WHITE PAPER

JUMPCLOUD DIRECTORY-AS-A-SERVICE® PLATFORM FOR GDPR

ANDREY SAZONOV | CISA, QSA(P2PE), PA-QSA(P2PE)
NICK TRENC | CISSP, CISA, QSA, PA-QSA

JumpCloud®
Directory-as-a-Service®

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

JumpCloud, Inc. (JumpCloud) engaged Coalfire Systems Inc. (Coalfire) to conduct an independent technical assessment of their JumpCloud Directory-as-a-Service® (DaaS) to determine the platform's suitability and compliance for meeting the General Data Protection Regulation (GDPR) controls for protecting personal data. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance validation.

In this paper, Coalfire will describe how the JumpCloud DaaS platform can be part of the 'appropriate technological measures' specified in Article 32 of the GDPR to support meeting the requirements of GDPR for protecting personal data based on the sample testing and evidence gathered during this assessment.

This paper briefly describes the origin of GDPR and presents the features of the software that can be leveraged for suitability and compliance with GDPR and provides a mapping of available features in the platform specific to GDPR and cybersecurity best practices.

GENERAL DATA PROTECTION REGULATION

The European Union (EU) GDPR replaces the Data Protection Directive 95/46/EC and is designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy.

GDPR was approved and adopted by the EU Parliament in April 2016. The regulation took effect after a two-year transition period, meaning it started being enforced in May 2018.

GDPR not only applies to organizations located within the EU, but also applies to organizations located outside of the EU if they offer goods or services to or monitor the behavior of EU data subjects. It also applies to all companies processing and holding the personal data of data subjects residing in the EU, regardless of the company's location.

Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 million, whichever is greater. This is the maximum fine that can be imposed for the most serious infringements, including not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines; a company can be fined only 2% for not having their records in order (Article 28), not notifying the supervising authority and data subject about a breach (Article 33), or not conducting an impact assessment (Article 35). It is important to note that these rules apply to both controllers and processors - meaning 'cloud' environments will not be exempt from GDPR enforcement.

ABOUT THE JUMPCLOUD DAAS PLATFORM

The JumpCloud DaaS platform is the cloud-based solution for a single point of authority to authenticate, authorize, and manage the identities of a business's employees and systems. DaaS securely connects employees with systems, applications, files, and other resources through a single unified cloud-based directory, replacing the need for on-prem solutions such as Active Directory and LDAP. The JumpCloud DaaS platform supports most of the major operating system (OS) platforms (Windows, Linux, and macOS) and is designed to control and manage user access to both internal and external IT resources such as servers and applications.

GDPR ARTICLE APPLICABILITY

GDPR ARTICLE 32

Security of Processing

The primary article of GDPR that has requirements where JumpCloud may be leveraged to assist is Article 32. The article states:

1. Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymization and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

This white paper focuses on the argument positioning JumpCloud as a level of security for ensuring the ongoing confidentiality, integrity, availability, and resiliency of processing systems and services. The overall goal of GDPR is to prevent a data breach from occurring and JumpCloud's capabilities, as outlined within, provide a reasonable measure to prevent a breach (enforcing strong authentication). Verizon's 2017 Data Breach Investigations Report (see reference section) identified that 81% of all breaches leveraged either stolen or weak passwords. The following use cases described below provide high-level examples that will further illustrate the argument that JumpCloud's robust capabilities can meet the definition of an appropriate technical measure to ensure a level of security for use within a GDPR data controller/processor environment:

USE CASES:

Scenario 1

The first scenario will be an easy one. A data processing organization processing European Union (EU) individual's personal data with an externally facing web application is targeted by malicious individuals who wish to gain access to such data stored by the organization. The web application login credentials are attacked via rainbow tables looking for weak passwords utilized for an individual login. In our example, this particular organization has chosen not to enforce complex passwords for all users and the administrator has chosen to use "password" to make it easier for him or her to remember. Due to lack of appropriate technical controls for authentication credentials within this organization, a rainbow table attack against any

variation of the word ‘password’ will be trivial to complete and then those credentials can be utilized to gain access to the web application.

JumpCloud can be configured to prevent this sort of attack by:

1 - Enforcing strong passwords. Using the JumpCloud solution as an appropriate technical control, administrators can enforce complexity requirements for all authentication methods managed by the solution. (See Figure 1, below, for a reference architecture that identifies types of authentication services that can be managed by the JumpCloud solution)

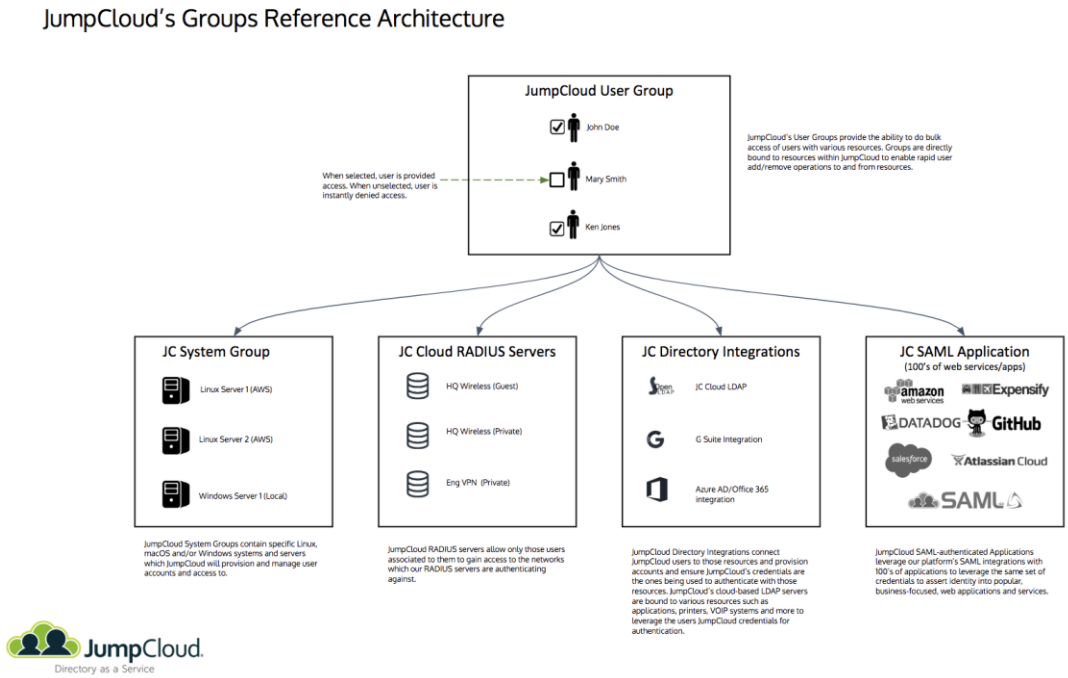

Figure 1 - JumpCloud's Groups Reference Architecture

2 – Utilizing multifactor authentication (MFA) should other appropriate technical controls fail (also called defense-in-depth). The JumpCloud solution provides MFA control over macOS and Linux systems and to the JumpCloud administrative and user consoles. The user console is often a path to application access and thus MFA can be leveraged to increase security. JumpCloud’s MFA functionality supports integration with several TOTP providers (e.g. Google Authenticator) that can be utilized to add additional technical controls for authenticating users.

Scenario 2

This scenario will get a bit more complicated. An attacker has completed a successful phising campaign and was successful in getting an employee’s login username and password. For ease of description, the organization does have a complex password policy but has chosen not to enforce MFA. The attacker finds a public-facing server (perhaps hosted at a cloud infrastructure platform such as AWS, Azure, or the Google Cloud Platform) that, when logged in with the stolen credentials, gives him access to the organization’s corporate network. In a typical network breach, the attacker is now going to try to leverage the access he/she has already gained to pivot to different machines within the network or on different networks within the organization. Without network segementation or an appropriate technical control, the attack could utilize

the single set of credentials to login to differing machines or networks to include those that contain personal data for EU individuals.

JumpCloud can help to prevent this type of attack with several key technical controls including:

1 – Enforcing the principle of least-privilege to include role-based access control. The JumpCloud solution allows for the implementation of user groups which can then be given specific privileges to gain access to certain systems, directories, and networks based on group membership. An organization's policy can be enforced to allow only the lowest level of privileges required for any particular group to complete their work duties.

2 - Leveraging public key infrastructure (PKI) for authenticating users and systems, especially SSH keys, in favor of passwords. SSH keys are inherently stronger than passwords primarily because they are much more complex than passwords and don't have to be transmitted to a remote system in order to verify them. The JumpCloud solution allows for the storage and management of SSH keys.

3 – Adding additional security controls. In this example, the organization has chosen not to use MFA, but JumpCloud could be enabled to provide MFA for any Linux servers within the environment, for example.

Note:

While not particular to a use case, Coalfire reviewed a number of areas of interest to organization's support for GDPR and "implementing appropriate technical and organizational measures." These included the ability to terminate user access across a wide range of IT resources immediately, enforcing password complexity for passwords, and managing security policies on systems such as password locking screens when idle. More information on these capabilities is listed below.

ASSESSMENT OVERVIEW

METHODOLOGY

Coalfire completed a multi-faceted technical assessment during the course of this project using the below industry and audit best practices. Coalfire conducted testing within JumpCloud-hosted infrastructure as well as test systems within the Coalfire test lab. Testing was conducted from April 12, 2018 to May 14, 2018.

At a high level, testing consisted of the following tasks:

1. Technical review of the architecture of the full solution and its components (the JumpCloud Agent and the JumpCloud Web Service).
2. Implementation of the JumpCloud Agent software in the Coalfire lab environment on all supported platforms (Windows, Linux, macOS).
3. Review and testing of the functionality provided to enforce authentication controls on tested systems.
4. Confirmation that the JumpCloud DaaS platform does not require or use any Personally Identifiable Information (PII) and instead only operates with user IDs that provide access to the systems within the organization.
5. Confirmation that there are policies and processes that allow any user account to be fully deleted from JumpCloud servers by the JumpCloud team upon request.

6. Confirmation that appropriate authentication controls are configured and enforced on all systems.
7. Confirmation that logging of appropriate events within the environment is enforced and that such logs provide sufficient information for each event.
8. Review of the systems to verify passwords are handled securely and in accordance with industry best practices.

SUMMARY FINDINGS

The following findings are relevant highlights from this assessment:

- The JumpCloud DaaS platform does not operate with any records containing sensitive information such as PII. Instead, systems and user IDs are managed by the JumpCloud DaaS platform to control all access to the organization's infrastructure.
- The JumpCloud Agent securely integrates with the underlying OS authentication methods (Windows 10 Professional 64 bit, Ubuntu 16.06 LTS, macOS Sierra 10.12 were tested) and allows performing user management tasks according to the policies configured within the JumpCloud cloud environment.
- The JumpCloud DaaS platform generated logs of all user actions that could then be utilized to reconstruct authentication events. These logs can be imported into a centralized logging platform of a user's choice.
- Coalfire verified that the JumpCloud DaaS agent cannot be disabled by unauthorized users (non-administrators).
- No user passwords were found to be stored either locally on the system or within the JumpCloud DaaS platform cloud environment in a non-compliant manner. The JumpCloud Agent does not have access to cleartext user passwords.
- No user data was left on the JumpCloud servers after the user termination (or deletion) process.
- No user passwords were found to be transmitted over the local or public network in cleartext or in a non-compliant manner. Passwords are protected in transit using the TLS 1.2 protocol.

ASSESSOR COMMENTS

The assessment scope put a significant focus on validating the use of the JumpCloud DaaS platform in a business environment. The JumpCloud DaaS platform, when properly implemented following guidance from JumpCloud, can form part of an organization's technical measures for GDPR (Article 32) used to protect personal data. However, as most computing environments and configurations differ drastically, it is important to note that use of this product does not guarantee security or compliance with GDPR and even the most robust user management solutions can fail when improperly implemented. A defense-in-depth strategy that provides multiple layers of protection for data should be followed as a best practice. Please consult with JumpCloud for policy and configuration questions and best practices.

It should not be construed that the use of the JumpCloud DaaS platform guarantees full compliance with GDPR. Disregarding these recommendations and security best practice controls for systems and networks inside or outside of the scope of the environment can introduce many other security or business continuity risks to the organization. Security and business risk mitigation should be any organization's goal and focus for selecting security controls.

APPLICATION ARCHITECTURE

The JumpCloud DaaS platform provides real-time user management for multiple supported OS endpoints and at a high level utilizes the following two components as shown in Figure 1:

- JumpCloud Agent: A lightweight software client designed to synchronize all settings with the JumpCloud Web Service and integrate securely with the underlying OS authentication functionality by taking over the account where it is initially set up. It supports multiple flavors of Linux, macOS, and Windows OSs and has the ability to add, modify, and delete local user accounts, including setting passwords, updating full name fields, and changing group membership.
- JumpCloud Web Service – Hosted in the cloud and managed by the vendor, JumpCloud, it provides a web interface for all administrative user and system management functionality. This component interacts with the agent software installed on each system within the organization to synchronize users, policies, and configurations, configured by the administrator. In addition, the architecture of the JumpCloud DaaS platform allows further integration with other services including Google G Suite, Amazon Web Services (AWS), Microsoft Office 365, as well as provides a bridge to existing Active Directory instances and other services; however, this functionality is out of scope for this white paper.

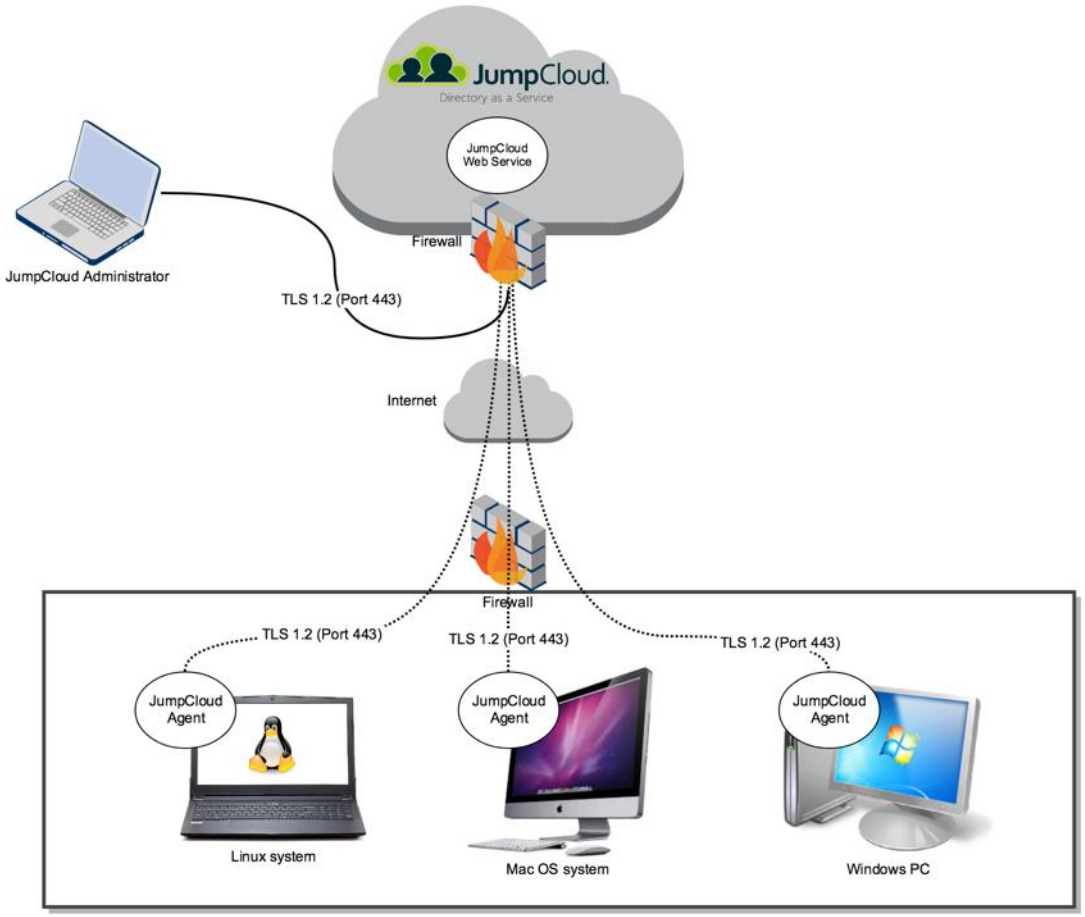

Figure 2: The JumpCloud DaaS Platform Architecture Diagram

TECHNICAL SECURITY ASSESSMENT

ASSESSMENT METHODS

The assessment used the following methods to assess the potential GDPR coverage of the solution:

1. Initial configuration of the JumpCloud DaaS platform in accordance with policies enforced by the organization according to their risk management policy.
2. Deployment of the JumpCloud Agent software to multiple platforms: Windows, Linux, and macOS. Examination of end-point configuration to confirm the JumpCloud Agent cannot be turned off by non-administrators.
3. Observation of integration with the underlying OS authentication and logging mechanisms and verification that these mechanisms could provide logging details that are sufficient for tracking necessary user activities and system events.
4. User creation, deletion, and configuration using guidance provided by JumpCloud.
5. Evaluation of methods for password protection while in transit.
6. Forensic analysis of the hard drive to confirm that no clear-text passwords are utilized or stored by the local JumpCloud Agent.
7. Review of administrative functionality and role-based access control (RBAC) in place for using different types of accounts.
8. Evaluation of multi-factor authentication (MFA) functionality.
9. Evaluation of the user deletion process.
10. Evaluation of the agent software update process to verify secure distribution processes.

ASSESSMENT ENVIRONMENT

The JumpCloud Agent was installed on the following systems:

- Windows 10 Professional 64 bit in a virtual environment
- Ubuntu 16.06 LTS in a virtual environment
- macOS Sierra 10.12 running on the MacBook Pro laptop

A separate laptop was also used to access the JumpCloud Web Service via a web browser to perform all administrative configurations.

INITIAL CONFIGURATION

The initial configuration of the solution included installation of the client software on all operating systems (OS) being tested:

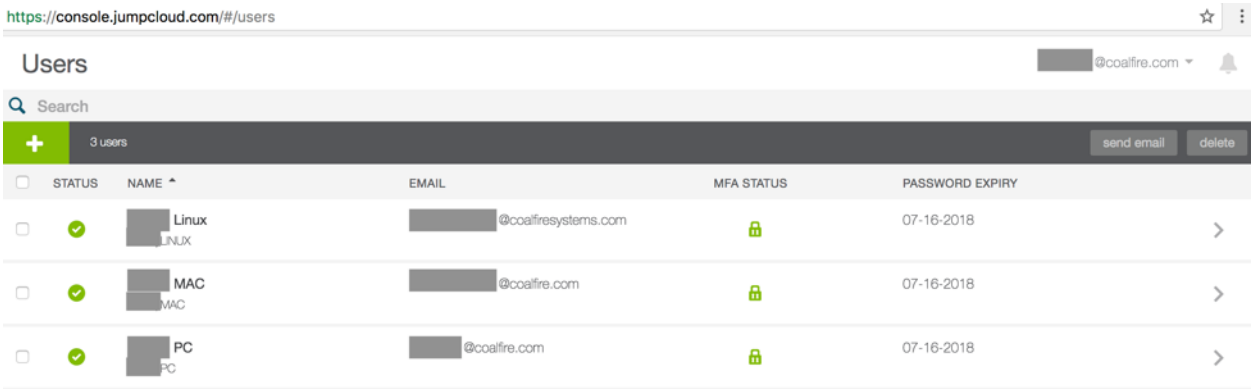

Figure 3: JumpCloud Users Configured

A local account was then configured with a matching username and password on each tested OS with a local instance of the JumpCloud Agent installed to allow for administrative control of the system:

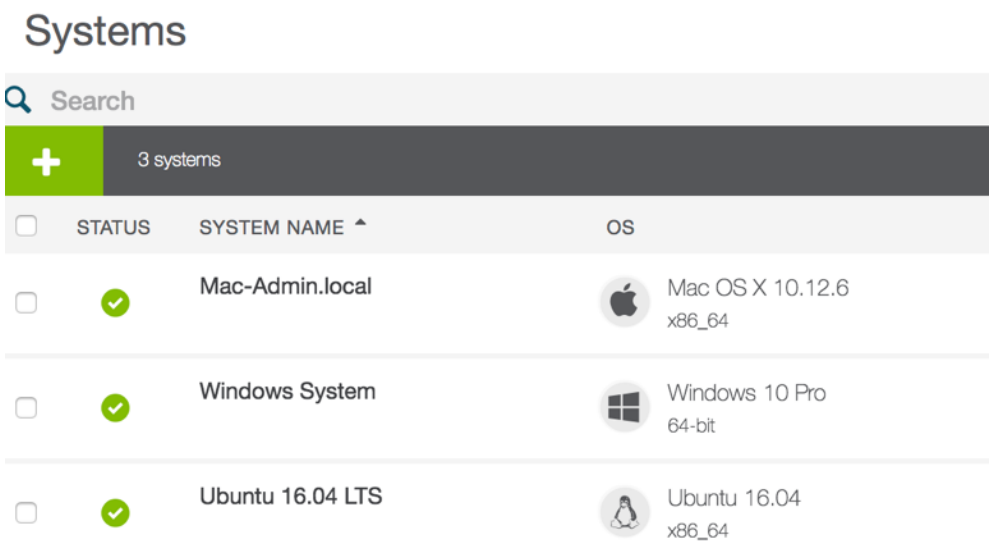

Figure 4: JumpCloud Systems Configured

The initial configuration guidance also suggested the following security settings within the JumpCloud Web Service:

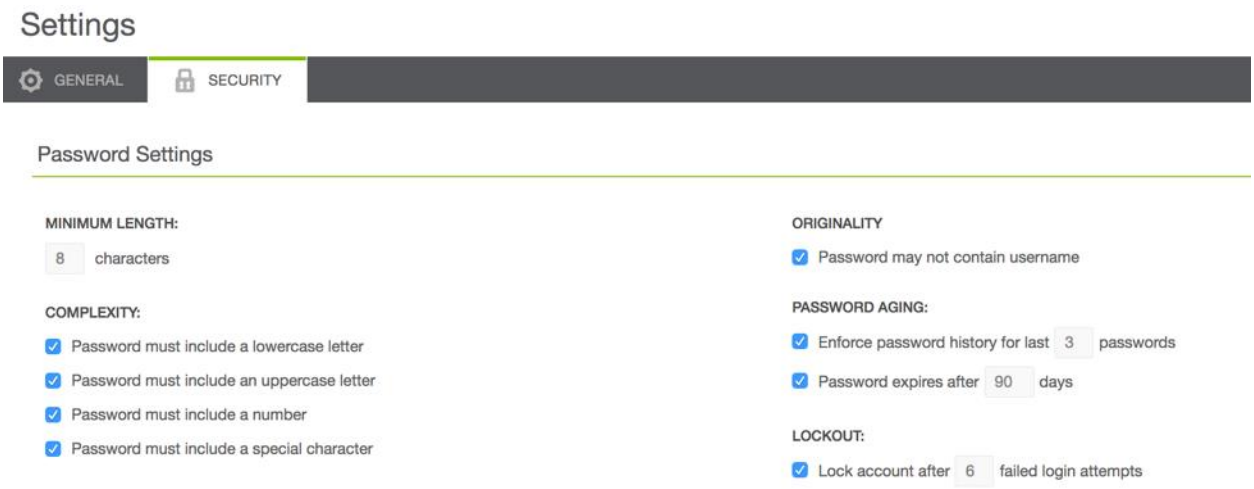

Figure 5: Initial Security Configuration

The "Policies" functionality of the JumpCloud DaaS platform was used to configure a fifteen-minute inactivity timeout as well as disable the default guest account and provide additional functionality that could be enforced as needed:

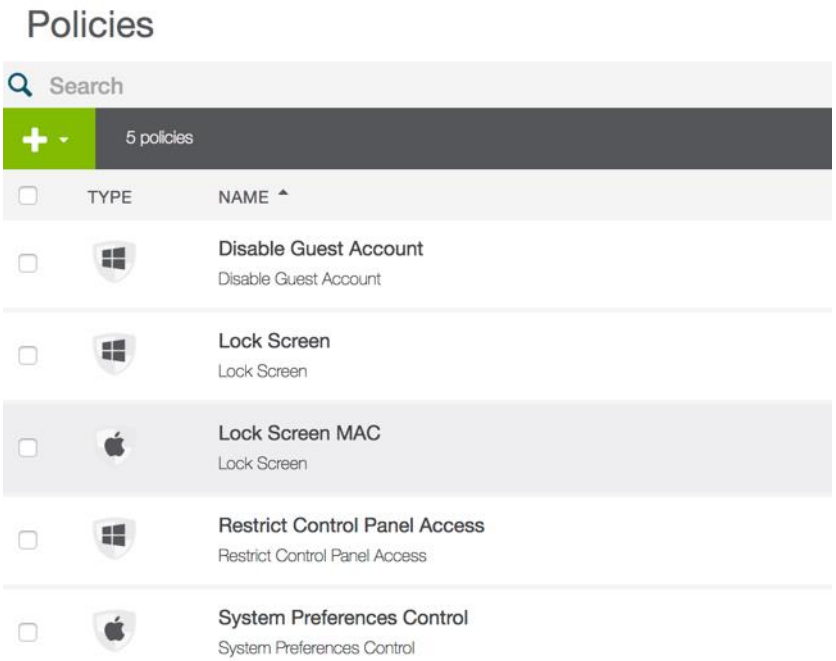

Figure 6: The JumpCloud DaaS Platform Policies Configured

It is important to note that the JumpCloud DaaS platform natively supports the "inactivity timeout" feature for Windows and macOS platforms but requires additional configuration for Linux Systems (using the JumpCloud Command Runner feature).

Lastly, MFA was configured for macOS and Ubuntu operating systems. Native MFA for Windows is in development by JumpCloud and was not tested.

All administrator access to the JumpCloud Web Service web interface was configured to use two-factor authentication.

INTEGRATION OF THE JUMPCLOUD AGENT WITH THE UNDERLYING OPERATING SYSTEM

The JumpCloud Agent operates by relying on the underlying OS authentication functionality. There are no additional authentication mechanisms or features for the application to introduce, other than those provided by the underlying OS (Windows, Linux, or Mac).

Coalfire confirmed that, when configured with the guidance provided by JumpCloud, the end user could not disable the JumpCloud Agent and bypass the policies enforced (except when logged in as administrator).

Coalfire performed interviews to understand integration mechanisms of the JumpCloud Agent software and confirmed with testing that it is not possible to disable, uninstall, or block the JumpCloud Agent software by non-administrators, as depicted in the figures below.

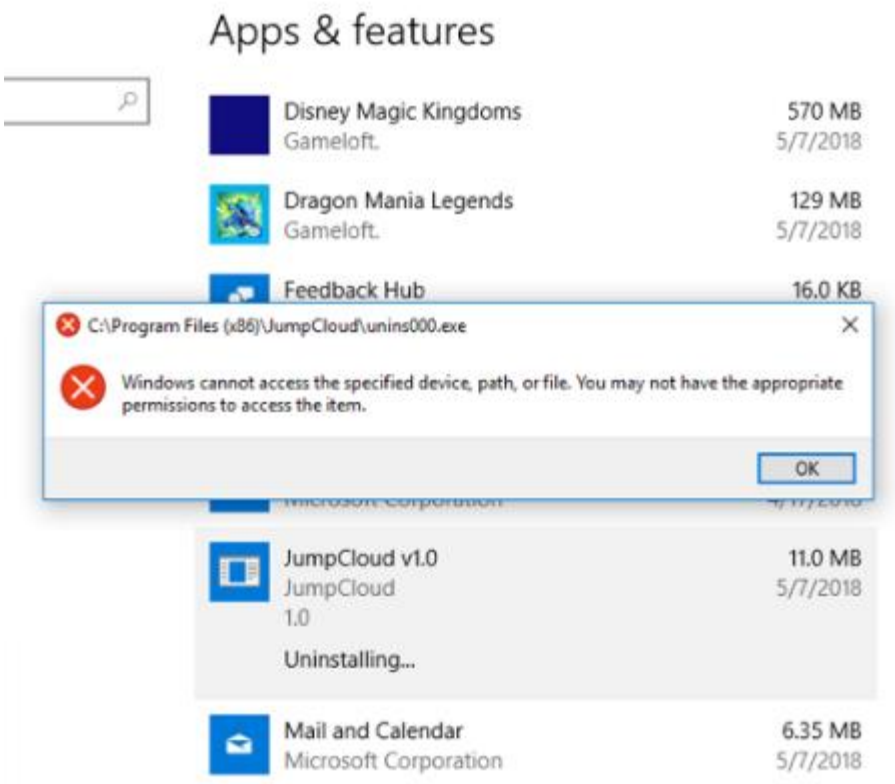

Figure 7: Failed Attempts to Uninstall the JumpCloud Agent

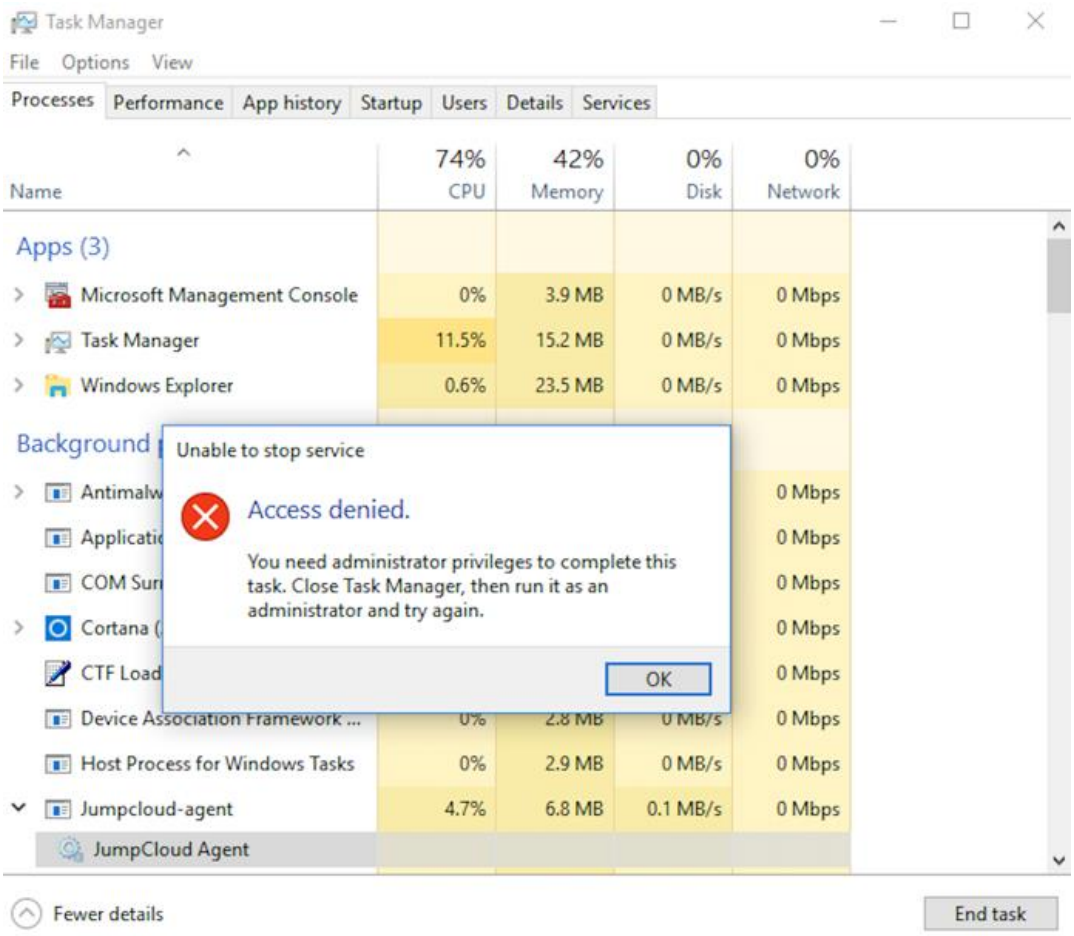

Figure 8: Failed Attempts to Disable or Block the JumpCloud Agent

AUTHENTICATION POLICY ENFORCEMENT

Coalfire reviewed all authentication controls that could be configured by the JumpCloud DaaS platform with the primary goal to verify that the solution would be able to help companies establish strong authentication policies and controls.

Coalfire observed that policies are enforced by the JumpCloud Agent software and properly implemented for all systems tested in a way that meets the strong authentication policy established by the organization.

LOGS REVIEWED

Logging functionality was reviewed for all authentication events.

Because the JumpCloud Agent relies on underlying OS authentication functionality, appropriate logging was also performed by the underlying OS. Coalfire observed that the mechanisms were in place by all tested OSs to properly log and monitor all actions performed by users.

The JumpCloud Web Service provides a comprehensive audit log of all automation activities. As identified in Article 32(1) of the GDPR, “The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk” and, as such, logging is a significant factor in understanding who has accessed data in the environment.

The JumpCloud DaaS platform utilizes a REST-based Event Server API for all log access, which is managed through remote calls to the JumpCloud Web Service, and access to the audit logs is view-only.

Logging functionality of the JumpCloud Solution allows to automatically capture all events related to creation, modification, enablement, disablement, and removal of users and systems.

All valid and invalid attempts of events and actions are logged, and examples of some of the events and actions that are logged are:

- JumpCloud Administrator Console Events
- JumpCloud User Portal Events
- JumpCloud General Access and System Context API Events
- System Events - events that occur on desktop, laptop, or server systems running JumpCloud Agent

All JumpCloud DaaS platform logs can be exported to a centralized logging system for further analysis to support incident response efforts or compliance needs. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. GDPR Recital 78 states that “In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet the principles of data protection by design and data protection by default.” A data protection implementation must have the ability to prove manageability and traceability of actions taken against data in the processing environment. The JumpCloud DaaS platform audit logs track the actions of end users as well as privileged or administrative users access to all data within the application.

NETWORK TRAFFIC ASSESSMENT

A Wireshark Ethernet port sniffer was used to monitor the following traffic for components within the test environment:

Traffic from the JumpCloud Agent to the JumpCloud Web Service (Figure 8): No sensitive data is transmitted over the network from the JumpCloud Agent running on the local system to the JumpCloud Web Service and all communication (login information, log requests, policy synchronization, and any other requests) is encrypted over the TLS 1.2 protocol.

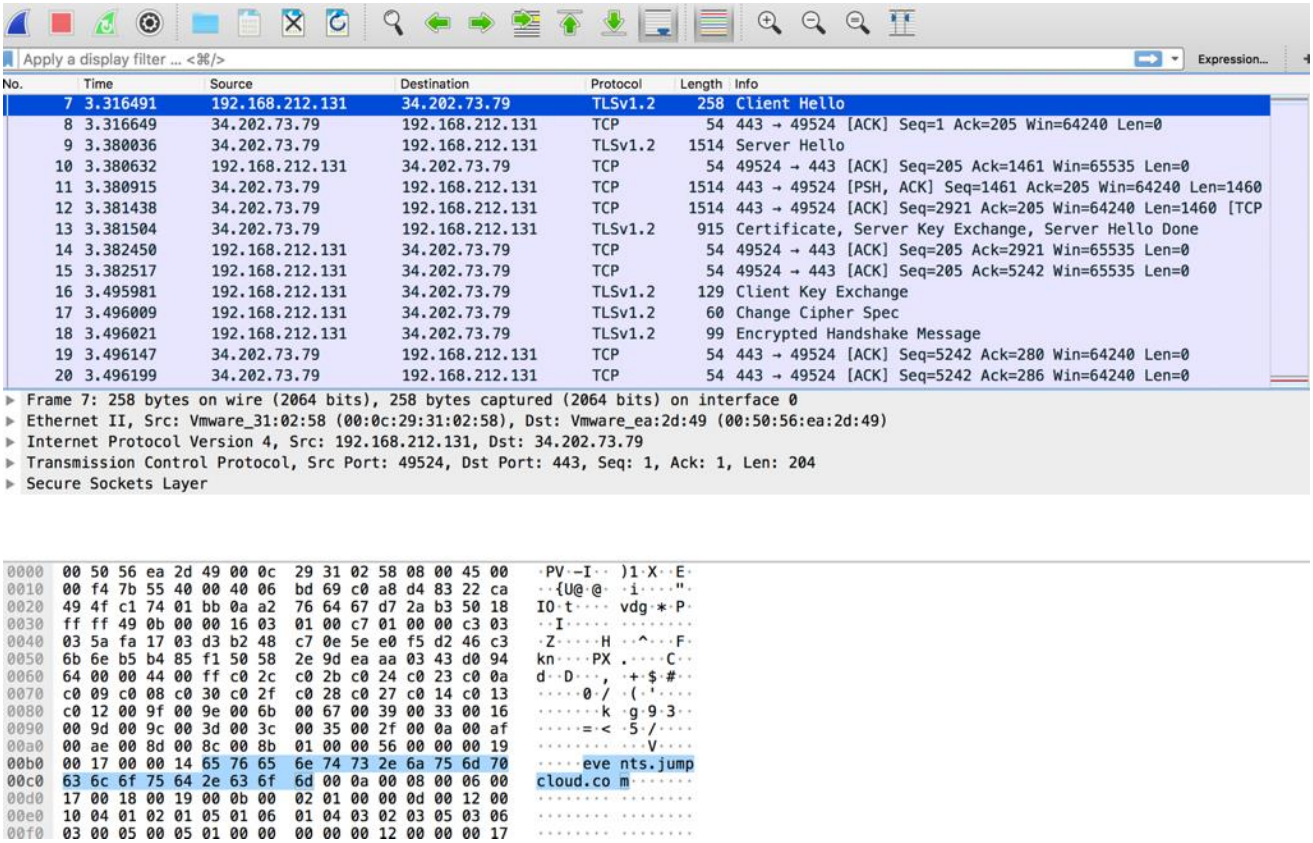

Figure 9: Communication between the JumpCloud Agent and the JumpCloud Web Service

FORENSIC ANALYSIS

The technical assessment included a forensic examination of the hard drive of the system running the JumpCloud Agent.

The process for examining the hard drive was as follows:

1. The whole disk image of the systems with the JumpCloud Agent was captured for forensic analysis. A total of three images were produced (Windows, macOS, Ubuntu).
2. The FTK forensic toolkit was used to search disk images for clear text passwords as well as common encoding formats of the passwords.

No findings were identified with the image when searched using the FTK forensic toolkit. The following represents the conclusions from performing forensic analysis:

- The forensic analysis demonstrates that there is no residual password data on the system running the JumpCloud Agent.

An interview with the developers and review of the JumpCloud DaaS platform confirmed that there is no intent to store any passwords in the clear for any reason.

USER DELETION PROCESS

User management and user deletion is something that is typically not controlled by the vendor, JumpCloud, and instead it is a responsibility of the customer to create processes and policies on deletion of user accounts according to risk management policies created within the target organization. There is one scenario however when user deletion is managed by the JumpCloud team and it only happens when the customer decides to remove the single administrative account.

Coalfire has reviewed the policies provided by JumpCloud during the account removal process to confirm that all user information and data is removed by the vendor from all storage locations.

AGENT SOFTWARE UPDATE PROCESS

The update process is performed by the JumpCloud Agent application automatically with no user interaction. The update package is delivered using the TLS 1.2 protocol with digital signature verification in place that would prevent the package from being installed if the digital signature is not valid.

TOOLS AND TECHNIQUES

Tools Coalfire utilized for this application security review included:

TOOL NAME	DESCRIPTION
FTK Forensic Toolkit	*Forensic tool for digital data and media analysis.
Wireshark	Wireshark Ethernet port sniffer was used to observe the traffic coming in and out of the system.
Additional tools	FTK Imager, Process Explorer

*Forensic tool: A tool or method for uncovering, analyzing and presenting forensic data, which provides robust ways to authenticate, search, and recover computer evidence rapidly and thoroughly.

CONCLUSION

After reviewing the JumpCloud DaaS platform, Coalfire determined, through a review of business impacts and technical assessment, that the JumpCloud DaaS platform, as outlined in this document, can help organizations meet applicable sections of the GDPR and form part of the appropriate technical measures organization are required to implement. The ability to achieve overall compliance with any regulation or standard will be dependent upon the specific design and implementation of the JumpCloud DaaS platform for use within a processing environment. However, when implemented following industry best practices and guidance provided by JumpCloud, the JumpCloud DaaS platform demonstrated a high level of flexibility for user management, customization of policies, policy enforcement, notifications, and configurations including logging.

REFERENCES

2017 Verizon Data Breach Investigation Report

https://www.verizonenterprise.com/verizon-insights-lab/dbir/

ABOUT THE AUTHORS

Andrey Sazonov CISA, QSA(P2PE), PA-QSA(P2PE) | **Author** | Senior Consultant, Solution Validation, Coalfire Systems

Nick Trenc CISSP, CISA, QSA, PA-QSA | **Author** | Director, Solution Validation, Coalfire Systems

Andrew Barratt QSA(P2PE), PA-QSA(P2PE), ISO 27001 CISSP, CISA | **Reviewer** | Managing Principal, Payments, Coalfire Systems

ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com