Data Sheet

# STEALTHbits Technologies & PCI-DSS

**Overview**

Over time, Government and industries have cooperated to create multiple security standards that protect you, your employees, and your customers against fraud, theft, and malicious attacks. PCI-DSS is one of the most common cross-vertical security compliance standards in the world. This standard is enforced worldwide by all major credit card companies. PCI-DSS is necessary to ensure security of your customer's credit card information, consumer identity, and to prevent theft and fraud.

PCI-DSS is continuously evolving, but breaks down to several essential security precepts that are directly supported by STEALTHbits Technologies.

## How STEALTHbits Can Help:

### Deep Insight and Access Enforcement to Cardholder Data

Organizations need to monitor systems that contain cardholder data in real-time to provide trend-information around creations, deletions and modifications associated with user and group access. This trend information allows organizations the ability to identify risk/abnormal/high -risk patterns of interest, allowing unauthorized access to be easily detected around critical systems storing cardholder data. Being able to discover, assess, protect, and enforce access to critical enterprise assets containing cardholder data enables organizations to adhere to PCI-DSS year over year, reducing the risk of sensitive information exposure. The **StealthAUDIT Management Platform**, **StealthINTERCEPT**, and **StealthSEEK** provide a strong organizational foundation ensuring cardholder data is protected and PCI-DSS compliance is observed organization wide.

### Real-Time Monitoring and Access Risk Analytics to Cardholder Data

Tracking and monitoring all access around cardholder data is a key requirement of PCI-DSS compliance. The **StealthAUDIT Management**

## Explore STEALTHbits' Solutions:

⇒ StealthAUDIT® Management Platform

- Audit and manage access to cardholder data while streamlining compliance processes

http://stealthbits.com/products/stealthaudit-management-platform

⇒ StealthINTERCEPT®

- Protect cardholder  data from breach and abuse

http://stealthbits.com/products/stealthintercept

⇒ StealthSEEK®

- Discover and identify cardholder  data

http://stealthbits.com/products/stealthseek

**Platform**, **StealthINTERCEPT**, and **StealthSEEK** provide visibility into the key questions your organization needs to answer not only for PCI-DSS compliance; but, enterprise security overall:

- Who is logging into a system that contains cardholder data?
- Where in my enterprise does card-holder data reside?
- What are users doing on systems that contain cardholder data?
- Why do resources outside of PCI-DSS compliance scope contain cardholder data, and why are my employees accessing, distributing, and interacting with this cardholder data?

Visibility is the key to answering the questions above; and visibility means combining real-time actions, monitoring log messages, and mapping user activity to security events – that is true visibility. This enterprise security visibility around cardholder data is presented in detailed event reports and interactive dashboards that allow an organization to zero in on risk patterns associated with PCI-DSS compliance.

An enterprise that installs STEALTHbits Technologies' solutions — choosing to perform no other action — ensures their organizational efforts will be successful towards creating and maintaining an enterprise security policy around PCI-sensitive data.

## Enterprise-Wide Enforcement of Cardholder Data Security Policies

Protecting stored cardholder data on servers, file-systems, Exchange, and SharePoint environments is paramount to PCI-DSS compliance. These source systems are typically defined as "unstructured data" repositories and quite often are overlooked as part of the PCI-DSS compliance process. "Structured data" systems that store cardholder data are always in-scope; however, the "unstructured data" systems and sources are often included in-scope after a material observation is found, or even worse when an organization's data becomes breached via an "unstructured data" repository.

> ***An enterprise that installs STEALTHbits Technologies' solutions — choosing to perform no other action — ensures their organizational efforts will be successful...***

The **StealthAUDIT Management Platform**, **StealthINTERCEPT**, and **StealthSEEK** provide the ability to detect, monitor, protect, and enforce enterprise security policies around the unstructured repositories containing cardholder data allowing your organization the ability to implement a 360 degree PCI-DSS compliance strategy.

## Enable Compliance

STEALTHbits' solutions specifically help facilitate compliance with PCI-DSS using out-of-the-box reporting templates fed by automated auditing routines and built-in business intelligence incorporating compliance classifications. By using STEALTHbits' solutions, organizations can be assured that they meet the intent of PCI-DSS security provisions, and can demonstrate their compliance for securing cardholder data and systems that house cardholder data as a normal part of their operational security.

The current version of the PCI-DSS standard consists of twelve (12) different sections, dealing with securing a network against unauthorized access. This includes physical security, information security, and security policies.

The specific areas where STEALTHbits Technologies can help organizations comply with the PCI-DSS Compliance standard are described below:

## PCI 2.1: Always change vendor-supplied defaults before installing a system on the network. This includes wireless devices that are connected to the cardholder data environment or are used to transmit cardholder data.

- The **StealthAUDIT Management Platform** provides system governance capabilities that would allow the auditing of critical system configurations to be monitored for deviations from vendor default settings. The analysis provides organizations the ability to immediately address default settings on critical systems to ensure cardholder data environment is protected.

## PCI 2.2: Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions. Update system configuration standards as new vulnerability issues are identified.

- The **StealthAUDIT Management Platform** provides system governance capabilities that would allow the auditing of critical system configurations standards to actual settings across system components within an organization. Baseline standards can be updated as new vulnerabilities are discovered, allowing the baseline to reflect the most recent security standards enabling organizations to assess their adherence to compliance standards at any time.

## PCI 3.1: Limit cardholder data storage and retention time to that required for business, legal, and/or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly.

- The **StealthAUDIT Management Platform** provides the ability to identify cardholder data stored within unstructured data repositories (file shares, SharePoint sites) and purge the data based off of data retention polices. For example, deletion of any PCI data older than seven (7) years.
- Cardholder Data Elements found:
    - Primary Account Number (PAN)
    - Cardholder Name
    - Service Code
    - Expiration Data

## PCI 5.2: Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

- The **StealthAUDIT Management Platform** provides the ability for organizations to verify .DAT file versions in the environment are at proper levels, anti-virus services are running and set properly, and event log settings conform to an organization’s defined policies.

## PCI 6.1: Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Deploy critical patches within a month of release.

- The **StealthAUDIT Management Platform** provides the ability for organizations to conduct patch validation auditing that is updated monthly to ensure the latest high-priority security bulletins are accounted for during scans.

## PCI 6.2: Establish a process to identity and assign a risk ranking to newly discovered security vulnerabilities. Risk rankings should be based on industry best practices and guidelines.

- The **StealthAUDIT Management Platform** helps customers determine based on scanning their computer and server infrastructure and analyzing the results of those scans providing what specific Microsoft security patches need to be applied to their environment to ensure cardholder data is secured on critical systems within their organization.

## PCI 7: Limit Access to Cardholder Data by Business Need to Know

- Organizations that restrict access cardholder data to authorized personnel only greatly reduce the risk of a data breach within their organization. Ensuring organizations limit user access to cardholder data by deploying a least privileged access model enabling users to perform their job function without compromising cardholder data is the definition of PCI-DSS requirement 7. **StealthAUDIT Management Platform** can automate the aggregation, management, and auditing of user access across all critical systems within the organization (domain controllers, Windows file servers, network attached storage devices) including Microsoft SharePoint. Understanding the “who, what, where, and when” around the systems that contain cardholder data allows an organization the ability to answer the why and subsequently streamline compliance efforts and processes.

## PCI 7.1: Limit access to system components and cardholder data to only those individuals whose job requires such access

- The **StealthAUDIT Management Platform** provides workflows for reviewing and revoking access to sensitive PCI data stored within file shares and SharePoint environments. This empowers the data owners to decide who needs access and revoke unwarranted access rights for users who no longer need it. (e.g. have change job roles). Auditing of groups and group membership is the basis for understanding who has access to what within systems that contain cardholder data. **StealthINTERCEPT** provides real-time monitoring of any and all access, system, application, administrative privileges, and changes to Active Directory, Microsoft Exchange Mailboxes, and File Shares on Windows, NetApp, and Isilon devices providing a complete audit trail of all critical events to the organization.

## PCI 7.2: Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed

- The **StealthAUDIT Management Platform** enables auditing and enforcement of proper permissions and access controls across unstructured data stores where PCI data is kept, as well as the ability to enable data owners to review and revoke unnecessary access rights. Detailed information about which users are in which groups combined with where those groups provide access informs how controls should be established.

- Real-time monitoring of any and all access changes to Active Directory with complete audit trail. System and Application-level auditing of Active Directory administrative privileges and changes.

## PCI 8.1: Assign all users a unique user name before allowing them to access system components of cardholder data.

- The **StealthAUDIT Management Platform** including **StealthINTERCEPT** provides complete auditing of user logons to analyze violations and through policy can prevent the usage of the same ID by multiple individuals from different computers.

## PCI 8.5: Disable Dormant User Accounts

- PCI-DSS compliance explicitly states that organizations need to ensure there is secure user authentication to their network and systems that contain cardholder data. The secure user authentication service according to PCI-DSS must also adhere to a password management process where according to PCI requirement 8.5.5 user accounts must be disabled after ninety (90) days of inactivity. 8.5.5 further states that any and all access privileges associated with terminated users must be revoked from their user authentication accounts. Organizations can schedule the distribution of reports and receive real-time alerts around user activity, dormant accounts within their environment, and terminated users with access ensuring PCI compliance is adhered to with deep insight provided by **StealthAUDIT**, **StealthINTERCEPT**, and **StealthSEEK** solutions.

## PCI 10: Audit All Access to Cardholder Data.

- PCI-DSS requirements state organizations must track and monitor all user access to systems that contain cardholder data. Systems can be defined as servers, file servers, laptops/desktops, even Microsoft SharePoint. Section 10 details within the sub-requirements how organizations must track all activity to individual users, audit privileged user activity and even more importantly track and restrict access to audit trails on systems containing cardholder data. The **StealthAUDIT Management Platform**, **StealthINTERCEPT,** and **StealthSEEK** combined provide the foundation for organizations to ensure section 10 of PCI-DSS is met without impacting their organization's services or requiring additional in-house audit and compliance tools. A single platform to discover, assess, remediate, protect, and enforce is the solution from STEALTHbits Technologies.

## PCI 10.1: Establish a process for linking all access to system components to each individual user – especially access done with administrative privileges

- The **StealthAUDIT Management Platform** and **StealthINTERCEPT** enables the tracking of all access events to network resources (file shares, SharePoint) with cardholder data. **StealthINTERCEPT's** real-time monitoring of any and all access changes to Active Directory with complete audit trail including system and application-level auditing of Active Directory administrative privileges and changes.

## PCI 10.2: Implement automated audit trails for all system components for reconstructing these events; all individual user accesses to cardholder data; all actions taken by an individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of identification and authentication mechanisms; initialization of the audit logs; creation and deletion of system-level objects

- The **StealthAUDIT Management Platform** and **StealthINTERCEPT** provide network level auditing to monitor user access events as well as local system auditing to monitor privileged access, escalation of access rights, the creation of admin accounts and manipulation of system permissions to grant elevated access. Active Directory change tracking reports provide insight into changes taking place within sensitive security groups, creation and deletions, object movements and more within the environment. **StealthINTERCEPT's** real-time monitoring of any and all access changes to Active Directory with complete audit trail including system and application-level auditing of Active Directory administrative privileges and changes.

## PCI 10.3: Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, data and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.

- The **StealthAUDIT Management Platform** and **StealthINTERCEPT** provide a complete audit trail for shared folders across Windows and Network Attached Storage (NAS) devices as well as SharePoint. Auditing of domain controller security logs provides detailed information on who is responsible for changes within the environment and illustrates additional information to provide context for the change. **StealthINTERCEPT's** real-time monitoring of any and all access changes to Active Directory with complete audit trail including system and application-level auditing of Active Directory administrative privileges and changes.

## PCI 10.5: Secure audit trails so they cannot be altered.

- STEALTHbits' **StealthINTERCEPT** solution receives information from managed devices in real-time, securing this information at a remote location as it is generated, preventing alteration or loss of this data by any action that can occur at the managed node. **StealthINTERCEPT** provides an organization the ability to secure audit trail information that can't be altered by storing the information within the **StealthINTERCEPT** solution framework. The solution has no dependency on native source logging.

- Real-time monitoring of audit logs and where they are located allows **StealthINTERCEPT** to protect native logs; but also provides an unprecedented level of protection against audit trail tampering.

- Using **StealthINTERCEPT's** audit logs, an organization can show detailed change records including changes to permissions. **StealthINTERCEPT's** internal self-auditing allows an organization to show audit records for **StealthINTERCEPT** itself, providing auditors a record of any change or exception to data capture.

## PCI 10.5.1: Limit viewing of audit trails to those with a job-related need.

- STEALTHbits' solutions are able to provide a verifiably secure way of limiting access to log data and audit trails. A secure login is needed to view data within **StealthAUDIT** and **StealthINTERCEPT** respective servers, employing AES-256 encryption. Within the **StealthAUDIT Management Platform** and **StealthINTERCEPT**, users are granted a permission level that can limit the view of data and operations performed on the data.

## PCI 10.5.2: Protect audit trail files from unauthorized modifications via access control mechanisms, physical segregation and/or network segregation.

- **StealthAUDIT Management Platform**, **StealthSEEK**, and **StealthINTERCEPT** both utilize techniques to protect audit trails within the respective solution. The data is firstly physically segregated from the system that generates it – the fast, flawless, agentless scanning within the **StealthAUDIT** platform and the real-time monitoring and scanning available within **StealthINTERCEPT** ensure all information collected is and transferred to the solution back-end repository – SQL Server. The **StealthAUDIT** Management console employs role based access controls based on secure encrypted logins to the system ensuring unauthorized access is prevented and all log information within the solution and collected from the environment are properly controlled and meet compliance requirements.

## PCI 10.5.4: Write log files for external facing technologies onto a server on an internal LAN. Verify that logs are offloaded or copied onto a secure centralized internal log server or media.

- Where **StealthAUDIT**, **StealthSEEK**, and **StealthINTERCEPT** log and archive data is stored is completely configurable within the respective solution platform. Archive information can be distributed and secured via a number of methodologies defined by the organization.

## PCI 10.7: Retain audit trail history for at least one year, with minimum of three months immediately available for analysis.

- The **StealthAUDIT Management Platform** and **StealthINTERCEPT** solutions provide customers the ability to configure online data availability to their organizations requirements. Archiving of data is customer defined and can be re-imported into the STEALTHbits solutions for analysis.

## PCI 11.4: Use network intrusion detection systems and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.

- Real-time monitoring of any and all access changes to Active Directory with complete audit trail. System and Application-level auditing of Active Directory administrative privileges and changes. Security policy definitions to lock down critical assets within the organization can be deployed via **StealthINTERCEPT** to ensure the protection of data and generate contextual alerts to security and process personnel if a process and or system is suspected or becomes compromised.

## PCI 11.5: Alert Personnel to Unauthorized Modification of Files

- The **StealthAUDIT Management Platform** Data Activity Tracking capabilities provides organizations the ability to ensure files and folders are tracked to determine if unauthorized modifications or access occurs.

PCD-DSS 11.5 requirement states that critical systems, their configurations, and content files containing cardholder data be monitored for unauthorized modification. Even authorized modifications can be subject to compliance inquiries allowing **StealthINTERCEPT** to be the perfect solution to monitor, protect, and enforce these critical areas containing cardholder data within the enterprise.

## CONTACT US

STEALTHbits Technologies, Inc. | 200 Central
Avenue | Hawthorne, NJ 07506 | USA

W. www.stealthbits.com

E. sales@stealthbits.com

P. +1-201-447-9300 | F. +1-201-447-1818

**Like:** www.facebook.com/stealthbits

**Follow:** www.twitter.com/stealthbits

**Watch & Learn:** www.youtube.com/stealthbits

**Read:** www.stealthbits.com/blog