



UNITRENDS CUSTOMER RESPONSIBILITY MATRIX

Powered by ControlCase (C3PAO) and KASEYA

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



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)

UNITRENDS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.1[a]	KASEYA Unitrends supports different user roles and Role-based access control (RBAC). Administrator: Full access to device settings, backups, and recovery options and Technician / Operator: Limited access, usually just monitoring or initiating restores.	CUSTOMER defines in policy, authorized users and roles (i.e., specifies Administrators, Technicians, Operators). Review user access periodically	Getting Started with Unitrends - Navigating the User Interface
AC.L2-3.1.1[b]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER responsible to determine if processes acting on behalf of authorized users are identified.	About this Guide
AC.L2-3.1.1[c]	KASEYA Unitrends provides agents on endpoints (servers, PCs, virtual machines), pre-configured with credentials and unique device IDs. Devices with a valid, registered agent can connect to the BCDR appliance or cloud portal.	CUSTOMER provides procedure(s) for authorization, installs Agents on endpoints, servers, or virtual machines that require backup and ensure devices meet minimum system requirements (OS version, disk space, memory).	Getting Started with Unitrends - Navigating the User Interface
AC.L2-3.1.1[d]	KASEYA Unitrends allows access to backup data to registered users, Datto agents and the Datto authorized portal (when local access is disabled)	CUSTOMER provides assignment and system access to authorized users through local access	Two Factor Authentication (2FA)
AC.L2-3.1.1[e]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER responsible to determine if processes acting on behalf of authorized users are identified.	About this Guide
AC.L2-3.1.1[f]	KASEYA Unitrends determines and enforces that system access is limited to authorized devices (and other systems)	CUSTOMER provides device access (endpoint agent installation) evidence (e.g., logs)	Getting Started with Unitrends - Navigating the User Interface

UNITRENDS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.2[a]	KASEYA Unitrends determines and enforces that system access is limited to authorized devices (and other systems) Granular permissions (restore, delete, configure, view) and Restriction of backup/restore actions to authorized roles	CUSTOMER to determine if the types of transactions and functions that authorized users are permitted to execute have been defined.	Appliance Management Requirements
AC.L2-3.1.2[b]	KASEYA Unitrends determines and enforces that system access is limited to authorized devices (and other systems)	CUSTOMER to determine if system access is limited to the defined types of transactions and functions	
AC.L2-3.1.5[a]	KASEYA Unitrends determines that privileged accounts are identified through role assignment to a user account(s) Role-based permissions apply and no default full admin for all users	CUSTOMER provides evidence that least privileged roles are (have been) identified, defining which accounts are privileged Create distinct "Backup Operator" role (run jobs, view status only) Create distinct "Restore Operator" role (restore only)	Appliance Management Requirements
AC.L2-3.1.5[b]	KASEYA Unitrends uses security levels (roles) where accounts are assigned against roles compliant with least privilege; actions outside the assigned role are automatically blocked	CUSTOMER determines if access to privileged accounts is (has been) authorized.	-
AC.L2-3.1.5[c]	KASEYA Unitrends relies on built-in features, configuration, and logging to identify security functions with enforcement	CUSTOMER determines if security functions are (have been) identified. Reviewed periodically	About this Guide
AC.L2-3.1.5[d]	KASEYA Unitrends enforces and technically restrict access based on roles and permissions assigned by the customer	CUSTOMER provides authorization access to security functions according to least privilege.	

UNITRENDS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AC.L2-3.1.6[a]	KASEYA Unitrends supports role-based access control (RBAC) note: routine backup/restore can be done without admin rights	CUSTOMER responsible for creating multiple user roles, assigning permissions based on job function, restricting administrative/system configuration access and separating operational tasks from system-level management	About this Guide
AC.L2-3.1.6[b]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER responsible to determine if users are required to use non-privileged accounts or roles when accessing nonsecurity functions.	
AU.L2-3.3.1[a]	KASEYA Unitrends provides audit capability such as login/out, success/failures, named user, timestamp, target systems	CUSTOMER specifies audit log content (i.e., user login and logout events, privileged actions (role changes, script execution, patch approvals), remote session activities, configuration changes and policy modifications)	Alerts Report
AU.L2-3.3.1[b]	KASEYA Unitrends provides audit content such as: User login / logout (successful & failed attempts) Account creation, modification, deletion Role/permission changes Configuration changes (network, storage, replication) Retention policy changes Encryption setting changes Backup schedule modifications System setting updates	CUSTOMER defines, then provides evidence of audit log content	Alerts Report
AU.L2-3.3.1[c]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER provides evidence of audit log generation	Alerts Report
AU.L2-3.3.1[d]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER determines if audit logs contain defined content	Alerts Report

UNITRENDS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.1[e]	KASEYA Unitrends retains audit logs for the active subscription period (typically 90 days)	CUSTOMER determines audit log export for long-term retention (i.e., 1 year)	Alerts Report
AU.L2-3.3.1[f]	KASEYA Unitrends provides audit records retention	CUSTOMER provides audit records as defined	Alerts Report
AU.L2-3.3.2[a]	KASEYA Unitrends provides who performed the action, what action occurred, timestamps and target system/device	CUSTOMER provides defined content	Alerts Report
AU.L2-3.3.2[b]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER to determine if defined content is supplied	Alerts Report
AU.L2-3.3.8[a]	KASEYA Unitrends provides tamper-resistant cloud-stored logs and Role-restricted access to logs	CUSTOMER to determine if audit information is protected from unauthorized access.	Alerts Report
AU.L2-3.3.8[b]	KASEYA Unitrends provides system-generated (not user-editable via UI) logs not directly editable through the web console. Logs are maintained within the appliance or SaaS backend environment.	CUSTOMER to determine if audit information is protected from unauthorized modification	Alerts Report

UNITRENDS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
AU.L2-3.3.8[c]	KASEYA Unitrends direct log file access is not available. CUSTOMER cannot modify backend audit files.	CUSTOMER to determine if audit information is protected from unauthorized deletion	Alerts Report
AU.L2-3.3.8[d]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER to determine if audit information is protected from unauthorized access	Alerts Report
AU.L2-3.3.8[e]	KASEYA Unitrends direct log file access is not available. CUSTOMER cannot modify backend audit files.	CUSTOMER to determine if audit tool is protected from unauthorized access	Alerts Report
AU.L2-3.3.8[f]	KASEYA Unitrends direct log file access is not available. CUSTOMER cannot modify backend audit files.	CUSTOMER to determine if audit tool is protected from unauthorized deletion	Alerts Report
CM.L2-3.4.2[a]	KASEYA Unitrends supports disabling unused features/services, controlling software updates/patching and managing storage thresholds and alerts	CUSTOMER to determine if security configuration settings for information technology products employed in the system are established and included in the baseline configuration.	Procedures for adding attached disk backup storage

UNITRENDS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
CM.L2-3.4.2[b]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER to determine if security configuration settings for information technology products employed in the system are established and included in the baseline configuration.	
IA.L2-3.5.1[a]	KASEYA Unitrends provides named user accounts and MFA for portal access	CUSTOMER determines if provided users are identified	
IA.L2-3.5.1[b]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER determines if provided processes are identified	
IA.L2-3.5.1[c]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER determines if provided devices are identified	Getting Started with Unitrends - Navigating the User Interface
IA.L2-3.5.2[a]	KASEYA Unitrends determines if each user is authenticated before granting system access	CUSTOMER to perform verification of identity (e.g., confirming HR status or background checks)	Two Factor Authentication (2FA)
IA.L2-3.5.2[b]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER to define which processes are allowed to run on endpoints	

UNITRENDS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
IA.L2-3.5.2[c]	KASEYA Unitrends determines if a device is authenticated before it can access or connect to the system (agent installed and registered)	CUSTOMER responsible for defining and controlling which devices are authorized to access the system	Getting Started with Unitrends - Navigating the User Interface
IA.L2-3.5.3[a]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER to determine if privileged accounts are identified.	Two Factor Authentication (2FA)
IA.L2-3.5.3[b]	KASEYA Unitrends supports MFA to web console access	CUSTOMER to determine if multifactor authentication is implemented for local access to privileged accounts.	Two Factor Authentication (2FA)
IA.L2-3.5.3[c]	KASEYA Unitrends supports MFA to web console access	CUSTOMER to determine if multifactor authentication is implemented for network access to privileged accounts.	Two Factor Authentication (2FA)
IA.L2-3.5.3[d]	KASEYA Unitrends supports MFA to web console access	CUSTOMER to determine if multifactor authentication is implemented for network access to non-privileged accounts.	Two Factor Authentication (2FA)
SC.L2-3.13.8[a]	KASEYA Unitrends encrypts data in transit and data at rest	CUSTOMER to determine if cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.	About this Guide

UNITRENDS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
SC.L2-3.13.8[b]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER provides/identifies alternative physical safeguards	Procedures for adding attached disk backup storage
SC.L2-3.13.8[c]	KASEYA Unitrends encrypts data in transit and data at rest	CUSTOMER provides/identifies alternative physical safeguards	Procedures for adding attached disk backup storage
SC.L2-3.13.11[a]	KASEYA Unitrends uses Crypto Module: Certificate #5040 (140-3) note: must be in FIPS mode	CUSTOMER to determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI.	
SC.L2-3.13.16[a]	KASEYA Unitrends protects data with AES-256 encryption at rest (Backup images, Snapshot data)	CUSTOMER to determine if the confidentiality of CUI at rest is protected.	
SI.L2-3.14.1[a]	KASEYA Unitrends provide alerting and monitoring capabilities and actively monitors for security advisories, firmware/software updates, and CVE notifications.	CUSTOMER determines in policy, the time (i.e., when) to identify system flaws	
SI.L2-3.14.1[b]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER determines if system flaws are identified within specified timeframe(s)	

UNITRENDS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
SI.L2-3.14.1[c]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER specifies in policy, the time to report system flaws	
SI.L2-3.14.1[d]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER determines if system flaws are (have been) reported within the specified timeframe	
SI.L2-3.14.1[e]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER specifies in policy, the time to correct system flaws Example: Critical vulnerabilities, corrected within 7 days, High vulnerabilities corrected within 14 days	
SI.L2-3.14.1[f]	KASEYA Unitrends updates are deployed in a Continuous Deployment model, with infrastructure patches occurring regularly. Agent updates are automatically rolled out across the fleet using a staged rollout process.	CUSTOMER to review reporting for when the vulnerability, missing patch, or misconfiguration was first flagged, then compare against established timeframes.	
SI.L2-3.14.6[a]	KASEYA Unitrends provides monitoring signals related to attacks within the backup environment through Audit and System Logs	CUSTOMER responsible for enterprise-wide attack detection	
SI.L2-3.14.6[b]	KASEYA Unitrends monitors agent-to-appliance connectivity, backup job traffic health (success/failure, integrity) and anomalous data patterns within backup streams	CUSTOMER responsible for monitoring inbound network communications traffic through perimeter security controls	Alerts Report

UNITRENDS CUSTOMER RESPONSIBILITY MATRIX

Assessment Objective	KASEYA Responsibility	CUSTOMER Responsibility	PRODUCT Links
SI.L2-3.14.6[c]	KASEYA Unitrends has no responsibility for this objective	CUSTOMER responsible for monitoring outbound communications traffic to detect attacks and indicators of potential attacks.	Alerts Report

CONTACT US



404.307.7235



mcline@controlcase.com



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

