stealthbits
NOW PART OF netwrix

EXECUTIVE BRIEF

STEALTHBITS TECHNOLOGIES AND PCI-DSS

AUDIT AND MANAGE ACCESS TO CARDHOLDER DATA

PCI-DSS is one of the most common cross-vertical security compliance standards in the world and is enforced 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.

BENEFITS

StealthAUDIT discovers and identifies cardholder data, manages and audits access to this data, and streamlines compliance processes. StealthINTERCEPT protects cardholder data from breach and abuse.

- **Gain insight and enforce access to cardholder data**
- **Enforce cardholder data security policies**
- **Monitor cardholder data in real-time**
- **Enable compliance**

DEEP INSIGHT AND ACCESS ENFORCEMENT

Discover, assess, protect, and enforce access to critical enterprise assets containing cardholder data to adhere to PCI-DSS year-over-year, reducing the risk of sensitive information exposure.

REAL-TIME MONITORING

Track and monitor all access around cardholder data in detailed event reports and interactive dashboards to zero –in on risk patterns associated with PCI-DSS compliance.

ENFORCEMENT OF SECURITY POLICIES

Detect, monitor, protect, and enforce enterprise security policies around the unstructured repositories containing cardholder data to implement a 360-degree PCI-DSS compliance strategy.

ENABLE COMPLIANCE

Use out-of-the-box reporting templates fed by automated auditing routines and built-in business intelligence incorporating compliance classifications to meet the intent of PCI-DSS security provisions and demonstrate compliance.

PCI-DSS STANDARDS WHERE STEALTHBITS CAN HELP

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

StealthAUDIT provides system governance capabilities that 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

StealthAUDIT provides system governance capabilities that enable the auditing of critical system configurations standards to actual settings across system components. Baseline standards can be updated as new vulnerabilities are discovered, allowing the baseline to reflect the most recent security standards.

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

StealthAUDIT 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

StealthAUDIT 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

StealthAUDIT 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

StealthAUDIT helps customers determine, based on scanning their computer and server infrastructure and analyzing scan results, the specific Microsoft security patches that 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

StealthAUDIT ensures organizations limit user access to cardholder data by deploying a least privileged access model that enables users to perform their job function without compromising cardholder data. StealthAUDIT automates the aggregation, management, and auditing of user access across critical systems to 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

StealthAUDIT provides workflows for reviewing and revoking access to sensitive PCI data stored within file shares and SharePoint environments. This empowers data owners to decide who needs access and to revoke unwarranted access rights for users who no longer need them (e.g. have changed job roles). StealthINTERCEPT provides real-time monitoring of 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

StealthAUDIT 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. StealthINTERCEPT provides real-time monitoring of all access changes to Active Directory, as well as 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

StealthAUDIT and StealthINTERCEPT provide complete auditing of user logons to analyze violations and use policy to 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. PCI requirement 8.5.5 states that 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 and StealthINTERCEPT.

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. StealthAUDIT and StealthINTERCEPT 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.

PCI 10.1: ESTABLISH A PROCESS FOR LINKING ALL ACCESS TO SYSTEM COMPONENTS TO EACH INDIVIDUAL USER – ESPECIALLY ACCESS DONE WITH ADMINISTRATIVE PRIVILEGES

StealthAUDIT and StealthINTERCEPT enable the tracking of all access events to network resources (file shares, SharePoint) with cardholder data. StealthINTERCEPT's real-time monitoring of all access changes to Active Directory provides a 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

StealthAUDIT 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 the manipulation of system permissions to grant elevated access. Active Directory change tracking reports provide insight into changes taking place within sensitive security groups, creations and deletions, object movements and more within the environment. StealthINTERCEPT's real-time monitoring of all access changes to Active Directory provides a 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

StealthAUDIT 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 all access changes to Active Directory provides a 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

StealthINTERCEPT 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. StealthINTERCEPT provides real-time monitoring of audit logs and shows where they are located to allow the protection of native logs—and 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 with 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's and StealthINTERCEPT's respective servers, employing AES-256 encryption. Within StealthAUDIT 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 and StealthINTERCEPT both utilize techniques to protect audit trails. The data is first physically segregated from the system that generates it – the fast, flawless, agentless scanning within StealthAUDIT, and the real-time monitoring and scanning available within StealthINTERCEPT, ensures all information is collected and transferred to the solution back-end repository – SQL Server. The StealthAUDIT 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 is properly controlled and meets 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

StealthAUDIT and StealthINTERCEPT log and archive data 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

StealthAUDIT and StealthINTERCEPT provide customers with the ability to configure online data availability to their organization's requirements. Archiving of data is customer-defined and can be re-imported into 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

StealthINTERCEPT provides real-time monitoring of all access changes to Active Directory with a complete audit trail, including 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

StealthAUDIT's Data Activity Tracking capabilities provide organizations with 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.

NEXT STEPS

Schedule a demo
stealthbits.com/demo

Download a free trial
stealthbits.com/free-trial

Contact us
info@stealthbits.com

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

stealthbits
NOW PART OF netwrix