

## **HALOCK White Paper on Leveraging Compensating Controls for Reducing Costs for PCI DSS Compliance**

**Introduction:** This whitepaper is designed to provide guidance to merchants and service providers seeking to reduce costs while achieving PCI Compliance. It provides specifics about a compensating control used to address PCI DSS Requirement 11.5 and how to use end point security to fulfill the intent of the requirement. Author: Will Redfield

### **Doing More with Less for PCI: Cost Savings Advice for PCI:**

PCI DSS compliance can cost most large merchants hundreds of thousands of dollars or more to remediate. PCI spending categories include people, processes, and procedures as well as technology controls to automate many of the manual processes for protecting cardholder data, and for proving that cardholder data is being protected at all times. Most organizations are challenged with facing limited budgets for PCI, and must consider their spending on PCI remediation carefully. Security and compliance management leaders are finding that they need to make careful choices on where they are investing for security and why.

Many organizations are reducing costs of PCI compliance by leveraging existing investments in technical and logical controls. PCI QSAs (Qualified Security Assessors) are best prepared to advise clients about respective states of PCI compliance and about where organizations can save. QSAs are approved by the PCI Security Standards Council (SSC) to conduct PCI DSS on-site assessments. QSAs endure rigorous training and annual re-certification in order to assess merchants' security programs for properly protecting cardholder data. According to Jeremy Simon, lead PCI QSA at HALOCK Security Labs, "A good example of making smart use of technology is with requirement 11.5, requiring File Integrity Monitoring software be deployed on all in-scope systems. The intent of this requirement is to alert IT staff to any modification of specific system/configuration files indicating an attempted compromise. While the risk is legitimate, the prescribed control can be costly and difficult to manage."

Simon emphasizes that the clear intent of PCI 11.5 is to proactively prevent unauthorized access to any cardholder data system related files and to any content files containing cardholder data. He believes that prior to investing in high cost file-integrity monitoring software, merchants should first focus on shoring up the security of the cardholder data management systems themselves. The primary area most organizations need to improve cardholder system security is with comprehensive end point protection. Simon notes, "End point protection solutions can be an effective way to address PCI 11.5 because they combine multiple layers of security initially; proactively preventing unauthorized access to critical files". Simon argues that this approach of using end point security satisfies the intent of PCI 11.5 in most cases, especially for merchants with tight budget constraints.

The challenge with file-integrity monitoring software is that it can be costly to implement and maintain. Simon estimates that organizations can easily spend a quarter or more of their security budgets on high cost file-integrity monitoring products. Therefore organizations faced with tight budget constraints for PCI compliance should consider more cost effective investments, such as leveraging existing technologies or considering a new deployment in endpoint protection technology for compensating controls.

What are compensating controls? The PCI SSC states “Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.”

*More about PCI Compensating Controls:*

While compensating controls can be used it is recommended that you have a QSA review these controls to ensure that they are adequately justified. PCI DSS states compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating controls sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against.
3. Be “above and beyond” other PCI DSS requirements.
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

The PCI DSS also states any compensating controls must be documented, reviewed, and validated by a PCI assessor and a Compensating Controls Worksheet must be included with the Report on Compliance (ROC). The following items about a compensating control must be explained and documented for PCI compliance:

- 1. Constraints:** List constraints precluding compliance with the original requirement.
- 2. Objective:** Define the objective of the original control; identify the objective met by the compensating control.
- 3. Identified Risk:** Identify any additional risk posed by the lack of the original control.
- 4. Definition of Compensating Controls:** Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.

**5. Validation of Compensating Controls:** Define how the compensating controls were validated and tested.

**6. Maintenance:** Define process and controls in place to maintain compensating controls.

As a properly documented PCI compensating control for file-integrity monitoring software, endpoint protection solutions can be deployed to all in-scope Microsoft Windows systems to prevent access to cardholder system files. The most widely used endpoint protection solution is Symantec Endpoint Protection. As an example, this solution provides comprehensive endpoint protection and includes host-based firewall, intrusion prevention, anti-virus, anti-spyware, generic exploit blocking, device and application control, and network access control. When configured properly, this and other endpoint protection solutions should protect against sophisticated attacks such as rootkits, zero-day attacks, and mutating spyware. Collectively, these controls provide a level of protection which prevents unauthorized access to cardholder environment system files thereby meeting the intent of PCI DSS requirement 11.5.

#### **More About Jeremy Simon, PCI QSA, CISSP, CISA:**

Jeremy is a Partner with HALOCK Security Labs and serves as its Chief Technology Officer. With a primary focus on Assessment and Compliance Services, Jeremy is ultimately responsible for the direction and quality of HALOCK's technical service offerings. Recognized as a PCI Subject Matter Expert, Jeremy was among the first nationwide to receive the PCI QSA certification and plays a key role in the interpretation and effective application of the standard. His in-depth knowledge of the PCI Data Security Standard ensures HALOCK's PCI services provide the highest level of value possible.

HALOCK Security Labs is a professional services organization focused 100% on information security. HALOCK's core services include Assessments, Security Strategy, Network Security, and Application Security. The company is in partnership with their clients to help them protect critical information assets and meet compliance needs in a manner that is aligned with international security standards.

***For More information please contact:***

**Will Redfield - +1.847.221.0203 - [wredfield@halock.com](mailto:wredfield@halock.com)**