

Certification Package Overview: Vbrick Enterprise Video Platform

FedRAMP 20x Class C

FedRAMP package FR2702852019
Human-readable rendering
08 November 2026

1 About this document

This document is a human-readable rendering of the Certification Package Overview (CPO) for Vbrick Enterprise Video Platform (EVP), FedRAMP package FR2702852019. It was generated from the machine-readable CPO, Version 2.0, on 08 November 2026. The machine-readable CPO remains the authoritative record; where the two differ, the machine-readable CPO governs.

Values are reproduced as recorded. Line breaks inside text fields of the source are treated as wrapping and joined into continuous text, and Yes/No is shown for true/false values.

2 Service identification

FedRAMP package ID	FR2702852019
UEI number	KSS9H8NC9LY3
Provider	Vbrick Systems, Inc.
Service name	Vbrick Enterprise Video Platform
Service short name	Vbrick EVP
Service acronym	EVP
Certification type	20x
Certification class	Class C
Certification path	Program
Website	https://vbrick.com/
Logo	https://www.fedramp.gov/assets/img/logos/CSP_logos/VBrick%20Logo.png

2.1 Service description

Vbrick Enterprise Video Platform (EVP) is a multi-tenant Software as a Service (SaaS) offering, operated on Amazon Web Services, that enables organizations to securely deliver live and on-demand video to organizational users, anonymous users, or both. It provides central management of video assets, user access and permissions, network delivery devices, and video publishing and distribution, and integrates with customer directory services, single sign-on, and applications such as Microsoft Teams, Webex and SharePoint.

3 Service properties

Service type	SaaS
Deployment model	Hybrid Cloud
Business category	Content Management System (CMS), Media

Next Ongoing Certification Report	29 January 2027
Next quarterly review	04 February 2027
Ongoing Certification Report location	Paramify Trust Center: https://trust.paramify.com/vbrick/vbrick-evp
Availability web service	https://status.vbrick.com/
Availability data (machine-readable)	https://status.vbrick.com/us.json

4 Repositories

4.1 Trust center

Repository type	Trust Center
URL	https://trust.paramify.com/vbrick/vbrick-evp
Description	Paramify-hosted Trust Center publishing our FedRAMP compliance posture, control implementation status. Documentation is available to approved visitors upon request.
Authentication required	Yes
Access request instructions	Go to Request Access -> Fill in the required information under Trust Center Access Request -> Submit for approval. Once approved, you will receive an email notification. Return to the Trust Center and login via the email option to access the requested deliverables.
Agency access denial process	Vbrick will notify FedRAMP within five (5) business days of denying an agency's request for access to FedRAMP Certification Data, using the required notification form (CSPs Agency Access Denial), available at: https://help.fedramp.gov/hc/en-us/requests/new?ticket_form_id=51829826617243

4.2 Secure configuration guidance

Repository type	Secure Configuration Guide
URL	https://revdocs.vbrick.com/docs/secure-configuration-guide
Description	Secure Configuration Guide (SCG) is provided by Vbrick Systems, Inc. to support agency customers in deploying and administering Vbrick EVP.
Authentication required	No

4.3 Additional repositories

Repository type	Policies and Procedures, Ongoing Certification Reports
URL	https://trust.paramify.com/vbrick/vbrick-evp

Description	FedRAMP Certification Data for Vbrick EVP, including policies and procedures, Ongoing Certification Reports, and Significant Change Notifications. Available to approved visitors through the Paramify Trust Center.
Authentication required	Yes
Access request instructions	Go to Request Access -> Fill in the required information under Trust Center Access Request -> Submit for approval. Once approved, you will receive an email notification. Return to the Trust Center and login via the email option to access the requested deliverables.

Repository type	Certification Package Overview
URL	https://portal.vbrick.com/part/Vbrick_CPO_Class_C.json
Description	Machine-readable Certification Package Overview for Vbrick EVP, conforming to the FedRAMP Certification Package Overview schema.
Authentication required	No

4.4 Documentation overview

Document	Description	Access
Certification Package Overview (this document)	Overview of the offering, scope, third parties, cryptographic modules and package metadata.	Public
Security Decision Record (SDR)	Implementation, verification and validation of each applicable FedRAMP rule and Key Security Indicator.	Trust Center (restricted)
Secure Configuration Guide	Guidance for agency customers on configuring and administering Vbrick EVP securely.	Public
System Boundary Definition (EVP-DOC-01-US)	Minimum Assessment Scope, information resources, interconnections and information flows.	Trust Center (restricted)
FIPS 199 Categorization (Appendix K)	Security categorization of the offering (Moderate).	Trust Center (restricted)
Inventory of Instances, Software and Databases (Appendix M)	Data types, holding components, protections and authorized roles.	Trust Center (restricted)
Cryptographic Modules Table (Appendix Q)	Cryptographic modules by service, CMVP certificates and validation status.	Trust Center (restricted)
Ongoing Certification Reports and Significant Change Notifications	Quarterly reports and change notifications.	Trust Center (restricted)
Policies and procedures	See policiesAndProcedures.	Trust Center (restricted)

5 Contact information

Contact type	Email
Security	fedramp@vbrick.com
Sales	sales@vbrick.com

6 Assessor

Assessor	Coalfire Systems, Inc.
Assessor ID	138514

7 Certified services

The following services are included in the FedRAMP Minimum Assessment Scope.

Service	Description	Security category
Video on Demand	Upload through the browser, API or customer devices; storage in tenant-specific encrypted storage; optional transcoding; permission management; and authenticated playback, including CDN-accelerated delivery.	Moderate
Live Webcasting	Authenticated access and unified URLs for live webcasts, including cloud live streaming through CloudFront.	Moderate
Video Conference Recording	Connection to SIP-enabled conferences, with recordings ingested and processed as video on demand.	Moderate
Microsoft Teams and Webex Integrations	Cloud-side endpoints for streaming and recording from Microsoft Teams and Webex meetings.	Moderate
Authentication and Directory Integration	Local accounts, SAML single sign-on, and LDAP/SCIM-based user and group synchronization and authentication (cloud side).	Moderate
Public REST API and Application Integrations	Authenticated API access for uploads, downloads and integrated applications.	Moderate
Transcription and Translation	Optional automated transcription and translation of video audio tracks.	Moderate
Generative AI Features	Optional automatic titles, descriptions, tags, chapters, summaries, semantic search and chat with video content.	Moderate
Text-to-Speech	Optional narration and spoken renditions of video metadata.	Moderate
Vbrick Video IQ Facial Recognition	Optional discovery and tagging of users in videos based on profile pictures.	Moderate
MCP Server	Lets an authorized user connect a customer-designated large language model to query content and metadata the user is authorized to see.	Moderate
Video Analytics and Reporting	Viewing and usage analytics generated by the platform.	Moderate

Service	Description	Security category
Content and Tenant Administration	Central management of video assets, user access and permissions, and tenant configuration.	Moderate
Device and Client Logging Service	Cloud receipt of troubleshooting logs from Vbrick devices and client software.	Moderate
Peer-to-Peer Delivery Coordination	Cloud-side endpoint that coordinates peer-to-peer video delivery.	Moderate
Email Notifications	System-generated email notifications to tenant users.	Moderate

7.1 Services not included

The following items are not part of the certified offering.

Item	Reason
WebRTC services	Disabled by default for federal tenants; not certified for agency use. Its resources remain in the Minimum Assessment Scope because the environment is shared between tenants.
Vbrick Distributed Media Engine (DME) and encoders	Customer-owned and customer-operated devices.
Vbrick LDAP/SCIM Connector	Software installed and operated in the customer's network.
Vbrick Peer-to-Peer client software	Software deployed and operated by the customer on its workstations.
Vbrick mobile applications	Separately delivered client software.
Video players and browsers on viewer devices	Installed on and controlled by the customer's systems.
Customer-designated LLMs connected through the MCP Server	Selected and operated by the customer.
Customer and third-party platforms (Microsoft Teams, Webex, SharePoint, customer SSO providers and directories)	Operated by the customer or a third party; only the EVP-side integration is in scope.
Vbrick Ramp ECDN	Separate Vbrick product.
EVP deployments in the EU (Frankfurt, Ireland) and AP (Sydney)	Non-US regional deployments; no federal customer data and no network path to the US environment.
Vbrick non-production environments	No customer data.

8 Minimum Assessment Scope

8.1 Scope basis

Metadata included in scope	Yes. Metadata about federal customer data (D3, and the tenant and user identifiers in D6 and D7) is in scope wherever it resides, including third-party resources that receive it. All tenant data in the US environment is treated as federal customer data.
Inclusion criterion A	Data handling: stores, processes or transmits federal customer data or metadata about it.

Inclusion criterion B	Impact path: could reasonably affect the confidentiality, integrity or availability of federal customer data.

8.2 Data sets

Code	Data set	Contents	Information type	Security category
D1	Customer Content	Videos, audio, images, presentations, thumbnails and live streams uploaded or produced by tenants.	Information Management	Moderate
D2	Derived Content	Transcripts, translations, generated titles, descriptions, tags, chapters and summaries, text-to-speech audio, and other outputs created from customer content by EVP features.	Information Management	Moderate
D3	Customer Metadata	Metadata about customer content and tenants: titles, descriptions, permissions, tenant configuration, entitlements, search indexes, and tenant names and identifiers.	Information Management	Moderate
D4	Provisioned Account Attributes	Limited user and group records provided by the customer through one-way synchronization from the customer's directory or SSO provider: user and group identifiers, display names and email addresses. Local-account credentials exist only where a customer chooses local accounts.	Information Management	Moderate
D5	Biometric Data	Profile pictures and facial-recognition data, present only for tenants that enable Vbrick Video IQ facial recognition.	Information Management	Moderate
D6	Usage, Client and Device Logs	Access logs, client experience logs and logs from customer devices such as DMEs, including user identifiers, email addresses and client IP addresses.	Information Management	Moderate
D7	System Security Data	Audit logs, security events, configuration, vulnerability and inventory data, keys and certificates for the EVP service. May reference tenants and users but contains no customer content.	Information Management	Moderate

8.3 Information resources

All information resources are machine-based and categorized Moderate. Resources whose inclusion criterion includes A handle federal customer data.

8.3.1 Vbrick-operated resources

Resource	Description and role	Location	Data sets	Data state	Criterion	Federal data
Elastic Load Balancers	Front end for the Proxy/WAF tier; FIPS TLS policy (TLS 1.3/1.2).	Production 01	D1, D2, D3, D4, D6	In transit	A	Yes
Proxy/WAF tier	HAProxy, NGINX/OpenResty and locally managed open-appsec; DMZ and IDS.	Production 01	D1, D2, D3, D4, D6	In transit	A	Yes
EVP Core Nodes and processing services	UI, API, video management, transcoding, video ingestion, analytics, AI service and recording packaging.	Production 01; Management (recording packaging)	D1, D2, D3, D4, D5, D6	In transit	A	Yes

Resource	Description and role	Location	Data sets	Data state	Criterion	Federal data
MongoDB cluster	Vbrick-managed on EC2; metadata and permissions.	Production 01; replica in DR-01	D2, D3, D4, D5	Both	A	Yes
RabbitMQ cluster	Internal messaging.	Production 01; DR-01	D3	In transit	A	Yes
Elasticsearch cluster	Vbrick-managed on EC2; search and analytics.	Production 01	D2, D3, D4	Both	A	Yes
License Service	Entitlements.	Production 01	D3	At rest	A	Yes
Audit Service	Application logging.	Production 01	D6, D7	Both	A, B	Yes
Integration endpoints	Microsoft Teams, Webex streaming, Video Conference Integration (SIP) and Vbrick Peer-to-Peer endpoints.	Production 01	D1, D3, D6	In transit	A	Yes
Video Conference Integration services	SIP recorder, streaming and Microsoft Teams bot hosts, ECS tasks and SQS queues.	Production 01; DR-01	D1, D3	In transit	A	Yes
WebRTC services	vci-webrtc hosts and rev-webrtc-listener containers. In scope because the environment is shared between tenants; disabled by default for federal tenants and not certified for agency use.	Production 01; DR-01	D1	In transit	A, B	Yes
MCP Server	Lets an authorized user connect a customer-designated LLM to query content and metadata the user is authorized to see.	us-east-1 (Amazon ECS)	D2, D3	In transit	A	Yes
Lambda functions (application)	AI services, request validation, authentication and media delivery.	us-east-1; us-west-2 (DR)	D1, D2, D3, D4, D5	In transit	A	Yes
S3 buckets: customer and derived content	Customer and derived content, live streaming and AI outputs; tenant-specific and encrypted.	us-east-1	D1, D2	Both	A	Yes
S3 buckets: DR replicas and snapshots	DR replicas and database and search snapshots.	us-east-1; us-west-2	D1, D2, D3, D4, D5	At rest	A	Yes
S3 buckets: logs	Access, CloudFront, load balancer, DME and data logs.	us-east-1; us-west-2	D6	At rest	A	Yes
S3 buckets: configuration and keys	Configuration, keys, certificates, Lambda code and static web assets.	us-east-1; us-west-2	D7	At rest	B	No
CloudFront distributions (US)	Content delivery for US tenants; serves content only from US-region origins.	Edge; US origins only	D1, D6	In transit (cached)	A	Yes
Central logging and SIEM	Logstash and Kibana, and log archive.	Management	D6, D7	Both	A, B	Yes
Zabbix and monitoring hosts	Infrastructure monitoring.	Management	D7	Both	B	No
Database management and backup	MongoDB Ops Manager and Elastic X-Pack; administrative access to D2–D5.	Management	D7	In transit	B	No

Resource	Description and role	Location	Data sets	Data state	Criterion	Federal data
Shield	Vbrick inventory, vulnerability findings and POA&M, and change-event monitoring platform.	Management	D7	At rest	B	No
Mail Host	Outbound system notifications.	Management	D3, D4	In transit	A	Yes
Bastion and Windows jump host	Administrative access.	Production 01; Management	D7	In transit	B	No
Egress proxy	Deny-by-default outbound traffic control.	Management	D7	In transit	B	No
Certificate authority	Internal certificate issuance.	Management	D7	At rest	B	No
Wazuh	Host security monitoring and file integrity.	Management	D6, D7	Both	B	No
Build and deployment pipeline	Jenkins build system, Ansible, image builder, build repositories and ECR images.	us-east-1; Jenkins server in co-location space, Ashburn, VA	D7	At rest	B	No
Security and inventory stores	AWS Config, Systems Manager inventory, container scanning and evidence.	us-east-1	D7	At rest	B	No
Operations automation	Lambda functions for patching, inventory, change-event alerting, scaling hooks and reports.	us-east-1; us-west-2	D7	In transit	B	No
DR-01 standby hosts	Disaster recovery standby hosts.	DR-01 (us-west-2)	D1, D2, D3, D4, D5, D6	Both	A	Yes
Deployment Validation environment	Tests production deployment scripts against a replica of the production database; not publicly accessible; data deleted on shutdown.	Staging-01 (us-east-1)	D3, D4, D5	At rest during a validation run only	A	Yes

8.3.2 AWS managed services

Resource	Description and role	Location	Data sets	Data state	Criterion	Federal data
Amazon EC2 and EBS	Hosts and block storage for EVP, management and DR, including Auto Scaling groups.	us-east-1; us-west-2	D1, D2, D3, D4, D5, D6, D7	Both	A	Yes
Amazon S3	Object storage for content, replicas, snapshots, logs and configuration.	us-east-1; us-west-2	D1, D2, D3, D4, D5, D6, D7	At rest	A	Yes
Amazon CloudFront	Content delivery for US tenants.	Edge; US origins only	D1, D6	In transit	A	Yes
Elastic Load Balancing	Front end for the Proxy/WAF tier. Covered under Amazon EC2.	us-east-1; us-west-2	D1, D2, D3, D4, D6	In transit	A	Yes
Amazon ECS and Amazon ECR	Video Conference Integration tasks and MCP Server; container images.	us-east-1; us-west-2	D1, D2, D3, D7	Both	A	Yes

Resource	Description and role	Location	Data sets	Data state	Criterion	Federal data
AWS Lambda	Serverless processing for AI services, media delivery and operations.	us-east-1; us-west-2	D1, D2, D3, D4, D5	In transit	A	Yes
Amazon SQS	Control messaging for Video Conference Integration.	us-east-1; us-west-2	D3	In transit	A	Yes
Amazon SES	Outbound system email delivery.	us-east-1	D3, D4	In transit	A	Yes
AWS KMS and AWS Secrets Manager	Encryption keys for data at rest; service credentials.	us-east-1; us-west-2	D7	At rest	B	No
AWS IAM, IAM Identity Center and AWS Organizations	Administrative access and service control policies.	Production, Management and Organizations accounts	D7	At rest	B	No
AWS CloudTrail, Amazon CloudWatch and Amazon Athena	Audit logging, monitoring and log queries.	Production and Audit accounts	D6, D7	Both	A, B	Yes
AWS Systems Manager	Session Manager brokered host access; inventory.	us-east-1; us-west-2	D7	Both	B	No
AWS Config and Amazon Inspector	Configuration recording; image and host vulnerability checks.	us-east-1; us-west-2	D7	At rest	B	No
Amazon Macie (optional feature)	Sensitive-data discovery on S3 (reads D1–D3; findings are D7).	us-east-1	D1, D2, D3, D7	In transit	A, B	Yes
Amazon Transcribe and Amazon Translate	Transcription and translation.	us-east-1	D1, D2	In transit	A	Yes
Amazon Polly	Text-to-speech.	us-east-1	D1, D2	In transit	A	Yes
Amazon Bedrock (Anthropic Claude)	Generative AI features; AWS and Anthropic do not train on customer data.	us-east-1	D1, D2, D3	In transit	A	Yes
Amazon Rekognition	Facial recognition for Vbrick Video IQ.	us-east-1	D1, D5	In transit	A	Yes

8.4 Supporting resources

Resource	EVP status page (status.vbrick.com)
Description and role	Vbrick-built availability service served from an S3 bucket and CloudFront in us-west-2. Holds no federal customer data or metadata and has no path to production systems.

8.5 Exclusions

Resource set	Reason code	Rationale
EU deployment: Prod-02, Staging-02 and Management (eu-central-1); DR-02 (eu-west-1)	X1	Serves non-US customers; no federal data; no network path, replication, shared keys or shared servers with the US environment.

Resource set	Reason code	Rationale
AP deployment: Prod-03 and its management VPC (ap-southeast-2)	X1	Serves non-US customers; no federal data; no network path, replication, shared keys or shared servers with the US environment.
Lambda@Edge functions for the EU and AP CloudFront distributions	X1	Belong to the excluded deployments; AWS requires Lambda@Edge functions to reside in us-east-1.
Ramp ECDN: S3 buckets, API Gateway and api.rampecdn.com distribution	X2	Separate Vbrick product; handles no EVP customer data; covered by the account-level controls.
Non-production account	X3	No customer data.
Customer-premises devices and customer systems	X4	Customer-owned or customer-operated.
Corporate tools, other ticketing systems, billing and cost reporting	X5	No federal customer data and no privileged path; production work cannot be initiated from them.
AWS Cloud Intelligence Dashboards	X5	Cost and usage reporting only; no federal customer data and no privileged path.

9 Information flows

Security category of the offering	Moderate
Data flow diagram reference	System Boundary Definition EVP-DOC-01-US, Appendix C – Data Flow Diagram

All information flows are categorized Moderate.

Flow	Source → destination	Data sets	Information carried	Explanation
Authentication – SAML SSO	User's browser; customer SSO provider → Proxy/WAF → EVP Core Nodes → MongoDB	D4	SAML assertions, session tokens, provisioned account attributes	Users authenticate through the customer's SAML identity provider over TLS. EVP does not store passwords for SSO users.
Authentication and directory sync – LDAP/SCIM Connector	Vbrick LDAP/SCIM Connector in the customer network → Proxy/WAF → EVP Core Nodes → MongoDB	D4	User and group records; forwarded LDAP authentication requests	The connector connects outbound from the customer network over an encrypted channel, synchronizes users and groups one way, and forwards LDAP authentication to the customer directory.
Authentication – local accounts	User's browser → Proxy/WAF → EVP Core Nodes → MongoDB	D4	Local-account credentials, session tokens	Used only where a customer chooses local accounts.
Media upload and download – browser	User's browser → Elastic Load Balancers → Proxy/WAF → EVP Core Nodes → Amazon S3; MongoDB	D1, D3	Video and other media files, metadata	Authenticated users upload and download media over HTTPS. Content is stored in tenant-specific encrypted S3 storage and may be transcoded.

Flow	Source → destination	Data sets	Information carried	Explanation
Media upload and download – DMEs and encoders	Customer-operated DME or encoder → Elastic Load Balancers → Proxy/WAF → EVP Core Nodes → Amazon S3; MongoDB	D1, D3, D6	Video files, device registration, heartbeat and configuration, software updates, device logs	Customer-owned devices authenticate with access keys and exchange media and configuration over HTTPS; device logs are sent to EVP.
Media upload and download – API and integrations	Customer-operated application or integration (e.g., SharePoint) → Elastic Load Balancers → Proxy/WAF → EVP Core Nodes → Amazon S3; MongoDB	D1, D2, D3	Media files, metadata, API credentials	Integrating applications authenticate to the public REST API and transfer content over HTTPS.
Video on demand playback	Amazon S3 via EVP Core Nodes and CloudFront → Viewer's browser or player	D1, D6	Video content, access logs	Video is served from cloud storage or through US-origin CloudFront distributions. Cached content is visible only to authenticated users unless marked public.
Live webcasts	Customer encoder or on-premises device → Proxy/WAF → EVP Core Nodes → CloudFront → viewer	D1, D3	Live video streams (in transit only), webcast metadata	EVP authenticates viewers and routes the webcast; live content is not stored in the cloud while in progress.
Video conference recording	SIP-enabled conference, Microsoft Teams or Webex → Integration endpoints → Video Conference Integration services (ECS, SQS) → Amazon S3	D1, D3	Conference audio and video, recording metadata	Conferences are recorded live, processed and added to the tenant as video on demand.
Client and device logging	DMEs and Vbrick Peer-to-Peer clients → CloudFront (dme-logs.us) → S3 log buckets → central logging	D6	Client and device logs including user identifiers, email addresses and client IP addresses	Used for remote troubleshooting.
Transcription and translation	EVP Core Nodes and Lambda → Amazon Transcribe and Amazon Translate → Amazon S3	D1, D2	Audio tracks, transcripts and translations	Optional feature; outputs are stored within the boundary; AWS does not train on customer data.
Generative AI and text-to-speech	EVP Core Nodes and Lambda → Amazon Bedrock (Anthropic Claude) and Amazon Polly → Amazon S3	D1, D2, D3	Transcripts, extracted video frames, metadata, generated text and audio	Optional features; only the minimum necessary data is sent; outputs are stored within the boundary; AWS and Anthropic do not train on customer data.
Facial recognition (Video IQ)	EVP Core Nodes and Lambda → Amazon Rekognition → Amazon S3; MongoDB	D1, D5	Video frames, profile pictures, facial-recognition data	Optional feature enabled per tenant; AWS does not train on customer data.
MCP Server queries	Customer-designated LLM → Proxy/WAF → MCP Server (ECS) → EVP Core Nodes	D2, D3	Content and metadata the user is authorized to see	Requests arrive over HTTPS; the customer selects and operates the LLM and is responsible for data sent to it.
System notifications	EVP Core Nodes → Mail Host → Amazon SES → tenant users	D3, D4	Notification content, user email addresses	Outbound system-generated email.

Flow	Source → destination	Data sets	Information carried	Explanation
Disaster recovery replication	Production 01 (us-east-1) → DR-01 (us-west-2)	D1, D2, D3, D4, D5	Replicated content and database records	S3 cross-region replication and a MongoDB replica over encrypted connections; no replication to non-US regions.
Deployment validation	Production 01 database → Staging-01 (us-east-1)	D3, D4, D5	Replica of the production database	Used only during a validation run; data never leaves the Production account and is deleted at shutdown.
Build and deployment	GitHub Enterprise Cloud → Jenkins (co-location) → ECR and S3 build repositories → Harness delegate in Production 01	D7	Source code, build artifacts, container images, configuration	Jenkins builds and publishes artifacts over HTTPS; deployment runs within AWS under an approved Jira change request.
Administrative and support access	Vbrick operations and support staff (Entra ID identities) → IAM Identity Center → AWS Console / Systems Manager Session Manager → Management VPC → hosts	D7	Administrative sessions; administrative access to D1–D6	SSO with MFA; host access is brokered by Session Manager with no direct network path from Vbrick offices.
Security and operations telemetry	Production hosts, Zabbix, CloudWatch, CloudTrail, Shield → CrowdStrike, Qualys, PagerDuty, Slack, Site24x7	D6, D7	Host telemetry, scan results, CloudTrail write events, alerts	Carries system security data and no customer content.
Compute scaling actions	nOps (cross-account role) → Lambda functions, EventBridge rules and Auto Scaling groups in the Production account	D7	Scaling instructions and instance events	Actions are recorded in CloudTrail in the Audit account and analyzed by CrowdStrike.

10 Third-party information resources

10.1 FedRAMP certified

Amazon Web Services – AWS US East/West

FedRAMP ID	AGENCYAMAZONEW
Provider	Amazon Web Services, Inc.
Use case	Infrastructure provider hosting the EVP service: compute (EC2, including Elastic Load Balancing and Auto Scaling; EBS), storage (S3), networking and delivery (VPC, CloudFront), containers (ECS, ECR), serverless (Lambda), messaging (SQS), email (SES), keys and secrets (KMS, Secrets Manager), identity and governance (IAM, IAM Identity Center, Organizations), logging and monitoring (CloudTrail, CloudWatch, Athena, Config, Inspector, Systems Manager, Macie), and the optional AI features (Transcribe, Translate, Polly, Bedrock with Anthropic Claude, Rekognition).
Usage and configuration	Services used only in us-east-1 (primary) and us-west-2 (disaster recovery) within the Production account, with the Organizations management account and the Audit account.

Justification for use	Hosting platform for the service.
Mitigation measures	Data at rest encrypted with AWS KMS; AI services configured so that AWS and Anthropic do not train on customer data.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

10.2 Not FedRAMP certified

CrowdStrike Falcon

Provider	CrowdStrike, Inc.
Website	https://www.crowdstrike.com/
Use case	Endpoint detection and response, vulnerability management, container image scanning, CSPM and DSPM.
Usage and configuration	Falcon sensor on every production host; container image scanning; CSPM of the Production account; DSPM scanners in a dedicated VPC in the account; receives CloudTrail write events for indicator-of-attack analysis.
Justification for use	Endpoint protection, vulnerability detection and configuration monitoring.
Mitigation measures	Integration roles limited to what each module needs; console access requires MFA; DSPM returns classification findings, not content.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

Microsoft Entra ID

Provider	Microsoft Corporation
Website	https://www.microsoft.com/security/business/microsoft-entra
Use case	Workforce identity source for administrative access.
Usage and configuration	Groups provisioned to IAM Identity Center by SCIM.
Justification for use	Central workforce identity with MFA for privileged access.
Mitigation measures	MFA for every production access holder; Conditional Access blocks the AWS applications on devices that are not company-owned; production access through Identity Center permission sets and time-boxed approval.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

GitHub Enterprise Cloud

Provider	GitHub, Inc.
Website	https://github.com/

Use case	Source control for software and infrastructure code deployed to production.
Usage and configuration	Source code, infrastructure-as-code templates and environment configuration; sign-in through Entra SSO; access by team. No access to the production environment.
Justification for use	Version control for software and infrastructure code.
Mitigation measures	Signed commits verified by GitHub; pull request with one approval required on the production branch; team access reviewed at least monthly.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

Atlassian Jira

Provider	Atlassian Corporation
Website	https://www.atlassian.com/software/jira
Use case	Change and work authorization.
Usage and configuration	The only system that authorizes work in production, including changes, access requests and log deletion; support escalations may reference tenants.
Justification for use	Change and work authorization.
Mitigation measures	Production work is performed only against an approved Jira ticket; tickets reference tenants by name or identifier, not customer content; access limited to Vbrick personnel through SSO.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

Salesforce

Provider	Salesforce, Inc.
Website	https://www.salesforce.com/
Use case	Customer support cases and customer maintenance notifications.
Usage and configuration	Support cases may include tenant names or identifiers; Marketing Cloud Account Engagement sends customer maintenance notifications.
Justification for use	Customer support and maintenance notifications.
Mitigation measures	No access to production; requests in Salesforce do not drive production work unless a Jira ticket is approved.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

Qualys Policy Audit

Provider	Qualys, Inc.
Website	https://www.qualys.com/
Use case	Configuration compliance scanning.
Usage and configuration	Checks EC2 images and MongoDB databases against CIS Benchmarks.
Justification for use	Configuration compliance scanning.
Mitigation measures	Scanning credentials limited to audit functions; results reviewed by Information Security.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

PagerDuty

Provider	PagerDuty, Inc.
Website	https://www.pagerduty.com/
Use case	On-call alerting.
Usage and configuration	Escalates alerts from Zabbix, Site24x7, CloudWatch, CloudTrail change events and Shield.
Justification for use	On-call alerting.
Mitigation measures	Receives notifications only; no access to production.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

Slack

Provider	Slack Technologies, LLC
Website	https://slack.com/
Use case	Operations alert visibility.
Usage and configuration	Operations channel for change-event alerts and FedRAMP message alerts.
Justification for use	Real-time alert visibility.
Mitigation measures	Receives notifications only; no access to production.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

Site24x7

Provider	Zoho Corporation

Website	https://www.site24x7.com/
Use case	External availability monitoring.
Usage and configuration	Monitors availability of public endpoints.
Justification for use	Availability monitoring.
Mitigation measures	Probes public endpoints only; no credentials or access to production.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

Paramify

Provider	Paramify, Inc.
Website	https://www.paramify.com/
Use case	GRC platform and Trust Center.
Usage and configuration	Holds the SDR, solution capabilities and Trust Center.
Justification for use	Certification data sharing.
Mitigation measures	No connection to production; holds system documentation, not customer data.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

Cobalt

Provider	Cobalt Labs, Inc.
Website	https://www.cobalt.io/
Use case	Independent penetration testing.
Usage and configuration	Annual penetration test of the EVP service using a dedicated test tenant.
Justification for use	Independent penetration testing.
Mitigation measures	Testers have no access to customer tenants; credentials limited to the test tenant and test period.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

nOps Compute Copilot

Provider	nOps
Website	https://www.nops.io/
Use case	Compute cost optimization for autoscaled capacity.

Usage and configuration	Manages selected Auto Scaling groups in the Production account through Lambda functions, EventBridge rules and IAM roles that nOps deploys and maintains through a cross-account role; a separate read-only role supports cost analysis.
Justification for use	Compute cost optimization for autoscaled capacity.
Mitigation measures	Actions by nOps roles are recorded in CloudTrail in the Audit account and analyzed by CrowdStrike; IAM changes raise immediate Shield alerts.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

Harness

Provider	Harness Inc.
Website	https://www.harness.io/
Use case	Deployment orchestration.
Usage and configuration	SaaS that orchestrates production deployment pipelines; a delegate in Production 01 connects outbound to Harness over HTTPS and runs pipeline steps with its host's IAM role.
Justification for use	Deployment orchestration.
Mitigation measures	Production deployments run only under an approved Jira change request; the delegate makes outbound connections only; delegate actions are recorded in CloudTrail in the Audit account; deployment credentials are held in AWS Secrets Manager.
Compensating controls	Tracked in the Vendor Supply Chain Risk Management Tracker and reviewed monthly; vendor SOC 2 Type II, ISO 27001 or equivalent reports and agreements reviewed annually.

11 Policies and procedures

All policies and procedures are available to approved parties in the Paramify Trust Center (restricted layer).

Name / file name	Summary	Version, date, words	Related FedRAMP practices
Addressing FedRAMP Communications Policy Addressing FedRAMP Communications Policy	Establishes requirements for maintaining a FedRAMP Security Inbox and receiving, acknowledging and acting on FedRAMP communications within required timeframes.	Version 1 01 July 2026 710 words	FedRAMP 20x: AFC (Addressing FedRAMP Communication)

Name / file name	Summary	Version, date, words	Related FedRAMP practices
Addressing FedRAMP Communications Procedures Addressing_FedRAMP_Communications_Procedures_AFC-PRO-01.pdf	Receiving, acknowledging and acting on FedRAMP communications through the FedRAMP Security Inbox, including Emergency and Important messages.	Version 1 01 July 2026 1,206 words	FedRAMP 20x: AFC (Addressing FedRAMP Communication)
Capacity Planning Procedure Capacity_Planning_Procedure_CAP-PRO-01.pdf	Implements the Capacity Planning Policy: defining capacity requirements, monitoring utilization and planning capacity for the EVP.	Version 1 04 August 2026 3,237 words	FedRAMP 20x: KSI-CNA (Cloud Native Architecture)
Certification Data Sharing Policy Certification Data Sharing - Policy	Defines requirements for sharing FedRAMP certification data, including use of a FedRAMP-compatible trust center.	Version 1 01 July 2026 2,479 words	FedRAMP 20x: CDS (Certification Data Sharing)
Certification Data Sharing Procedure Certification_Data_Sharing_Procedure_CDS-PRO-01.pdf	Implements the Certification Data Sharing Policy: Trust Center content, machine-readable schema conformance, agency access and historical certification data.	Version 1 03 August 2026 2,219 words	FedRAMP 20x: CDS (Certification Data Sharing)
Collaborative Continuous Monitoring Handbook Collaborative_Continuous_Monitoring_Handbook_CCM-PRO-01.pdf	Collaborative Continuous Monitoring: Ongoing Certification Reports, quarterly reviews and sharing of current certification information with agencies.	Version 1 01 July 2026 3,952 words	FedRAMP 20x: CCM (Collaborative Continuous Monitoring)
Collaborative Continuous Monitoring Policy Collaborative Continuous Monitoring Policy	Establishes requirements for collaborative continuous monitoring, including Ongoing Certification Reports and quarterly reviews shared with agencies.	Version 1 01 July 2026 1,604 words	FedRAMP 20x: CCM (Collaborative Continuous Monitoring)
Configuration Management Handbook Configuration_Management_Handbook_CM-PRO-02.pdf	Configuration and change management: baselines, change control, deployment and configuration monitoring for the EVP.	Version 6 06 July 2026 4,974 words	NIST SP 800-53 Rev 5: CM (Configuration Management)
Configuration Management Policy Configuration Management Policy	Establishes configuration and change management requirements for the EVP, including baselines, change approval and configuration monitoring.	Version 7 08 July 2026 1,409 words	NIST SP 800-53 Rev 5: CM (Configuration Management)

Name / file name	Summary	Version, date, words	Related FedRAMP practices
Contingency Planning Handbook Contingency_Planning_Handbook_CP-PRO-03.pdf	Contingency planning: backup, recovery planning and contingency plan testing for the EVP.	Version 5 01 January 2026 2,325 words	NIST SP 800-53 Rev 5: CP (Contingency Planning)
Incident Evaluation and Communication Policy Incident Evaluation and Communication Policy	Establishes requirements for evaluating incidents for FedRAMP reportability and communicating FedRAMP Reportable Incidents to FedRAMP, agencies and necessary parties.	Version 1 01 July 2026 1,278 words	FedRAMP 20x: IEC (Incident Evaluation and Communication)
Incident Evaluation and Communication Procedure Incident_Evaluation_and_CommunicationProcedure_IEC-PRO-01.pdf	Evaluating incidents for FedRAMP reportability and communicating FedRAMP Reportable Incidents to FedRAMP, agencies and necessary parties.	Version 2 30 October 2026 1,616 words	FedRAMP 20x: IEC (Incident Evaluation and Communication)
Incident Response Handbook Incident_Response_Handbook_IR-PRO-02.pdf	Incident response: triage, containment, remediation and notification for security incidents affecting the EVP.	Version 7 31 July 2026 6,758 words	NIST SP 800-53 Rev 5: IR (Incident Response)
Incident Response Plan Incident Response Plan	Defines the coordinated plan for detecting, responding to, recovering from and reporting security incidents affecting the EVP.	Version 4 01 July 2026 3,514 words	NIST SP 800-53 Rev 5: IR (Incident Response)
Incident Response Policy Incident Response Policy	Establishes incident response requirements for the EVP, including roles, response phases and notification.	Version 7 21 July 2026 2,362 words	NIST SP 800-53 Rev 5: IR (Incident Response)
InfoSec Program Goals and Executive Review – CY2027 InfoSec_Goals_and_Executive_Review_IS-GER-01.pdf	Annual Information Security program goals, resourcing and executive review for CY2027.	Version 1 01 August 2026 1,687 words	FedRAMP 20x: KSI-PIY (Policy and Inventory)
Information Security Policy Information Security Policy	Establishes Vbrick's information security program for the EVP, including governance, roles and responsibilities, and the policy framework under which the family policies operate.	Version 6 01 January 2026 30,813 words	NIST SP 800-53 Rev 5: PM (Program Management)
Information System Contingency Plan Information_System_Contingency_Plan_CP-PRO-04.pdf	Information System Contingency Plan: recovery roles, procedures and restoration of the EVP following disruption.	Version 7 01 January 2026 12,250 words	NIST SP 800-53 Rev 5: CP (Contingency Planning)

Name / file name	Summary	Version, date, words	Related FedRAMP practices
Key Security Indicators Policy Key Security Indicators Policy	Establishes requirements for meeting, measuring and validating each FedRAMP 20x Key Security Indicator for the EVP.	Version 1 01 July 2026 2,546 words	FedRAMP 20x: KSI-CED (Cybersecurity Education) FedRAMP 20x: KSI-CMT (Change Management) FedRAMP 20x: KSI-CNA (Cloud Native Architecture) FedRAMP 20x: KSI-IAM (Identity and Access Management) FedRAMP 20x: KSI-INR (Incident Response) FedRAMP 20x: KSI-MLA (Monitoring, Logging and Auditing) FedRAMP 20x: KSI-PIY (Policy and Inventory) FedRAMP 20x: KSI-RPL (Recovery Planning) FedRAMP 20x: KSI-SCR (Supply Chain Risk) FedRAMP 20x: KSI-SVC (Service Configuration)
Key Security Indicators Procedure Key_Security_Indicators_Procedure_KSI-PRO-01.pdf	Implements the Key Security Indicators Policy: operational workflows by which Vbrick meets and measures each Key Security Indicator.	Version 1 01 July 2026 4,270 words	FedRAMP 20x: KSI-CED (Cybersecurity Education) FedRAMP 20x: KSI-CMT (Change Management) FedRAMP 20x: KSI-CNA (Cloud Native Architecture) FedRAMP 20x: KSI-IAM (Identity and Access Management) FedRAMP 20x: KSI-INR (Incident Response) FedRAMP 20x: KSI-MLA (Monitoring, Logging and Auditing) FedRAMP 20x: KSI-PIY (Policy and Inventory) FedRAMP 20x: KSI-RPL (Recovery Planning) FedRAMP 20x: KSI-SCR (Supply Chain Risk) FedRAMP 20x: KSI-SVC (Service Configuration)

Name / file name	Summary	Version, date, words	Related FedRAMP practices
Significant Change Notification Policy Significant Change Notification Policy	Establishes requirements for identifying, classifying, documenting and notifying significant changes to the EVP.	Version 1 01 July 2026 2,703 words	FedRAMP 20x: SCN (Significant Change Notification)
Significant Change Notification Procedure Significant_Change_Notification_Procedure_SCN-PRO-01.pdf	Implements the Significant Change Notification Policy: identifying, classifying, documenting and communicating significant changes.	Version 2 04 September 2026 3,650 words	FedRAMP 20x: SCN (Significant Change Notification)
Software Development Life Cycle Procedure Handbook Software_Development_Lifecycle_Procedure_SDLC-PRO-01.pdf	Implements the Software Development Life Cycle Policy: secure development, testing and release of EVP software.	Version 2 01 January 2026 3,481 words	NIST SP 800-53 Rev 5: SA (System and Services Acquisition)
Software Development Lifecycle Policy Software Development Lifecycle Policy	Establishes secure software development requirements for the EVP, including design, code review, testing and release.	Version 9 01 January 2026 3,454 words	NIST SP 800-53 Rev 5: SA (System and Services Acquisition)
Supply Chain Risk Management Plan Supply Chain Risk Management Plan	Defines how suppliers and third-party components that handle federal customer data or affect the EVP are identified, risk-rated, monitored and reviewed.	Version 5 04 August 2026 2,255 words	NIST SP 800-53 Rev 5: SR (Supply Chain Risk Management)
System and Communication Protection Handbook System_and_Communications_Protection_Handbook_SC-PRO-02.pdf	System and communications protection: boundary protection, encryption in transit and at rest, and network segregation.	Version 6 01 July 2026 4,384 words	NIST SP 800-53 Rev 5: SC (System and Communications Protection)
System and Communications Protection Policy System and Communications Protection Policy	Establishes system and communications protection requirements, including boundary protection, network segregation and encryption of data in transit and at rest.	Version 7 01 July 2026 1,520 words	NIST SP 800-53 Rev 5: SC (System and Communications Protection)
Vulnerability Management Procedure Vulnerability Management Procedure	Defines how vulnerabilities in the EVP are detected, evaluated, prioritized, remediated and reported.	Version 1 01 July 2026 2,256 words	NIST SP 800-53 Rev 5: RA (Risk Assessment)

12 Cryptographic modules

Data at rest in Amazon EBS (including MongoDB and Elasticsearch volumes), Amazon S3 and backups is encrypted with AES-256 using keys held in AWS KMS. Connections from users and customer systems terminate at load balancers that use a FIPS TLS policy accepting TLS 1.3 and 1.2; unencrypted connections are not accepted. Within the production VPCs, all production instances use supported Nitro-based instance types, which use the offload capabilities of the underlying Nitro System hardware to encrypt in-transit traffic between instances automatically. Agency tenants use these modules by default. Modules by service are listed in the Cryptographic Modules Table (Appendix Q).

Module	Services covered	Cryptographic services	CMVP validation
AWS Key Management Service HSM	Data at rest: Amazon EBS (full disk, including MongoDB and Elasticsearch volumes) and Amazon S3 (SSE-KMS), backups and snapshots	Data at rest	Active validation
AWS-LC	Data in transit: user and customer connections at the Elastic Load Balancing FIPS TLS policy (TLS 1.3/1.2)	Data in transit	Active validation
Amazon Linux 2023 cryptographic modules	EVP hosts (Amazon Linux 2023)	Operating system cryptography	Operated in FIPS mode; CMVP certificate not identified

13 Package metadata

Responsible official	Todd Kistner, VP, Cloud Operations
Email	todd.kistner@vbrick.com
Phone	203-303-0259
Version	Version 2.0
Date and time of last update	08 November 2026 00:00 UTC
Source of update	Vbrick Information Security
Package maintenance interval	2 weeks
Security Decision Record version	1.0.12
System Boundary Definition	EVP-DOC-01-US Rev 15