

# backupta for U.S. Federal Agencies

## Keep identity dependable across the providers your business runs on

Identity is one of the most critical assets behind public services, connecting employees, contractors, administrators, applications, and external users to the systems they need. IAM and IT teams are under pressure to keep access highly available, recoverable, and compliant across complex identity environments. Backupta provides the visibility, control, recovery, and failover workflows needed to keep identity dependable when public services depend on it.



### Own your side of the identity shared responsibility model

Identity providers deliver the core service: platform availability, infrastructure security, and access management controls.

Your organization owns the operational state of identity: users, groups, applications, policies, workflows, roles, authentication settings, tenant configurations, and the relationships between them.

For public sector teams, that responsibility carries across the authorization lifecycle. Even when the IDP is FedRAMP authorized, agencies still need to protect, recover, and produce evidence for the identity configurations they operate, including backup and recovery expectations aligned to NIST SP 800-53 controls such as CP-9 and CP-10.

Backupta helps teams meet this responsibility with continuous identity state capture, change visibility, dependency-aware recovery, guided disaster recovery workflows, and audit-ready evidence.



#### See every identity change

Gain visibility into all changes across your identity providers, who made them, and when they happened. Get a clear history of identity activity so you can investigate faster without relying on scattered logs, tickets, or manual exports.



#### Control configuration drift

Keep your identity environment aligned with its expected state. Compare configurations over time, identify unintended drift, and validate changes before they create access, security, or compliance issues.



#### Recover safely

Restore the specific object, attribute, policy, workflow, automation, or configuration that changed. Recover what is needed with the right dependencies, without broad rollbacks or manual reconstruction.



#### Execute identity disaster recovery

Maintain a synchronized failover tenant ready to activate during a major outage, cyberattack, or tenant-level disruption. Run failover, fallback, and validation with guided procedures and audit-ready reporting.

Backupta provides coverage for:



## Support mission continuity and ATO activities

**Mission delivery depends on identity availability.** Backupta helps public sector teams keep services accessible while preserving the evidence needed for authorization, continuous monitoring, and recovery reviews.

**Access continuity:** Activate a synchronized failover tenant during an outage, cyberattack, misconfiguration cascade, or tenant-level disruption.

**Contingency planning:** Support backup, recovery, and reconstitution expectations with incremental backups, dependency-aware recovery, and guided runbooks.

**Authorization evidence:** Preserve change history, backup records, recovery activity, timestamps, operators, notes, and runbook reports for A&A, POA&M closure, and 3PAO reviews.

**Continuous monitoring:** Record drift, policy changes, and administrative actions, with integrations into SIEM, ITSM, and workflow tools.

**Trusted recovery state:** Maintain an external record of identity configurations to support reconstitution when the primary tenant is unavailable, unsafe, or misconfigured.

Backupta helps agencies maintain access, accelerate recovery, and meet compliance requirements with confidence.

## Deployment support for FedRAMP environments

FedRamp  
Moderate

### Support summary

Full identity resilience platform support, including backup and restore, release management and cloning, dependency-aware recovery, release management, failover tenants, guided DR runbooks, Compliance Center, APIs, customer-owned storage, and extended retention.

FedRAMP  
High considerations

| Area               | FedRAMP High support                                                                                                                                                                          |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage            | Customer-owned storage with FedRamp certified AWS GovCloud, Azure, or GCP storage. Backupta-hosted storage supported with AWS GovCloud.                                                       |
| Core resilience    | Backup and restore, release management and cloning, dependency-aware recovery, granular recovery, full tenant recovery, failover tenant, guided DR runbooks, and Last Mile support available. |
| Logs and retention | One-year logs and backups included. Extended retention of two years or more available.                                                                                                        |
| Integrations       | Alerting through Teams, Workspace, Slack, ITSM, and webhook: planned support. Connected applications must meet customer environment requirements.                                             |
| Guardrails         | Golden Tenant and Guardrails: planned Support.                                                                                                                                                |

Availability may depend on deployment model, storage configuration, connected applications, and the customer's approved FedRAMP operating environment.

## Built to work with public sector workflows

The platform integrates with the tools identity, IT, security, and compliance teams already use to investigate changes, coordinate response, and maintain evidence. Supported workflows include collaboration, ticketing, ITSM, webhooks, APIs, and security operations integrations such as ServiceNow, Jira, Slack, Microsoft Teams, Google Workspace, and SIEM workflows, subject to the customer's environment.

