v1.0

ControlCase Kaseya

ROCKET CYBER CUSTOMER RESPONSIBILITY MATRIX

Powered by ControlCase (C3PAO) and KASEYA

Mark Cline | SVP, Sales
404.307.7235
mcline@controlcase.com

NIST 800-171 Rev 2

AGENDA

1. Access Control (AC)
2. Awareness and Training (AT)
3. Audit and Accountability (AU)
4. Configuration Management (CM)
5. Identification and Authentication (IA)
6. Incident Response (IR)
7. Maintenance (MA)
8. Media Protection (MP)
9. Personnel Security (PS)
10. Physical Protection (PE)
11. Risk Assessment (RA)
12. Security Assessment (CA)
13. System and Communications Protection (SC)
14. System and Information Integrity (SI)

ROCKET CYBER CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.1[a]	KASEYA provisions the initial CUSTOMER admin account using the email address supplied during onboarding. This account is designated as a backup and excluded from regular operational use. All other user accounts must be created via the CUSTOMER's identity source using KASEYA's SSO capability.	CUSTOMER manages user identities via their own identity source and provisions accounts through the KASEYA's SSO capability. The initial admin account, created from the onboarding email, is retained solely for backup and not used for regular access.	Enabling SSO Login with KaseyaOne
AC.L2-3.1.1[b]	KASEYA ensures all actions within the system are attributed to authenticated SSO user identities, captured in audit logs.	CUSTOMER ensures users authenticate via SSO; process attribution is handled by the PRODUCT.	Office 365 Login Analyzer
AC.L2-3.1.1[c]	KASEYA supplies agent software for CUSTOMER deployment; access is scoped to agent-installed systems.	CUSTOMER installs agents only on systems authorized to connect to the PRODUCT.	Agent Deployment
AC.L2-3.1.1[d]	KASEYA enforces access control via SSO integration and role-based permissions.	CUSTOMER controls identity source and ensures only authorized users are provisioned and granted access via SSO.	Identity and Access Management
AC.L2-3.1.1[e]	KASEYA ensures all system actions are tied to authenticated user sessions via SSO.	CUSTOMER ensures proper identity governance; enforcement is handled by the PRODUCT.	Securing Your Account with 2FA
AC.L2-3.1.1[f]	KASEYA enables agent-based access control; only agent-equipped systems are reachable.	CUSTOMER controls agent deployment to restrict access to approved systems.	Endpoint Security
AC.L2-3.1.2[a]	KASEYA defines default roles (Owner, Incident Responder, Reviewer) with scoped permissions.	CUSTOMER may define additional roles and assign users based on operational needs.	-
AC.L2-3.1.2[b]	KASEYA enforces role-based access control aligned with defined role permissions.	CUSTOMER assigns roles appropriately; PRODUCT enforces access based on role configuration.	Identity and Access Management

ROCKET CYBER CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.5[a]	KASEYA identifies the initial privileged account as the CUSTOMER admin user account during environment provisioning.	CUSTOMER identifies any additional privileged accounts beyond the initial admin account and determines who will be assigned.	Enabling SSO Login with KaseyaOne
AC.L2-3.1.5[b]	KASEYA enforces role-based access controls within the PRODUCT to support least privilege; CUSTOMER must assign roles appropriately.	CUSTOMER assigns users to privileged accounts based on operational need, ensuring alignment with least privilege principles.	Identity and Access Management
AC.L2-3.1.5[c]	KASEYA designates general use of the PRODUCT—including account management and configuration—as a security function.	CUSTOMER recognizes that use of the PRODUCT constitutes access to security functions and governs access accordingly.	Identity and Access Management
AC.L2-3.1.5[d]	KASEYA enforces access restrictions to security functions via role-based access control mechanisms.	CUSTOMER uses account management and role-based access control to ensure only authorized users can access security functions.	
AC.L2-3.1.8[a]	KASEYA supplies single sign-on (SSO) capability, which can support integration with CUSTOMER identity sources.	CUSTOMER defines logon attempt limitations (e.g., lockout thresholds, retry intervals) within its identity source.	Enabling SSO Login with KaseyaOne
AC.L2-3.1.8[b]	KASEYA does not implement or enforce logon attempt limitations; this is outside their operational scope.	CUSTOMER enforces these limitations through configuration of its identity KASEYA integrated with the SSO.	Identity and Access Management
AC.L2-3.1.11[a]	KASEYA enables a configurable setting within the PRODUCT for session termination based on inactivity	CUSTOMER defines the inactivity threshold by configuring the session timeout value within the PRODUCT	Identity and Access Management
AC.L2-3.1.11[b]	KASEYA ensures the PRODUCT enforces session termination once the CUSTOMER-defined inactivity threshold is reached	CUSTOMER ensures the session termination setting is properly configured to enforce automatic termination	Identity and Access Management

ROCKET CYBER CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AT.L2-3.2.2[a]	KASEYA does not define CUSTOMER-specific security roles or responsibilities.	CUSTOMER defines roles and responsibilities based on organizational structure and regulatory requirements.	-
AT.L2-3.2.2[b]	KASEYA does not assign CUSTOMER personnel to roles.	CUSTOMER assigns personnel to defined roles and ensures accountability.	-
AT.L2-3.2.2[c]	KASEYA develops training materials related to the use of the PRODUCT, which may support CUSTOMER training.	CUSTOMER ensures personnel receive appropriate training, potentially incorporating KASEYA materials.	Rocketcyber KB Home
AU.L2-3.3.1[a]	KASEYA defines event types captured in the PRODUCT portal: failed logins, clearing security logs, unauthorized activity, etc.	CUSTOMER defines event types to be captured by PRODUCT agents on their systems	Configuring the Syslog Collector
AU.L2-3.3.1[b]	KASEYA specifies required fields (e.g., timestamp, user ID, event type, source IP) for portal-generated audit records	CUSTOMER specifies required fields for system-generated audit records	Configuring the Syslog Collector
AU.L2-3.3.1[c]	PRODUCT portal automatically generates audit records for defined event types	CUSTOMER configures systems to generate audit records via PRODUCT agents	Configuring the Syslog Collector
AU.L2-3.3.1[d]	KASEYA validates that generated records include all required fields	CUSTOMER validates system-generated records contain all required fields	Configuring the Syslog Collector
AU.L2-3.3.1[e]	KASEYA enforces a 1-year retention policy for audit records stored in the PRODUCT portal	CUSTOMER may define internal retention policies; PRODUCT retains agent logs in portal for 1 year	Configuring the Syslog Collector
AU.L2-3.3.1[f]	PRODUCT portal retains logs for 1 year per policy	CUSTOMER ensures retention aligns with internal policies or relies on PRODUCT's 1-year retention	Configuring the Syslog Collector

ROCKET CYBER CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.2[a]	KASEYA ensures audit records include user identifiers, timestamps, and contextual metadata	CUSTOMER defines traceability requirements for audit records generated in their environment	-
AU.L2-3.3.2[b]	Audit records in the PRODUCT portal support user-to-action traceability	CUSTOMER validates agent-generated records support user-to-action traceability	-
AU.L2-3.3.3[a]	KASEYA defines an internal process to review event types captured in the PRODUCT portal on an annual basis	CUSTOMER is responsible for defining a process to periodically review event types captured by PRODUCT agents	-
AU.L2-3.3.3[b]	KASEYA conducts an annual review of logged event types (e.g., failed logins, unauthorized activity, log clearing)	CUSTOMER must conduct reviews of agent-captured event types according to their defined process	-
AU.L2-3.3.3[c]	KASEYA updates the event types in the PRODUCT portal as needed based on findings from the annual review	CUSTOMER updates the configuration of PRODUCT agents via the PRODUCT portal to reflect changes in logging requirements based on review	Identity and Access Management
AU.L2-3.3.8[a]	KASEYA enforces role-based access controls (RBAC) and encryption for PRODUCT portal logs	CUSTOMER must implement access controls and system-generated logs	Configuring the Syslog Collector
AU.L2-3.3.8[b]	KASEYA applies write-once storage policies and integrity checks to prevent tampering	CUSTOMER must ensure logs are stored in tamper-evident formats or write-once media	-
AU.L2-3.3.8[c]	KASEYA enforces retention policies and privileged access restrictions to prevent deletion	CUSTOMER must configure retention policies and restrict deletion permissions on system-generated logs	Identity and Access Management
AU.L2-3.3.8[d]	KASEYA restricts access to logging infrastructure via network segmentation and authentication controls	CUSTOMER must restrict access to PRODUCT agent binaries and configuration files	-

ROCKET CYBER CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.8[e]	KASEYA uses configuration management and change control processes to prevent unauthorized changes	CUSTOMER must apply file integrity monitoring and change control to PRODUCT agent configurations	-
AU.L2-3.3.8[f]	KASEYA applies system hardening and privileged access restrictions to prevent deletion of logging tools	CUSTOMER must prevent unauthorized removal of PRODUCT agents through OS-level controls and software policies	Configuring Endpoint Security
CM.L2-3.4.2[a]	KASEYA develops the PRODUCT and enables certain settings to be configurable by the CUSTOMER, allowing customization within defined parameters. KASEYA does not manage or enforce the CUSTOMER's chosen configurations.	CUSTOMER determines and establishes security configurations within the available configurable settings of the PRODUCT, ensuring alignment with organizational security requirements.	Office 365 Configuration & Monitoring
CM.L2-3.4.2[b]	While KASEYA does not manage CUSTOMER configurations, it ensures that mechanisms within the PRODUCT support enforcement of configurable security settings according to industry best practices.	CUSTOMER is responsible for managing and enforcing security configurations within the PRODUCT, ensuring compliance with policies and operational needs.	-
IA.L2-3.5.1[a]	KASEYA does not identify CUSTOMER users; user identity is managed via CUSTOMER's identity source.	CUSTOMER identifies all system users via its identity source.	-
IA.L2-3.5.1[b]	KASEYA does not define or manage CUSTOMER-side service accounts or automation.	CUSTOMER identifies and manages service accounts and automated processes.	-
IA.L2-3.5.1[c]	KASEYA does not identify CUSTOMER devices; access is gated by CUSTOMER agent deployment.	CUSTOMER tracks and manages device identities through endpoint management and identity integration.	-
IA.L2-3.5.2[a]	KASEYA enables single sign-on (SSO) integration; actual authentication is performed by CUSTOMER identity source.	CUSTOMER enforces user authentication via its identity source.	-
IA.L2-3.5.2[b]	KASEYA does not authenticate CUSTOMER-side processes; attribution is based on authenticated user context.	CUSTOMER authenticates service accounts and associated processes.	

ROCKET CYBER CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.2[c]	KASEYA does not authenticate CUSTOMER devices; access is scoped by agent installation.	CUSTOMER enforces device authentication through its identity and endpoint management systems.	
IA.L2-3.5.3[a]	KASEYA provisions the initial CUSTOMER admin account; all other privileged accounts are CUSTOMER-defined.	CUSTOMER identifies privileged accounts within its identity source.	
IA.L2-3.5.3[b]	KASEYA does not enforce MFA for local access; CUSTOMER identity source governs this.	CUSTOMER enforces MFA for local privileged access.	
IA.L2-3.5.3[c]	KASEYA does not enforce MFA for network access; CUSTOMER identity source governs this.	CUSTOMER enforces MFA for network privileged access.	
IA.L2-3.5.3[d]	KASEYA does not enforce MFA for non-privileged accounts; CUSTOMER identity source governs this.	CUSTOMER enforces MFA for non-privileged network access.	
IA.L2-3.5.4[a]	KASEYA does not implement replay resistance; CUSTOMER identity source governs this.	CUSTOMER implements replay-resistant protocols (e.g., Kerberos, FIDO2, TLS) via its identity source.	
IA.L2-3.5.5[a]	KASEYA does not define identifier reuse periods; CUSTOMER identity source governs this.	CUSTOMER defines identifier reuse periods in identity policy.	
IA.L2-3.5.5[b]	KASEYA does not enforce identifier reuse restrictions.	CUSTOMER enforces identifier reuse restrictions.	
IA.L2-3.5.6[a]	KASEYA does not define inactivity thresholds for identifiers.	CUSTOMER defines inactivity thresholds for disabling identifiers.	
IA.L2-3.5.6[b]	KASEYA does not enforce identifier deactivation.	CUSTOMER enforces identifier deactivation policies.	

ROCKET CYBER CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.7[a]	KASEYA does not define password complexity; CUSTOMER identity source governs this.	CUSTOMER defines password complexity policies.	
IA.L2-3.5.7[b]	KASEYA does not define character change requirements.	CUSTOMER defines character change requirements for password updates.	
IA.L2-3.5.7[c]	KASEYA does not enforce password complexity.	CUSTOMER enforces password complexity during creation.	
IA.L2-3.5.7[d]	KASEYA does not enforce character change requirements.	CUSTOMER enforces character change requirements during password updates.	
IA.L2-3.5.8[a]	KASEYA does not define password history policies.	CUSTOMER defines password history retention policies.	
IA.L2-3.5.8[b]	KASEYA does not enforce password reuse restrictions.	CUSTOMER enforces password reuse restrictions.	
IA.L2-3.5.9[a]	KASEYA does not enforce temporary-to-permanent password transitions.	CUSTOMER enforces temporary-to-permanent password change policies.	
IA.L2-3.5.10[a]	KASEYA does not store CUSTOMER passwords; authentication is handled by CUSTOMER identity source.	CUSTOMER ensures password storage uses cryptographic protection (e.g., hashing, salting).	
IA.L2-3.5.10[b]	KASEYA does not transmit CUSTOMER passwords; authentication occurs via CUSTOMER identity source.	CUSTOMER enforces secure transmission protocols (e.g., TLS).	
IA.L2-3.5.11[a]	KASEYA does not control authentication UI or flows; CUSTOMER identity source governs this.	CUSTOMER ensures authentication inputs (e.g., passwords) are obscured during entry and transmission.	

ROCKET CYBER CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IR.L2-3.6.1[a]	KASEYA delivers a 24/7/365 SOC capability integrated with the PRODUCT to support incident response	CUSTOMER leverages the KASEYA's SOC capability by deploying and configuring PRODUCT agents	Managed SOC Overview
IR.L2-3.6.1[b]	KASEYA prepares detection and response workflows, SOC staffing, and PRODUCT integration to support readiness	CUSTOMER prepares by installing agents and integrating them with network infrastructure	Managed SOC Incident Response Guide
IR.L2-3.6.1[c]	KASEYA detects threats using data collected by PRODUCT agents and analyzed by the SOC	CUSTOMER enables detection by configuring agents to collect relevant system and network data	Managed SOC Overview
IR.L2-3.6.1[d]	KASEYA performs analysis of collected data to identify root causes and attack vectors	CUSTOMER may perform internal analysis or rely on KASEYA's SOC for deeper investigation	Managed SOC Overview
IR.L2-3.6.1[e]	KASEYA supports containment actions through alerting, escalation, and guidance based on SOC analysis	CUSTOMER executes containment actions within their environment based on SOC alerts and guidance	Managed SOC Overview
IR.L2-3.6.1[f]	KASEYA contributes to recovery by providing incident reports and recommendations for remediation	CUSTOMER performs recovery actions on affected systems based on incident findings	Incident Response Guide
IR.L2-3.6.1[g]	KASEYA enables CUSTOMER response through alerts, dashboards, and SOC engagement	CUSTOMER coordinates internal user response activities and follows SOC recommendations	Managed SOC Overview
MA.L2-3.7.1[a]	ROVIDER performs maintenance on the PRODUCT agent by automatically pushing updates as part of lifecycle management.	CUSTOMER is responsible for maintaining the systems where the PRODUCT agent is installed, including OS patching, resource availability, and host-level security.	Endpoint Security
SC.L2-3.13.15[a]	KASEYA ensures secure, authenticated communication between the PRODUCT agent and the PRODUCT portal, and between the CUSTOMER and the PRODUCT portal.	CUSTOMER relies on the KASEYA's implementation for session authenticity. No direct responsibility unless integrating with third-party systems or proxies.	Cloud Security

ROCKET CYBER CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
SI.L2-3.14.1[a]	KASEYA defines timelines for flaw identification in the PRODUCT agent (e.g., via internal SLAs or release cadence).	CUSTOMER may define timelines for flaw identification on the host system, but not for the PRODUCT agent.	Vulnerability Scanner
SI.L2-3.14.1[b]	KASEYA monitors and identifies flaws in the PRODUCT agent within defined timeframes.	CUSTOMER is responsible for identifying flaws in the host system within their own operational timelines.	Endpoint Security
SI.L2-3.14.1[c]	KASEYA specifies reporting timelines (e.g., via security advisories or release notes).	CUSTOMER defines internal reporting timelines for host system flaws.	Release Notes
SI.L2-3.14.1[d]	KASEYA reports flaws in accordance with its defined timelines.	CUSTOMER reports host system flaws according to their own defined timelines.	Release Notes
SI.L2-3.14.1[e]	KASEYA defines remediation timelines for flaws in the PRODUCT agent (e.g., patch release SLAs).	CUSTOMER defines remediation timelines for host system flaws.	Release Notes
SI.L2-3.14.1[f]	KASEYA corrects flaws by pushing automatic updates to the agent within the specified timeframes.	CUSTOMER is responsible for correcting host system flaws within their specified timeframes.	Module Administration
SI.L2-3.14.6[a]	KASEYA monitors agent-collected system data continuously via the SOC	CUSTOMER ensures agents are installed and configured to enable monitoring	Managed SOC Overview
SI.L2-3.14.6[b]	KASEYA monitors inbound traffic when CUSTOMER configures agents to receive data from network firewalls	CUSTOMER configures agents to receive inbound traffic data from network firewalls	Firewall Intergration
SI.L2-3.14.6[c]	KASEYA monitors outbound traffic when CUSTOMER configures agents accordingly	CUSTOMER configures agents to receive outbound traffic data from network firewalls	Firewall Intergration

CONTACT US

404.307.7235

mcline@controlcase.com

Corporate Headquarters
3975 FAIR RIDGE DR STE T25S-D
FAIRFAX, VA 22033