Smart-RIA Ventures Inc.

Powered by DRATA

Security & Compliance Report › Last Updated: May 18, 2022

Report Summary

Drata tests SmartRIA'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, SmartRIA:

- 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 SmartRIA improves its security posture, those efforts will be instantly visible.

Intended Use:

This SmartRIA Report can be used by:

- SmartRIA to identify issues critical for remediation
- SmartRIA'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

SmartRIA 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 SmartRIA'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 SmartRIA'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

SmartRIA 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 SmartRIA'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

SmartRIA 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 SmartRIA'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

SmartRIA 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

SmartRIA 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 SmartRIA's version control system and confirmed it is being used

Only Authorized Employees Access Version Control

Inspected SmartRIA'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 SmartRIA'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 SmartRIA'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 SmartRIA'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 SmartRIA personnel can push or make changes to production code.

Continuously Monitored via 1 Drata Test:

Production Code Changes Restricted

Drata inspected SmartRIA'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 SmartRIA's application

Responsible Disclosure Policy

2 CONTROLS:

Employee Disclosure Process

SmartRIA 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 SmartRIA'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

SmartRIA 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

SmartRIA 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 SmartRIA 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

SmartRIA 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 SmartRIA'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

SmartRIA performs annual access control reviews.

Hardening Standards in Place

Hardening standards are in place to ensure that newly deployed server instances are appropriately secured.

Vulnerability Management

10 CONTROLS:

Network segmentation in place

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

Annual Risk Assessment

SmartRIA conducts a Risk Assessment at least annually.

Continuously Monitored via 1 Drata Test:

Records of Risk Assessments

Drata inspected SmartRIA's report from the latest Risk Assessment, which was performed within the last 12 months.

Quarterly Vulnerability Scan

SmartRIA 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.

Continuously Monitored via 1 Drata Test:

Records of Vulnerability Scans

Drata inspected SmartRIA's report from the latest vulnerability scan, which was performed within the last 3 months.

Annual Penetration Tests

SmartRIA 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.

Continuously Monitored via 1 Drata Test:

Records of Penetration Testing

Drata inspects SmartRIA's records to determine if a penetration test has been conducted within the last 12 months.

Organizational Chart Maintained

SmartRIA 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 SmartRIA's records and confirmed that it had a time-stamped organizational chart.

Information Security Policy

SmartRIA 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 SmartRIA's Information Security Policy and confirmed that it covers policies and procedures to support the functioning of internal control.

Maintains Asset Inventory

SmartRIA identifies, inventories and classifies virtualized assets.

Architecture Diagram

SmartRIA maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.

Continuously Monitored via 1 Drata Test:

Architectural Diagram

Drata inspected SmartRIA's records and confirmed that it maintained an architectural diagram.

Risk Assessment Policy

SmartRIA 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 SmartRIA'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

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

Continuously Monitored via 1 Drata Test:

Remediation Plan Recorded

Drata inspects SmartRIA's records to determine if a Risk Remediation Plan has been provided within the last 12 months.

Security Issues

3 CONTROLS:

SLA for Security Bugs

SmartRIA 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 SmartRIA's procedure settings in Drata and determined that an SLA for P0 security bugs was set.

Security Issues are Prioritized

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

Continuously Monitored via 1 Drata Test:

Security Issues are Prioritized

Inspected SmartRIA's task tracking system and confirmed that security issues are being tagged and prioritized accordingly.

Continuous Control Monitoring

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

Business Continuity

3 CONTROLS:

Disaster Recovery Plan

SmartRIA 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 SmartRIA's Disaster Recovery Plan and confirmed that it outlines roles and responsibilities and detailed procedures for recovery of systems.

BCP/DR Tests Conducted Annually

SmartRIA conducts annual BCP/DR tests and documents according to the BCDR Plan.

Continuously Monitored via 1 Drata Test:

Annual BCP/DR Test

Drata inspects SmartRIA's records to determine if a Business Continuity and Disaster Recovery Plan are in place and has been approved within the last 12 months.Drata inspects SmartRIA's records to determine if a BCP/DR test has been conducted within the last 12 months.

Multiple Availability Zones

SmartRIA utilizes multiple availability zones to replicate production data across different zones.

Continuously Monitored via 1 Drata Test:

Availability Zones Used

Drata inspected SmartRIA's configurations and confirmed that multiple availability zones are utilized.

Incident Response Plan

4 CONTROLS:

Follow-Ups Tracked

SmartRIA has implemented an Incident Response Policy that includes creating, prioritizing, assigning, and tracking follow-ups to completion.

Continuously Monitored via 1 Drata Test:

Policies for Tracking Security Items

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

Incident Response Team

SmartRIA 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 SmartRIA's Incident Response Plan and confirmed that it names the individuals responsible for monitoring and responding to incidents.

Lessons Learned

SmartRIA has implemented an Incident Response Policy that includes documenting “Lessons Learned” and "Root Cause Analysis" after incidents and sharing them with the broader engineering team.

Continuously Monitored via 1 Drata Test:

IRP Includes Lessons Learned

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

Incident Response Plan

SmartRIA has an established Incident Response Policy 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 SmartRIA'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

SmartRIA Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.

Continuously Monitored via 3 Drata Tests:

Has Security Policies

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

Security Policies are Accepted by Employees

Drata inspected SmartRIA's security policy records and confirmed that assigned employees have accepted them.

Security Policies are Accepted by Contractors

Drata inspected SmartRIA's security policy records to determine if all contractors have accepted 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 SmartRIA's records and confirmed that Management reviewed and approved its security policies within the last 12 months.

Software Development Life Cycle Policy

SmartRIA 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 SmartRIA's records and confirmed it has a Software Development Life Cycle Policy in place.

Security Program

3 CONTROLS:

Security Team/Steering Committee

SmartRIA 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 SmartRIA's records and confirmed that they identify individuals responsible for the security of the company's operations, services, and systems.

Security Training

SmartRIA has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with SmartRIA'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 SmartRIA'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 SmartRIA'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

11 CONTROLS:

Termination/Offboarding Checklist

A termination checklist is used to ensure that system access, including physical access, for terminated employees has been removed within one specified time

Acceptable Use Policy

SmartRIA 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 accept the Acceptable Use Policy upon hire.

Continuously Monitored via 2 Drata Tests:

Acceptable Use Policy

Drata inspected SmartRIA'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 Accept the Acceptable Use Policy

Drata inspected SmartRIA's records and confirmed that assigned employees have accepted the Acceptable Use Policy.

Background Checks

SmartRIA'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 SmartRIA's records and confirmed that all new employees had completed background checks upon hire.

Contractor Requirements

SmartRIA requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.

Continuously Monitored via 4 Drata Tests:

Employees Accept the Acceptable Use Policy

Drata inspected SmartRIA's records and confirmed that assigned employees have accepted the Acceptable Use Policy.

Contractors Accept the Code of Conduct

Drata inspected SmartRIA's records and confirmed that assigned contractors have accepted the company's Code of Conduct.

Contractors Accept the Acceptable Use Policy

Drata inspected SmartRIA's records and confirmed that assigned contractors have accepted the company's Acceptable Use Policy.

Contractor Background Checks

Drata inspected SmartRIA's records and confirmed that all new contractors had completed background checks upon hire.

Code of Conduct

SmartRIA has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.

Continuously Monitored via 2 Drata Tests:

Formal Code of Conduct

Drata inspected SmartRIA's policy that documents the Code of Conduct and confirmed that it was in place and provides guidance on employee conduct standards.

Employees Accept the Code of Conduct

Drata inspected SmartRIA's records and confirmed that assigned employees have accepted the company's Code of Conduct upon hire.

Data Protection Policy

SmartRIA has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.

Continuously Monitored via 3 Drata Tests:

- Data Protection Policy
  Drata inspected SmartRIA's Data Protection Policy and confirmed that it was indeed in place.
- Employees Accept the Data Protection Policy
  Drata inspected SmartRIA's records and confirmed that assigned employees have accepted the company's Data Protection Policy upon hire.
- Contractors Accept the Data Protection Policy
  SmartRIA has established a Data Protection Policy and requires all contractors to accept it. Management monitors contractors' acceptance of the policy.

Independent Board of Directors

Members of the Board of Directors are independent of management.

Continuously Monitored via 1 Drata Test:

- Independent Board of Directors
  Drata inspected SmartRIA's records and confirmed that all of its Board of Directors' biographies were saved.

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

SmartRIA evaluates the performance of all employees through a formal, annual performance evaluation.

Continuously Monitored via 1 Drata Test:

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

Formal Recruiting Process

SmartRIA'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 SmartRIA's sample new hire contract.

Job Descriptions

All SmartRIA 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 SmartRIA.

Continuously Monitored via 2 Drata Tests:

- Job Descriptions
  SmartRIA has provided Drata with a URL to their external jobs webpage.
- Engineering Job Description
  Drata inspected SmartRIA's sample engineering job description.

Endpoints Laptops

5 CONTROLS:

Password Manager

SmartRIA ensures that a password manager is installed on all company-issued laptops.

Continuously Monitored via 2 Drata Tests:

- Password Manager Required
  Drata inspected SmartRIA'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 SmartRIA's computers and confirmed that each was running a password manager.

Hard-Disk Encryption

SmartRIA ensures that company-issued laptops have encrypted hard-disks.

Continuously Monitored via 1 Drata Test:

- Hard-Disk Encryption Enabled on Employee Computers
  Drata inspects SmartRIA's computers and confirmed that hard-disks are encrypted for company-owned computers that connect to the public internet.

Login Password

SmartRIA 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 SmartRIA'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

SmartRIA 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 SmartRIA's computers and confirmed that each was running an antivirus software.

Security Patches Automatically Applied

SmartRIA'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 SmartRIA's computers and confirmed that operating system security patches are applied automatically.

Product Security

Data Encryption

3 CONTROLS:

SSL/TLS Enforced

SmartRIA ensures that all connections to its web application from its users are encrypted.

Continuously Monitored via 3 Drata Tests:

SSL/TLS Enforced on Company Website

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

SSL Certificate has Not Expired

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

Cryptography Policies

SmartRIA has an established policy and procedures that governs the use of cryptographic controls.

Continuously Monitored via 1 Drata Test:

Cryptography Policy

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

Customer Data is Encrypted at Rest

SmartRIA stores customer data in databases that is encrypted at rest.

Continuously Monitored via 2 Drata Tests:

Customer Data is Encrypted at Rest

Drata inspected SmartRIA's configuration of the database(s) storing customer data and confirmed that the data is encrypted at rest.

Customer Data in Cloud Storage is Encrypted at Rest

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

Vendor Management

2 CONTROLS:

Vendor Agreements Maintained

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

Vendor Compliance Reports

SmartRIA 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

SmartRIA's customer data is segregated from the data of other customers

Password Storage

SmartRIA'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

SmartRIA 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

SmartRIA's security commitments are communicated to external users, as appropriate.

Continuously Monitored via 1 Drata Test:

MSAs Offered to Customers

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

Maintains a Privacy Policy

SmartRIA 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 SmartRIA has provided a URL to their public Privacy Policy.

Maintains a Terms of Service

SmartRIA 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.

Continuously Monitored via 1 Drata Test:

Terms of Service Publicly Available

Drata inspected and confirmed SmartRIA has provided a URL to their public Terms of Service.

Infrastructure Security

Authentication and Authorization

6 CONTROLS:

MFA on Accounts

SmartRIA 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

SmartRIA has established formal guidelines for passwords to govern the management and use of authentication mechanisms.

Continuously Monitored via 1 Drata Test:

- Internal Password Policy for Employees
  Drata inspected SmartRIA'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 SmartRIA's configuration of its email provider and confirmed that employees have unique accounts on the service.
- Employees have Unique Version Control Accounts
  Drata inspected SmartRIA's configuration of its version control provider and confirmed that employees have unique accounts on the service.
- Employees have Unique Infrastructure Accounts
  Drata inspected SmartRIA'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 SmartRIA'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 SmartRIA's records and confirmed that terminated employees' accounts were removed from the infrastructure provider within the specified SLA of the employee becoming unauthorized.

Denial of Public SSH

No public SSH is allowed.

Continuously Monitored via 1 Drata Test:

Public SSH Denied

Drata inspected and confirmed that public SSH access is denied.

Availability

1 CONTROL:

Customers Informed of Changes

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

Storage

1 CONTROL:

Cloud Data Storage Restricted

Read/Write access to cloud data storage is configured to restrict public access.

Continuously Monitored via 1 Drata Test:

Cloud Data Storage Exposure

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

Backup

2 CONTROLS:

Daily Database Backups

SmartRIA 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 SmartRIA's database configuration and confirmed that backups are made daily using the infrastructure provider's automated backup service.

Storage Buckets are Versioned

Storage buckets that contain customer data are versioned.

Continuously Monitored via 1 Drata Test:

Storage Data Versioned or Retained

Drata inspects all data stores to determine if the data versioning configuration is enabled.

Monitoring

4 CONTROLS:

Databases Monitored and Alarmed

SmartRIA has implemented tools to monitor SmartRIA'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 SmartRIA'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 SmartRIA'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 SmartRIA's database monitoring configuration and confirmed that read I/O is monitored, with alerts to appropriate personnel at certain thresholds.

Messaging Queues Monitored and Alarmed

SmartRIA has implemented tools to monitor SmartRIA's messaging queues and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.

Continuously Monitored via 1 Drata Test:

Messaging Queue Message Age Monitored

Drata inspected SmartRIA's messaging queue monitoring configuration and confirmed that message age is monitored, with alerts to appropriate personnel at certain thresholds.

NoSQL Database Monitored and Alarmed

SmartRIA has implemented tools to monitor SmartRIA'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 SmartRIA's NoSQL cluster monitoring configuration and confirmed that storage utilization is monitored, with alerts to appropriate personnel at certain thresholds.

Servers Monitored and Alarmed

SmartRIA has implemented tools to monitor SmartRIA'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 SmartRIA's server monitoring configuration and confirmed that server CPU use is monitored, with alerts to appropriate personnel at certain thresholds.

Network

6 CONTROLS:

Firewalls

SmartRIA uses configurations that ensure only approved networking ports and protocols are implemented, including firewalls.

Continuously Monitored via 1 Drata Test:

Firewall Default Disallows Traffic

Drata inspected SmartRIA's firewall configuration files for each perimeter device type and confirmed that they were configured to deny all traffic that is not explicitly allowed.

Web Application Firewall

WAF in place to protect SmartRIA's application from outside threats.

Continuously Monitored via 1 Drata Test:

Web Application Firewall in Place

Drata inspects the WAF configurations to determine if WAF is appropriately deployed and is configured to appropriately block malicious traffic.

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

SmartRIA 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.

Continuously Monitored via 1 Drata Test:

Threat Detection in Place

SmartRIA has Threat Detection in place to detect unauthorized file additions within the cloud environment, server instances, and application containers.

Cloud Infrastructure Linked to Drata

SmartRIA 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 SmartRIA's cloud infrastructure is linked to Drata

Root Infrastructure Account Unused

SmartRIA does not use Root Account on Infrastructure provider

Continuously Monitored via 1 Drata Test:

Root Infrastructure Account Unused

Drata inspected SmartRIA's infrastructure provider configurations and confirmed that the Root account is unused.

Protecting Secrets

1 CONTROL:

Credential Keys Managed

SmartRIA 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 SmartRIA's security policies and confirmed that they explain the procedures for encrypting sensitive data.

Physical Security

Data Center Security

1 CONTROL:

Physical Security

SmartRIA 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 SmartRIA's physical security policy and confirmed that it outlines procedures for accessing the company's physical office.

Availability

Scaling

1 CONTROL:

Load Balancer Used

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

Continuously Monitored via 1 Drata Test:

Load Balancer Used

Drata inspected SmartRIA's load balancer configuration to determine that a load balancer was used to automatically distribute incoming application traffic across multiple instances and availability zones.

Backups

3 CONTROLS:

Daily Backup Statuses Monitored

SmartRIA monitors the status of backups on a daily basis and action is taken when the backup process fails.

Failed Backup Alert and Action

SmartRIA has an automated email sent to appropriate personnel when the backup process fails. Failed backups are resolved in a timely manner.

Backup Integrity and Completeness

SmartRIA tests the integrity and completeness of back-up information on an annual basis.

Confidentiality

Data

4 CONTROLS:

Data Retention

SmartRIA establishes written policies related to retention periods for the confidential information it maintains.

Continuously Monitored via 1 Drata Test:

Data Retention Policy

Drata inspected and confirmed that SmartRIA has a data retention period specified for customer data.

Data Classification

SmartRIA 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 SmartRIA 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

SmartRIA uses test data within test environments.

Customer Data Deletion Upon Termination

SmartRIA 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 SmartRIA's records and confirmed that upon termination of a contract with a customer, the customer's data was deleted within 30 days.

Employee Responsibilities

4 CONTROLS:

Employee Non-Disclosure Agreement (NDA)

SmartRIA's new hire contracts include a non-disclosure agreement (NDA)

Clean Desk Policy in Place

SmartRIA has a clean desk policy in place to ensure that documents containing sensitive data are not in public areas or laying on unattended employee work areas

Continuously Monitored via 1 Drata Test:

Clean Desk Policy

Drata inspected SmartRIA's policies and confirmed that they include a clean desk policy.

Disposal of Sensitive Data on Paper

SmartRIA has formal policies and procedures in place to guide personnel in the disposal of paper documents containing sensitive data.

Continuously Monitored via 1 Drata Test:

Sensitive Data Disposal Policy

Drata inspected SmartRIA's policies and confirmed that they include policies and procedures to guide personnel in the disposal of paper documents containing sensitive data.

Disposal of Sensitive Data on Hardware

SmartRIA has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.

Uncategorized Controls

12 CONTROLS:

Annual Incident Response Test

SmartRIA ensures that incident response plan testing is performed on an annual basis.

Board Charter Documented

The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.

Board Expertise Developed

The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.

Board Meetings Conducted

The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.

Board Oversight Briefings Conducted

The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.

Code Changes are Tested

SmartRIA ensures that code changes are tested prior to implementation to ensure quality and security.

Cybersecurity Insurance Maintained

SmartRIA maintains cybersecurity insurance to mitigate the financial impact of business disruptions.

DLP (Data Loss Prevention) Software is Used

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

MFA Available for External Users

SmartRIA 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

SmartRIA 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

SmartRIA ensures that releases are approved by appropriate members of management prior to production release.

Removable Media Device Encryption

SmartRIA ensures that company-issued removable media devices (USB drives) are encrypted.

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 SmartRIA's security controls to ensure SmartRIA 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.