Powered by DRATA

Vision Menu, Inc

Security & Compliance Report › Last Updated: October 16, 2025

Report Summary

Drata tests Vision Dealer Solutions's security and IT infrastructure daily to ensure the company maintains a strong security posture, as defined by industry-standard security standards.

In this report, Vision Dealer Solutions:

- Tests a complete set of security and infrastructure controls that may appear in an audit
- Identifies gaps and vulnerabilities in infrastructure and processes

This document is updated continuously. As Vision Dealer Solutions improves its security posture, those efforts will be instantly visible.

Intended Use:

This Vision Dealer Solutions Report can be used by:

- Vision Dealer Solutions to identify issues critical for remediation
- Vision Dealer Solutions's customers to understand the company's security posture

Drata's Approach of Continuous Monitoring:

Drata continuously monitors the company's policies, procedures, and IT infrastructure to ensure the company adheres to industry standards.

To do this, Drata connects directly to the company's infrastructure accounts, version control and developer tools, task trackers, endpoints, hosts, HR tools, and internal policies. Drata then continuously monitors these resources to determine if the company meets defined framework standards.

Data and Privacy

Customer Data Policies

2 CONTROLS:

Customer Data Policies

Vision Dealer Solutions Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.

Continuously Monitored via 2 Drata Tests:

Policies Cover Employee Access

Inspected Vision Dealer Solutions's policies and confirmed that they outline the requirements for granting employees access to and removing employees access from customer data.

Policies Cover Employee Confidentiality

Inspected Vision Dealer Solutions's policies and confirmed that they require employees to keep confidential any information they learn while handling customer data.

Least-Privileged Policy for Customer Data Access

Vision Dealer Solutions authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.

Continuously Monitored via 1 Drata Test:

Least Privilege Policy for Customer Data Access

Inspected Vision Dealer Solutions's security policies and confirmed that they require that employees may only access the customer data they need in order to complete their jobs.

Internal Admin Tool

1 CONTROL:

Require Encryption of Web-Based Admin Access

Vision Dealer Solutions uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.

Continuously Monitored via 1 Drata Test:

SSL/TLS on Admin Page of Infrastructure Console

Inspected Vision Dealer Solutions's admin page and login of the company's Infrastructure as a Service provider and determined that all connections happen over SSL/TLS with a valid certificate from a reliable Certificate Authority.

Internal Security Procedures

Software Development Life Cycle

5 CONTROLS:

Critical Change Management

Vision Dealer Solutions authorizes designated member(s) with the autonomy to validate, change, and release critical security patches and bug fixes, outside of the standard change management process, when absolutely necessary to ensure security standards and availability of the systems.

Version Control System

Vision Dealer Solutions uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.

Continuously Monitored via 3 Drata Tests:

A Version Control System is being Used

Inspected Vision Dealer Solutions's version control system and confirmed it is being used

Only Authorized Employees Access Version Control

Inspected Vision Dealer Solutions's version control system and confirmed that the users of the tool were all authenticated to the company's account.

Only Authorized Employees Change Code

Inspected Vision Dealer Solutions's version control system and confirmed that approved employees can make changes to the code on a branch to which they have approval.

Code Review Process

When Vision Dealer Solutions's application code changes, code reviews and tests are performed by someone other than the person who made the code change.

Continuously Monitored via 1 Drata Test:

Formal Code Review Process

Drata inspected Vision Dealer Solutions's SDLC and confirmed that code changes are reviewed and tested by someone other than the person who made the code change.

Production Code Changes Restricted

Only authorized Vision Dealer Solutions personnel can push or make changes to production code.

Continuously Monitored via 1 Drata Test:

Production Code Changes Restricted

Drata inspected Vision Dealer Solutions's version control tool and confirmed that only authorized personnel push or make changes to production code.

Separate Testing and Production Environments

Separate environments are used for testing and production for Vision Dealer Solutions's application

Responsible Disclosure Policy

2 CONTROLS:

Employee Disclosure Process

Vision Dealer Solutions provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.

Continuously Monitored via 1 Drata Test:

Process for Responsible Disclosure

Drata inspected Vision Dealer Solutions's security policies and confirmed that they detail a process for employees to report security, confidentiality, integrity, and availability failures, incidents, and concerns.

Disclosure Process for Customers

Vision Dealer Solutions provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.

Continuously Monitored via 1 Drata Test:

Contact Information Available to Customers

Vision Dealer Solutions has provided a URL to their customer-accessible support documentation where support contact information is readily available. Drata also confirmed that users are encouraged to contact appropriate Vision Dealer Solutions personnel if they become aware of items such as operational or security failures, incidents, system problems, concerns, or other issues/complaints.

Access Control

3 CONTROLS:

System Access Control Policy

Vision Dealer Solutions has a defined System Access Control Policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.

Continuously Monitored via 1 Drata Test:

System Access Control Policy

Drata inspected Vision Dealer Solutions's System Access Control Policy and confirmed that it includes annual access control review requirements, and requires access request forms for new hires and employee transfers.

Annual Access Control Review

Vision Dealer Solutions performs annual access control reviews.

Baseline Configuration and Hardening Standards

Vision Dealer Solutions has identified and documented baseline security configuration standards for all system components in accordance with industry-accepted hardening standards or vendor recommendations. These standards are reviewed periodically and updated as needed (e.g., when vulnerabilities are identified) and verified to be in place before or immediately after a production system component is installed or modified (e.g., through infrastructure as code, configuration checklists, etc.).

Vulnerability Management

11 CONTROLS:

Network segmentation in place

Vision Dealer Solutions maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.

Annual Risk Assessment

Vision Dealer Solutions conducts a Risk Assessment at least annually.

Quarterly Vulnerability Scan

Vision Dealer Solutions engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.

Annual Penetration Tests

Vision Dealer Solutions engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.

Organizational Chart Maintained

Vision Dealer Solutions reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.

Continuously Monitored via 1 Drata Test:

Maintains Organization Chart

Drata inspected Vision Dealer Solutions's records and confirmed that it had a time-stamped organizational chart.

Information Security Policy

Vision Dealer Solutions has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.

Continuously Monitored via 1 Drata Test:

Information Security Policy

Drata inspected Vision Dealer Solutions's Information Security Policy and confirmed that it covers policies and procedures to support the functioning of internal control.

Maintains Asset Inventory

Vision Dealer Solutions identifies, inventories, classifies, and assigns owners to IT assets.

Architectural Diagram

Vision Dealer Solutions maintains an accurate architectural diagram to document system boundaries to support the functioning of internal control.

Asset Management Policy

Vision Dealer Solutions has a defined policy that establishes requirements for the proper management and tracking of organizational assets.

Risk Assessment Policy

Vision Dealer Solutions has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.

Continuously Monitored via 1 Drata Test:

Risk Assessment Policy

Drata inspected Vision Dealer Solutions's Risk Assessment Policy and confirmed that it specifies risk tolerances and the process for evaluating risks based on identified threats and specified tolerances.

Remediation Plan

Vision Dealer Solutions's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.

Security Issues

3 CONTROLS:

Continuous Control Monitoring

Vision Dealer Solutions conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.

SLA for Security Bugs

Vision Dealer Solutions tracks security deficiencies through internal tools and closes them within an SLA that management has pre-specified.

Continuously Monitored via 1 Drata Test:

SLA for Security Bugs

Drata inspected Vision Dealer Solutions's procedure settings in Drata and determined that an SLA for P0 security bugs was set.

Security Issues are Prioritized

Vision Dealer Solutions tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.

Business Continuity

4 CONTROLS:

Disaster Recovery Plan

Vision Dealer Solutions has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.

Continuously Monitored via 1 Drata Test:

Disaster Recovery Plan

Drata inspected Vision Dealer Solutions's Disaster Recovery Plan and confirmed that it outlines roles and responsibilities and detailed procedures for recovery of systems.

BCP/DR Tests Conducted Annually

Vision Dealer Solutions conducts annual BCP/DR tests and documents according to the BCDR Plan.

Multiple Availability Zones

Vision Dealer Solutions utilizes multiple availability zones to replicate production data across different zones.

Business Continuity Plan

Vision Dealer Solutions has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.

Incident Response Plan

4 CONTROLS:

Follow-Ups Tracked

Vision Dealer Solutions has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.

Continuously Monitored via 1 Drata Test:

Policies for Tracking Security Items

Drata inspected Vision Dealer Solutions's Incident Response Plan and confirmed that it included a section about tracking follow-ups after an incident.

Incident Response Team

Vision Dealer Solutions has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.

Continuously Monitored via 1 Drata Test:

IRP Designates Responsible Team Members

Drata inspected Vision Dealer Solutions's Incident Response Plan and confirmed that it names the individuals responsible for monitoring and responding to incidents.

Lessons Learned

Vision Dealer Solutions has implemented an Incident Response Plan that includes documenting “Lessons Learned” and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.

Continuously Monitored via 1 Drata Test:

IRP Includes Lessons Learned

Drata inspected Vision Dealer Solutions's Incident Response Plan and confirmed that it included a section about documenting "Lessons Learned" after incidents.

Incident Response Plan

Vision Dealer Solutions has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.

Continuously Monitored via 1 Drata Test:

Incident Response Plan (IRP)

Drata inspected Vision Dealer Solutions's Incident Response Plan and confirmed that it outlines a formal procedure for responding to security events as well as requiring annual testing.

Organizational Security

Security Policies

3 CONTROLS:

Security Policies

Company policies are accessible to all employees and, as appropriate, third parties. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.

Continuously Monitored via 3 Drata Tests:

Has Security Policies

Drata inspected Vision Dealer Solutions's security policies and confirmed that they outline requirements for securing the company's operations, services, and systems.

Policies are Acknowledged by Employees

Drata inspected Vision Dealer Solutions's policy records and confirmed that assigned employees have acknowledged them.

Policies are Acknowledged by Contractors

Drata inspected Vision Dealer Solutions's policy records and confirmed that assigned contractors have acknowledged them.

Oversight of Security Controls

Management reviews security policies on an annual basis.

Continuously Monitored via 1 Drata Test:

Security Policies are Reviewed

Drata inspected Vision Dealer Solutions's records and confirmed that Management reviewed and approved its security policies before the renewal date.

Software Development Life Cycle Policy

Vision Dealer Solutions has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.

Continuously Monitored via 1 Drata Test:

Has a SDLC Policy

Drata inspected Vision Dealer Solutions's records and confirmed it has a Software Development Life Cycle Policy in place.

Security Program

3 CONTROLS:

Security Team/Steering Committee

Vision Dealer Solutions has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.

Continuously Monitored via 1 Drata Test:

Security Team Designated

Drata inspected Vision Dealer Solutions's records and confirmed that they identify individuals responsible for the security of the company's operations, services, and systems.

Security Training

Vision Dealer Solutions has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Vision Dealer Solutions's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.

Continuously Monitored via 2 Drata Tests:

Policies for Security Awareness Training

Drata inspected Vision Dealer Solutions's security policies and confirmed that the security team is responsible for training all employees on security at the company.

Security Awareness Training Completed

Drata inspected Vision Dealer Solutions's security awareness training that all employees must complete on hire and confirmed that it provides information related to the tactics that hackers take that could compromise the security of the company and its customers' data.

Security Team Communicates in a Timely Manner

The security team communicates important information security events to company management in a timely manner.

Personnel Security

10 CONTROLS:

Termination/Offboarding Checklist

Vision Dealer Solutions uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.

Acceptable Use Policy

Vision Dealer Solutions has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must acknowledge the Acceptable Use Policy upon hire.

Continuously Monitored via 2 Drata Tests:

Acceptable Use Policy

Drata inspected Vision Dealer Solutions's policies and confirmed that there is an Acceptable Use Policy that establishes the acceptable use of information assets, and it has been approved by management, and is accessible to all employees.

Employees Acknowledge the Acceptable Use Policy

Drata inspected Vision Dealer Solutions's records and confirmed that assigned employees have acknowledged the Acceptable Use Policy.

Background Checks

Vision Dealer Solutions's new hires are required to pass a background check as a condition of their employment.

Continuously Monitored via 1 Drata Test:

Employee Background Checks

Drata inspected Vision Dealer Solutions's records and confirmed that all new employees had completed background checks upon hire.

Contractor Requirements

Vision Dealer Solutions requires its contractors to read and acknowledge the Code of Conduct, read and acknowledge the Acceptable Use Policy, and pass a background check.

Continuously Monitored via 3 Drata Tests:

- Contractors Acknowledge The Code of Conduct
  Drata inspected Vision Dealer Solutions's records and confirmed that assigned contractors have acknowledged the company's Code of Conduct.
- Contractors Acknowledge the Acceptable Use Policy
  Drata inspected Vision Dealer Solutions's records and confirmed that all employees have acknowledged the Acceptable Use Policy.
- Contractor Background Checks
  Drata inspected Vision Dealer Solutions's records and confirmed that all new contractors had completed background checks upon hire.

Code of Conduct

Vision Dealer Solutions has a formal Code of Conduct approved by management and accessible to all employees. All employees must acknowledge the Code of Conduct upon hire.

Continuously Monitored via 2 Drata Tests:

- Formal Code of Conduct
  Drata inspected Vision Dealer Solutions's policy that documents the Code of Conduct and confirmed that it was in place and provides guidance on employee conduct standards.
- Employees Acknowledge the Code of Conduct
  Drata inspected Vision Dealer Solutions's records and confirmed that assigned employees have acknowledged the company's Code of Conduct upon hire.

Data Protection Policy

Vision Dealer Solutions has established a Data Protection Policy and requires all employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy.

Continuously Monitored via 3 Drata Tests:

- Data Protection Policy
  Drata inspected Vision Dealer Solutions's Data Protection Policy and confirmed that it was indeed in place.
- Employees Acknowledge Data Protection Policy
  Vision Dealer Solutions has established a Data Protection Policy and requires assigned employees to acknowledge it upon hire. Management monitors employees' acknowledgement of the policy.
- Contractors Acknowledge the Data Protection Policy
  Drata inspected Vision Dealer Solutions's records and confirmed that all contractors have acknowledged the company's Data Protection Policy.

Defined Management Roles & Responsibilities

Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.

Annual Performance Evaluations

Vision Dealer Solutions evaluates the performance of all employees through a formal, annual performance evaluation.

Continuously Monitored via 1 Drata Test:

- Performance Evaluation Process
  Drata inspected Vision Dealer Solutions's process for formal performance evaluations and confirmed that they outline a formal process to evaluate employee performance.

Formal Recruiting Process

Vision Dealer Solutions's new hires and/or internal transfers are required to go through an official recruiting process during which their qualifications and experience are screened to ensure that they are competent and capable of fulfilling their responsibilities.

Continuously Monitored via 1 Drata Test:

New Hire Contracts

Drata inspected Vision Dealer Solutions's sample new hire contract.

Job Descriptions

All Vision Dealer Solutions positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Vision Dealer Solutions.

Continuously Monitored via 2 Drata Tests:

Job Descriptions

Vision Dealer Solutions has provided Drata with a URL to their external jobs webpage.

Engineering Job Description

Drata inspected Vision Dealer Solutions's sample engineering job description.

Endpoints Laptops

5 CONTROLS:

Password Manager

Vision Dealer Solutions ensures that a password manager is installed on all company-issued laptops.

Continuously Monitored via 2 Drata Tests:

Password Manager Required

Drata inspected Vision Dealer Solutions's security policies and confirmed that employees are required to use a password manager to set, store, and retrieve passwords for cloud services.

Password Manager Records on Employee Computers

Drata inspected Vision Dealer Solutions's computers and confirmed that each was running a password manager.

Hard-Disk Encryption

Vision Dealer Solutions ensures that company-issued laptops have encrypted hard-disks.

Continuously Monitored via 1 Drata Test:

Hard-Disk Encryption Enabled on Employee Computers

Drata inspects Vision Dealer Solutions's computers and confirmed that hard-disks are encrypted for company-owned computers that connect to the public internet.

Session Lock

Vision Dealer Solutions ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.

Continuously Monitored via 1 Drata Test:

Screensaver Lock Required on Employee Computers

Drata inspected Vision Dealer Solutions's security policies and confirmed that employee computers must have a login password that activates after the machine has been idle for at least 15 minutes.

Malware Detection Software Installed

Vision Dealer Solutions requires antivirus software to be installed on workstations to protect the network against malware.

Continuously Monitored via 1 Drata Test:

Malware Detection Software Installed on Employee Computers

Drata inspected Vision Dealer Solutions's computers and confirmed that each was running an antivirus software.

Security Patches Automatically Applied

Vision Dealer Solutions's workstations operating system (OS) security patches are applied automatically.

Continuously Monitored via 1 Drata Test:

Security Patches Auto-Applied on Employee Computers

Drata inspected Vision Dealer Solutions's computers and confirmed that operating system security patches are applied automatically.

Product Security

Data Encryption

3 CONTROLS:

Encryption in Transit

Data in transit is encrypted using strong cryptographic algorithms.

Continuously Monitored via 3 Drata Tests:

SSL/TLS Enforced on Company Website

Drata inspected Vision Dealer Solutions's website and application, and confirmed that both are reachable exclusively over HTTPS. Drata also confirmed that if the URL was manually submitted to start with 'http://', that the user would be redirected to 'https://'.

SSL/TLS Configuration has No Known Issues

Drata inspected Vision Dealer Solutions's SSL/TLS configurations used to encrypt all data in transit and confirmed that there are no known issues.

SSL/TLS Certificate has Not Expired

Drata inspected Vision Dealer Solutions's certificate used to encrypt all data in transit and confirmed that it has not expired.

Cryptography Policies

Vision Dealer Solutions has an established policy and procedures that governs the use of cryptographic controls.

Continuously Monitored via 1 Drata Test:

Cryptography Policy

Drata inspected Vision Dealer Solutions's cryptography policies and confirmed that they list resources that employees may access to ensure they understand the procedures and their responsibilities.

Encryption at Rest

Data at rest is encrypted using strong cryptographic algorithms.

Continuously Monitored via 1 Drata Test:

Customer Data in Cloud Storage is Encrypted at Rest

Drata inspected Vision Dealer Solutions's configuration of its cloud storage bucket(s) storing customer data and confirmed that it is (they are) encrypted at rest.

Vendor Management

3 CONTROLS:

Vendor Management Policy

Vision Dealer Solutions has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.

Vendor Agreements Maintained

Vision Dealer Solutions maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.

Vendor Compliance Reports

Vision Dealer Solutions maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.

Software Application Security

6 CONTROLS:

Authentication Protocol

Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.

Role-Based Security Implementation

Role-based security is in place for internal and external users, including super admin users.

Customer Data Segregation

Vision Dealer Solutions's customer data is segregated from the data of other customers

Password Storage

Vision Dealer Solutions's application user passwords are stored using a salted password hash.

Accepting The Terms of Service

External users must accept the Terms of Service prior to their account being created.

Inactivity and Browser Exit Logout

Vision Dealer Solutions automatically logs users out after a predefined inactivity interval and/or closure of the internet browser, and requires users to reauthenticate

Customer Communication

3 CONTROLS:

Commitments Explained to Customers

Vision Dealer Solutions's security commitments are communicated to external users, as appropriate.

Continuously Monitored via 1 Drata Test:

MSAs Offered to Customers

Drata inspected Vision Dealer Solutions's Master Service Agreement (MSA) and confirmed that security commitments are included, and available to authorized customers.

Maintains a Privacy Policy

Vision Dealer Solutions maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.

Continuously Monitored via 1 Drata Test:

Privacy Policy Publicly Available

Drata inspected and confirmed Vision Dealer Solutions has provided a URL to their public Privacy Policy.

Maintains a Terms of Service

Vision Dealer Solutions maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client Agreements or Master Service Agreements are in place for when the Terms of Service may not apply.

Infrastructure Security

Authentication and Authorization

7 CONTROLS:

MFA on Accounts

Vision Dealer Solutions requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.

Continuously Monitored via 3 Drata Tests:

MFA on Identity Provider

Drata inspected all of the identity provider's users and confirmed that each account is configured with MFA.

MFA on Version Control System

Drata inspected all version control users and confirmed that each account is configured with MFA.

MFA on Infrastructure Console

Drata inspected how users access the Infrastructure Management Console and confirmed that MFA is required.

Password Policy and Configuration

Vision Dealer Solutions has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.

Continuously Monitored via 1 Drata Test:

Internal Password Policy for Employees

Drata inspected Vision Dealer Solutions's internal policy that governs the passwords employees set across services.

System Access Granted

Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.

Unique Accounts Used

Access to corporate network, production machines, network devices, and support tools requires a unique ID.

Continuously Monitored via 3 Drata Tests:

Employees have Unique Email Accounts

Drata inspected Vision Dealer Solutions's configuration of its email provider and confirmed that employees have unique accounts on the service.

Employees have Unique Version Control Accounts

Drata inspected Vision Dealer Solutions's configuration of its version control provider and confirmed that employees have unique accounts on the service.

Employees have Unique Infrastructure Accounts

Drata inspected Vision Dealer Solutions's configuration of its infrastructure provider and confirmed that employees have unique accounts on the service.

Terminated Employee Access Revoked Within One Business Day

Access to infrastructure and code review tools is removed from terminated employees within one business day.

Continuously Monitored via 2 Drata Tests:

Version Control Accounts Removed Properly

Drata inspected Vision Dealer Solutions's records and confirmed that terminated employees' accounts were removed from the version control system within the specified SLA of the employee becoming unauthorized.

Infrastructure Accounts Properly Removed

Drata inspected Vision Dealer Solutions's records and confirmed that terminated employees' accounts were removed from the infrastructure provider within the specified SLA of the employee becoming unauthorized.

Unique SSH

SSH users use unique accounts to access production machines. Additionally, the use of the “Root” account is not allowed.

Access to Remote Server Administration Ports Restricted

Network security controls are in place to restrict public access to remote server administration ports (e.g., SSH, RDP) to authorized IP addresses or address ranges only.

Availability

1 CONTROL:

Customers Informed of Changes

Vision Dealer Solutions communicates system changes to customers that may affect security, availability, processing integrity, or confidentiality.

Storage

1 CONTROL:

Restricted Public Access

Cloud resources are configured to deny public access.

Continuously Monitored via 1 Drata Test:

Cloud Data Storage Exposure

Drata inspected Vision Dealer Solutions's cloud data storage access configurations to determine if Read/Write access is configured to restrict public access.

Backup

3 CONTROLS:

Daily Database Backups

Vision Dealer Solutions performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.

Continuously Monitored via 1 Drata Test:

Daily Database Backups

Drata inspected Vision Dealer Solutions's database configuration and confirmed that backups are made daily using the infrastructure provider's automated backup service.

Backup Policy

Vision Dealer Solutions has a defined backup policy that establishes the requirements for backup information, software and systems.

Continuously Monitored via 1 Drata Test:

Has a Backup Policy

Drata inspected Vision Dealer Solutions's Backup Policy and confirmed it specified how often backups should be taken and for how long they should be retained.

Storage Buckets are Versioned

Storage buckets that contain customer data are versioned.

Continuously Monitored via 1 Drata Test:

Storage Data Versioned or Retained

Drata inspected Vision Dealer Solutions's storage bucket configuration and confirmed that all buckets containing customer data have a versioning configuration or retention policy set.

Logging

2 CONTROLS:

Logs Centrally Stored

Vision Dealer Solutions uses a system that collects and stores server logs in a central location. The system can be queried in an ad hoc fashion by authorized users.

Log Management System

Vision Dealer Solutions uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.

Monitoring

3 CONTROLS:

Databases Monitored and Alarmed

Vision Dealer Solutions has implemented tools to monitor Vision Dealer Solutions's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.

Continuously Monitored via 3 Drata Tests:

Database CPU Monitored

Drata inspected Vision Dealer Solutions's database monitoring configuration and confirmed that server CPU use is monitored, with alerts to appropriate personnel at certain thresholds.

Database Free Storage Space Monitored

Drata inspected Vision Dealer Solutions's database monitoring configuration and confirmed that free storage space is monitored, with alerts to appropriate personnel at certain thresholds.

Database Read I/O Monitored

Drata inspected Vision Dealer Solutions's database monitoring configuration and confirmed that read I/O is monitored, with alerts to appropriate personnel at certain thresholds.

NoSQL Database Monitored and Alarmed

Vision Dealer Solutions has implemented tools to monitor Vision Dealer Solutions's NoSQL databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.

Continuously Monitored via 1 Drata Test:

NoSQL Cluster Storage Utilization Monitored

Drata inspected Vision Dealer Solutions's NoSQL cluster monitoring configuration and confirmed that storage utilization is monitored, with alerts to appropriate personnel at certain thresholds.

Servers Monitored and Alarmed

Vision Dealer Solutions has implemented tools to monitor Vision Dealer Solutions's servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.

Continuously Monitored via 1 Drata Test:

Infrastructure Instance CPU Monitored

Drata inspected Vision Dealer Solutions's server monitoring configuration and confirmed that server CPU use is monitored, with alerts to appropriate personnel at certain thresholds.

Network

8 CONTROLS:

System Monitoring

Production systems and resources are monitored and automated alerts are sent out personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary.

Continuously Monitored via 5 Drata Tests:

Database CPU Monitored

Drata inspected Vision Dealer Solutions's database monitoring configuration and confirmed that server CPU use is monitored, with alerts to appropriate personnel at certain thresholds.

Database Free Storage Space Monitored

Drata inspected Vision Dealer Solutions's database monitoring configuration and confirmed that free storage space is monitored, with alerts to appropriate personnel at certain thresholds.

Database Read I/O Monitored

Drata inspected Vision Dealer Solutions's database monitoring configuration and confirmed that read I/O is monitored, with alerts to appropriate personnel at certain thresholds.

NoSQL Cluster Storage Utilization Monitored

Drata inspected Vision Dealer Solutions's NoSQL cluster monitoring configuration and confirmed that storage utilization is monitored, with alerts to appropriate personnel at certain thresholds.

Infrastructure Instance CPU Monitored

Drata inspected Vision Dealer Solutions's server monitoring configuration and confirmed that server CPU use is monitored, with alerts to appropriate personnel at certain thresholds.

VPN Required for Production Access

Users can only access the production system remotely through the use of encrypted communication systems.

Network Security Controls

Network security controls are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.

Web Application Firewall

A web application firewall is in place to protect public-facing web applications from outside threats.

Intrusion Detection System in Place

An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected

Logging/Monitoring

Vision Dealer Solutions has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.

Cloud Infrastructure Linked to Drata

Vision Dealer Solutions is using Drata to monitor the security and compliance of its cloud infrastructure configuration

Continuously Monitored via 1 Drata Test:

Cloud Infrastructure Linked to Drata

Drata inspected and confirmed that Vision Dealer Solutions's cloud infrastructure is linked to Drata

Root Infrastructure Account Monitored

Access to the root account in the cloud infrastructure provider is monitored. Login activity for the root account is investigated and validated for appropriateness.

Protecting Secrets

2 CONTROLS:

Credential Keys Managed

Vision Dealer Solutions has an established key management process in place to support the organization's use of cryptographic techniques.

Continuously Monitored via 1 Drata Test:

Security Policies Cover Encryption

Drata inspected Vision Dealer Solutions's security policies and confirmed that they explain the procedures for encrypting sensitive data.

Encryption Policy

Vision Dealer Solutions has a defined policy that establishes requirements for the use of cryptographic controls.

Continuously Monitored via 1 Drata Test:

Security Policies Cover Encryption

Drata inspected Vision Dealer Solutions's security policies and confirmed that they explain the procedures for encrypting sensitive data.

Physical Security

Data Center Security

1 CONTROL:

Physical Security

Vision Dealer Solutions has security policies that have been approved by management and detail how physical security for the company's headquarters is maintained. These policies are accessible to all employees and contractors.

Continuously Monitored via 1 Drata Test:

Physical Security Policy

Drata inspected Vision Dealer Solutions's physical security policy and confirmed that it outlines procedures for accessing the company's physical office.

Availability

Scaling

3 CONTROLS:

Monitoring Processing Capacity and Usage

Vision Dealer Solutions monitors its processing capacity and usage on a quarterly basis in order to appropriately manage capacity demand and to enable the implementation of additional capacity to meet availability commitments.

Load Balancer Used

Vision Dealer Solutions uses a load balancer to automatically distribute incoming application traffic across multiple instances and availability zones.

Auto-Scale Configuration

Vision Dealer Solutions automatically provisions new server instances when predefined capacity thresholds are met.

Backups

3 CONTROLS:

Backup Storage

Backups are encrypted and segmented from production systems (e.g., air-gapped, replicated to a different region, stored offsite, etc.) to ensure protection from a disaster or incident.

Backup Monitoring

Automated notifications are sent to personnel in the event of a backup failure. Backup failures are investigated and resolved by engineering personnel following company policies and procedures.

Backup Integrity and Completeness

Vision Dealer Solutions tests the integrity and completeness of back-up information on an annual basis.

Confidentiality

Data

4 CONTROLS:

Data Retention Policy

Vision Dealer Solutions has a documented policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained.

Continuously Monitored via 1 Drata Test:

Data Retention Policy

Drata inspected and confirmed that Vision Dealer Solutions has a data retention period specified for customer data.

Data Classification

Vision Dealer Solutions has established a data classification policy in order to identify the types of confidential information possessed by the entity and types of protection that are required.

Continuously Monitored via 1 Drata Test:

Data Classification Policy

Drata inspected and confirmed that Vision Dealer Solutions has a Data Classification Policy in order to identify the types of confidential information possessed by the entity and types of protection that were required.

Test Data Used in Test Environment

Vision Dealer Solutions uses test data within test environments.

Customer Data Deletion Upon Termination

Vision Dealer Solutions deletes customer data within 30 days of the customer terminating its contract.

Continuously Monitored via 1 Drata Test:

Deleting Customer Data Upon Terminated Contract

Drata inspected Vision Dealer Solutions's records and confirmed that upon termination of a contract with a customer, the customer's data was deleted within 30 days.

Additional Controls

19 CONTROLS:

Annual Incident Response Test

Vision Dealer Solutions ensures that incident response plan testing is performed on an annual basis.

Anti-Malware Scans of Media

The implemented anti-malware solutions are configured to perform automatic scans or continuous behavioral analysis of systems or processes when removable electronic media is inserted, connected, or logically mounted within the environment.

Automated Security Updates

Vision Dealer Solutions has implemented automated mechanisms (e.g., unattended upgrades, automated patching tools, etc.) to install security fixes to systems.

Code Changes are Tested

Vision Dealer Solutions ensures that code changes are tested prior to deployment to ensure quality and security.

Conduct Control Self-Assessments

Vision Dealer Solutions performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.

Cybersecurity Insurance Maintained

Vision Dealer Solutions maintains cybersecurity insurance to mitigate the financial impact of business disruptions.

Data Processing Monitoring

Application/data processing for Vision Dealer Solutions's system is logged and monitored to ensure processing is done completely and accurately. Errors in application/data processing are documented, investigated, escalated and corrected in accordance with policies and procedures.

Defined Company Objectives

Management has defined company objectives, including operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate to serve as the basis for risk assessment activities (e.g., objectives related to security, compliance, risk mitigation, etc.). Management communicates its objectives and any changes to those objectives to personnel.

DLP (Data Loss Prevention) Software is Used

Vision Dealer Solutions uses DLP (Data Loss Prevention) software to prevent unencrypted sensitive information from being transmitted over email

FIM (File Integrity Monitoring) Software in Place

Vision Dealer Solutions ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with.

Fraud Risk Assessment

Vision Dealer Solutions performs an evaluation of fraud risks at least annually, either as a separate evaluation or as part of the overall enterprise risk assessment. The evaluation of fraud risk is performed in accordance with the company's risk assessment methodology.

Management Oversight Briefings Conducted

The company's executive management team or a relevant appointee is briefed at least annually on the state of the company's cybersecurity and privacy risk. Executive management or their appointee provides feedback and direction as needed.

MFA Available for External Users

Vision Dealer Solutions allows for external users to implement multi-factor authentication on their accounts in order to require two forms of authentication prior to authentication

Physical Access to Facilities is Protected

Vision Dealer Solutions has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors.

Production Code Released by Appropriate Personnel

Vision Dealer Solutions ensures that releases are approved by appropriate members of management prior to production release.

Removable Media Device Encryption

Vision Dealer Solutions ensures that company-issued removable media devices (USB drives) are encrypted.

Responsibility for Control Environment Documented

The responsibility for managing the controls in place within the organization has been formally documented.

Secure Runtime Configurations

Vision Dealer Solutions maintains secure and supported configuration standards for application and platform runtimes.

User and System Guides

Vision Dealer Solutions provides user guides, help articles, system documentation or other mechanisms to users to share information about the design and operation of the system and its boundaries. The information provided includes functional and nonfunctional requirements related to system processing and information specifications required to support the use of the system.

Appendix A: Definitions

DDoS:

Distributed Denial of Service. A DDoS attack is an attack in which multiple compromised computer systems flood a target—such as a server, website, or other network resource—with messages or requests to cause a denial of service for users of the targeted resource.

Multi-Factor Authentication (MFA):

A security system that requires multiple methods of authentication using different types of credentials to verify users' identities before they can access a service.

Penetration Test:

The practice of testing a computer system, network, or web application to find vulnerabilities that an attacker might exploit.

Principle of Least Privilege:

The principle of giving a user or account only the privileges that are required to perform a job or necessary function.

SDLC: Software Development Lifecycle.

A process for planning, creating, testing, and deploying a software system.

SSH: Secure Shell.

A cryptographic network protocol for operating network services securely over an unsecured network.

SSL: Secure Sockets Layer.

The standard security technology for establishing an encrypted link between a web server and a browser.

Appendix B: Document History

Drata performs continuous, automated monitoring of Vision Dealer Solutions's security controls to ensure Vision Dealer Solutions complies with industry-accepted security standards. Due to the continuous monitoring Drata performs, this report is automatically updated to reflect the latest findings.

About Drata

Drata provides companies with a product suite designed to continuously monitor and collect evidence of hundreds of security controls across the company's IT systems and processes. Drata's cloud-based software connects with companies' infrastructure, identity providers, developer tools, HRIS, version control tools, and more to provide a comprehensive view of their security and compliance posture, while automating and streamlining the workflows, processes, and manual compliance tasks.

Drata is a software as a service company based in San Diego, California. Learn more at drata.com.