Engaging Networks ControlCase Webinar Questions & Answers		
CATEGORY	**QUESTION**	**ANSWER**
Alternative scanner	What is the process if we are using a different AVS vendor?	Alternative ASV scanners need to be on the PCI Council list of approved scanners which can be found here. However, not all scanners are compatible with Engaging Networks (which is partially why we encourage you to use ControlCase, in addition to the great pricing we have negotiated for you). Please fill out this form to request to use an alternate ASV scanner and we will get back to you with our findings & share next steps.
	If we already have a contract with another vendor, I assume it is OK for us to use our contracted vendor?	Great to hear that you have been scanning! As you scan, in order to be PCI compliant, we actually need to whitelist your scanner within Engaging Networks Cloudflare Web Application firewall, otherwise our firewall would have interfered with your scanning (this is known as scan interference). To request us to do this for you, please fill out this form and we will get back to you with our findings.
	Can we see a list of the vendors who do and do not scan at the deeper level, so if we look at alternatives we do not waste time?	Yes - please reach out to your Account Success Manager and they will share this list.
ControlCase Services	Does ControlCases's scan account for PCIv4.1 DSS 6.4.3 and 11.6.1 requirements (Resource Integrity, Change Detection, Weekly Header Monitoring and Alerts, etc…)	The ASV scan report will address control 6.4.3 in that it will show a list of embedded links or code from out-of-scope domains. For Q1 there is no required client action. But beginning in Q2 clients will be required to confirm: - Business need for the software. - Declaration that the software is implemented with strong security controls, as well as the details that comprise those controls. - Confirmation of removal of software if service is disabled or public access is restricted. Control 11.6.1 (which also becomes effective April 1, 2025) is not addressed via the scan; however, we are

		currently working through a plan for how EN can assist clients with this control. In addition, in January we will be hosting a 2025 roadmap session and will address any & all upcoming compliance initiatives that have been mandated on us all.
	Does Control Case help with fixing any scans that don't pass or is that up to us?	ControlCase does not do any remediation themselves, but they will walk you through what needs to be fixed. If you need support to implement a fix, we can provide a list of Accredited Partners who are very familiar with this work.
	Does CC also scan any pages we have with a different application? (i.e. not EN)	Yes, ControlCase will be able to scan non-EN pages, should you engage them to do so.
	Does Control Case provide phone support or only chat/email?	Yes, the client can send an email to the assigned Project Manager and set up a time to connect.
Cost	Do we have to pay for ControlCase, or is that a service provided by EN?	This is a cost that clients will pay to ControlCase directly, at a discounted rate. We understand that these new requirements in PCI compliance, mandated by the credit card industry, may feel like a significant adjustment (we are feeling it too) and so please reach out to your Account Success Manager if you need support navigating this. We may be able to help.
	ControlCases pricing is significantly higher, with other ASVs such as Sectigo (USD 100), TrustGuard (USD 170), and Qualys (USD 375) charging up to 8 times less. Could you kindly provide justification for this price difference?	In most cases, these do not appear to be apples-to-apples comparisons to the individualized, high-touch service Control Case will provide to EN clients. This service includes scanning for you, setting up a compliance hub, walking you through any results that need to be discussed, uploading your report, etc. These alternative ASVs are typically quoting scan-only pricing models, or reflect only a low number of external IPs to scan. The customer would receive a portal login; they would have to schedule their scans, pull the report, and remediate themselves. In most cases, you would need to buy additional

		support, and if it is included, typically a multi-day SLA and via email only. Sectigo and TrustGuard appear to be e-commerce and SSL providers who are adding this service as an add-on. TrustGuard is also not an approved PCI scanner. In contrast, ControlCase is a Cybersecurity Compliance company with an ASV team on staff and a PCI compliance audit staff of over 45 team members, with several PCI board members' seats.
	Can you share that ControlCase pricing again?	Please visit our Trust Center and look for the resources section titled 'PCI DSS Related Documents' for this information.
	Is the ControlCase pricing per quarter or annually? Will the cost change if we close/remove pages?	The cost is annual, and covers scanning each quarter, with up to three scans per quarter, as needed. All costs shown are in USD, but ControlCase will work with you in your home currency. If you close or remove pages in your account, in an effort to reduce your costs, you will work with ControlCase to adjust the scope of your scans and the pricing on your contract.
	I would prefer EN to do all this work for us, we don't have the resources. Is that an option?	At this time, this is not an option; however, we are looking into the possibility of adding such an option in the future, whereby clients could add the scanning cost to their EN subscription fee, and EN would handle getting the scans done for the client. For now, we hope the white glove service that ControlCase provides (scanning for you, setting up a compliance hub, walking you through any results that need to be discussed, uploading your report, etc.) will take a huge logistical burden off of our clients.
EN vulnerability scans	So after this, EN will no longer scan pages like before?	We will continue to perform scans each week to help detect and find vulnerabilities on client pages. We will update the scans results page each week as well, but this is not a substitute for scanning by a PCI Council Approved Scanning Vendor ("ASV"). This is simply to help you achieve a clean scan each quarter from an ASV and ultimately, to keep your

		pages and the Engaging Networks platform safe and in compliance with PCI rules.
Getting a list of pages	Does EN have an easy way for us to pull a list of pages to run through the scanner? Can there be a self-service way to pull a list of all pages that will be scanned by ControlCase?	Right now, the list of page URLs that should be considered for your scan is pulled from the back-end when it is requested by ControlCase. We are working on a self-serve option for clients and will keep you posted. In the meantime, we are happy to share your list with you. Please contact your Account Success Manager or our Support Team to request this.
	Can you talk about how ControlCase knows which pages to scan, once we sign up?	ControlCase lets us know every time a client enrolls in their services. At that time, we provide a list of page URLs to ControlCase. From there, you will work with ControlCase to determine how many of those pages will need scanning.
	How can we run a report in EN of our pages to see when they were last used?	Right now, your best option is to take a look at our Low Volume Page Report. We hope to provide an easier way to see the full extent of the pages in your account in the future.
Getting help	Will you send me the slide deck from the presentation?	Please visit our Trust Center and look for the resources section titled 'PCI DSS Related Documents' for a copy of the slide deck.
	Are Engaging Networks Partners who may have designed our templates being briefed on this and 1) how they can help us rectify any vulnerabilities if needed and 2) knowing how to ensure new templates are compliant?	Yes, all of our Accredited Partners are receiving all of this information as well, and many of them would be more than happy to help you. Please reach out to your Account Success Manager and we can recommend someone to work with.
Outcomes	Also, since everyone is responsible for their own scanning, is it possible that a delinquent client that doesn't get the scan done and/or vulnerabilities remediated in time could affect the entire Engaging Networks platform?	No. Engaging Networks will be working with each and every client to understand their plan to scan and their pass/fail status and will ensure that our overall compliance is not at risk. For clients who do not scan at all through any vendor/who do not pass a scan, there will be a 30/60 day grace period to fix the vulnerabilities within the quarter. If not fixed, those client pages will be closed or stripped of external libraries by putting them into compatibility mode.

	What types of things could make a page fail the check?	Reasons above and beyond vulnerable javascript libraries, include (but are not limited to) cross-site scripting, SQL injection, error handling, security patches, iframes, and input validation. Note, an example summary scan report from ControlCase is available for download from our Trust Center under the Resources section titled 'PCI DSS Related Documents'.
	Will the scan results be limited to changes that the client is responsible for or will they also return vulnerabilities that could be for EN to address? If the latter, will there be a way to distinguish what is for the client to fix vs. EN?	It is possible scans may also detect items that EN will need to address, which we will absolutely do once we are informed by ControlCase of the findings.
	So is EN non-compliant if all EN clients do not opt into the Control Case ASV?	No, EN's compliance does not hinge on clients opting-in to ControlCase. What is true is that clients must use a PCI-approved scanner (ASV) and obtain a compliant PCI ASV scan report (whether that is from ControlCase or another ASV) in order for your organization and EN to remain PCI compliant. If the ASV scan report finds vulnerabilities and they are not addressed, your organization risks facing fines or even losing your PCI compliant status, thereby losing the ability to accept credit card payments. Engaging Networks will be required (by the credit card industry) to close or modify client pages with vulnerabilities that are not fixed in order to address security concerns.
Timeline	Making a comment but it's important. We're all in the middle of CYE. If it takes 4 weeks to scan pages, that means we can't really start until Jan 2025. That means a very tight timeframe to address vulnerabilities by Feb 14.	The 4 week timeframe was mentioned because it could take **up to** that amount of time if you need additional scans to pass (for example, the initial scan fails and ControlCase re-scans for you up to 2 times). If you can't start until January (which is totally understandable), ControlCase will be staffed up and ready to work with you to scan quickly & efficiently, ideally still meeting all timelines. If you have any specific concerns about the timeline, please reach out to your Account Success Manager

		and they can walk through the details with you and make a plan.
	Is there any flexibility with the deadline? Someone else noted that we are all in YE efforts now, so that is the natural focus. This feels very rushed. We shouldn't be forced to pay extra if we have a vendor just because it could take a few weeks longer. Larger organizations that use your service may also need more time.	Engaging Networks' annual PCI DSS Level 1 certification renewal date is early March 2025. Engaging Networks will work with each client to understand their plan to scan and their pass/fail status and will ensure that our overall compliance is not at risk. For clients who do not scan at all through any vendor/who do not pass a scan, there will be a 30/60 day grace period to fix the vulnerabilities within the quarter. If not fixed, those client pages will be closed or stripped of external libraries by putting them into compatibility mode.
	How soon do pages need to be scanned after creation?	The timing relates to a quarterly scanning cadence for PCI compliance. Clients can coordinate with ControlCase on a quarterly timing that includes new page-creation dates. Quarterly scans are required 4 times a year and at the start of every scan, EN will provide a list of pages to ControlCase (as well as the clients if desired) to know what is in scope.
What needs to be scanned	Will tagmanager/tracking pixels/analytics/etc cause issues for PCI compliance?	No, none of these will cause any issues for PCI compliance.
	Does that list of pages to be scanned only include “New” and “Live” or do “Test” and other publish states also apply?	If the page is accessible from the Internet, and someone can input credit card data, or debit card data, it must be included in the scan. You will have an opportunity to verify what is in scope with ControlCase.
	Will this list account for Locales, Profiles, etc.. that can have different code?	The list provided to ControlCase does **not** include all potential variations of a single page. Clients using locales and profiles on their pages should raise this with their scanning vendor to determine the final scope of their scan.
	Will this list have a way to view Page 2 of the Supporter Hub pages, which can process credit card payment?	Engaging Networks is responsible for scanning these pages, so they are not included in the scope for clients.

	We often clone existing donation pages and make updates? Do cloned pages need to go through AVS if the original page is approved?	Yes, cloned pages will be included in the list of pages that we send to ControlCase. You will work with ControlCase directly to determine which pages ultimately need to be scanned.
	So to confirm, 'closed' pages don't need to be scanned, even if they are processing recurring donations?	That's correct. If the page is closed and cannot be interacted with via the Internet, then it does not need to be scanned.
	If pages are 'new' in EN they are not accessible online so why do they need to be scanned?	Even pages with a "New" status are accessible online with the ?mode=DEMO URL parameter. If the page is accessible from the Internet and someone can input credit card data, it must be included in the scan. You will have an opportunity to verify what is in scope with ControlCase.
	Do pages geared for fundraising outside of the US with gateways in other countries also need to be scanned?	Yes, the Payment Card Industry Data Security Standard (PCI DSS) is a global standard
	How will it be handling conditional content/profiles/locales which can all have different code? Same goes for 3rd party scripts, does it let the full page load (e.g. Ad Networks) and then scan, or is it only the initial page load?	We feel like ControlCase is best suited to answer this question as they know their scanner the best. You can kickstart speaking with ControlCase by signing up here.
	Are peer-to-peer pages included in the page count, and if so will ControlCase scan to tell how many there are? Is it be based on the number of donation form templates per site or the number of live fundraiser pages?	Pages in the legacy P2P tool are not included in the EN page list/count that is currently provided to ControlCase, but ControlCase has been made aware of any P2P clients so that they can discuss with you directly what the scope of your scanning should be.
	It’s only donation page urls correct, NOT other data captures as well?	The PCI-DSS ASV scan requirement only applies to pages where credit card data can be entered, which includes the following page types: Donation, Premium Donation, Symbolic Giving, Membership, Peer-to-peer, and Events. Other page types do not require ASV scanning.

	Do we need to scan non-production systems? (Sandbox environment)	If the sandbox account is set up with a payment gateway and has pages where credit card data can be entered, which includes the following page types: Donation, Premium Donation, Symbolic Giving, Membership, Peer-to-peer, and Events -- then yes, the sandbox pages should be included in the scan.
	The ControlCase pricing slide indicates that it is for one domain. Does that mean we need to pay twice that amount if we have donation pages on one domain and P2P classic pages on another? Or is it still considered one EN domain?	Engaging Networks has set up a dedicated domain that the ControlCase will use to conduct ASV scanning. So clients will only be charged for 1 domain, regardless of how many custom hostname/SSL certificates they use.
	What is the scope of the scans? E.g. non-live pages, ETTs - And we add quite a few test pages - In most cases these never go live, or may be made live temporarily. What about stale pages? And is there a minimum # of pages, and a max # of pages we can have?	The PCI-DSS ASV scan requirement only applies to pages where credit card and/or debit card data can be entered, which includes the following page types: Donation, Premium Donation, Symbolic Giving, Membership, Peer-to-peer, and Events. Other page types do not require ASV scanning. Even pages with a "New" status are accessible online with the ?mode=DEMO URL parameter. If the page is accessible from the Internet and someone can input payment card data, it must be included in the scan. You will have an opportunity to verify what is in scope with ControlCase. Historically, EN has set very few limits on the number of pages a client can create on our platform.
	Do we need to notify someone every time we create a new donation form?	No, that will not be required. When it comes time for quarterly scanning, an updated page count will be provided.
	Can you please define page? For example, the area in the Engaging Networks is called Pages. Is pages at that level or is all pages within the main Page. We have a multi step process to collect information that is	At this time, our understanding is that a multistep page would still be considered 1 page from a scanning standpoint, but this is something that you should discuss with ControlCase when determining the final scope.

	technically different web pages but all roll up to the main Page...33333 /donate1, 33333/donate2 where 33333 is the main overarching page in EN.	
	What about new or live pages that are not processing donations, but are donation templates. For example, we have a page set up for Gift-in-kinds and the payment fields are disabled.	If the page is accessible from the Internet and someone can input credit card data, it must be included in the scan. Even pages with a "New" status are accessible online with the ?mode=DEMO URL parameter. When the list of your pages is sent to ControlCase, it would include any Donation Pages you have, and then you will work with ControlCase directly to verify what is in scope. If a donation page does not have credit card fields on it, then it would be removed from the scope.
	So if we are using templates - 4site makes our templates - do we simply scan templates and any pages that vary from our templates?	Yes, but only pages that accept credit cards or debit cards need to be scanned, which includes the following page types: Donation, Premium Donation, Symbolic Giving, Membership, Peer-to-peer, and Events.
	We use the same customized template on all of our donation pages, even though we have a lot of donation pages. Why do we need to scan each live page and not just the template?	The Engaging Networks system allows customization to happen at the page level, so all pages where credit card data can be entered (Donation, Premium Donation, Symbolic Giving, Membership, Peer-to-peer, and Events) will be included in the file sent to the Approved Scanning Vendor. It is up to the client to work with the vendor to determine the ultimate scope of the scan.
	I believe the tools scans pages with a URL, not individual templates, code blocks, etc.. that construct the page, only the final page itself.	The scanner will scan/evaluate a rendered page. It will also send a series of GET and POST requests to interact with the page itself.
	Are pages that have a test gateway applied excluded from the pages that have to be scanned?	Pages using a test gateway would be included in the list of pages sent to ControlCase; however, it is up to the client to work with the scanning vendor to determine the ultimate scope of what is scanned.

Why only 1 endorsed ASV	Who else was vetted? Why was ControlCase selected as your only ASV vendor?	We have carefully selected ControlCase as our preferred Approved Scanning Vendor (ASV) to ensure a smooth and efficient compliance process. Control Case offers several key advantages that streamline PCI DSS scanning, including: - 1/ Seamless Integration: ControlCase is fully compatible with EN's directory hierarchy, enabling comprehensive scanning of all payment pages without disruption - 2/ Thorough Evaluation: We have conducted extensive testing to validate Control Case's compatibility with our platform, minimizing the risk of unexpected issues or delays - 3/ Enhanced User Experience: We aim to provide a frustration-free compliance journey by proactively addressing potential compatibility challenges
	Does EN get any monetary benefit from endorsing ControlCase?	No, Engaging Networks does not get any financial benefit from presenting Control Case as our preferred ASV for our clients. We chose ControlCase because we are confident that they will provide good service to our clients at a fair price.
Why this process	What date did this ASV requirement come into effect?	The new compliance requirements (PCI DSS v4.0) were first announced for all merchants -- including Engaging Networks and our clients -- by the PCI Council in 2022, and are part of an industry-wide effort to enhance security standards. The new requirements mandate that payment pages must be scanned at least quarterly by an Approved Scanning Vendor. A number of the new PCI DSS v4.0 requirements will officially go into effect 31 March 2025, including the scanning requirement. While these changes are not within our control, we have been working to find solutions that make the transition as manageable as possible for our clients.

	Can Engaging Networks provide a responsibility matrix of which PCI requirements EN is responsible for covering, and which requirements clients are responsible for?	Please visit our Trust Center and look for the resources section titled 'PCI DSS Related Documents' for this information.
	Just curious what the reasoning is for having each client coordinate/manage the scanning process themselves vs. Engaging Networks managing the process from a global level and passing on the findings to individual clients for them to remediate any vulnerabilities?	We did consider the possibility of fully serving as a go-between – between the ASV and our clients -- in this situation. For that matter, we may yet introduce such an approach next year as an alternative, additional option for those clients who would prefer for EN to act as a buffer between Control Case and themselves. But for now, in this first roll-out of the scanning process, we decided that it's important and valuable for our clients – who are all "merchants" and therefore must obey PCI rules -- to fully grasp how scanning works, and to understand the imperative to promptly remedy any security vulnerabilities detected by page scans. We might have chosen differently if EN fully controlled the software code on our clients' pages, but we don't. Unlike most of our competitors, EN gives our clients an extreme level of flexibility to build pages using their own custom code, and a high level of "sovereignty" to control the pages that they build on our platform. That's why clients must take ultimate responsibility for maintaining their PCI compliant status by fixing any security issues that they themselves created when they built their EN-hosted pages. In the end, these new security requirements will actually be better for everyone, to keep your pages and donations safe from bad actors that are increasingly looking to exploit security vulnerabilities.
Other	We just completed our certification for our PayPal gateway/merchant account. Will we still get the requests to show compliance from our merchant accounts like PayPal and Stripe?	Clients will need to check with their gateway/merchants on their individual reporting schedules.