

## white paper PCI DSS

### In Brief



### In Detail



## What is PCI DSS?

PCI DSS is a **standard** aimed at assuring that **sensitive payment card data is handled in a secure way** and that unauthorized access to this data is impeded

The Payment Card Industry Data Security Standard (PCI DSS) is a standard developed by the Payment Card Industry Security Standards Council (PCI SSC). The aim of the standard is, to prevent theft and fraudulent use of cardholder data on payment cards. Version 1.2 of the standard was released October 1, 2008.

The PCI SSC was established by the major payment card brands: American Express, Discover, JCB, MasterCard and VISA. These organizations are the driving force behind PCI DSS and their member banks in their role as acquiring organizations for payment card transactions mandate compliance to the standard.

## Who has to be compliant to PCI DSS?

PCI DSS is relevant to **anyone handling cardholder data**, be it as a merchant, a service provider or a bank.

Anyone processing, transmitting or storing cardholder data has to be compliant to PCI DSS. Cardholder data by this definition is the Primary Account Number (PAN), e.g. the number on the payment card, alone or in conjunction with other information stored on the card, as for instance the expiration date. This can apply to web shops accepting card payments as well as retail stores where cardholder data is processed in point of sale terminals. Less obvious are call centers recording conversations containing cardholder data and loyalty schemes based on payment card numbers as primary identifier of the customer.

## Why should I invest in becoming compliant to PCI DSS?

**Non-compliance to PCI DSS can have severe financial drawbacks.**

If you are a merchant, accepting payment cards, your acquiring bank will by now have updated its contract with you, stating that you will be held liable for all costs that arise in the wake of a loss of cardholder data from systems under your responsibility.

This covers

- the costs for issuing new cards
- compensation for any fraudulent use
- costs for a forensic investigation of the security breach
- legal fees
- fines by each card brand involved

In addition, many acquiring banks level fines for mere non compliance to PCI DSS. If your security is breached and you are found to be in compliance at the time of the breach, the card brands will usually cover for most if not all of these costs.

If you are a service provider, offering infrastructure and/or application services, a successful PCI DSS audit will avoid losing existing customers and can act as a market enabler, facilitating the acquisition of new customers.

PCI DSS was developed as a pragmatic and achievable standard, aimed at securing cardholder data. Compliance with PCI DSS therefore significantly reduces the risk of suffering a successful attack on systems handling cardholder data. The most devastating effect of such an attack, once it becomes public, is the loss in customer confidence, as according to recent surveys, the majority of customers will cease spending at firms that have lost cardholder data.

As it is in the interest of the card brands that payment card transactions are perceived as a secure method of payment, especially over the internet, they have gone to great length to assure that non-compliance with PCI DSS is financially less attractive overall than compliance.



## How can hyperguard help me achieve compliance?

art of defence offers the **web application firewall** *hyperguard* that **can significantly reduce the cost of compliance** in regard to public-facing web applications. According to PCI DSS these applications have either to be subjected to regular security reviews or to be protected by a WAF.

*hyperguard* is a **highly automated** product, **optimized for usability and accountability**.

It **conforms to all relevant requirements** of the standard.

*hyperguard* is **easily integrated** into the existing infrastructure.

Overall, hyperguard combines adequate, pragmatic security with minimal total cost of ownership. **always current protection**

against the OWASP Top 10 - section 6.5

### Compliance with Section 6.6

Section 6.6 of PCI DSS 1.2 requires that for **all public-facing web applications**, new threats and vulnerabilities are addressed on an ongoing basis and that these applications are protected against known attacks. This can be done by **either reviewing the applications** '... via manual or automated application vulnerability security assessment tools or methods ...', **or by** '... installing a **web application firewall** ...' in front of these applications. The first alternative requires, that all applications are reviewed at least annually and after any changes, that reviews are conducted '... by an organization ...', whether external or internal, '... that specialises in application security ...', that all detected vulnerabilities are corrected before release of the application and that '... the application is re-evaluated after the corrections ...'.

Using a web application which is certified according to the Payment Application Data Security Standard (PA DSS) to safely handle cardholder data does not exempt the user from compliance to PCI DSS section 6.6. This means that even a PA DSS compliant, public facing web application has either to be objected to security reviews or to be protected by a web application firewall.

#### First Alternative: regular Security Review

Reviewing an application is only a viable approach, if

- there is either access to the source code and to the developers of the application

or

- there is a **reliable communication channel** to the **vendor** of the application

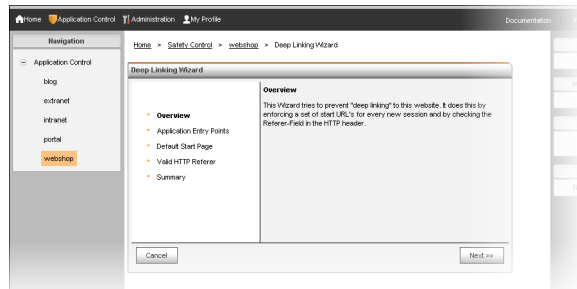
so that detected vulnerabilities can be corrected rapidly and efficiently.

This applies to all components of a web application, including frameworks and other third-party products. In some cases, waiting for a vendor to supply security patches can make fielding a web application or one of its components in compliance with PCI DSS utterly impossible, as any new patch supplied by the vendor introduces additional vulnerabilities, sometimes without fully addressing all known bugs. In addition, regular security reviews of large applications, even if automated, can be very time-consuming and expensive.

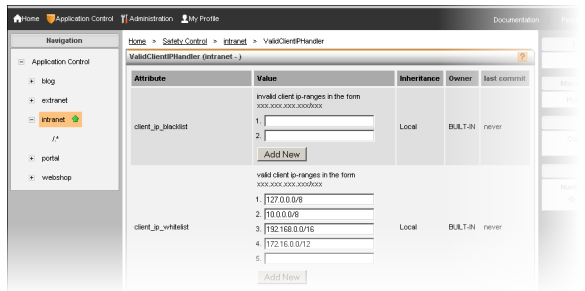
#### Second Alternative: installing a Web Application Firewall

These possible pitfalls can be avoided by choosing the second alternative: installing a web application firewall (WAF). These products **extend the protection provided by a classical network firewall** to the application level. They analyse all requests and responses and can discriminate between legitimate user interaction and malicious penetration attempts. In case an attack has been detected, it can be immediately blocked before reaching the application. Common attacks a WAF can protect against are SQL and code injection as well as cross-site scripting. In the current Information Supplement: Requirement 6.6, an 'application firewall' is defined as '... a web application firewall (WAF), which is a security policy enforcement point positioned between a web application and the client end point. **This functionality can be implemented in software or hardware, running in an appliance device, or in a typical server** running a common operating system. It may be a **stand-alone device or integrated into other network components**. ...' *hyperguard* is such a web application firewall.

Configuring basic protection for a web application in accordance to the PCI DSS criteria, as described in section 6.5 can be accomplished with a few mouse clicks. *hyperguard* is **highly automated and optimized for usability**, significantly reducing administrative costs and avoiding expensive configuration errors. It offers two levels of detail to the administrator: a Basic Mode and an Expert Mode.



The **Basic Mode** allows for a rapid, wizard driven configuration.



In **Expert Mode**, all rule sets can be examined and configured down to the individual regular expression and protection levels can be further extended up to custom protection of every single input field.

Before deploying changes to a rule set, they can be activated in a **Detection Mode**. This can be useful in verifying that none of the changes have a negative impact on the legitimate use of the application. All changes to the WAF are automatically recorded, giving a **complete audit trail**, as required for all system components by sections 10.2 and 10.3 of PCI DSS. The resulting logs can be **automatically monitored** and an alerting by mail, by writing to a log file or by posting a http request can be configured. This is very useful in fulfilling the requirements in section 10.6, which states, that logs for all system components have to be reviewed daily, either manually or with the help of appropriate tools. As manual review of the logs is in most cases less than impractical, the alerting mechanisms of *hyperguard* offer a convenient and efficient way of compliance.

The deployment of *hyperguard* requires **no changes to the underlying web-infrastructure**, as *hyperguard* is available as a plugin for most web and application servers as well as for selected network firewalls and load balancers. Not only does this **reduce the total cost of ownership** in comparison to an appliance based WAF by making optimum use of the existing infrastructure. It also enhances the theoretical availability of the protected applications by avoiding another component which can fail.

An additional advantage of this architecture is the **horizontal scalability** together with the number of web or application server instances. *hyperguard* can be deployed in the same cluster configuration as the underlying infrastructure, offering the same **high availability** features without any additional hardware or software.

All instances of *hyperguard* can be remotely administrated from a single management server via a web-interface.

automated and complete audit trail - sections 10.2 and 10.3

automated log review via alerting - section 10.6



unique IDs for all users - section 8.1

secure authentication - section 8.2

strong cryptography for password storage and transmission - section 8.4



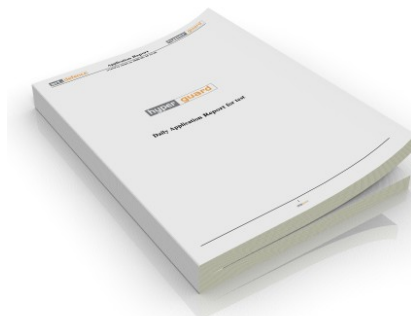
The **web based administration front end** gives an overview of the current status of all protected applications. New rule sets can be defined and deployed from the central administration server, **greatly reducing costs for management and deployment** in larger infrastructures.

As required by section 8.1 **users accounts with unique IDs** can be set up for each individual user of *hyperguard*.

In accordance with section 8.2, login is only possible by entering user name and valid password.

**Login is encrypted** via SSL, using strong cryptography in order to comply to section 8.4 of PCI DSS. As mentioned earlier, all access to the hyperguard front end is logged, thus providing a complete audit trail.

**Segregation of duties** is supported by offering two different authorization levels: hyperguard admin and application admin. As the name implies, a user with hyperguard admin privileges has full access to all configuration items. An application admin can only change configuration items related to the application(s) he has been authorized for. Each authorization level can also be configured as read-only, for instance allowing management users to access real time security information without the risk of accidentally changing the configuration.



With the help of *hyperguard*, concise and comprehensible **web security reports** are available at the click of a button. Besides details on the configuration, the reports contain textual and graphical information on **allowed** and **denied** application access and the audit log. These reports offer the ability to easily **prove that adequate security measures** were and are in place to protect cardholder data.