jumpcloud

Security & Compliance for Modern Identity Management

Contents

Data Security & Privacy Controls 3
- Organizational Security 3
- Data Security Controls 3
- Penetration Testing 3
- Vulnerability Research & Disclosure 3
- Securing The Software Development Lifecycle (SDLC) 4
- Encryption: Data in Transit 4
- Encryption: Data at Rest 4
- Network and Server Security 4
- Endpoints 4
- Access Control 4
- System Logging and Monitoring 5
- Disaster Recovery 5

Business Continuity 6
- Privacy 6
- Compliance and Data Deletion 6
- Vendor Management 7

Introduction

JumpCloud creates a safer identity for our customers. Our customers entrust us with some of their most confidential secrets, and we reciprocate that trust by putting security first. We're asking you to trust us, and we want to make sure you're comfortable with our security practice so that you know your identity is well-protected.

How does JumpCloud, an identity and directory management company, maintain a product offering that protects customer data from risks while also providing business value and enablement? The answer lies in our multi-faceted approach to security:

- Designing and maintaining an architectural foundation for security and privacy based on industry best practices.
- Implementing a combination of security, privacy, and compliance controls that address security risks throughout the product life cycle.
- Promoting a company culture that encourages each and every member of our team to uphold our commitment to protect customer data, and proactively think about how actions translate into security outcomes.

This document details JumpCloud's approach to security, including the processes, certifications, and protocols that help our customers meet their data protection and compliance requirements and keep our platform secure.

People

All JumpCloud employees and contractors go through background checks based on their roles and interactions with JumpCloud customers and technology. All employees and contractors are trained and tested on JumpCloud security policies, incident response, acceptable use, data privacy, and security best practices.

As a first principle of JumpCloud, we regularly update and refresh this training, including user-based training to support the mitigation of phishing attacks and on-line best practices.

Incident Response

JumpCloud's Security Engineering Team maintains our Digital Forensics and Incident Response Program. Our Incident Response Program defines clear and concise processes executed through run-books for handling events and incidents with time and severity-based escalation procedures. Our plan is regularly tested using relevant tabletop situations.

JumpCloud follows relevant practices around secrets management using key management services to create and destroy secrets as necessary during deployment. JumpCloud automation enables workflow using secrets across our infrastructure for automated tooling as well as users.

Data Security & Privacy Controls

Introduction

Privacy and security are integrated into the foundation of JumpCloud's architecture from the very beginning.

JumpCloud has an industry-leading security program focused on Security, Confidentiality, Integrity, and Availability by design.

- Securing JumpCloud infrastructure
- Securing JumpCloud user information and data
  - Storage of data
  - Transmission of data
  - Access to data
  - Sharing or observation of data
- Securing software developed by JumpCloud

Our security program also has an obligation to enforce and uphold our commitments to our customers' data. We undergo annual compliance audits, which serve as an independent attestation of the efficiency and effectiveness of our data protection controls and security program objectives. JumpCloud also undergoes regular external assessments of our products and infrastructure, in addition to our own.

Organizational Security

JumpCloud's Security Team is responsible for the implementation and management of our security program. JumpCloud's Security Team focuses on the following areas:

- Product security
- Security engineering
- Data governance
- Compliance
- Security operations

Data Security Controls

The focus of JumpCloud's data security controls is to prevent unauthorized access or observations to protected customer data. Our team of security practitioners in partnership with teams across the organization work together to identify and mitigate risks, develop solutions, and implement best practices.

Penetration Testing

In addition to compliance audits and security scanning, JumpCloud engages independent entities to conduct application, infrastructure, and network-level penetration tests (at minimum) twice per year. Results of these tests are shared with the appropriate members of management and then triaged, prioritized, and remediated in a timely manner.

Customers can receive a recent penetration test summary (under MNDA) by request from their Success team representative.

Vulnerability Research and Disclosure

JumpCloud is committed to protecting the privacy and security of our customers. Although we make every effort to minimize security bugs in our systems, we realize that sometimes these flaws make their way through. We encourage individual security researchers to study and analyze our platform to find these issues and make it even safer. Our Vulnerability Disclosure Program (VDP) is intended to minimize any security flaws found in our infrastructure and software.

If you believe you have found a security vulnerability in our platform or have any questions about our Vulnerability Disclosure Program (VDP), please contact vulnerability@jumpcloud.com. We investigate all legitimate reports and triage discoveries in a timely manner.

Securing The Software Development Lifecycle (SDLC)

Starting with Product and Service Development, JumpCloud has implemented a secure software development lifecycle that begins by scanning and remediating security issues found during development and design phases before code is ever merged to a project.

Web and network security development is designed around guidelines such as the OWASP Top 10, Common Vulnerabilities and Exposures, CIS benchmarks, and observed through the lens of the MITRE ATT&CK and kill chain frameworks.

Encryption: Data in Transit

As a cloud-based service, JumpCloud transmits data over public networks using strong encryption and security protocols. This includes data transmitted between JumpCloud agents and our public endpoints. Across our broad array of authentication protocols, including LDAP, RADIUS, SAML, and our agent-based binding for computers and servers, we support the use of TLS 1.2+ protocols coupled with industry best practice ciphers and key sizes. The transmission of sensitive information over the Internet or other public communications paths is prohibited unless encrypted.

Encryption: Data at Rest

JumpCloud uses industry best practice algorithms, ciphers, and key lengths to protect confidential data and personal identifiable information (PII) at rest. Encrypted backup data is automatically and asynchronously replicated in a separate data center region to ensure availability in the event of a disaster, and resiliently supported across multiple availability zones. This automated backup system is configured to encrypt backup data as a component of the backup process. Access to encryption keys is restricted to user accounts accessible by authorized personnel and audited regularly.

Network and Server Security

JumpCloud segments systems into separate networks to protect sensitive data. Strict firewall rules and communication protocols protect connections made with our networks.

Systems used for development or testing purposes are hosted separately from production systems. All servers in our production environment are hardened and validated against industry-standard CIS benchmarks regularly.

Access to JumpCloud's systems are based on the least privilege principle. JumpCloud only explicitly allows internet facing services for the service role they perform, with the edge being the only internet-facing accessibility point. We log, monitor, and audit all access attempts and connections.

Endpoints

All Company assets assigned to JumpCloud personnel are hardened, configured, and managed by JumpCloud based on our internal security policy and acceptable use standards. This includes disk encryption, password complexity, and endpoint compliance policy (such as predefined lock screen durations).

Assets are monitored by endpoint software to monitor, prevent and detect potentially concerning behavior, malware, or other indicators of compromise.

Access Control

To reduce the risk of data exposure, JumpCloud follows the principles of least privilege, and uses role-based permissions for provisioning access. Associates are only permitted to access systems and data that they must have in order to meet their current job responsibilities, and such access is provisioned following an approved Access Control Matrix. All provisioned access is, at minimum, reviewed quarterly, and more frequently whenever any change in access occurs.

JumpCloud requires personnel to use a controlled password manager. Password managers generate, store, and enter unique and complex passwords to avoid potential password-related risks.

To further reduce the risk of unauthorized access to systems or data, JumpCloud enforces multi-factor authentication for access to internal systems. Additionally, VPN provisioned permissions are required for accessing our production environments, from managed JumpCloud endpoints following Zero Trust concepts.

System Logging and Monitoring

JumpCloud monitors all identities, networks, applications, servers and workstations to maintain a comprehensive view of the security footprint of our corporate and production infrastructure.

Admin access, use of privileged commands, privilege escalation, connections, and system calls are logged and monitored for indicators of compromise. Logs are prioritized, aggregated, and analyzed to detect potential issues and alert responsible Security personnel.

Disaster Recovery

JumpCloud uses many layers of defense, monitoring, and automation to ensure that its infrastructure is resilient and available. JumpCloud's infrastructure leverages multi-tenant services meshed across availability zones and geographic regions to make JumpCloud infrastructure resilient to data center failures, extreme geographic conditions and other disaster factors. This architecture is focused on preventing a failure at the cloud service provider level or within any one region or zone down to the service model for each JumpCloud service.

JumpCloud leverages configuration automation tools to provision and manage its infrastructure. In the case of a disaster at our cloud service provider, JumpCloud can immediately provision a new infrastructure stack via our configuration automation tool in a non-impacted cloud provider or zone. If necessary, data would be restored from the encrypted backup data.

A number of our services have inherent resiliency built into their architecture. Our agent-based, native authentication platform for Windows®, Linux®, and Mac® OS X would not be impacted by a widespread outage of the JumpCloud platform. Users would continue to access their devices as they normally would with their current credentials.

Authentication service availability is even more dispersed. JumpCloud has deployed infrastructure across a global network capable of operating autonomously from the JumpCloud central infrastructure.

If for any reason the central JumpCloud infrastructure were to experience an outage, these systems would continue to operate autonomously. Our customers' systems and applications can continue authenticating against these global services as normal.

JumpCloud uses many layers of defense, monitoring, and automation to ensure that its infrastructure is resilient and available.

Business Continuity

As JumpCloud's size, influence, and market position have grown, the increased opportunity has been met with increased risk. Emerging and ongoing events can threaten the mission, operations, reputation, assets, and brand of JumpCloud.

This unified, comprehensive business continuity plan details roles and responsibilities, response procedures, recovery tasks, internal and external communication, coordination procedures, and addresses five best practice areas of disruptive event management:

1. Emergency Preparedness
2. Event Management
3. Crisis Communications
4. Business Continuity
5. IT Disaster Recovery

The purpose of maintaining and testing this plan is to minimize downtime, support the protection of life-safety and property, enable continuity of critical business processes, and ensure all efforts associated with the response to and management of an unplanned disruptive event are appropriately executed by JumpCloud.

Privacy

JumpCloud's Privacy Policy was designed around GDPR and ISO27701 frameworks. We have put into practice acceptable use, verified consent, and transparency of collection (and processing) as a data processor and, in cases, as a data controller. In addition, associated controls are designed to uphold our obligations and commitments about how we collect, process, use and share protected data, as well as our processes to support data retention and disclosure in compliance with legitimate business purposes.

We use a variety of security measures, from the first touch on our website through customer conversion and customer departure to maintain the confidentiality, availability, and integrity of personal information. Personal information is contained behind secure networks and is only accessible to a limited number of vetted persons who have access rights commensurate with their role, and are trained to protect confidential information in place.

To request additional information, including JumpCloud's formal Privacy Policy, please visit JumpCloud's Privacy Policy. We have a formal process for data subjects to request data deletion outside their company requirements.

Compliance and Data Deletion

JumpCloud adheres to obligations under laws such as GDPR related to the processing and sharing of customer data. We operate by the primary principle to only collect, process, and store customer data according to the obligations by which it is classified. This includes our obligations to:

- Protect this data.
- Provide users with the right to access or delete it at any time.
- Provide users the opt-in option for tracking cookies on our website to verify consent to be tracked.
- Provide controls to make sure that any vendors agree to the use of customer data only for the purpose of provision of services.
- Share and notify customers of our subprocessors and update based on change through our website.

For additional information, including JumpCloud's formal Policies around GDPR, Data Collection, or Data Deletion, please see **JumpCloud GDPR Compliance**.

Vendor Management

JumpCloud relies on sub-processors to efficiently and effectively provide internal and external services. We acknowledge and take very seriously the fact that our critical sub-processors can impact the security of JumpCloud's environments.

We take appropriate steps to ensure our security posture is maintained by establishing sub-processor agreements that require such parties to adhere to the same level of confidentiality and service commitments we adhere to internally. JumpCloud monitors the operation of such critical sub-processing organization's safeguards by conducting reviews of their controls annually or upon changing the scope of usage. The list of our critical sub-processors is maintained on our external website (JumpCloud GDPR Compliance).

Conclusion

JumpCloud is built upon a strong foundation for security that helps protect our customers from emerging data protection and identity risks, as well as ongoing threats to privacy and security. Our approach to security puts us in a position to meet both internal and external security requirements while keeping our product and services agile.

If you have questions or concerns at any time, please contact your Customer Success Manager for more details.