sysnet global solutions

New PCI SSC Scoping & Segmentation Guidance

What does it mean? Natasja Bolton, Senior Acquirer Support QSA

Introduction

For many years QSAs, ISAs and organisations working towards PCI DSS compliance have been clamouring for guidance on PCI DSS assessment scoping. Even though the concepts of both scoping and segmentation have been around since the earliest iterations of the PCI DSS, organisations sought further clarity on these topics to help them implement effective segmentation and achieve scope reduction.

In response the PCI SSC has published their long-awaited guidance on PCI DSS scoping and segmentation. This new document formalises the PCI SSC's views on how segmentation can be used to reduce scope: that is, reduce the number of systems that require PCI DSS controls.

Expanding on concepts from the PCI DSS

The concepts and principles of scoping and network segmentation from the PCI DSS are further explained and expanded upon in the guidance. It defines when systems will be in scope for PCI DSS and when systems may be considered out of scope.

For reference, the original PCI DSS concepts and principles are:

PCI DSS scoping and segmentation

PCI DSS controls apply to:

- The Cardholder Data Environment (CDE): comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data
- Any network device, server or application that is included in or connected to the CDE (defined as System Components)

System Components include network devices, servers, computing devices, and applications.
Examples of system components include systems that:

- Provide security services
- Facilitate segmentation
- May impact the security of the CDE

Network segmentation:

- Isolating (segmenting) the CDE from the remainder of an entity's network to reduce scope, cost and difficulty of achieving and maintaining PCI DSS compliance
- When properly implemented, ensures that a segmented (out-of-scope) system component cannot impact the security of the CDE, even if an attacker obtained administrative access on that out-of-scope system

Nothing in this new PCI DSS scoping & segmentation guidance changes or contradicts the original PCI DSS concepts and principles, or any of the FAQs or earlier guidance released by the PCI SSC. However, as a result of the scoping definitions and criteria, additional detail and illustrative examples included in the guidance, assessors and organisations may have to deal with some implications for their assessments.

Criteria for systems to be considered out-of-scope

One of the most useful sections in the guidance is the definition of explicit criteria that must be met for a system component to be considered out-of-scope (pages 10 and 12). Only systems determined to be out-of-scope do not require PCI DSS controls. To be out-of-scope **all** of the following criteria must be met:

- System component does **not** store, process, or transmit cardholder data (CHD) or sensitive authentication data (SAD);
- System component is **not** on the same network segment (or same subnet or VLAN) as systems that store, process, or transmit CHD or SAD;
- System component **cannot connect to or access** any system in the CDE;
- System component cannot gain access to the CDE nor impact a security control for CDE **via an in-scope system;**
- System component does not meet any criteria described for connected-to or security-impacting systems (i.e. **does not meet any criteria defined for in-scope system components).**

If organisations or their assessors cannot show that all of these criteria are met, then the system component must be in scope for PCI DSS.

In-scope system components – a summary

In scope for PCI DSS controls

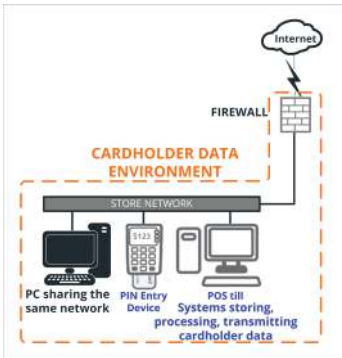
Systems components in the CDE:

- Systems storing, process or transmitting CHD or SAD;
- Systems that do not in themselves store, process, or transmit CHD but are 'adjacent to' (e.g. on the same network as) a system that does.

'Connected-to or security-impacting' systems components that:

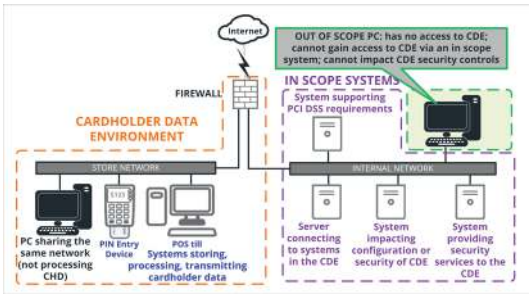
- Connect or have access to the CDE either directly or indirectly, e.g. via a jump server;
- Can impact the configuration or security of the CDE, e.g. server providing name resolution (DNS) for the CDE;
- Provide security services to the CDE, e.g. identification & authentication server, such as Active Directory;
- Support PCI DSS requirements, e.g. audit log server;
- Provide segmentation of the CDE from out-of-scope systems.

Key concepts to be aware of are:



- System components that store, process or transmit cardholder data are 'infectious' and will always bring other systems on the same network (or subnet or VLAN) into scope.

For example, the PC shown is on the same network as the store POS system and must be in scope for PCI DSS, even if it is not used to store, process or transmit CHD or SAD itself.



- An out-of-scope system can be on the same network as, or connect to, an in-scope system. Controls must be in place to make sure the out-of-scope system has no access to the CDE, either directly or via an in-scope system it shares a network with or has a connection to.

For example: the PC on the same network as the in-scope systems may be considered out-of-scope for PCI DSS if there are controls in place that prevent the out-of-scope system:

- gaining direct access to the CDE;
- gaining indirect access to the CDE, via one of the in-scope systems.

When a system component is categorised as in-scope it does not necessarily mean that all PCI DSS requirements apply to it. Rather all *"applicable PCI DSS requirements"* must be implemented and these will depend on the function, location and/or connectivity of the system component.

A holistic approach to security is still recommended

Determining that a system is out-of-scope (for PCI DSS) is not intended to imply that the system does not need protection. A system that is not in scope for PCI DSS could still present a risk to the CDE and to the organisation as a whole. The guidance is at pains to point out and *"strongly recommends"*, in three separate places, that organisations should still implement best practice security controls to protect their entire infrastructure, including those system components deemed to be out-of-scope for PCI DSS. As is noted on page 3, *"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".*

It is highly likely that payment card data is only one class of sensitive or confidential data an organisation stores, processes or transmits. As we explored in the recent Sysnet article on the upcoming General Data Protection Regulation, organisations also have a legal responsibility to protect the personal data they hold. As a comprehensive baseline security measures and practices, the controls in the PCI DSS may be appropriate not only for payment card data but also for the protection of other classes of sensitive data and the entire enterprise.

How is segmentation achieved?

The guidance adheres to the network segmentation statements made in the PCI DSS, that segmentation can be achieved through a number physical or logical means, for example:

- **Physical controls:** isolation of CDE systems from out-of-scope systems through implementation on physically separate network devices, firewalls, servers, etc. No physical connectivity exists.
- **Logical controls:** isolation of CDE systems from out-of-scope systems using properly configured internal network firewalls, routers with strong access control lists, or other technologies that enforce the restriction of access to/from a particular network segment.

One useful clarification in the guidance is that use of separate network segments (or VLANs) does not automatically imply a reduced scope. Network segmentation must be intentionally and effectively configured *('purpose-built')*, enforcing separation of the CDE from the other subnets/ systems.

The document gives examples of the other technologies that can be used to *"provide reasonable assurance that [an] out-of-scope system cannot be used to compromise an in-scope system component"* when an out-of-scope system shares a network with, or is connected to an in-scope system, including:

- Host-based firewall and/or intrusion detection and prevention system (IDS/IPS) on in-scope systems.
- Controlling physical and/or logical access to in-scope systems, permitting only designated user access.
- Using multi-factor authentication on in-scope systems.
- Restricting administrative access privileges to designated users and systems/networks.
- Actively monitoring for suspicious network or system behaviour by or from out-of-scope systems.

Organisations are also required to fully test and verify their segmentation controls. Only once they have confirmed the controls are actually providing effective segmentation can the organisation claim the intended scope reduction for their assessment. This testing and verification must be undertaken annually to ensure the continued effectiveness of the segmentation controls.

What isn't mentioned?

The guidance addresses only scoping and segmentation and, though it confirms that CDE systems and in-scope systems are *"fully in-scope for all applicable PCI DSS requirements"*, it does not consider what those applicable PCI DSS requirements might be for the different categories of connected-to or security-impacting in-scope systems.

Over-reliance on the examples

The document explains the principles of segmentation and scoping using examples to illustrate the points made. One concern is, that by providing examples, organisations will use them 'as read' without appropriate consideration for their suitability and effectiveness in the specific organisation's environment. Past experience tells us that organisations often want to be told what to do (i.e. given a prescriptive 'to do' list). The danger in producing illustrative examples in the guidance, is that entities will use them 'as is' assuming they are *'approved'* or

'PCI compliant' without thoroughly considering their own systems or network configuration. We highly recommend, if any of your merchant businesses rely on segmentation to reduce their assessment scope, that you seek specific assurances from them as to the testing and verification they have performed of their segmentation controls.

What does this guidance mean for your merchants?

We anticipate that organisations will fall into one of two camps once they have had the opportunity to fully digest the PCI DSS scoping & segmentation guidance:

1. Those overjoyed to have a robust foundation to define and verify their PCI DSS assessment scope;
2. Those concerned about their PCI DSS compliance status as the scope & segmentation criteria triggers a re-evaluation of their assessment scope.

It is likely that some organisations will need to review their segmentation controls, re-visit the categorisation of their system components and re-validate their assessment scope, as a result of this PCI SSC guidance. It is possible, therefore, that some of your merchant organisations may, in the short-term, 'fall out' of compliance.

This is because organisations may find that networks or systems considered out of scope for PCI DSS can no longer be justified as such. Segmentation controls may be found not to provide the required level of *"reasonable assurance"* that an out of scope system is unable to compromise a connected-to or security-impacting in-scope system. Assessors may determine that the PCI DSS controls securing connections from connected-to or security-impacting systems are insufficient given the risk. And / or additional time may be needed to create or re-affirm segmentation controls or to implement additional PCI DSS controls on in-scope system components.

Sysnet therefore recommend that you make your merchants aware of the publication of this new guidance. While it does not contradict or change anything previously published, some of the guidance and in particular examples such as the CDE Administration Workstation in Example 2 (page 18), may cause consternation. Organisations may find that the in-scope and out-of-scope criteria do have an impact, requiring them to take steps to make sure that their out-of-scope systems are truly out-of-scope and their in-scope systems are appropriately secured.