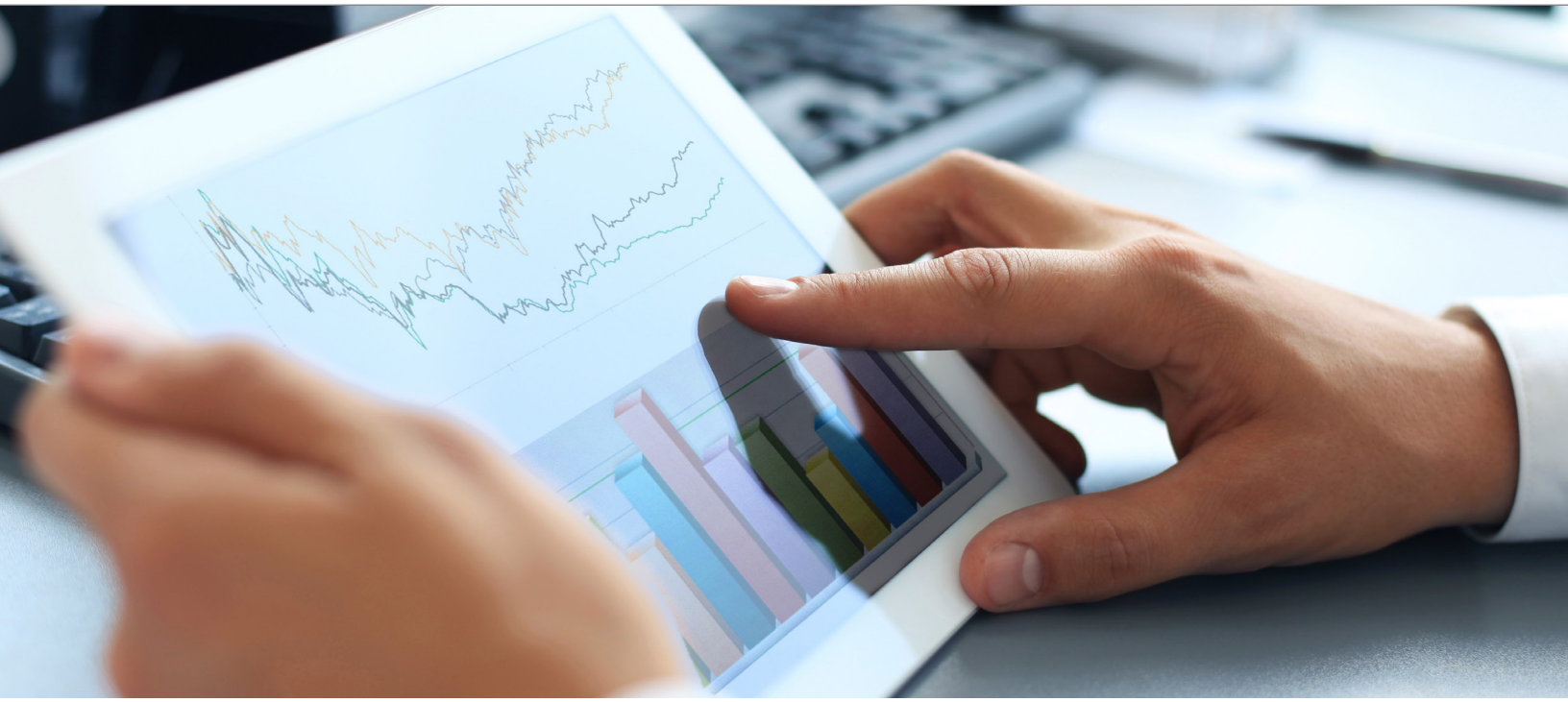
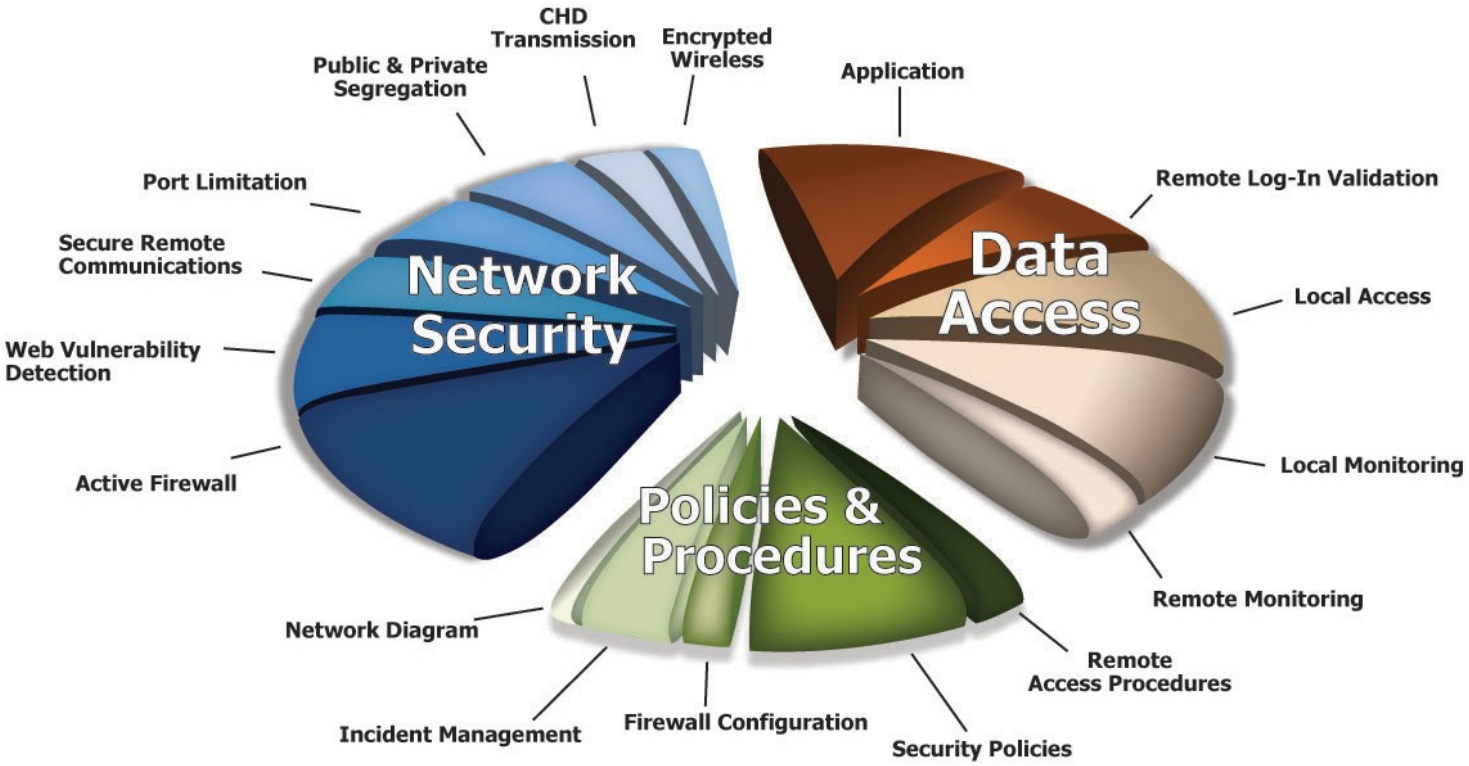


Approved Software Does Not Equate to PCI Compliance

The four most vital actions to accelerate your network and credit card data security

By Bradley K. Cyprus - Chief of Security and Compliance, Netsurion



There is a misconception with many merchants concerning how to become PCI compliant. Frequently, in our dealings with merchants, we have heard, "My software is approved, so that should make me compliant." This is simply a fallacy, and any merchant who makes this erroneous conclusion could be open to any number of vulnerabilities which by themselves would negate the possibility of PCI compliance. When describing the requirements for Visa's Payment Application Best Practices, a Visa specific standard that was replaced by the Payment Application Data Security (PA-DSS) Standard in 2009, Visa states that, "Visa prohibits the retention of full magnetic-stripe ("track") data, Card Verification Value 2 ("CVV2") and PIN blocks—all critical impediments to achieving PCI DSS compliance." This shows Visa's own acknowledgment that secure software is required to support PCI, but it is not sufficient by itself.

Simply stated, PCI, whose full name is Payment Card Industry Data Security Standard, is a standard that was created by the major credit card companies in December of 2004. On January 1, 2014, the current standard, version 3.0, was officially implemented. The purpose of the standard is to protect customers and to ensure that merchants are meeting a minimum level of security while in possession of cardholder data. Some of the standard pertains to the Point of Sale (POS) software in use at a location, and merchants can rest assured that if they are using approved software in the manner envisioned by the developers that they will meet the software requirements of the standard. However, that is only part of the equation. Here are the 12 primary components of PCI:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

It is clear that requirement 3, part of 4, and 6 pertain to using secure applications, but that is only a part of the PCI picture. A failure to meet the other components will result in opening the merchant up to the liability associated with noncompliance.

A source for the confusion may be the credit card processors themselves as they ask their merchants the following two questions:

1. Are you PCI compliant?
2. What is the software you are using (Manufacturer and Version)?

It is possible that the nature of this inquiry has led merchants to believe that if their software is on the PA-DSS list of approved software that they will be compliant. It is important to understand why the processors ask these two questions because while they are related, they are designed to protect the processor and not the merchant.

Credit card processors are interested in protecting themselves from liability. By asking a merchant, "Are you PCI compliant?", the processor verifies that the merchant claims to have already taken the necessary steps to protect their environment. This puts the burden on the merchant to maintain the proper level of security, and it limits the processor's exposure in the event of a breach. A merchant who answers "no" to this question will be prohibited from taking credit cards, even though processors in many instances are not validating an affirmative response. Furthermore, the processor asks "What is the software you are using?" This verifies that the software communicates to the processor safely. Software that is on the PA-DSS will transmit credit card data securely, further mitigating the processor's risk. In other words, the processor has taken care of its interests here, but the merchant has not, unless they can truthfully claim that they are PCI compliant. What merchants must understand is that the processor wants to pass the liability of credit card and I.D. theft to the merchant, and these questions open the way for them to accomplish their goals.

Originally, smaller merchants were only encouraged to participate in PCI, but it was not mandatory. This is no longer the case. Every merchant who accepts credit cards is required to comply with PCI. As stated on the PCI Security Standards Council Website, "If you are a merchant that accepts payment cards, you are required to be compliant with the PCI Data Security Standard." How to Be Compliant (PCI Security Standards Council Website) To access the Customer Portal, CLICK HERE.

There is no doubt that using a PA-DSS approved software is a crucial component of PCI DSS, but if network security is not also implemented properly, then the application will be vulnerable to hackers and other security breaches. In the modern world where identity and credit card theft are becoming more pervasive every day, it is no longer acceptable for locations to ignore potential issues associated with credit card processing. Merchants looking to protect themselves and their customers will make sure that security is a priority when planning their credit card environment.

7324 Southwest Freeway
Suite 1700, Arena Tower II
Houston, Texas 77074

P: 713.929.0200
F: 713.541.1065
Netsurion.com