Uplevel

Security FAQ

Basic questions:

Are you certified to any information security, quality, or business continuity standards such as ISO27001, SOC 2 Type 2? If yes, please provide a copy of the certificate.

- SOC 2 Type 2

Will you be subcontracting any of the services you provide through a third party? If so, will any third-party staff have access to Dave's data? If yes, please list all the sub-processors.

- AWS

Do you own and manage your email infrastructure? If not, how do you enforce TLS? (O365, Google GSuite, etc.)

- GSuite

Please provide details of your organization's options for data portability particularly data export, or off-boarding? i.e if XYZ company decided to move to a new supplier.

- All data outputs are owned by the XYZ team and can be exported at any time from the connector hub.

Describe the process for handling specific incidents involving assets belonging to XYZ company and suspected incidents or incidents that could have affected (but didn't) assets belonging to XYZ company.

- Please see Uplevel's Incident Management Policy

Describe how you will be able to guarantee that all data belonging to XYZ company will either be returned or permanently destroyed depending on the request of XYZ company?

- Please review our Information Security Policy for details (pg 62)

Audit & Compliance:

Has your organization been subject to any internal or external audits or reviews of your information security arrangements in the last 12 months? If so, please provide details of the findings including any weaknesses or improvements that have been identified.

- Connector Hub Pentest
- Dashboard Pentest

Could you please describe how the multitenant environment is handled at the "org" level and via org-specific encryption?

- Each tenant is given a client ID and vault password (through HashiCorp vault) which specifies the location of tenant data.

Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?

- Yes

Change and Configuration Management:

Do you have policies and procedures established for management authorization for the development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?

- Yes. Please take a look at our SOC 2 Type 2 report for more information

Do you have controls in place to ensure that security code reviews, threat modeling is incorporated in the software development process?

- Yes

Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?

- Yes

Is documentation describing known issues with certain products/services available?

- Yes, the Uplevel team will reach out as soon as an issue is known.

Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within them?

- Yes. Please take a look at our SOC 2 Type 2 report for more information

Identity and Access Management:

How does your organization manage and ensure unique usernames and passwords?

- 1password

Does your organization enforce system lockouts and systems enforced password expires and complexity? Please also explain how your password reset process works?

- Uplevel integrates with client SSO platforms — password resets are done on the client level

Does your organization have a password policy? If so, do you regularly review the policy, and who in the organization is responsible for this?

- Annually – CISO Albert Strong

If passwords are sent to XYZ employees in individual emails do they have to change them on the initial login?

- Yes

Do you restrict, log and monitor access to your information systems? (E.g., firewalls, vulnerability scanners, network sniffers, APIs, etc.). Restriction of personal assets must be based on the principle of least privileged access and supported through technical controls. For example (2FA, IP address filtering, firewalls, TLS encapsulation)

- Yes

Are system access logs maintained and reviewed? If so, who is responsible for doing so and how long are they retained?

- Yes. Please take a look at our SOC 2 Type 2 report

Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)? If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?

- Yes

Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?

- SSO integrations allow tenants to specify their own MFA.

How often do you review user access to ensure only the minimum access to Dave information and systems is provided for staff to perform their current roles?

- Annually

Do you have a cryptography key management process and is this managed?

- AWS KMS for our encryption purposes, which has automatically managed cryptography keys.

What is your practice for controlling access to clients' data?

- Uplevel uses the principle of least privilege when granting access to customer data. Beyond that, SSH and VPN connections are required to access any customer data.

Do you assign unique IDs to all system users?

- Yes

What is your practice for disabling or deleting User IDs if there is no activity?

- User IDs are disabled/deleted if the contractual agreement is terminated or if it is requested by the customer.

Do you require system administrators to use multi-factor authentication methods to gain system access?

- Yes

Do you display a warning banner regarding unauthorized access on systems that process data?

- No

What is your practice for reviewing access rights?

- Access rights are reviewed as part of SOC 2 Type 2 audit.

How do you secure paper and electronic media containing clients' data during storage and transmission?

- Data is transferred using a pre-signed url allowing only PUT requests that expire in one our Access to databases requires ssh and a unique ID and password. All access is logged.

Cloud Computing

Are Cloud Services provided? If yes, list all that apply, i.e., SaaS, PaaS, and/or IaaS.

- Yes Uplevel dashboard

What deployment models are provided, i.e., private cloud, public cloud, hybrid cloud, and/or community cloud? List all that apply.

- Yes Hybrid cloud - connector hub on customer side, Uplevel hosted on our side.

List all locations where client data will be stored.

- Yes AWS S3, After processing, data is stored in an RDS database

If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?

- Yes AWS supports automatic recovery

Is data segmentation and separation capability between clients provided? If yes, is it physical segmentation, network segmentation, system segmentation, and/or application segmentation?

- Yes System and application

Does the ability exist to legally demonstrate sufficient data segmentation in the event of a client subpoena or a forensics incident?

- Yes

Does the cloud services provider maintain a copy of any information even after removal from the cloud?

- Yes AWS retains data for 90 days before permanently deleting

Is staff required to use two factor authentication to access the production cloud environment containing client data?

- Yes

Is staff able to access client data in an unencrypted state?

- Yes

Is staff technically prevented from access to the cloud environment via non-managed private devices?

- No Every access attempt is fully logged from any device.

Are there controls to prevent one client attempting to compromise another client in a resource pooled environment? If so, please describe controls.

- No

Is a default hardened base virtual image available to clients?

- No

Are security logs applicable available to client's upon request?

- Yes

Is there a date retention/destruction schedule?

- Yes

Are all critical technology service providers described on an architecture diagram that includes physical systems and facilities?

- Yes

Does your cloud solution include software/provider independent restore and recovery capabilities?

- Yes AWS provides auto recovery capabilities

Encryption:

If the data is encrypted in the cloud, is encryption done locally or in the cloud?

- Yes Encryption is done in the cloud in almost all circumstances. There are some select instances where we opt to use client-side encryption

Are clients provided with the ability to generate a unique encryption key?

- N/A

Are clients provided with the ability to rotate their encryption key on a scheduled basis?

- Yes Clients are able to rotate their Hashicorp Vault keys. The AWS KMS keys are not directly managed by clients. They are rotated automatically annually.

Is cloud service provider staff able to access client encryption keys?

- No Even AWS employees cannot access AWS KMS keys.

What level of encryption is used?

- Yes 256-bit AES keys

Logging & Monitoring:

What is your practice for tracking and reviewing unauthorized logon attempts?

- Auth0 keeps a log of unauthorized login attempts.

What is your practice for tracking and reviewing modifications to system security settings ?

- All modifications affecting security settings are documented and flagged appropriately for review.

What other system activity do you track and review?

- CPU, disk space, network traffic, etc.

What information is included in your audit logs?

- Requests to servers, server responses

Who has access to your audit logs and what type of access is granted (read-only, modify, etc.)?

- Uplevel engineering team, all logs are read only

How long do you retain your audit logs online and in archive?

- 15 months

How often do you review your audit logs?

- As needed

Do you use an automated log-management solution? If yes, please describe.

- Data dog, AWS Cloudwatch

Do you have an automated synchronization process to a centralized time standard configured on all your company’s servers, network equipment, and access control devices that support it?

- No. Timestamps are noted