



Raytheon Oakley Systems

USE CASE — COMPLYING WITH PCI-DSS REGULATIONS

PCI-DSS Regulations

PCI DSS (Payment Card Industry Security Standard) is a common set of security standards for processing, storing, or transmitting credit card numbers. It was developed by the credit card industry as a guideline to help both vendor and merchant organizations that process card payments to prevent credit card fraud, hacking and various other security issues.

The regulations list a broad range of requirements for controls and monitoring procedures for safeguarding customer credit card and other Personal Identifying Information (PII). Oakley's solution helps its customers meet these requirements and ensure PCI compliance. All vendors and merchants must comply or they risk losing the ability to process credit card payments.

Monitor Use of Customer Data

Oakley solutions will monitor the use of customer data as it is handled by your employees and moves across or leaves your network so that you can identify and assess potential policy violations and risks. Oakley technology can recognize when your employees or contractors are using customer PII and, if it is mishandled, will alert you, log

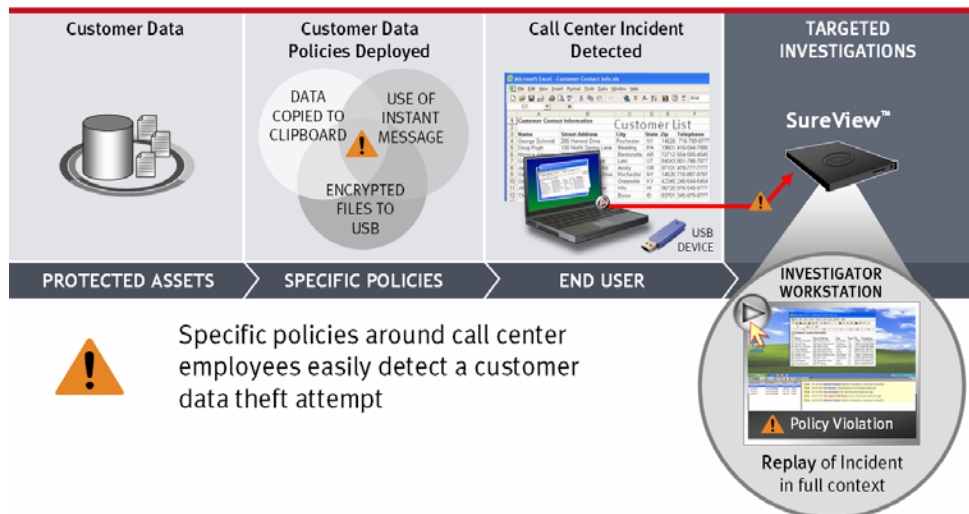
the incident, and enforce a control if you desire. Automated reporting tools provide clear and easy auditing visibility to this activity.

With these capabilities, Oakley solutions can be deployed at a network segment boundary, in front of a critical database or application, or on the computers of high-risk individuals who handle customer data, such as outsourced customer service representatives, to ensure that policy is being followed and accountability measures are in place as required by PCI. Policy is consistently enforced, through unified policy management, whether the user is on the wired or wireless intranet, across a corporate Wide Area Network (WAN) link, or at a remote location.

Policy Driven Control

Raytheon Oakley Systems will help you implement a policy-driven, baseline monitoring threshold, so you can find and remediate careless or accidental policy violations. To help effectively manage these incidents, Oakley products provide a number of automated remediation capabilities, such as prompting to educate users or blocking for situations related to e-mail, copying to removable media, printing, or any other form of input/output.

At the other end of the spectrum, a small



USE CASE

COMPLYING WITH PCI-DSS REGULATIONS

number of people who engage in deliberate or truly malicious activities can sometimes do the greatest harm. These users often take pains to hide their actions or cover their tracks. Oakley has the uniquely powerful ability to recognize and expose the nuances of evasive, complex behavior.

Specific Requirements

The current version of the standard (version 1.1, released in September, 2006) specifies 12 requirements for compliance, organized into 6 logically related groups, which are called "control objectives." The requirements that Oakley meets, along with a description of the functionality, are listed below.

Requirement	Requirement Description	How Oakley Helps
# 3	Protect stored cardholder data	Sensitive data files and types can be identified and fingerprinted so that they are recognizable and trackable anywhere they are stored or moved on client systems or on the network. This capability provides protection when the data is at rest, in motion or at the end point.
#4	Encrypt transmission of cardholder data across open, public networks	Data files and even data expressions, such as Social Security and account numbers, can be recognized when they are part of data transmissions or email. An unencrypted transmission can be stopped or quarantined, or in the case of email, can be dynamically encrypted before it is allowed past the email gateway according to policy.
#7	Restrict access to cardholder data by business need-to-know	The business policy specifying who is allowed to access customer data can be monitored and enforced through Oakley's ability to integrate with an organization's Microsoft Directory Service. Violations or attempted violations of policy will be flagged, the incident will be logged, an alert will be sent to administrators and the access can be stopped if desired.
#8	Assign a unique ID to each person with computer access	Content monitoring analytics are identity and group aware and can enforce policy at that level. Thus each policy can be unique for each group or individual so that each type of organizational role can operate with its own set of rules and restrictions. Any incidents detected and logged will identify the user along with a detailed record of the actions they taken.
#10	Track and monitor all access to network resources and cardholder data	Monitoring capabilities are robust on both the network and on individual computers. All log entries will contain resource IP addresses for all systems to facilitate easy identification. Network streams such as HTTP, FTP, SMTP and others will be inspected and analyzed for content such as fingerprinted documents or regular expressions that might indicated PII. All client communications channels will be monitored and inspected, including web, email, instant messaging printing, USB resources and other removable media.
#12	Maintain a policy that addresses information security	No matter what your business policy, Raytheon Oakley Systems policy and analytics engine are well-suited to allow you to express that policy in rules and then monitor network and user activity for events and incidents that may be violations. Oakley's unique policy language helps you eliminate false positives so you don't interfere with productivity even as you keep close watch of your data.

USE CASE

COMPLYING WITH PCI-DSS REGULATIONS

Avoid Costly and Embarrassing Public Disclosures

In addition to meeting PCI requirements, Oakley will help you manage risks to your organization's brand and reputation. By protecting your customer data, Oakley will prevent you from having to make embarrassing disclosures as required under regulations such as California SB 1386 when personal customer data is breached. Likewise, it helps avoid civil suits or regulatory fines, as are possible under the PCI contract itself or through tort actions from customers that may be affected by the breach.

Oakley even has a solution for mobile computers that may contain customer data. Should that mobile computer ever be lost or stolen, when the computer is reattached to the network, Oakley can check to see whether the data has been compromised and can destroy the data before it can be discovered.

Conclusion

Raytheon Oakley Systems solutions provide network security controls that satisfy role based access and user accountability requirements for the Payment Card Industry (PCI) Data Security Standard. Oakley's unique and powerful monitoring capabilities can detect any policy violation with regards to the use of customer data and Personally Identifying Information.

Raytheon Oakley Systems

2755 E. Cottonwood Parkway
Suite 600
Salt Lake City, UT 84121

T 1.800.662.9120

E info@oakleynetworks.com

www.ravtheon.com/oaklev

Raytheon
Oakley Systems