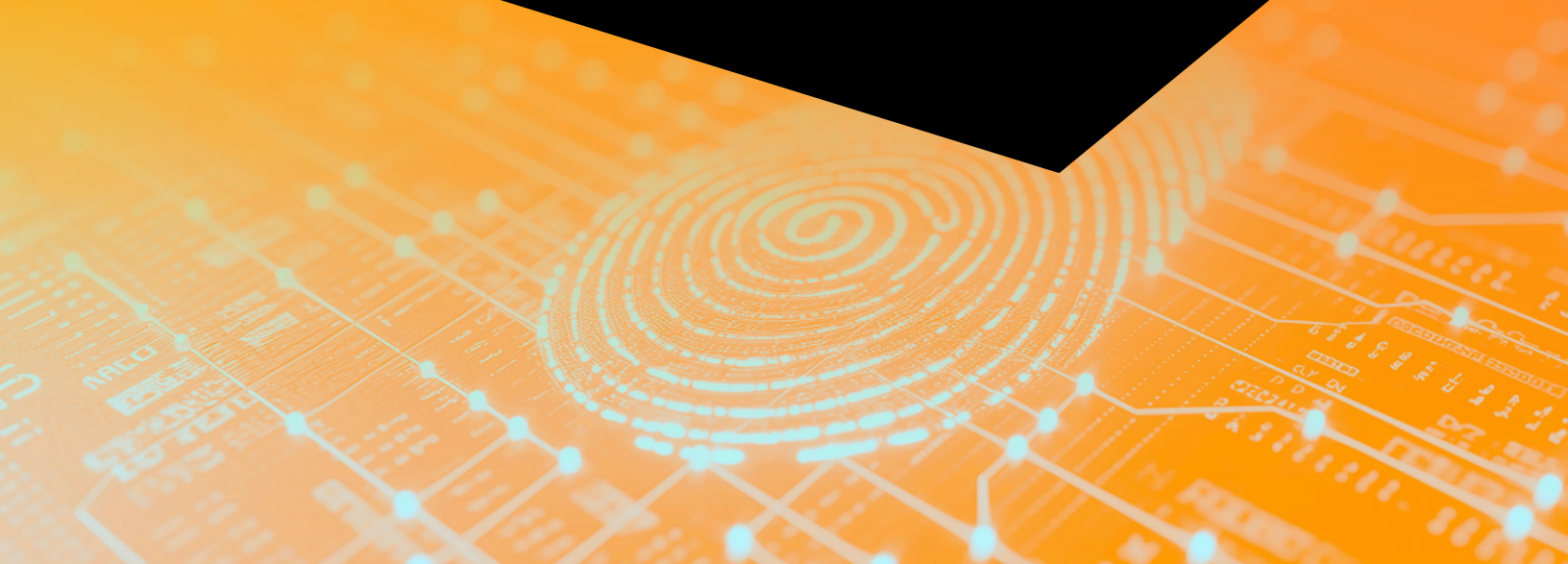
Silverfort

Meeting the identity security requirements of the CJIS security policy with Silverfort

Whitepaper



Executive summary

CJIS compliance is a set of minimum requirements for accessing and handling Criminal Justice Information (CJI), which is any information that cannot be publicly disclosed except under certain circumstances, like by court order or when necessary for public safety. In particular, it refers to Federal Bureau of Investigation (FBI) data such as biometrics, biographics, case records, and other identifiable information about individuals, vehicles, or properties related to criminal activity.

Organizations that handle CJI are required to comply with the CJIS Security Policy as soon as they begin accessing, storing, or transmitting this data. CJIS is not only relevant to law enforcement agencies but also to civil agencies. CJIS compliance requirements include access control, identification and authentication, the adoption of advanced authentication measures such as MFA and risk-based authentication, incident response, visibility into all accounts, and auditing.

Addressing the identity security aspects of CJIS

CJIS addresses identity security concerns by requiring strong authentication mechanisms, including multi-factor authentication (MFA), to ensure that only authorized individuals can access CJI. This proactive approach to identity security significantly reduces the risk of unauthorized access, even if one factor is compromised. As part of the framework, special attention is given to the need to secure privileged users through strict controls and continuous monitoring and response to cyber threats.

Additionally, the CJIS policy mandates strict management of privileged accounts in line with the principle of least privilege and requires regular auditing and monitoring to detect any unauthorized activities. Continuous monitoring and detailed logging of user activities are also vital components of CJIS compliance. Organizations must track who accesses CJI and when, so identifying and responding to suspicious actions can occur quickly and easily.

Silverfort Identity Security Platform

The Silverfort platform integrates with all Identity and Access Management (IAM) infrastructures in the entity's environment to provide continuous monitoring, risk analysis, and active enforcement of every user's authentication and access attempts.

Using these capabilities, Silverfort provides Identity Security Posture Management (ISPM), advanced MFA, service account protection, and Identity Threat Detection and Response (ITDR).

Silverfort for CJIS protection highlights

Multi-factor authentication

Extend MFA protection to command-line access, legacy apps, IT infrastructure, and other critical resources that couldn't be protected before.

Continuous monitoring

Gain comprehensive visibility into all authentication and access attempts, monitor and review them continuously to detect anomalies and prevent malicious access in real-time.

Securing privileged users

Discover, classify, and enforce least privilege and Just-In-Time (JIT) access policies for all your privileged users.

Detect and respond to identity threats

Detect common credential access, privilege escalation and lateral movement attacks, and respond automatically with real-time blocking.

Mapping Silverfort capabilities to CJIS

5.3 Policy Area 3: Incident Response (IR)

The security risk of both accidental and malicious attacks against government and private agencies remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

CJIS regulation	Silverfort security controls
5.3.2 Management of Security Incidents A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.	Silverfort enables organizations to begin the IRprocess with a complete malicious access lockdown. Depending on the intensity and scope of the ongoing attack, they can determine the level of lockdown and the balance between MFA and block access policies. Most often, MFA would achieve the same level of containment as block access, while allowing legitimate users to continue to access resources. By utilizing both MFA and block access policies with Silverfort, further malicious access attempts are prevented. MFA is especially effective since it provides a clear indication of which accounts have been compromised, achieving both containment and discovery simultaneously. This will allow you to rapidly shut down an attack by automatically denying users access to resources until the attack has been eradicated and is in recovery mode.
5.3.2.1 Incident Handling The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.	Silverfort assists with incident analysis by providingdetailed logs of all authentication and access activities. This allows security teams to understand what occurred during an incident and determine the root cause. Using comprehensive data on user accessrequests and behaviors, Silverfort facilitates a comprehensive investigation and understanding of the events leading up to and during a security incident. Silverfort's real-time monitoring capabilities enable it to detect anomalies and suspicious activities, providing insights into the course of an incident. As a result of this detailed analysis, it is possible to pinpoint the exact nature and origin of the problem, thereby facilitating effective remediation and strengthening security overall.

5.4 Policy Area 4: Auditing and accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

CJIS regulation	Silverfort security controls
5.4.3 Audit Monitoring, Analysis, and Reporting The agency shall implement a process for monitoring, analyzing, and reporting audit logs in order to detect and respond to potential incidents. This process shall include reviewing audit logs for indications of suspicious activity, which may include patterns of access inconsistent with the user's role or deviations from expected behavior.	Silverfort monitors all identity traffic and authentication activities across an organization's environment, providing visibility into every authentication and access request. With complete visibility across all user activity, Silverfort's risk engine can determine the risk of every authentication, so organizations can detect and respond to potential security threats in real-time — including blocking the access of any accounts that display anomalous behavior.
5.3.2.1 Incident handling The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.	Silverfort provides centralized identity-related logs across all users and systems in an organization's environment. These logs are stored securely for at least one year and can be archived for longer if needed. This provides reliable evidence for legal audits and operational purposes. Silverfort also integrates with SIEM systems for automated and continuous logs monitoring.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

CJIS regulation	Silverfort security controls
5.5.1 Account Management The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.	Silverfort integrates with all IAM providers to help manage, modify, and deactivate user accounts across all environments. It provides continuous monitoring, automates account reviews, and enforces policies in real-time, ensuring accounts are managed consistently and securely throughout their lifecycle.
5.5.2 Access Enforcement The information system shall enforce assigned authorizations for controlling access to the system in accordance with applicable policy. Access control policies (e.g., identity-based policies, role-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by the information system to control access between users (or processes acting on behalf of users) and objects in the system.	Silverfort enforces flexible access policies, and organizations can embed cybersecurity into their policies, processes, and procedures. Admins can define access control policies based on specific user roles, risk scenarios, and organizational security policies. Silverfort enforces these policies in real-time, so only authorized users and devices can gain access to the resources they are assigned to. As a result of these policies, alerting, MFA, or blocking access to all users defined in the policy can be enforced.

5.5 Policy Area 5: Access Control (continued)

CJIS regulation	Silverfort security controls
5.5.2.1 Least Privilege The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/ privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.	Silverfort streamlines the implementation of the least privilege model required by providing granular, adaptive access controls that enforce access policies across all environments, including legacy systems. It integrates with existing IAM solutions to ensure consistent enforcement, offers real-time monitoring to prevent unauthorized access, and provides comprehensive visibility for auditing and compliance, helping organizations minimize access rights to only what is necessary for each user.
5.5.6 Remote Access The agency shall authorize, monitor, and control all methods of remote access to the information system. The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points.	Silverfort enables organizations to manage and secure remote access by authorizing and monitoring all remote connections through identity-based policies and real-time monitoring. It centralizes control via managed access points, enforces MFA, and secures privileged access, ensuring only authorized users can remotely access systems, with all activities closely monitored and documented.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

CJIS regulation	Silverfort security controls
5.6.1 Identification Policy and Procedures Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit.	Silverfort enables organizations to enforce the use of unique credentials for every user authorized to store, process, or transmit Criminal Justice Information (CJI). Through integration with existing identity management systems, it ensures all users, including administrators, maintain secure access to systems and networks handling CJI. With Silverfort, user identities can be centrally controlled, which ensures only authenticated and uniquely identified individuals can access sensitive systems, which maintains the integrity and security of CJI.
5.6.2 Authentication Policy and Procedures Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance.	Silverfort helps organizations authenticate each user's identity by enforcing strong multi-factor authentication (MFA) across all systems, even those that don't natively support modern authentication protocols. This ensures every user must verify their identity before accessing resources.

5.6 Policy Area 6: Identification and Authentication (continued)

CJIS regulation	Silverfort security controls
5.6.2.2 Advanced Authentication Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or "Risk-based Authentication" that includes a software token element comprised of a number of factors.	Silverfort enhances Advanced Authentication (AA) by integrating and enforcing additional security measures, such as Multi-Factor Authentication (MFA), across all systems. It supports various AA methods, including biometric systems, OTPs, number matching, FIDO2, and push notifications, enabling flexible authentication across all systems. This ensures enhanced security by requiring multiple verification factors before granting access to sensitive resources. Furthermore, Silverfort supports risk-based authentication, which dynamically adjusts authentication requirements based on contextual factors.
5.6.2.2.1 Advanced Authentication Policy and Rationale The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access).	Silverfort helps organizations navigate the requirement for Advanced Authentication (AA) by dynamically applying or enforcing MFA protection based on access policies assigned to specific users and the specific context of the user's location and access method. It assesses whether users are within a physically secure location, comply with security controls, or have indirect access to CJI. Based on this assessment, Silverfort enforces or extends MFA as needed, ensuring compliance with CJIS requirements while maintaining appropriate security levels.

5.7 Policy Area 7: Configuration Management

CJIS regulation	Silverfort security controls
5.7.1 Access Restrictions for Changes Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.	Silverfort helps enforce access restrictions for changes to information systems by ensuring that only qualified and authorized individuals can access critical system components. By verifying users' identities and enforcing strict access policies, Silverfort ensures that only users who are authorized to access the system are able to do so. It reduces the risk of unauthorized changes that could compromise system security since all changes are controlled and made by authorized individuals.

5.10.1.1 Boundary Protection

CJIS regulation	Silverfort security controls
Control access to networks processing CJI.	Silverfort helps organizations control access to networks processing Criminal Justice Information (CJI) by enforcing strong access controls across the entire network. By applying MFA and enforcing access policies to ensure all users' access requests are secure, only authenticated and authorized users have access to network resources that handle CJI. Silverfort also provides real-time monitoring and alerts to all unauthorized access attempts.
Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.	Silverfort monitors security incidents, detects attacks, and identifies unauthorized access attempts by providing organizations with continuous visibility into access attempts and user activities across their environments. As Silverfort integrates with all IdPs, it is capable of detecting anomalies, unauthorized access, and potential threats in real time. Silverfort also alerts on suspicious activities, ensuring real- time detection of security events.

5.10.4.4 Security Alerts and Advisories

CJIS regulation	Silverfort security controls
The agency shall: Receive information system security alerts/advisories on a regular basis.	Silverfort monitors all authentications between all endpoints and the other assets of the organization and alerts/denies access upon detecting anomalous activity, including but not limited to lateral movement attempts. In addition, Silverfort requires MFA to be performed on every "hop" (move from one asset to another), ensuring stolen credentials cannot be used to progress in the attack path.
Take appropriate actions in response	Silverfort helps organizations take appropriate actions in response to security alerts by automating the enforcement of security policies based on the nature of the alert. When a security advisory or alert is received, Silverfort can automatically trigger actions such as requiring additional authentication, blocking access to sensitive resources, or isolating potentially compromised accounts. This rapid, automated response minimizes the risk of breaches and ensures security measures are promptly applied.