# COMPLIANCE BRIEF:
# HOW VARONIS HELPS WITH PCI DSS 3.1

## OVERVIEW

The Payment Card Industry Data Security Standard (PCI-DSS) 3.1 is a set of regulations that govern how firms that process credit card and other similar transactions  handle cardholder data. The standard applies to all organizations which hold, process, or exchange cardholder information from any card branded with the logo of MasterCard, Visa, American Express, or Discover.

While the majority of this type of information is usually stored in a structured environment—a database—it also makes its way onto unstructured and semi-structured systems. How? Users *pull from databases* and import credit card data to spreadsheets, documents, PowerPoints and emails. These unstructured data files containing sensitive customer data are generally kept for long periods of time. As such, it's important for organizations to have the ability to identify, monitor and manage access to this unstructured data, not just its structured data.

PCI DSS lays out twelve requirements for the handling of cardholder data, organized into six logical "control objectives." Keep in mind, though, that DSS is not only about  passing an annual compliance audit, but also having programs in place for continual assessments, implementation of remediations, and monitoring.

### Mapping Requirements to Varonis

Varonis products can assist an organization in meeting many of these compliance objectives with regard to any cardholder data that resides on unstructured and semi-structured file systems. See the following chart for a point-by-point analysis of these requirements and the corresponding Varonis solution.

| PCI DSS 3.1 | Description | Varonis Solutions |
|---|---|---|
| 3. Protect stored cardholder data | 3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows:<br>3.1.1 Implement a data retention and disposal policy that includes:<br>- Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements<br>- Processes for secure deletion of data when no longer needed<br>- Specific retention requirements for cardholder data<br>- A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements<br>3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:<br>• There is a business justification<br>• The data is stored securely | **Identify Sensitive Cardholder Data**<br>Use an efficient, incremental data classification and indexing engine like Varonis' IDU Classification Framework to first identify where sensitive cardholder data is stored. You'll be able to understand where cardholder data is located so it can be properly retained or disposed of when no longer needed.<br>**Retain, Archive or Dispose Cardholder Data**<br>Varonis Data Transport Engine in conjunction with Varonis Data-Classification Framework provides the flexibility to configure complete end-to-end migration rules: define source criteria based on path, and/or content, classification rule, Varonis ownership and follow-up (flag/ tag) criteria, define destination path, folder, and permissions translation, and when the migration will take place. The ability to configure these rules allow for the rapid and safe execution of complex data migrations, and to easily implement and enforce policies for data retention and location based on content, accessibility, and activity. |
| 7. Restrict access to cardholder data | 7.1 Limit access to system components and cardholder data to only those | Varonis provides a comprehensive system to restrict access to business need-to-know |

| | | |
|---|---|---|
| by business need-to-know | individuals whose job requires such access.<br>• 7.1.1 Define access needs for each role, including:<br>○ System components and data resources that each role needs to access for their job function<br>○ Level of privilege required (for example, user, administrator, etc.) for accessing resources.<br>• 7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.<br>• 7.1.3 Assign access based on individual personnel's job classification and function.<br>• 7.1.4 Require documented approval by authorized parties specifying required privileges.<br>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.<br>This access control system must include the following:<br>• 7.2.1 Coverage of all system components<br>• 7.2.2 Assignment of privileges to individuals based on job classification and function | **Access Control System**<br>Varonis DatAdvantage monitors every user's file touch and stores in a searchable format, all aspects of data use for information stored on file servers and Network Attached Storage (NAS) devices.<br>Because DatAdvantage reveals who has access to data and every use file touch, it also recommends the revocation of permissions to data for users who do not have a business need-to-know to the data – this ensures that user access to data is always warranted and driven by least privilege.<br>DatAdvantage provides data stewards with detailed reports, including: data use (i.e. every user's every file-touch), user activity on sensitive data, permission changes that affect the access of a given file or folder, a detailed record of permission revocations including the users and the data for which permissions were revoked.<br>Varonis DataPrivilege is a web-based application that controls, monitors and administers a user's requests to unstructured data (files, emails, SharePoint, etc.)<br>**Attestations**<br>DatAdvantage and DataPrivilege gives the means to conduct a full in depth data entitlement review by which all user privileges to data is reported. It also provides reports of historical access rights to data sets showing any trends toward overly permissive access. |

| | | |
|---|---|---|
| | - 7.2.3 Default —deny-all setting Note: Some access control systems are set by default to —allow-all, thereby permitting access unless/until a rule is written to specifically deny it. | |
| 8. Identify and authenticate access to system components | 8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators<br>8.1.3 Immediately revoke access for any terminated users.<br>8.1.4 Remove/disable inactive user accounts within 90 days.<br>8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:<br>• Enabled only during the time period needed and disabled when not in use.<br>• Monitored when in use. | **Revoke Access for Terminated and Inactive Users**<br>Varonis identifies disabled user accounts as well as inactive users. Specifically, Varonis can run an automated report for users who are inactive for a set period of time including 90 days period. These users can then be removed within Varonis DatAdvantage.<br>Varonis DataPrivilege allows for accounts used by vendors to have automated expiration dates.<br>[JR1] |
| 10. Track and monitor all access to network resources and cardholder data | 10.1 Implement audit trails to link all access to system components to each individual user.<br>10.2 Implement automated audit trails for all system components to reconstruct the following events:<br>• 10.2.1 All individual accesses to cardholder data<br>• 10.2.2 All actions taken by any individual with root or administrative privileges | DatAdvantage helps organizations examine and audit the use of privileged access accounts to detect and prevent abuse. The Varonis audit trail includes date, time, user who touched the data, the operation type (open, rename, modify, delete, etc.) and the object that was touched.<br>With a continual audit record of all file, email, SharePoint, and Directory Services activity, DatAdvantage provides visibility into administrative users' actions. The log can be viewed interactively or via email reports. The audit trail can also be set to auto archive and can be retained. |

| | | |
|---|---|---|
| | • 10.2.3 Access to all audit trail<br>10.3 Record at least the following audit trail entries for all system components for each event:<br>• 10.3.1 User identification<br>• 10.3.2 Type of event<br>• 10.3.3 Date and time<br>• 10.3.5 Origination of event<br>• 10.3.6 Identity or name of affected data, system component, or resource.<br>10.5 Secure audit trails so they cannot be altered.<br>• 10.5.1 Limit viewing of audit trails to those with a job-related need.<br>• 10.5.2 Protect audit trail files from unauthorized modifications.<br>• 10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.<br>10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.<br>• 10.6.1 Review the following at least daily:<br>○ All security events<br>10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up). | DatAdvantage can also identify when users have administrative rights they do not use or need and provides a way to safely remove excess privileges without impacting the business. Through DataPrivilege, membership in administrative groups can be tightly controlled, audited and reviewed.<br>DatAlert can be configured to send real-time alerts on a number of actions including the granting of administrative rights to a user or group. This allows the organization to detect, in real-time, when privileged access has been granted erroneously and act before abuse occurs. |

| | | |
|---|---|---|
| 12. Maintain a policy that addresses information security for all personnel. | 12.2 Implement a risk-assessment process that:<br>• Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),<br>• Identifies critical assets, threats, and vulnerabilities, and<br>• Results in a formal, documented analysis of risk.<br>12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)<br>12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use<br>12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.<br>12.5.5 Monitor and control all access to data.<br>12.6.1 Educate personnel upon hire and at least annually.<br>12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.<br>12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually. | **Risk Assessment**<br>Varonis DatAdvantage and IDU Classification Framework identifies and prioritizes areas of risk by highlighting where sensitive information is overexposed and at risk, where employees have oversubscribed access, and alerts on abnormal behavior and potential abuse.<br>DatAdvantage and DataPrivilege gives the means to conduct a full in depth data entitlement review that follows a company's Security Policy by which all user privileges to data is reported.<br>It also provides reports of historical access rights to data sets showing any trends toward overly permissive access.<br>**Educating Personnel**<br>Varonis staff are also avid learners and educators. Here are some of the educational opportunities we offer and provide:<br>• Professional Services: ensures our customers can effectively use the product to fulfill all their use cases and to use our products.<br>• Varonis Blog: learn more about security, privacy, IT Operations and more on our blog. We post approximately 3-4 blog posts per week<br>• Office Hours: 1 free hour one-on-one live web session with your local<br>--<br>To see how Varonis can help identify data owners, monitor access, as well as reporting features, read how Varonis helps with Requirement 7 and 10. |

| | | |
|---|---|---|
| | 12.10.5 Include alerts from security monitoring systems file-integrity monitoring systems. | |