

Requirement 5: Protect all Systems Against Malware and Regularly Update Anti-virus Software or Programs



John Elliott

PRIVACY, PAYMENTS, SECURITY AND RISK SPECIALIST

@withoutfire www.withoutfire.com



Requirement 5



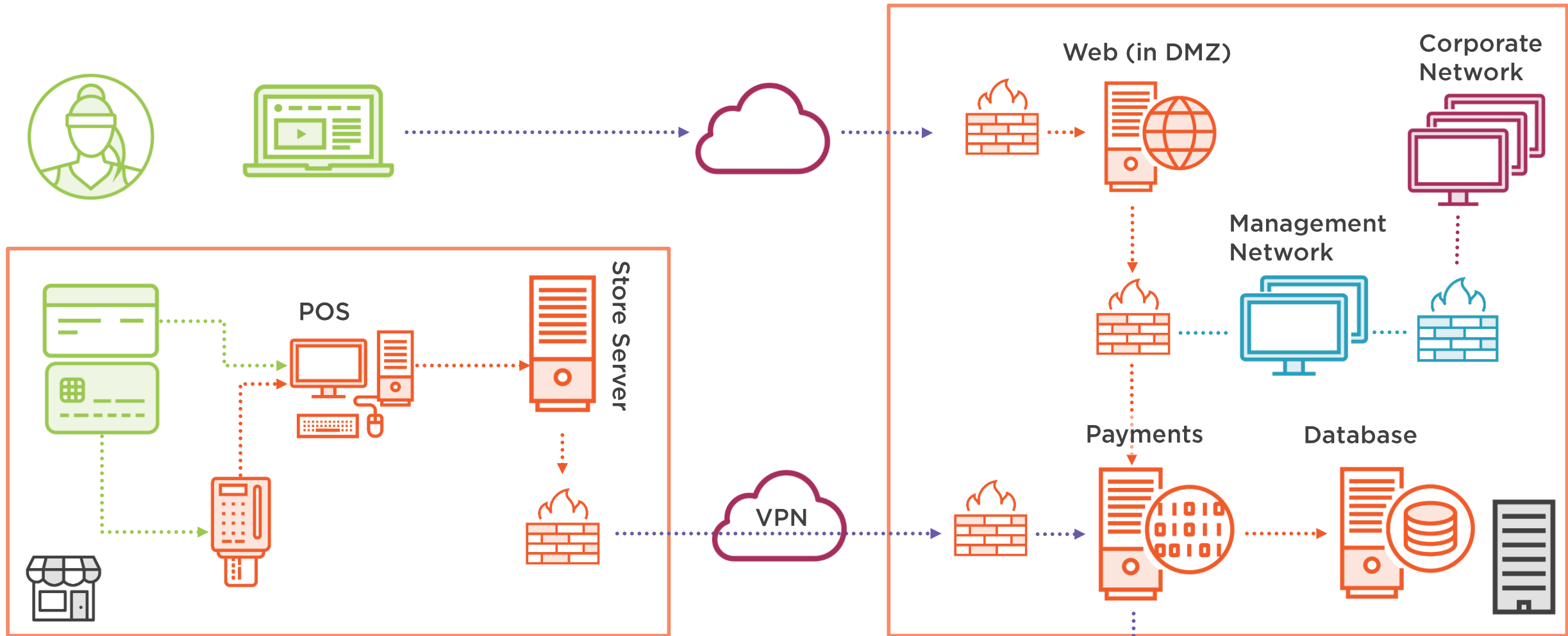
Have anti-virus (anti-malware) software

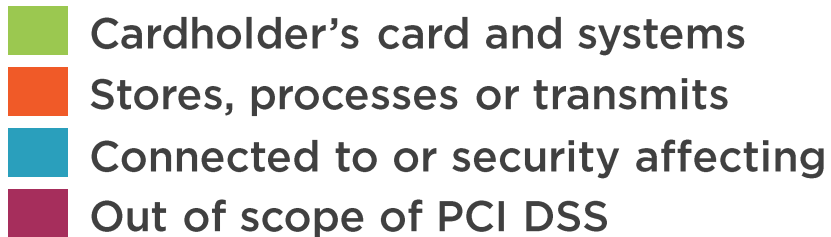
Make sure it operates properly

Don't let users disable it!

Have policies and procedures







- 



Requirement 5.1

Have anti-virus software on all systems
“commonly affected by malicious software”



Requirement 5.1

Deploy anti-virus software on **all systems commonly affected by malicious software** (particularly personal computers and servers).



Requirement Guidance

- There is a constant stream of attacks using widely published exploits, often called "zero day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. Without an anti-virus solution that is updated regularly, these new forms of malicious software can attack systems, disable a network, or lead to compromise of data.

5.1 Testing Procedures

Observe/examine systems and settings	Y	System components, including operating systems
Examine documentation	!	Definition of which systems need anti-virus software
Examine records	-	
Interview people	-	

Requirement 5 | Protect all systems against malware and regularly update anti-virus software or programs





Requirement 5.1.1

Use good anti-virus software



Requirement 5.1.1

Ensure that anti-virus programs are capable of **detecting, removing, and protecting** against **all known types of malicious software**.



Requirement Guidance

- It is important to protect against **ALL** types and forms of malicious software.

5.1.1 Testing Procedures

Observe/examine systems and settings	Y	Anti-virus configurations
Examine documentation	Y	Vendor documentation!
Examine records	-	
Interview people	-	

Requirement 5 | Protect all systems against malware and regularly update anti-virus software or programs





Requirement 5.1.2

Keep an eye on systems you decided were not “commonly affected by malicious software”



Requirement 5.1.2

For systems considered to be not commonly affected by malicious software, **perform periodic evaluations to identify and evaluate evolving malware threats** in order to confirm whether such systems continue to not require anti-virus software.



Requirement Guidance

- Typically, mainframes, mid-range and similar systems may not currently be commonly targeted or affected by malware. However, trends for malicious software can change quickly, so it is important for organizations to be aware of new malware that might affect their systems—for example, by monitoring vendor security notices and anti-virus news groups.
- Trends in malicious software should be included in the identification of new security vulnerabilities, and methods to address new trends should be incorporated into the company's configuration standards and protection mechanisms as needed

5.1.2 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	-	
Examine records	!	Evidence of reviews, annual risk assessment
Interview people	Y	Interview people involved in the evaluation





Requirement 5.2

Ensure that all anti-virus software is actually working



Requirement 5.2

Ensure that all anti-virus mechanisms are maintained as follows:

Are **kept current**

- *'virus' definitions*
- *application updates*

Perform **periodic scans**

Generate **audit logs** which are retained per PCI DSS Requirement 10.7.



Requirement Guidance

- Even the best anti-virus solutions are limited in effectiveness if they are not maintained and kept current with the latest security updates, signature files, or malware protections.
- Audit logs provide the ability to monitor virus and malware activity and anti-malware reactions. Thus, it is imperative that anti-malware solutions be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.

5.2 Testing Procedures

Observe/examine systems and settings	Y	Anti-virus configurations, system components including Oses Log files
Examine documentation	Y	Policies and procedures
Examine records	-	
Interview people	-	





Requirement 5.3

Anti-virus must be running (not disabled) and can't be disabled



Requirement 5.3

Ensure that anti-virus mechanisms are **actively running** and **cannot be disabled** or altered **by users, unless** specifically **authorized** by management on a **case-by-case** basis for a **limited time period**.



Requirement Guidance

- Anti-virus that continually runs and can't be altered will provide persistent security against malware.
- Use of policy-based controls on all systems to ensure anti-malware protections cannot be altered or disabled will help prevent system weaknesses from being exploited by malicious software.
- Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.

5.3 Testing Procedures

Observe/examine systems and settings	Y	Anti-virus configurations, processes
Examine documentation	Y	Process to authorize disablement
Examine records	!	Of authorizations
Interview people	Y	Responsible people

Requirement 5 | Protect all systems against malware and regularly update anti-virus software or programs





Requirement 5.4

Have policies and procedures



Requirement 5.4

Ensure that security policies and operational procedures for protecting systems against malware are **documented, in use, and known to all affected parties.**



Requirement Guidance

- Personnel need to be aware of and following security policies and operational procedures to ensure systems are protected from malware on a continuous basis.

5.4 Testing Procedures

Observe/examine systems and settings	-	
Examine documentation	Y	Security policies, Operational procedures
Examine records	-	
Interview people	Y	Responsible people and people who need to know



That's Fine in Theory

