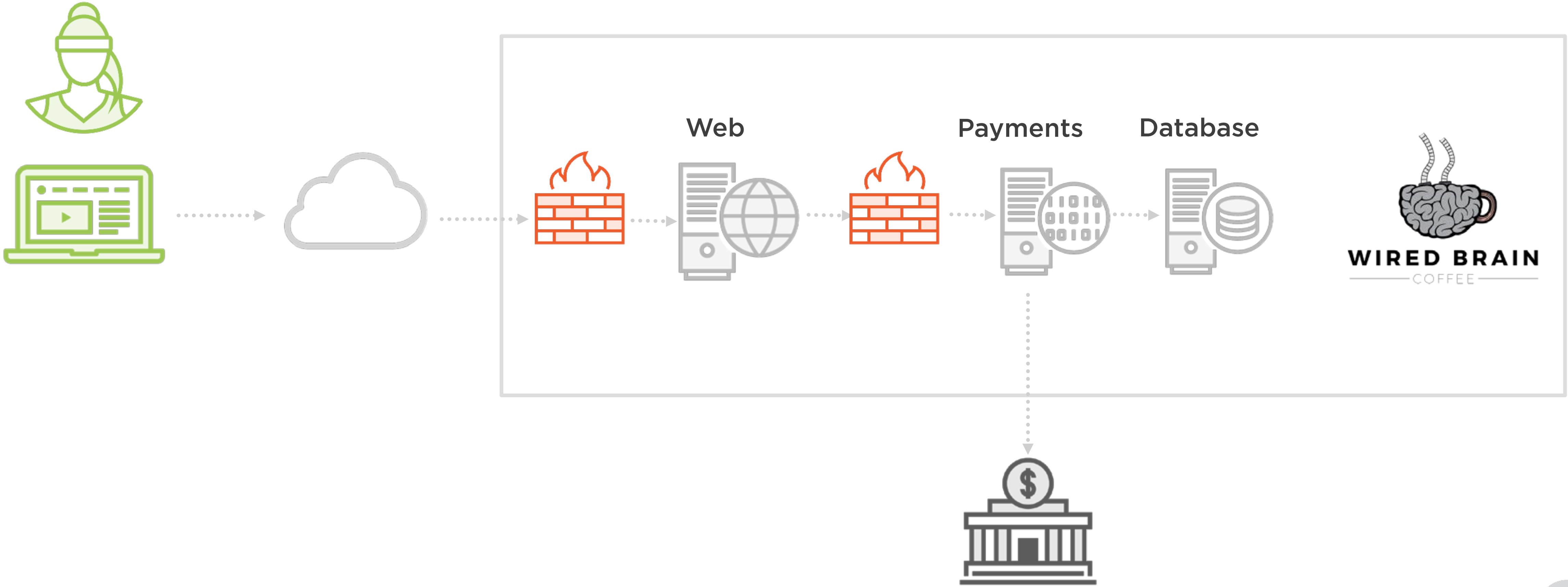
Put personal firewalls on devices

Have written policies for this

1. Have Firewalls



1. Have Firewalls



2. Do Not Use Vendor-supplied Defaults for System Passwords and Other Security Parameters

admin

Change default credentials

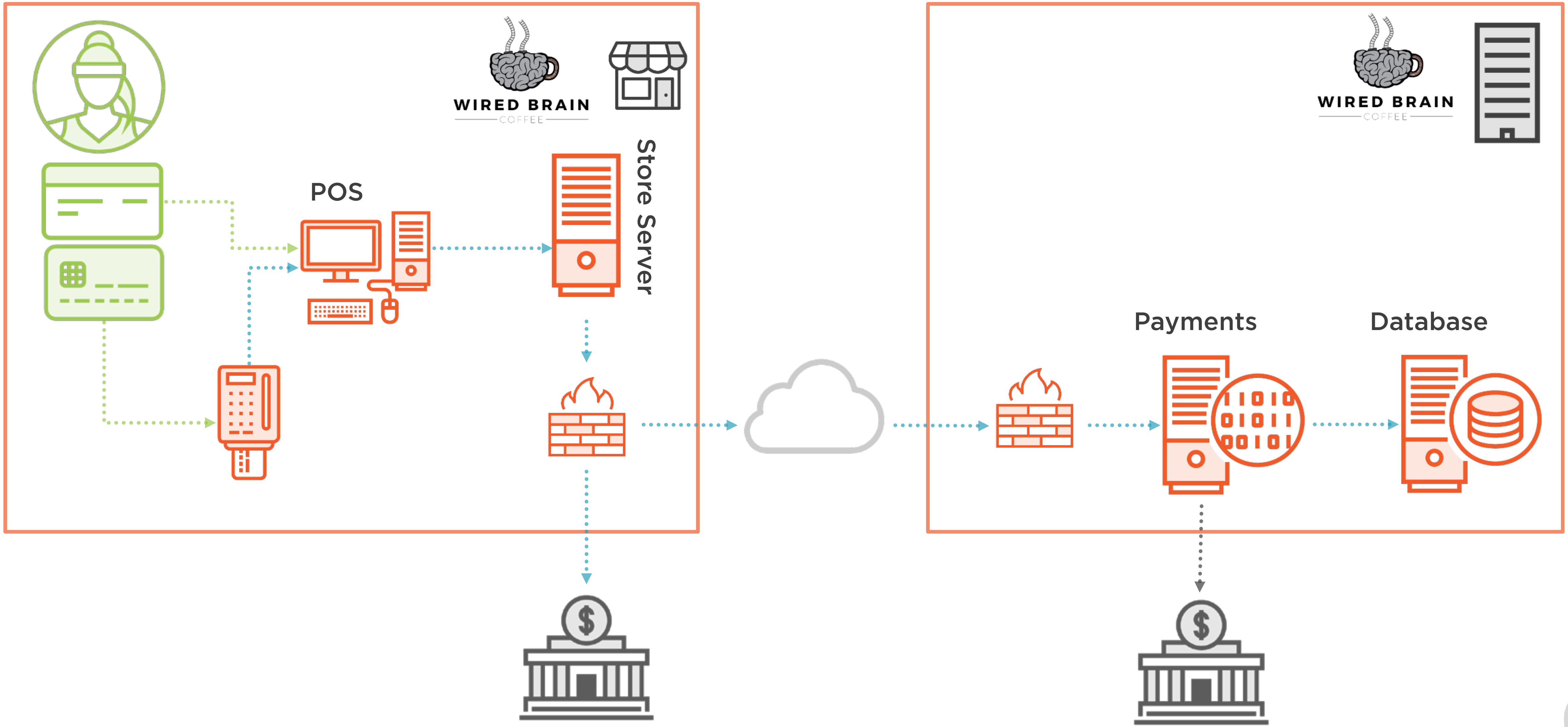
Have secure (hardened) builds that only enable what’s needed

Encrypt non-console access

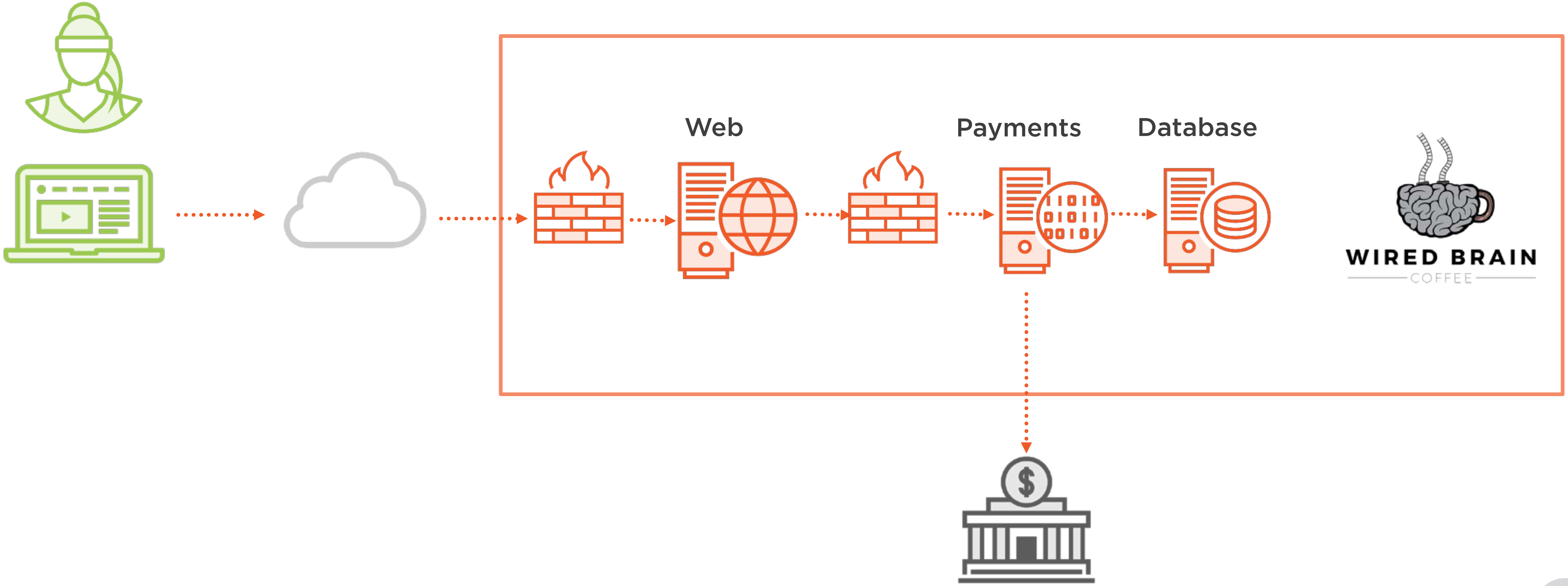
Keep an inventory

Have policies for this

2. No Defaults



2. No Defaults



3. Protect Stored Cardholder Data

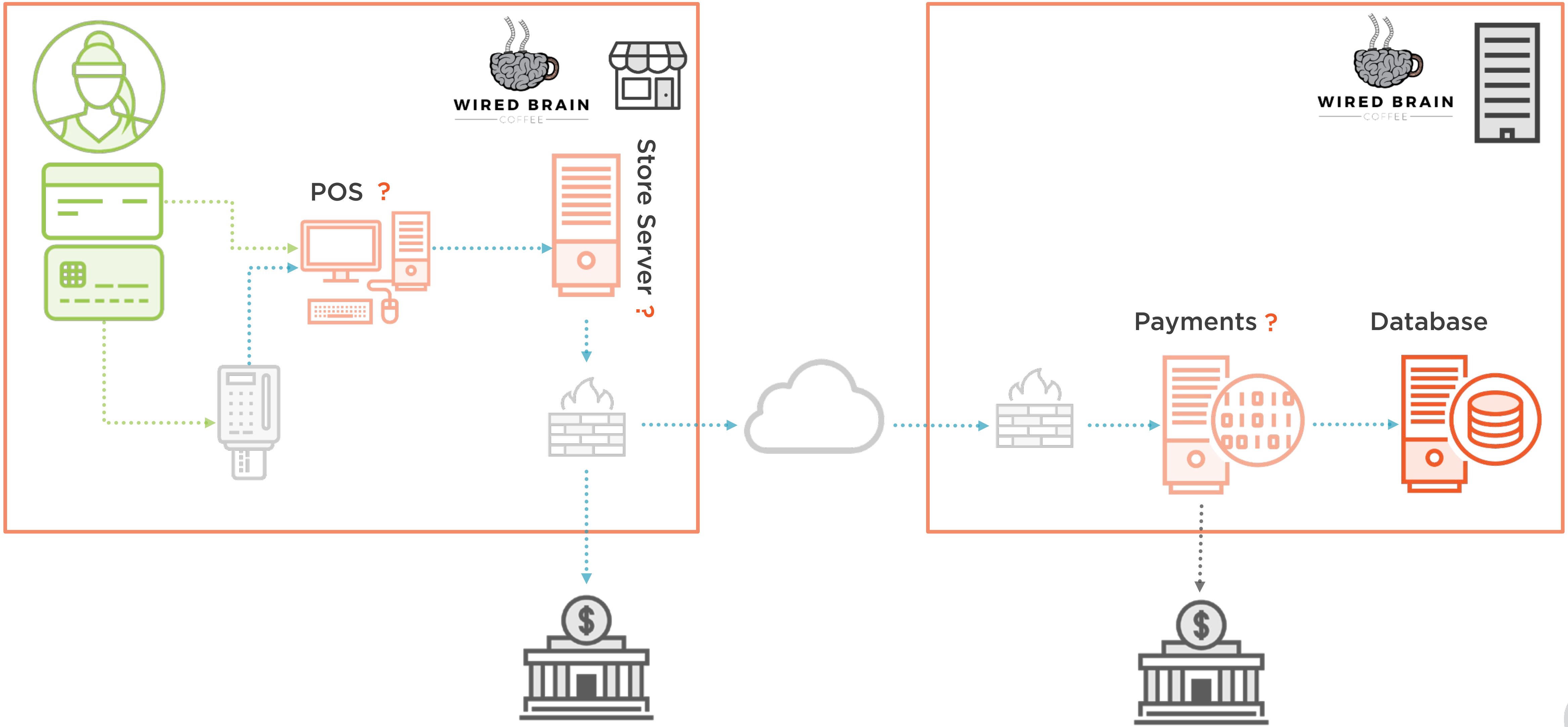
Retain only minimal cardholder data

Don’t store plaintext cardholder data

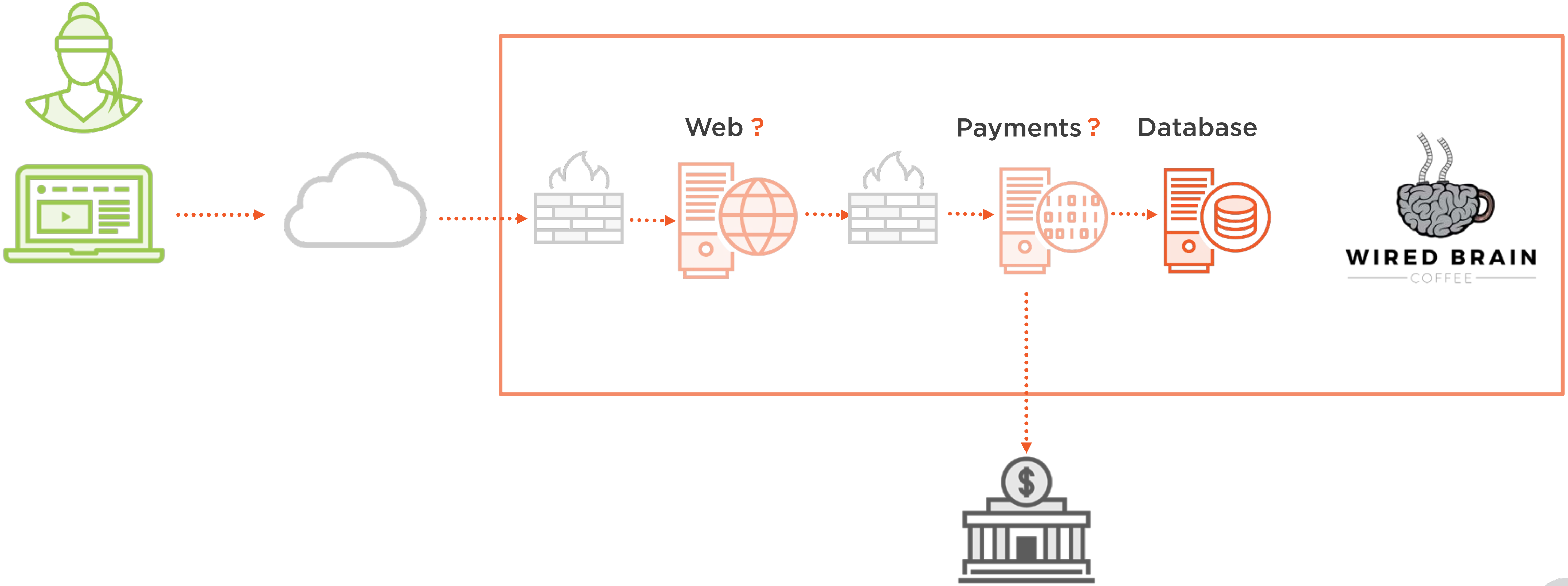
Never store track data, CVV2 or PINs

Do encryption properly

3. Protect Stored Data



3. Protect Stored Data



4. Encrypt Transmission of Cardholder Data Across Open, Public Networks

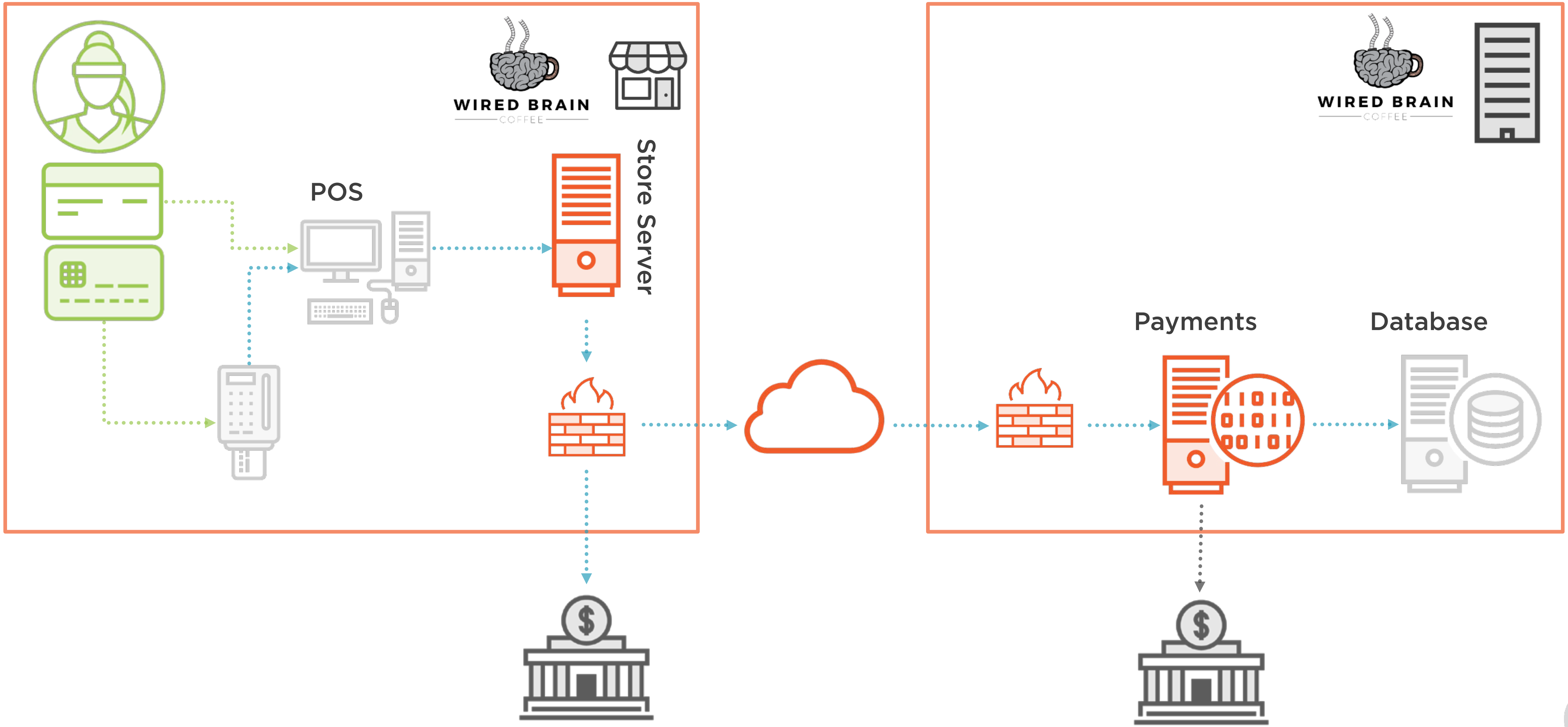
Accept and send cardholder data using strong cryptography

Move away from SSL and TLS 1.0

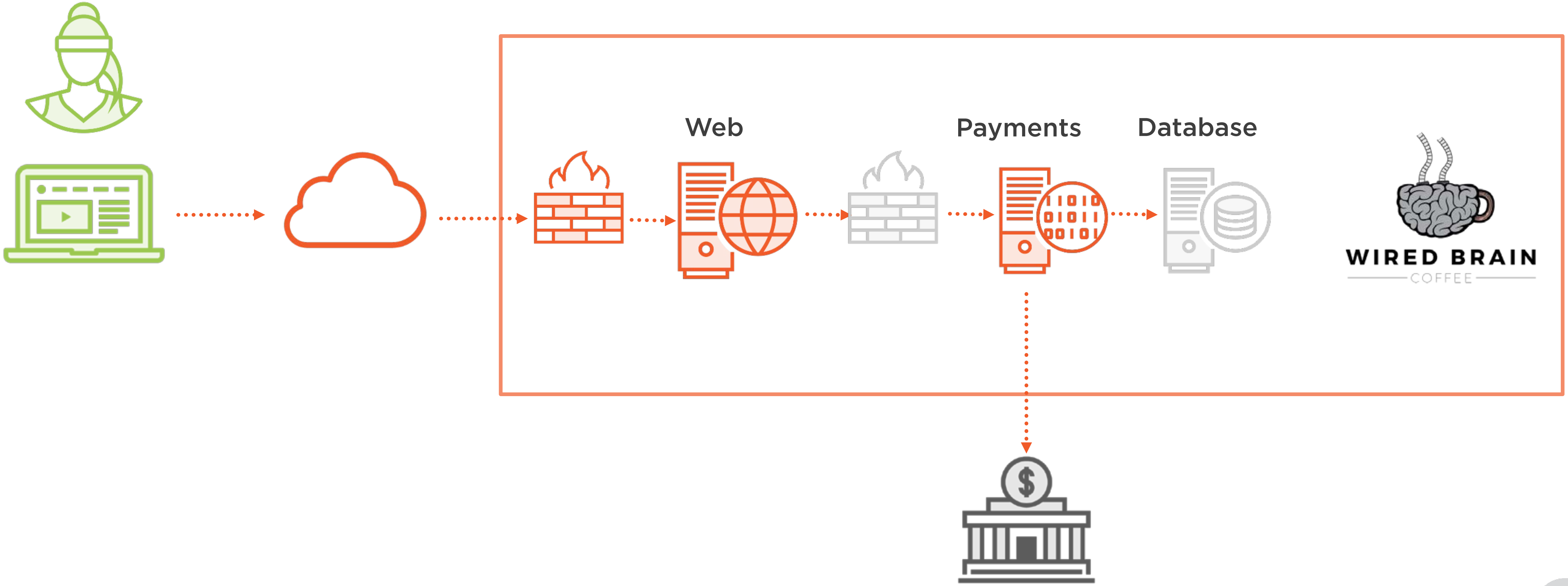
Don’t send cardholder data via email, IM, and other messaging channels

Have policies for all of this

4. Encrypt Transmissions on Public Networks



4. Encrypt Transmissions on Public Networks



5. Protect All Systems Against Malware and Regularly Update Anti-virus Software or Programs

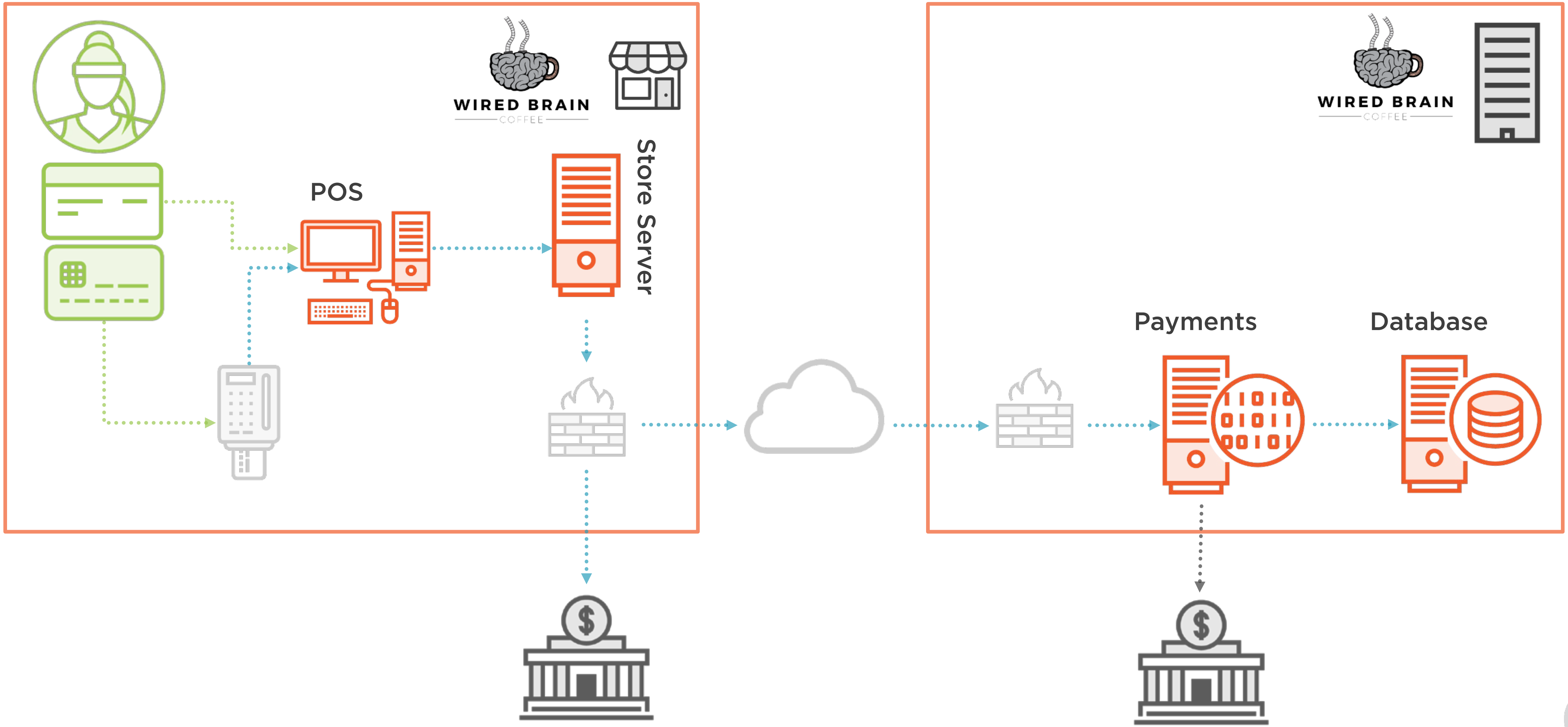
Have operational anti-virus software (please use anti-malware)

Keep the AV logs

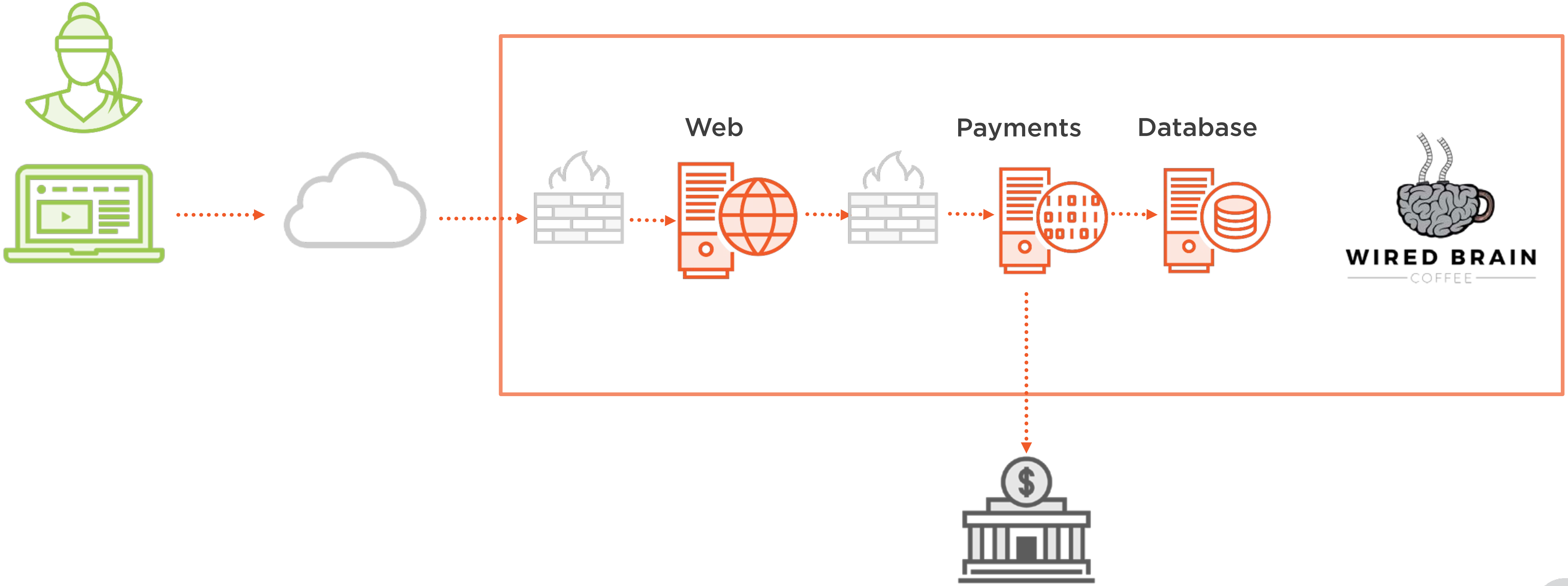
Don’t let people disable AV

Have policies for all of this

5. Use Anti-virus



5. Use Anti-virus



6. Develop and Maintain Secure Systems and Applications

Track published vulnerabilities for all your software: applications and OS

Patch regularly

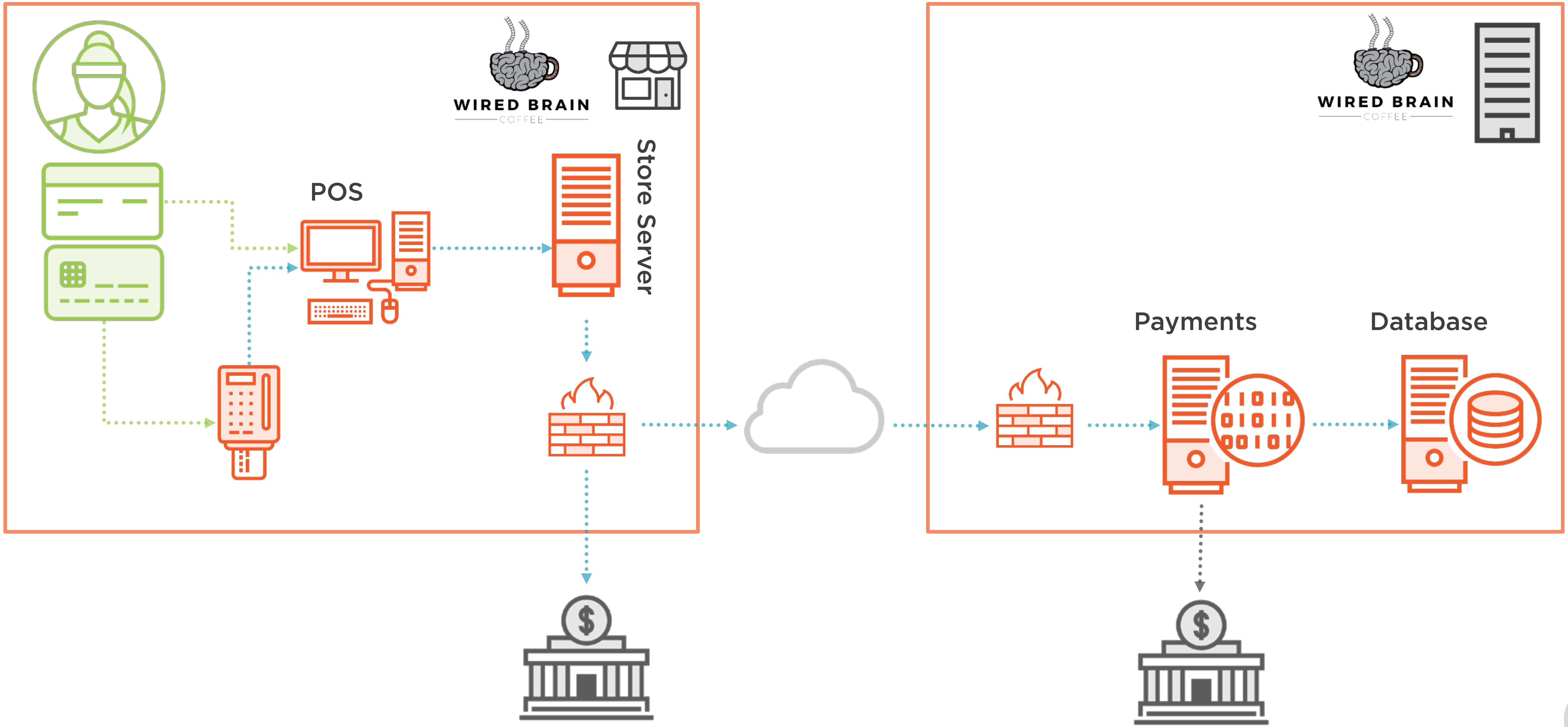
Have a secure SDLC

Have proper change control

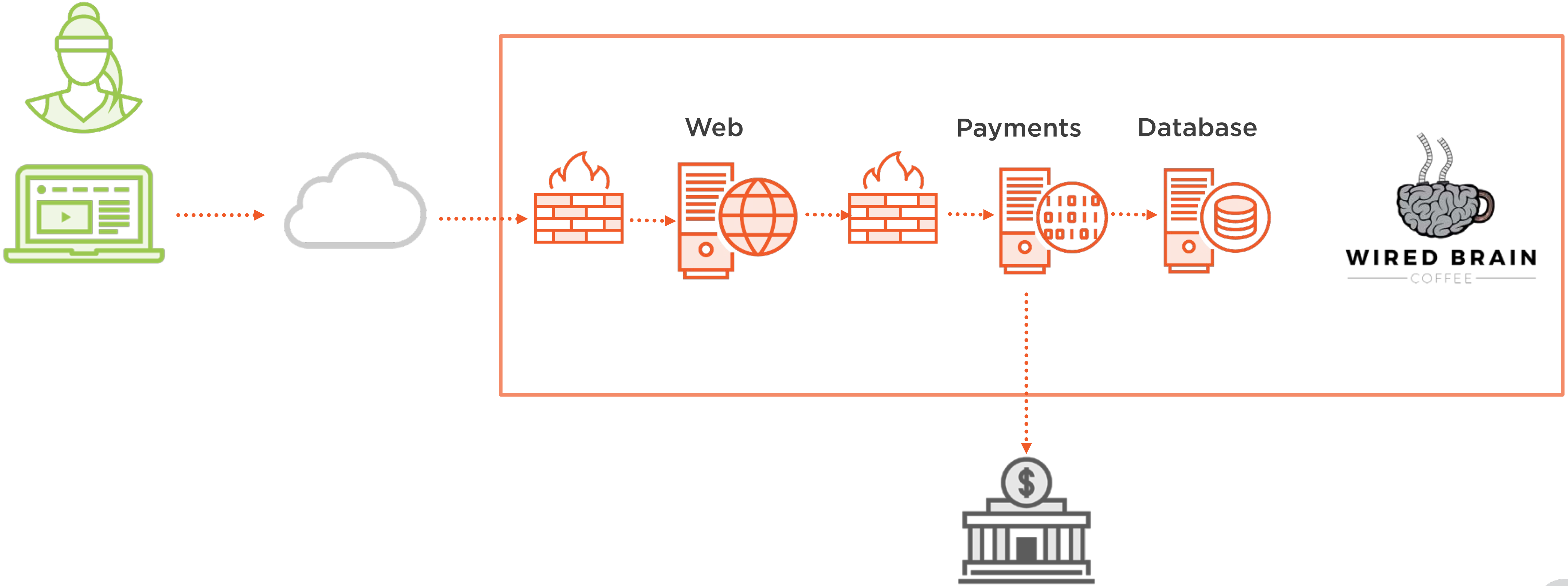
Test the security of web-facing apps or use a Web Application Firewall

Have policies for all of this

6. Secure Systems and Applications



6. Secure Systems and Applications



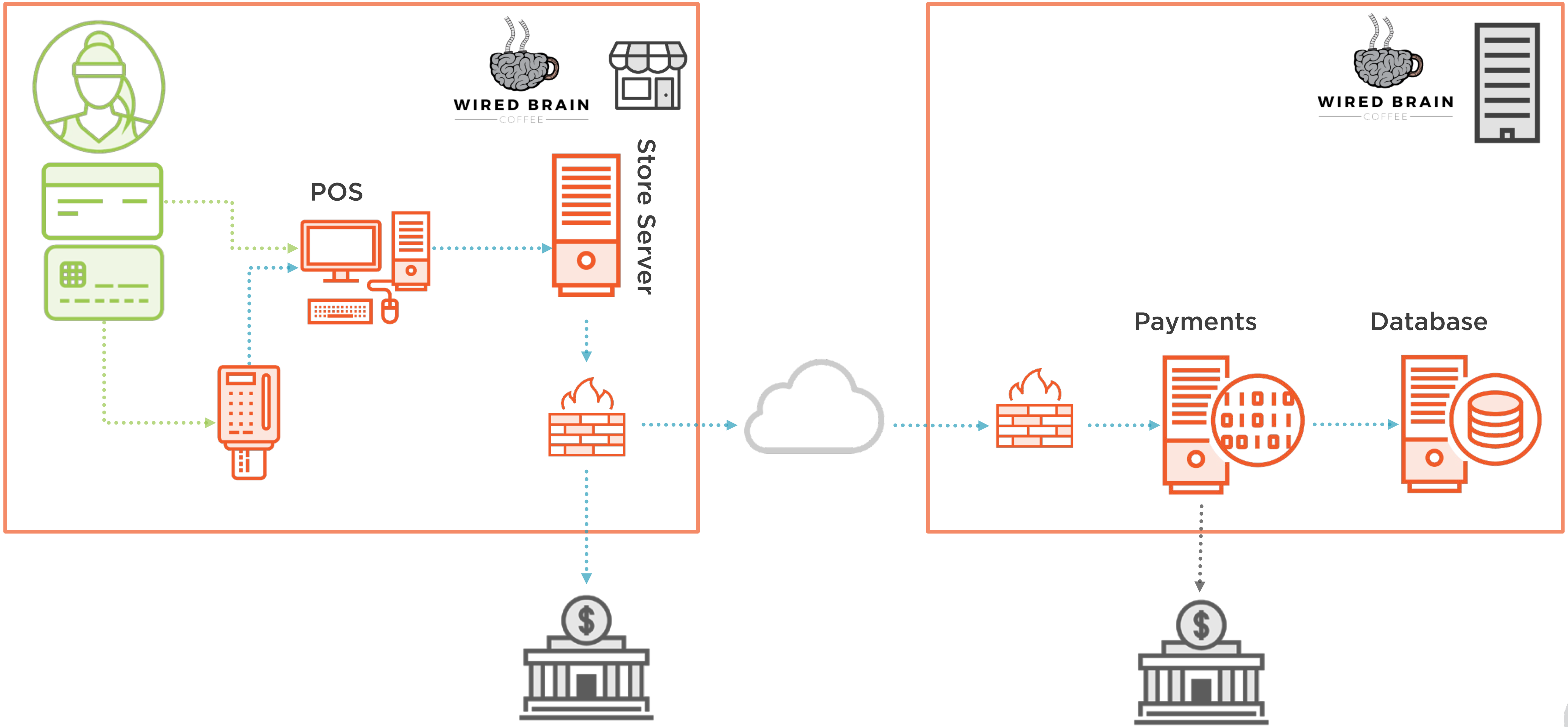
7. Restrict Access to Cardholder Data by Business Need to Know

Only give people access to systems and cardholder data when they really need it

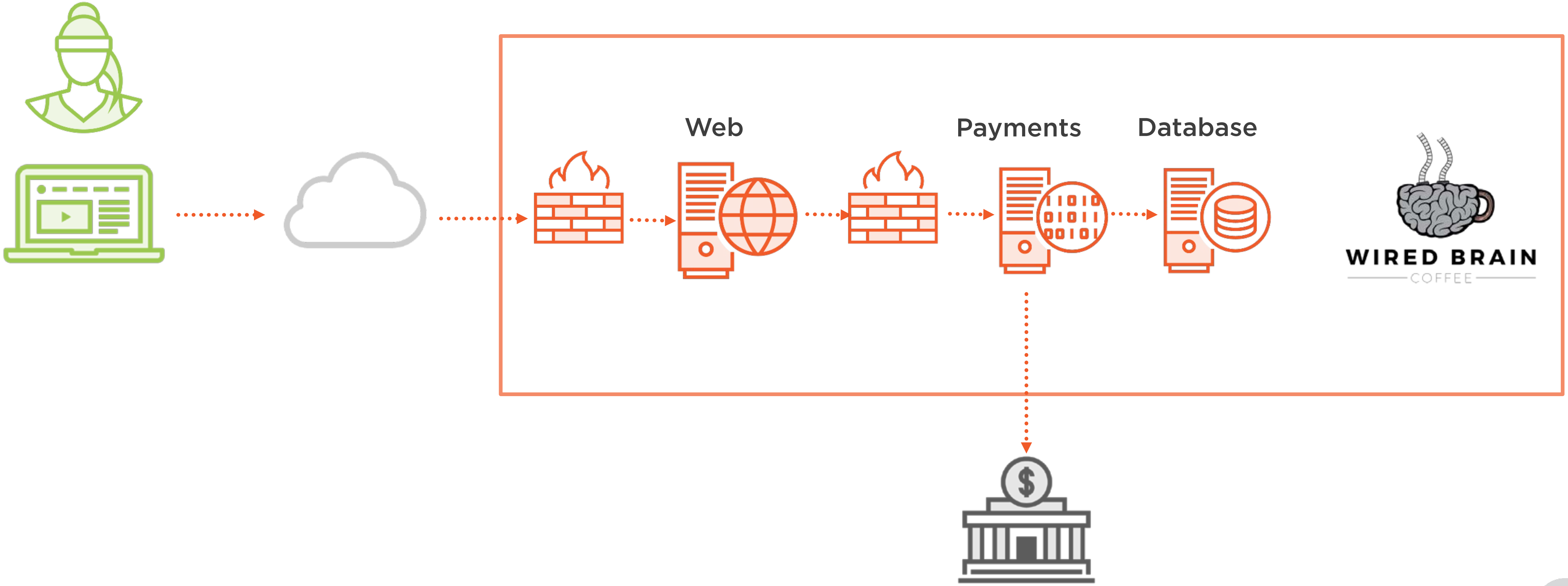
Use an access control system
(eg AD, LDAP)

Have policies for all of this

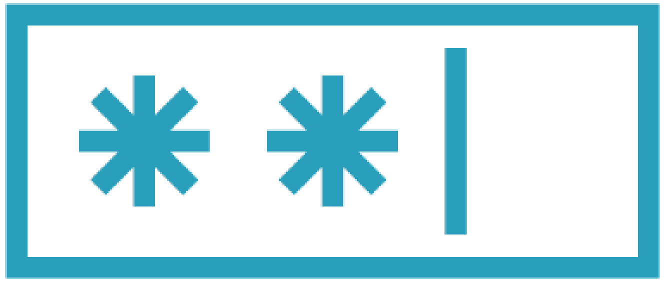
7. Restrict Access



7. Restrict Access



8. Identify and Authenticate Access to System Components



Manage unique user IDs

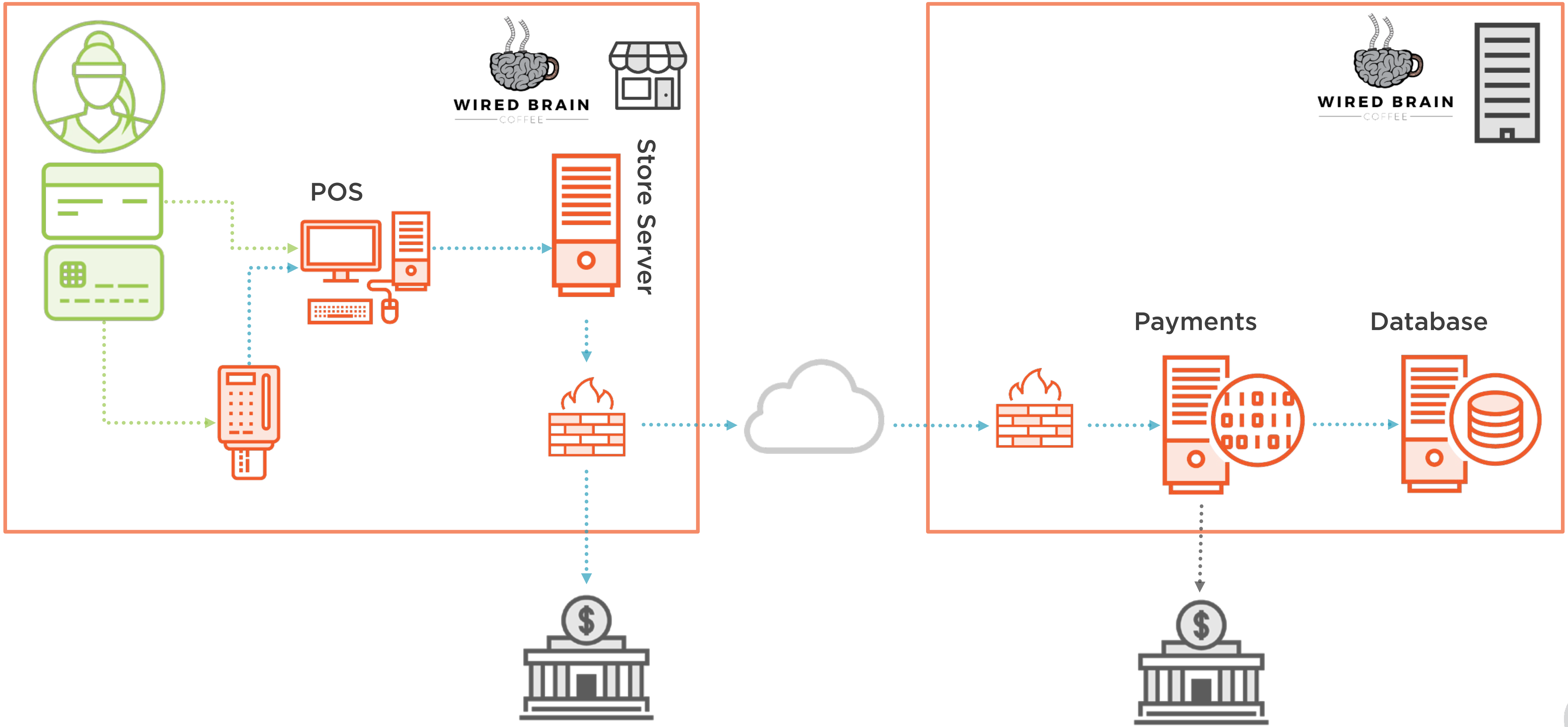
Have strong(ish) passwords

Use MFA for admin and all remote access

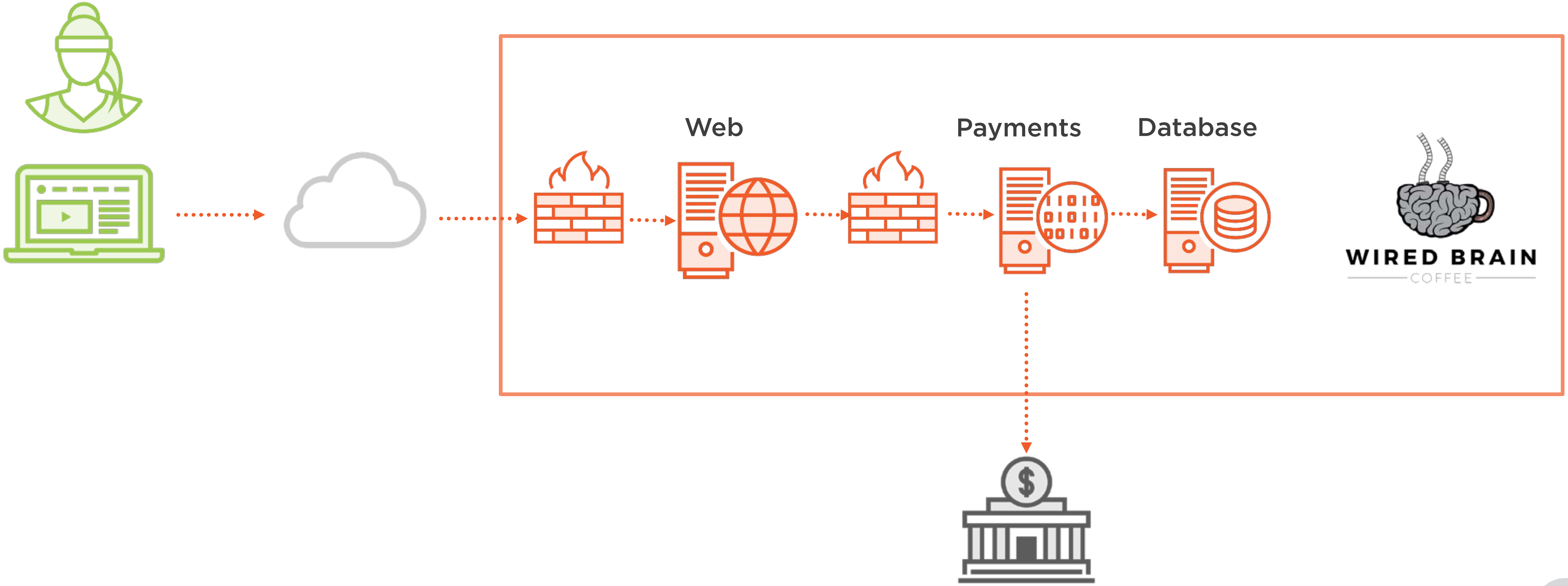
Don’t allow direct query access to databases containing cardholder data

Have polices for all of this

8. Identify and Authenticate



8. Identify and Authenticate



9. Restrict Physical Access to Cardholder Data

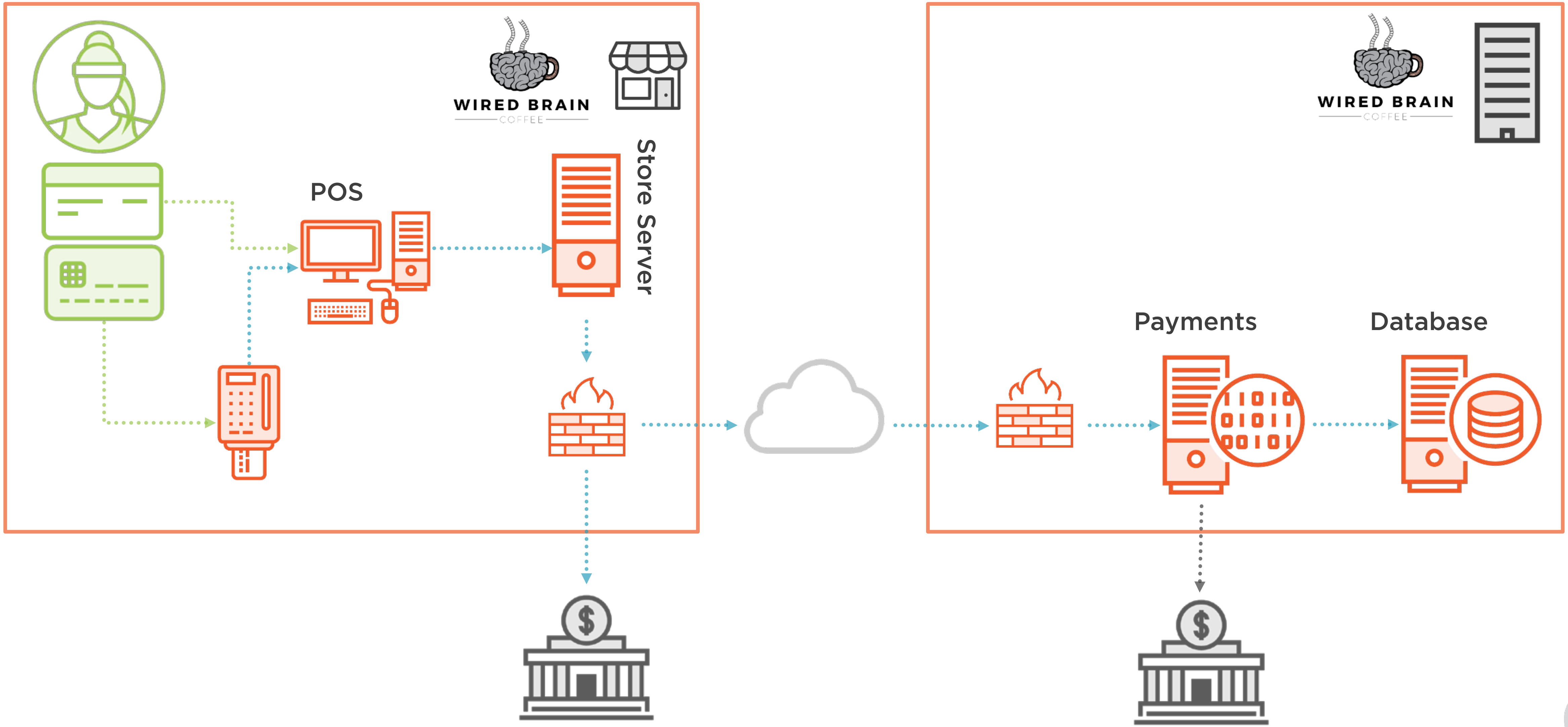
Control and log physical access to the CDE

Secure physical media (paper and electronic) containing cardholder data. Dispose of media securely

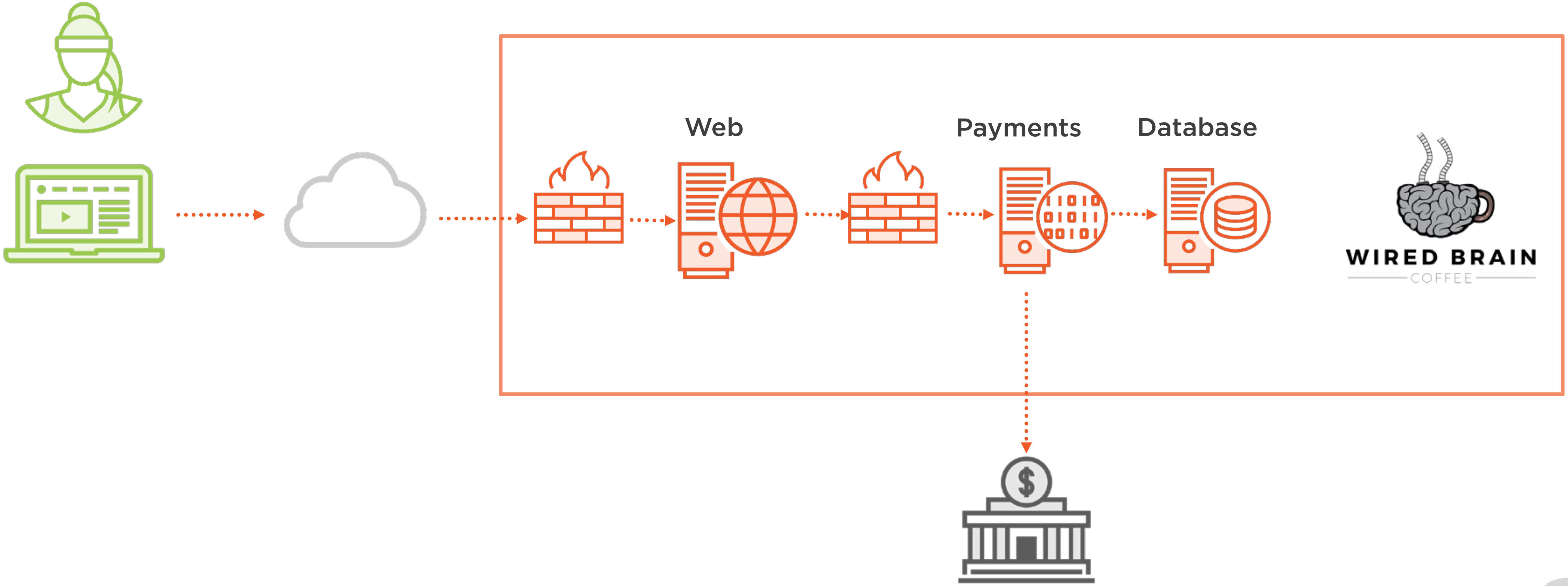
Protect card-reading devices (e.g. chip and PIN / EMV readers)

Have polices for all of this

9. Physical Protection



9. Physical Protection



10. Track and Monitor All Access to Network Resources and Cardholder Data

Create audit logs, retain them for a year

Secure the logs against tampering

Make sure everything is time synchronized

Review logs daily :-o

Have polices for all of this

11. Regularly Test Security Systems and Processes

Check for rogue wireless access points

Do internal and external vulnerability scans

Do internal and external penetration tests

Have IDS and/or IPS

Use change detection software (FIM)

Have policies for all of this

12. Maintain a Policy That Addresses Information Security for All Personnel

- Have an information security policy
- Do risk assessments
- Assign key security tasks to individuals
- Have a security awareness program
- Screen employees
- Manage third party service providers
- Have & practice an incident response plan

Reduce Scope by Segmentation

With a flat network, **everything** is in scope of all 280+ PCI DSS requirements

Reduce Scope by Segmentation

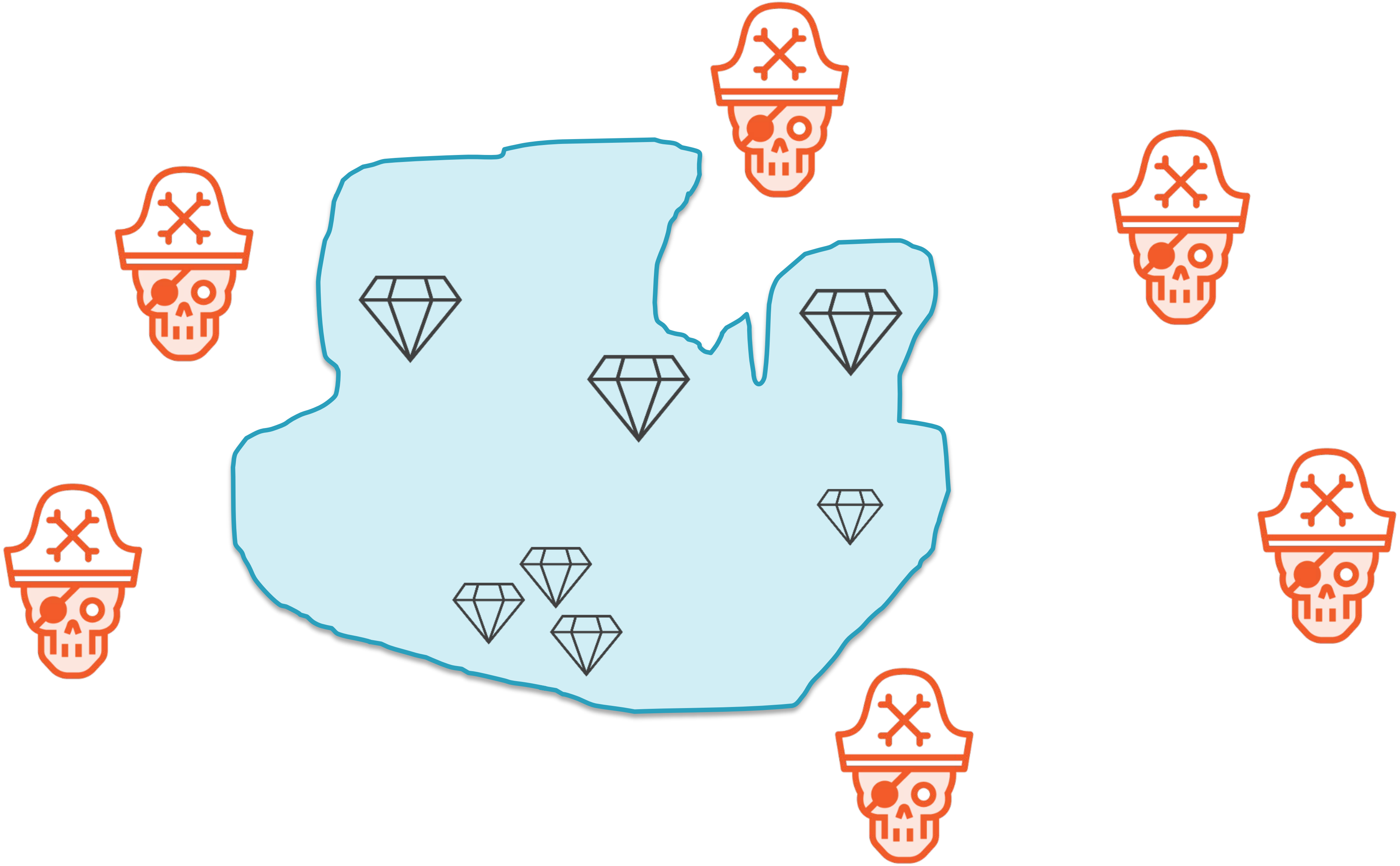
Recommended, NOT a requirement

Reduce complexity, cost, risk and maintainability

Can be dangerous

Why is the standard so prescriptive?

Protecting Diamonds From Pirates



Protecting the Diamonds

Let’s design a security standard that protects the diamonds from the pirates …

Pirate Control Initiative – Diamond Security Standard

Protecting the Diamonds

Give awareness training to the diamonds

Install watchtowers and searchlights

Put land mines on the beach

Deploy mines around the island

Build a fence

Build a Fence

or

Build a Fence

1.1 Build a fence that restricts pirates from entering the Controlled Diamond Environment (CDE)

1.1.1 Ensure fence is pirate-resistant

1.1.2 Ensure fence completely encircles CDE

1.1.3 Ensure fence is buried 1m below ground

1.2 Ensure all fence doors prevent pirates from entering the CDE through the door

But What Does It Mean?

1.1.1 Ensure fence is pirate-resistant

Pirates carry very sharp swords and they really like diamonds. A soft fence made out of wood will easily be cut by a pirate. Fences should be made of a material – typically metal - that can resist a pirate’s sword hacking at the fence for a considerable period of time

The intent of the requirement

How Would You Test?

1.1.1 Ensure fence is pirate-resistant

a) Examine test certificate from manufacturer

b) Stand behind fence holding a diamond shouting “here Mr. Pirate”, validate it takes the Pirate more than 120 minutes to cut through the fence

c) Try cutting the fence with your penknife

Components of a Standard

1.1.2 Ensure fence is pirate-resistant

Requirement

Pirates carry very sharp swords and they really like diamonds. A soft fence made out of wood will easily be cut by a pirate. Fences should be made of a material – typically metal - that can resist a pirate's sword hacking at the fence for a considerable period of time

Intent

a) Examine test certificate from manufacturer
b) Stand behind fence holding a diamond shouting "here Mr Pirate", validate it takes the Pirate more than 120 minutes to cut through the fence
c) Try cutting the fence with your penknife

Testing Procedure

Components of a Standard

6.4.3 Production data (live PANs) are not used for testing or development

Requirement

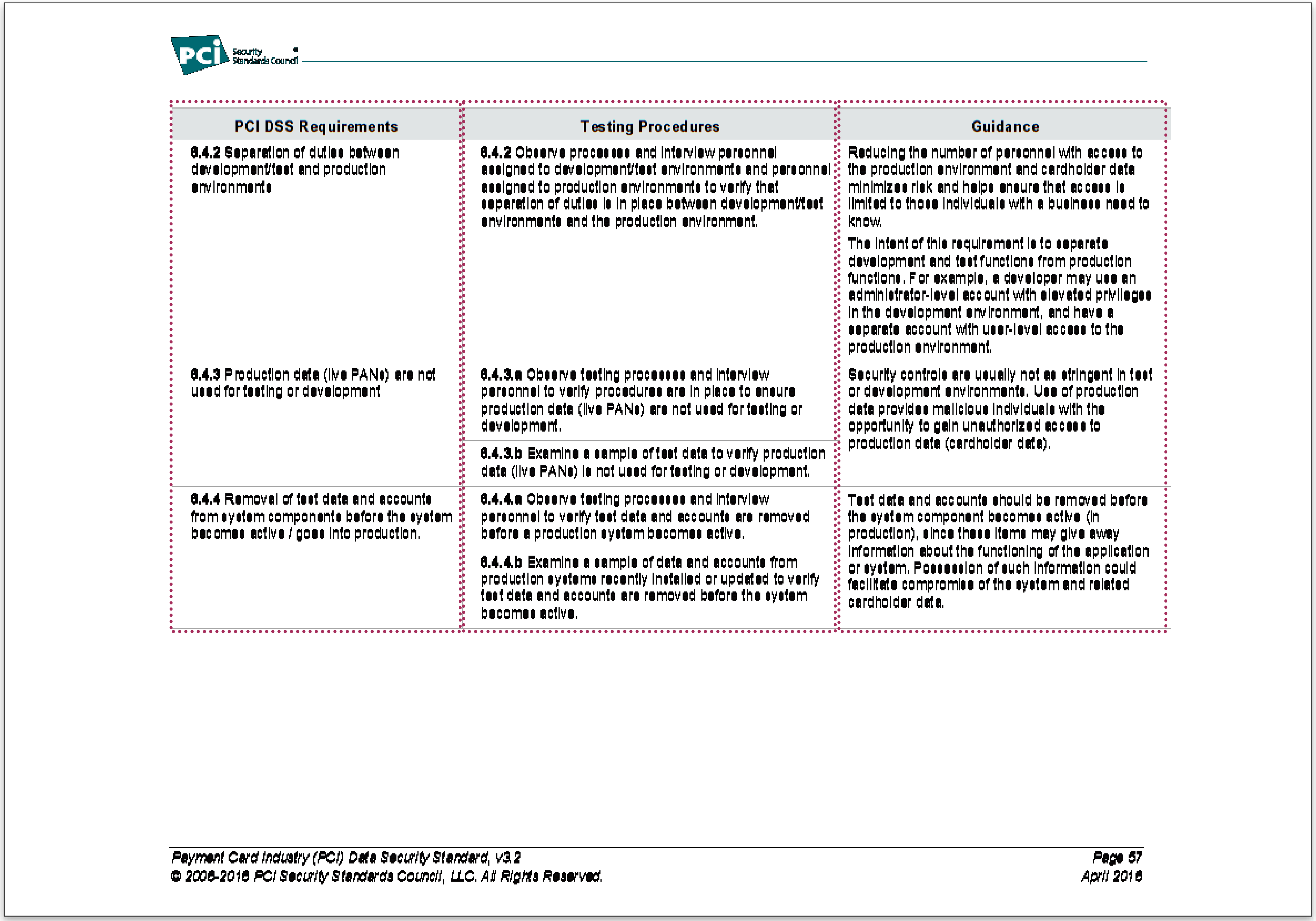
Security controls are usually not as stringent in test or development environments. Use of production data provides malicious individuals with the opportunity to gain unauthorized access to production data (cardholder data)

Intent

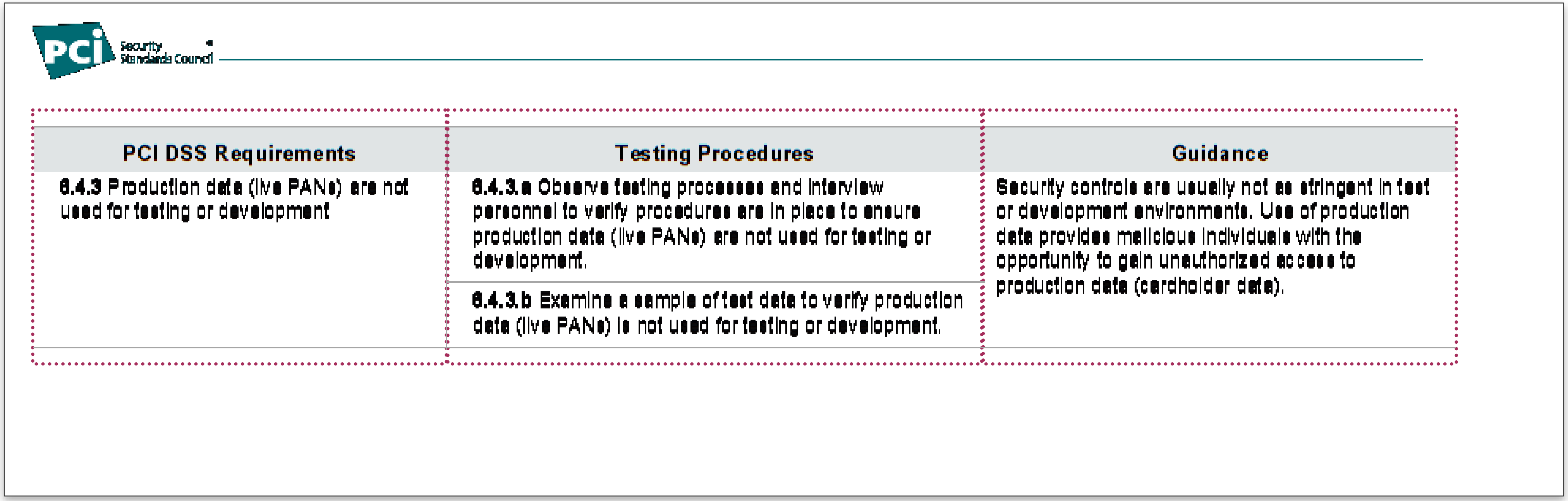
a) Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development

b) Examine a sample of test data to verify production data (live PANs) is not used for testing or development

Testing Procedure



PCI DSS Requirements	Testing Procedures	Guidance
6.4.2 Separation of duties between development/test and production environments	**6.4.2** Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment.	Reducing the number of personnel with access to the production environment and cardholder data minimizes risk and helps ensure that access is limited to those individuals with a business need to know. The intent of this requirement is to separate development and test functions from production functions. For example, a developer may use an administrator-level account with elevated privileges in the development environment, and have a separate account with user-level access to the production environment.
6.4.3 Production data (live PANs) are not used for testing or development	**6.4.3.a** Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development. **6.4.3.b** Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	Security controls are usually not as stringent in test or development environments. Use of production data provides malicious individuals with the opportunity to gain unauthorized access to production data (cardholder data).
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.	**6.4.4.a** Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active. **6.4.4.b** Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active.	Test data and accounts should be removed before the system component becomes active (in production), since these items may give away information about the functioning of the application or system. Possession of such information could facilitate compromise of the system and related cardholder data.



PCI DSS Requirements	Testing Procedures	Guidance
6.4.3 Production data (live PANs) are not used for testing or development	**6.4.3.a** Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development.	Security controls are usually not as stringent in test or development environments. Use of production data provides malicious individuals with the opportunity to gain unauthorized access to production data (cardholder data).
	6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	

When You Can’t Comply

Legitimate Technical Reasons

Documented Business Constraints

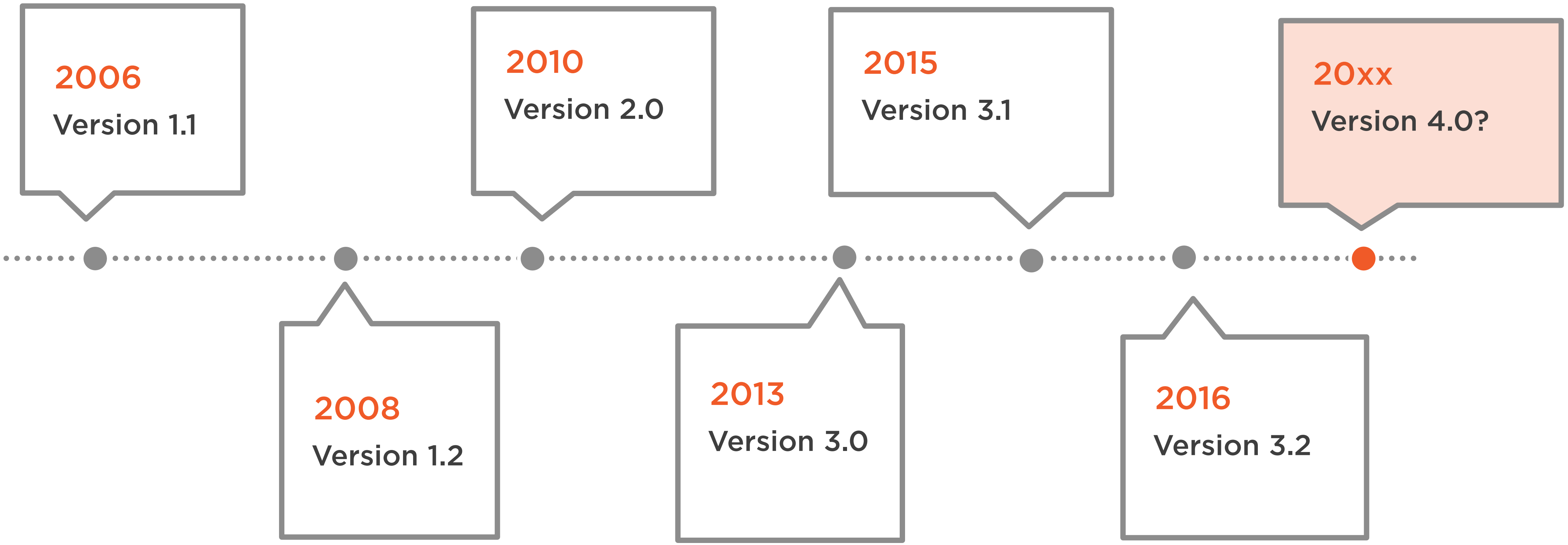
Compensating Controls

Meet the intent of the requirement

As strong as the requirement

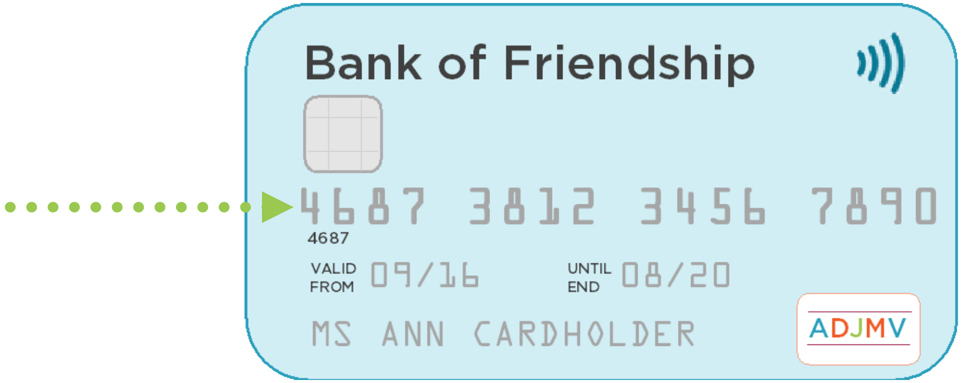
Can’t just be another PCI DSS control …

Review Cycle



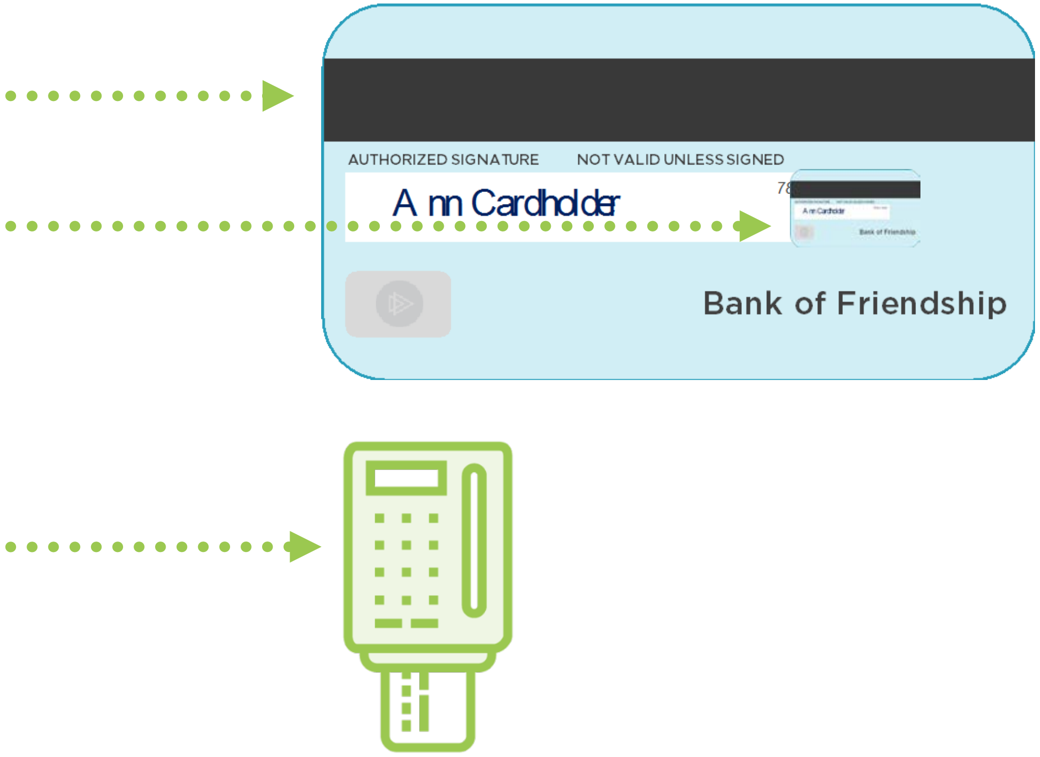
PAN

Primary Account Number



SAD

Sensitive Authentication Data



Summary

Highly prescriptive technical standard

- 12 requirements
- 280+ sub-requirements

Intent and testing procedures

Applies to:

- Anything that stores, processes, or transmits cardholder data (the CDE)
- Anything ‘connected to’ the CDE

Why comply with it?