COGNITE

Cognite Data Fusion® Support for NIST Cyber Security Framework (CSF)

Cognite Data Fusion® Support for NIST Cyber Security Framework (CSF)

Table of contents

About Cognite

Cognite is a global industrial SaaS company that supports the full-scale digital transformation of asset-heavy industries around the world. Our core Industrial DataOps platform, **Cognite Data Fusion®**, enables data and domain users to collaborate to quickly and safely develop, operationalize, and scale industrial AI solutions and applications.

Cognite Data Fusion® codifies industrial domain knowledge into software that fits into your existing ecosystem and enables scale from proofs of concepts to truly data-driven operations to deliver both profitability and sustainability.

WHY COGNITE DATA FUSION® → BENEFITS FOR YOUR TEAMS → CONTACT SALES →

Introduction

Background

Governments, industry sectors, and organizations around the world are increasingly recognizing the NIST Cybersecurity Framework (CSF) as a recommended cybersecurity baseline to help improve the cybersecurity risk management and resilience of their systems. This paper evaluates how Cognite Data Fusion® aligns to and supports customer adoption of NIST CSF.

NIST Cyber Security Framework (NIST CSF)

Recognizing that the national and economic security of the United States depends on the reliable function of critical infrastructure, President Obama in February 2013 issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity. The EO directed NIST to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyberrisks to critical infrastructure.

Created through a collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure manage cybersecurity-related risk.

According to Gartner, the CSF is used by approximately 30 percent of US private sector organizations and was projected to reach 50 percent by 2020. Sixteen US critical infrastructure sectors use the CSF, and more than 21 states have implemented it. Other countries, including Italy and Israel, are using the CSF as the foundation for their national cybersecurity guidelines.

Applying NIST CSF

NIST CSF is a tool that can be used to support assessment, acquisition, and in the assessment of software as a service (SaaS) providers, enabling a uniform basis for the prioritization of technology purchases and security program investments. The framework can help support the definition of organization wide security and compliance objectives.

WHY COGNITE DATA FUSION® → BENEFITS FOR YOUR TEAMS → CONTACT SALES →

Cognite Data Fusion®

Cognite is a SaaS provider, and Cognite Data Fusion® is our industrial DataOps platform product. We also offer subscription-based access to configurable business applications.

Cognite Data Fusion® streams data into the CDF data model, where the data is normalized and enriched by adding connections between data resources of different types and stored in a graph index in the cloud. With your data in the cloud, you can use services and tools in Cognite Data Fusion® to build solutions and applications to meet your business needs.

With Cognite, you own your data. We use your data only to provide agreed-upon services. We handle your data securely, and we comply with privacy and legal regulations. If you leave our services, Cognite ensures that customers maintain data ownership.

You can interact with your data through the portal application, or work with the data with our API and SDKs.

Cognite Data Fusion® solution security

As more industries that rely on operational technology adopt cloud technology, it's critical to apply robust and more automated cybersecurity risk management practices for each interconnected system to protect the confidentiality, integrity, and availability of data. Cognite Data Fusion® integrates with existing equipment and infrastructure to provide insights and realize value from your industrial data. To fulfill our responsibility as a trusted custodian, we have developed and implemented the Cognite security commitment: a set of principles focusing on people, processes, and technology that inform the design and operation of Cognite Data Fusion®.

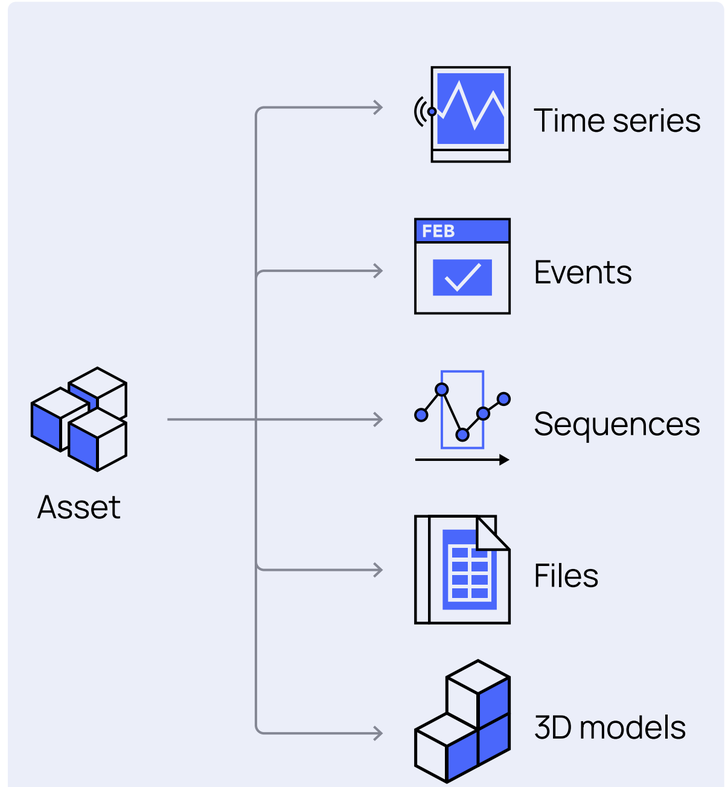
Defense in depth

Cognite operates in mission critical, asset-heavy industries where operational technology security is table stakes. With Cognite Data Fusion®, security is a collaboration between the customer, Cognite, and cloud provider (for example Microsoft or Google).

Cognite supports defense in depth through:

- Industry security compliance and regulations
- Secure development life cycle
- Security logging and monitoring
- Incident response

Security stakeholders are critical to the successful scaling and sustaining of Industry 4.0 programs. We welcome the opportunity to engage and support security stakeholders.



Secure by design

- Meeting product standards: Cognite's management system (QMS and ISMS) is ISO 9001 and ISO 27001 certified. The operation and data processing in Cognite Data Fusion® comply with the

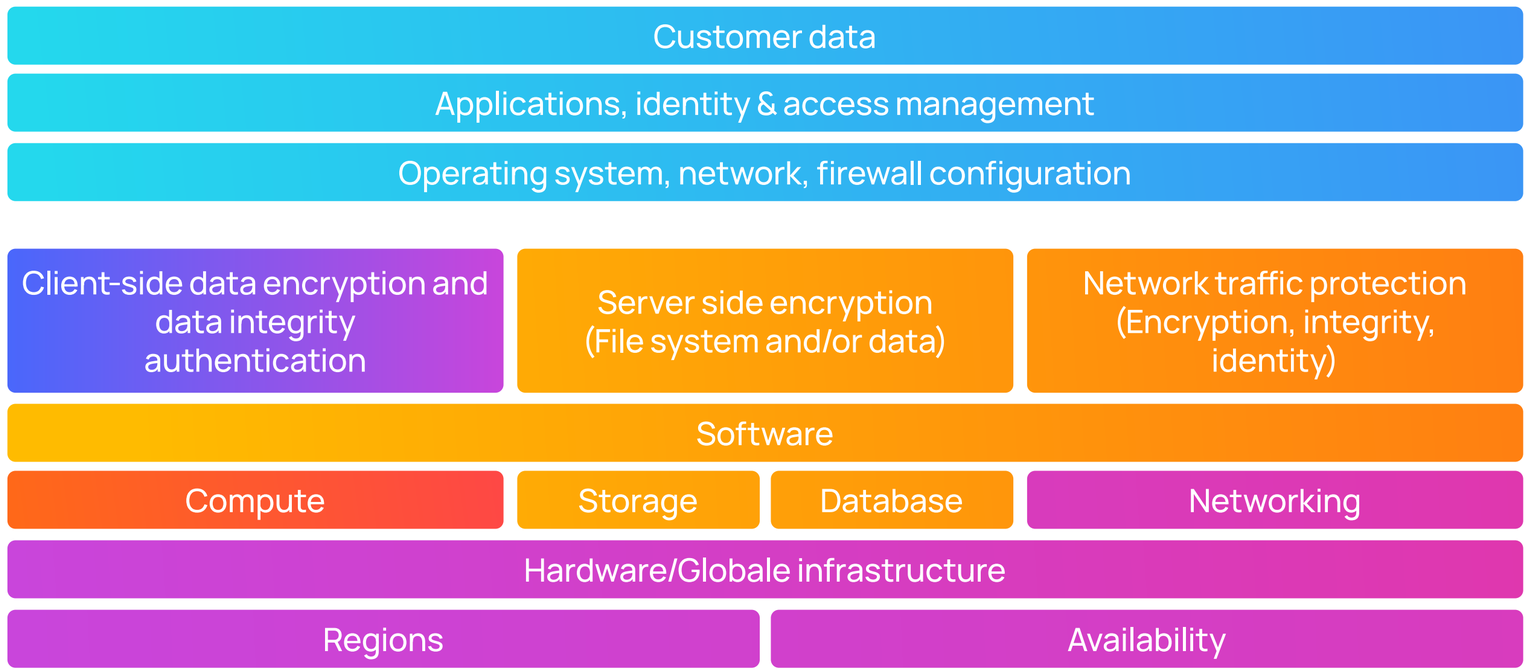
WHY COGNITE DATA FUSION® → BENEFITS FOR YOUR TEAMS → CONTACT SALES →

General Data Protection Regulation (GDPR).

- Secure development life cycle: Cognite invests in security awareness and training to support integrated DevSecOps practices. Security practices supported with: (1) a comprehensive audit and observability stack, (2) test and security automation (2), and a robust incident response process and practices.

- Least privilege and access control: Customers control access to data through integration using their organization's identity provider. Within Cognite project engagements, privileged access to customer data is strictly limited and role-based.

- Secure data: Encryption at rest and in transit.



Shared responsibility

The shared responsibility model is fundamental to understanding the respective roles of the context of the cloud security principles. This model identifies ownership across the customer organization, Cognite, and the customer's cloud service provider (CSP).

Cognite's world-class CSP partners are responsible for infrastructure composed of the hardware, software, networking, and facilities that run cloud services.

Cognite maintains a strong relationship with CSPs to use platform and infrastructure security controls that comply with industry standards. These processes, procedures, and tools support the strong security foundation of Cognite Data Fusion®. As new technologies and threats emerge, Cognite is uniquely positioned to take advantage of these security updates in its products.

Customers retain control of the security program that they choose to implement to protect their content, applications, systems, and networks. Cognite supports data encryption in transit and at rest in collaboration with CSP. Cognite holds responsibility for the application's secure development lifecycle and associated vulnerability management.

Data security and access control

- Access control. Customer-defined users, roles, and privileges, as structured in the customer's identity provider (IdP), determine how access control to customer data is managed. Cognite employees' access to customer data is granted via the IdP, and the customer can choose when to enable and revoke that access.

WHY COGNITE DATA FUSION® → BENEFITS FOR YOUR TEAMS → CONTACT SALES →

- Data security. Encryption in transit: Data owner/source, Cognite APIs, and traffic internal to Cognite Data Fusion® are encrypted with TLS 1.2 and higher.

  Encryption at rest: Server-side encryption using cloud service-managed keys for encryption and decryption.

Cognite controls in place to prevent data leakage or intentional or accidental compromise include:

- Data encryption with cloud service provider (CSP) encryption key
- Customer controlled data access: integration with customer's identity provider (IdP) service. Requests and API calls are mapped to roles and permissions from the IdP.
- Principle of least privilege and changes managed in code with approval (peer-review) flow.
- Network and infrastructure policies that control and restrict access to only authenticated or authorized services.
- Logical separation inside shared data stores.
- CSPs use cryptographic authentication and authorization at the application layer for inter-service communication.
- CSPs rely on ingress and egress filtering throughout the network to prevent IP spoofing as a further security layer.

Resilience

Cognite Data Fusion® is built on cloud infrastructure configured to be highly available. Deployment is continuous and incremental with smaller changes to minimize impact and potential for disruption, while ensuring the ability to quickly validate or confirm changes. Cognite routinely performs testing of business continuity and disaster recovery plans (tabletop and real exercises) that validate scenarios and functionality including confidentiality, integrity, and availability.

Specific security controls supporting NIST 800-61 standard guidelines to support detection, response, and recovery include:

Incident handling processes guided independently certified compliant to ISO 9001 and 27001.

- Preparation: Processes and tools in place and continuous improvement through applying lessons learned.
- Containment: Organizing and limiting or preventing damage.
- Eradication: Eliminate root cause and prepare for system restore.
- Recovery: Bring systems back to production in desired state and monitor.

Cognite Data Fusion® alignment to NIST CSF

As a SaaS solution, Cognite Data Fusion® maintains management best practices defined in the CSF and supports customers that align and measure their security postures relative to CSF. Appendix 1, which follows, details how Cognite Data Fusion® aligns to NIST CSF core functions and subcontrols.

Appendix: Cognite Data Fusion® alignment to NIST CSF

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Access Management Program	DE.DP-1 DE.DP-2 ID.AM-3 ID.AM-6 PR.AC-1 PR.PT-3	Cognite's Code of Conduct defines employee and contractor information security responsibilities regarding confidentiality, data protection, appropriate use of Cognite's equipment and facilities, and practices expected by the organization. Cognite uses cloud provider identity repository and cloud services to provide authentication, authorization, and access control for an organization's users, groups, and objects. The identity repository utilizes role-based access control (RBAC) to grant access to resources. Multifactor authentication (MFA) is used to secure access to sensitive information and minimize risk of malicious attack.
Access Revocation	PR.IP-11	Cognite's Human Resources Security Policy outlines the employee/contractor/third-party access termination process and clearly defines associated responsibilities related to termination of employment and change of role. Cognite uses internal procedures to effectively manage departing employees and the withdrawal of assigned responsibilities for employees, contractors, and other third-party users. Access rights to information and information systems are removed upon termination of employment or contractual relationship. Cognite has an established and logged procedure for the withdrawal or modification of access rights for departing employees, contractors, and third-party users. These rights are removed via the identity management (IDM) system. Changes in responsibilities and duties within Cognite include removal of all rights associated with prior roles and duties, and creation of rights appropriate to the new roles and duties. Removal or reduction of access rights prior to the termination is performed where risks indicate this step to be appropriate.

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Asset Inventory	ID.AM-1 ID.AM-2 ID.AM-5	Cognite assets associated with information and information processing facilities are inventoried throughout the respective life cycles. The inventory is documented and maintained in an inventory database system, which provides an accurate and up-to-date inventory through new installations and decommis- sioning of devices. Classification is based on standards set by Cognite's security group.
Configuration Change Management	PR.DS-3 PR.DS-4 PR.DS-5 PR.DS-6 PR.DS-7 PR.DS-8 PR.IP-3 PR.MA-1 PR.MA-2	Cognite's cloud service provider (CSP) annually reviews and updates configuration settings and baseline configu- rations of hardware, software, and network devices. Changes are developed, tested, and approved prior to being introduced into the production environment from development or test environ- ments. Baseline configurations are documented, managed, and maintained along with the source code control repositories. Prior to being intro- duced, information security impact analysis is performed and reviewed by each service team. Changes to base- line configurations go through the SDL process, which requires security sign-offs prior to production deployment. Cognite's Change Management Policy brings discipline and quality control to the change lifecycle. Cognite prac- tices continuous delivery (CD) through breaking down significant changes into subcompo- nents. This disci- pline reduces the chance of changes causing problems and enables more rapid reversion when needed. When changes are executed, the process is recorded, classified, and documented in an automated tracking system. All change management is supported by design documents, code review, test, and approval through the Change Advisory Board. Any accepted changes are identified with a roll- out date and impact analysis. The communica- tion of the change is handled through the project management process. A roll-out plan is executed with provision if any failure should occur. All affected users are notified prior to release of the change.

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Configuration Monitoring	DE.AE-1 PR.IP-1	Cognite uses a source code control repository to document evidence of approval and to track all changes. These tools provide auditing capabilities ensuring that changes to the baselines and configuration changes within tools. This repository also provides versioning systems for software code. These tools track the identity of individuals who check code out, the time of the change, and changes are made to identified files. In addition, Cognite executes an annual review of the change management process. As part of the review, a sample of changes is selected and reviewed to determine if the change management process is consistently followed. This process ensures that no unauthorized changes are made to baselines.
Cyber Security Incident Response Plan Implementation and Testing	ID.SC-5 PR.IP-10 PR.IP-9	Cognite's CSPs test incident response methodology and tools annually to ensure optimal performance during incidents in the cloud environment. Testing occurs in both test and production environments. A quarterly comprehensive production exercise is conducted to validate the effectiveness in a live fire exercise. All results are documented in the CSP's incident response test plan. Cognite monitors infrastructure, services, accounts, and logs for vulnerabilities and irregular activities using standard third-party tools and custom-built tools and solutions. Cognite uses internal and third- party security specialists and auditors to test, evaluate, and audit operations and environments. Issues and vulnerabilities that are reported or detected are logged, tracked, and prioritized. All items have a named owner, priority, and management visibility and tracking. Cognite's security team conducts incident response testing and exercises per protocols and procedures as part of the external validation layer. Relevant summaries or reports are shared with comments and status updates. A formal incident report is produced by the service teams and augmented by Cognite's Incident Management team's additions. These reports, which include lessons learned, are created for all events. The incident reports are maintained by Cognite's security team and are provided to the relevant stakeholders for review. On a monthly basis, all incidents from the previous month are reviewed with the leadership team, including (1) impact and resolution of the incident and (2) changes to the Incident Response Plan. The Incident Response Plan is revised to address system or organizational changes or problems encountered during plan implementation, execution, or testing.

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Cyber Security Incident Response Plan Specifications	ID.SC-5 RS.AN-1 RS.AN-2 RS.AN-3 RS.AN-4 RS.AN-5 RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5 RS.IM-1 RS.IM-2 RS.MI-1 RS.MI-2 RS.MI-3 RS.RP-1	Cognite's Incident Management Policy provides the organization-wide guidance on proper response to, and efficient and timely reporting of service and security incidents. The policy governs how Cognite ensures that support resources are focusing on the issues that have the greatest urgency and potentially the greatest impact on the business. The control and management information provided by this process, provides Cognite's management decision support required to prioritize resources for managing risks to Cognite achieving the company objectives. Cognite utilizes CI/CD method of development to restore normal service operation as quickly as possible and to minimize the adverse impact on business operations, thereby ensuring that the best possible levels of service quality and availability are maintained.

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Cyber Security Policies	ID.AM-3 ID.GV-1 ID.RM-1 ID.RM-2 ID.RM-3	Cognite's security policy applies to all processes and information used to conduct business. Cognite maintains ISO 9001 and ISO 27001 certification, which outline security training, controls, and incident response. These policies are reviewed annually by independent auditors. Security policies for cloud service providers are reviewed prior to engagement.
Cyber Security Training Program	ID.AM-6 ID.GV-2 PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	Cognite administers annual cybersecurity training programs to educate Cognite personnel on security basics and recent trends in security and privacy to reinforce cybersecurity practices for personnel with authorized electronic access to cloud-based resources. Cognite provides role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties. Employees with access to sensitive information receive periodic reminders of their responsibilities and receive ongoing updated security awareness training to ensure their understanding of current threats and corresponding security practices to mitigate such threats. Community engagements of incident simulations and exercises reinforce responsibilities consistent with Cognite's policies and procedures. Electronic records of training are retained by Cognite's security group to ensure compliance to industry standards.
Electronic /Security Perimeter	DE.CM-5 DE.CM-6 DE.CM-7 PR.AC-3 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.PT-4 PR.PT-5	Cognite's cloud service providers' security posture is deny by default, allowing only connection and communication that is necessary for systems to operate, blocking all other ports, protocols, and connections by default. Connections are managed at the system boundary using the cloud service providers' boundary protection devices. Connections within the boundary are managed using IP filtering and firewalls. Cognite uses a layered architecture to protect services and data. This is to allow only connections and communications that are necessary for a virtualized solution to operate, blocking all other ports and connections. The cloud service provider provides the load balancer and firewall, while the services proxy helps isolate deployments at the network level. This layered approach provides a combination of broad (non-granular) protections coupled with a fine (granular) service-to-service level of control and observability. Customers must authorize Cognite before remote access is granted. Before service team personnel can connect remotely, they must first be approved for remote access by an authorized Cognite manager. Users are identified via two-factor authentication based on a unique identifier and password from the customer's environment. The remote session uses encryption to prevent information disclosure. Customers are required to provide users with privileged or elevated access to cloud production systems for platform troubleshooting and maintenance.

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Information Protection	PR.DS-2	Cognite uses the Transport Layer Security (TLS) protocol to protect data traveling between Cognite Data Fusion® and cloud service providers. TLS provides strong authentication, message privacy, and integrity. Data at rest is deployed and regionally restricted using AES-256 CSP default encryption and CSP-managed keys. Access to servers where information is stored is restricted through identity repository security group membership in the domain where the server resides. Cognite supports additional requirements as part of contract negotiation, if it is deemed that change of operational models would be necessary for customer-driven regulatory or legal requirements.
Malicious Code Prevention	DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5 DE.CM-1 DE.CM-2 DE.CM-3 DE.CM-4	Cognite uses CSP event monitoring and logging at the platform level to protect Cognite Data Fusion® from intrusions and malicious code using the latest threat telemetry. Audit log review occurs no less than weekly and can be triggered at any time by a security incident, customer request or escalation, or any other incident impacting production functionality. Logs are retained in a central repository for at least 90 days to support investigations of security incidents and to meet regulatory retention requirements. **Information Protection** Cognite uses the Transport Layer Security (TLS) protocol to protect data traveling between Cognite Data Fusion® and cloud service providers. TLS provides strong authentication, message privacy, and integrity. Data at rest is deployed and regionally restricted using AES-256 CSP default encryption and CSP-managed keys. Access to servers where information is stored is restricted through identity repository security group membership in the domain where the server resides. Cognite supports additional requirements as part of contract negotiation, if it is deemed that change of operational models would be necessary for customer-driven regulatory or legal requirements. Cognite has 24-7 support and monitoring. In addition there is an on-call engineer rotation for escalation. Cognite uses an automated solution to scramble critical alerts to the on-call engineer outside business hours. On-call engineers are preselected and assigned roles to perform the required to identify, contain, and restore. Additional resources, either internally or by cloud service providers, are engaged by the on-call engineer when needed

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Personnel Risk Assessment Program	ID.GV-4	The Cognite human resources (HR) department conducts background checks and enforces the screening poli- cies for all personnel (including contractors and vendors). Background checks are required for new hires or personnel transferring to positions that involve potential access to customer data. Background verification includes relevant privacy, protection of personally identifiable information, and employment-based legislation. Screening, disclosure, and retention of information (seven years) is coordinated by Cognite's HR department. The process is described in Cognite's Employee Background Verification Policy.
Physical Access Control System Maintenance and Testing Program	ID.AM-1 ID.AM-2	Cognite's CSPs ensures that all access control devices are inventoried at least annually. Moreover, access control devices in data centers are linked to the physical security system where device status is monitored continuously. Therefore, it is not necessary to have separate testing every 24 months to ensure devices function properly. If an access control device stops working, a device malfunction alert is issued immediately.
Physical Security Plan	PR.AC-2 PR.AT-5	Cognite's CSPs enforce physical access authorizations for all physical access points to data centers. The exteri- ors of the data center buildings are nondescript and do not advertise that they are data centers. Depending on the design of a data center, physical access authorizations may begin at a controlled perim- eter gate or secured facil- ity door that require either access badge authorization or security officer authori- zation. Main access to data center facilities is restricted to a single point of entry that is monitored 24-7 by secu- rity personnel. Emergency exits are alarmed and under video surveillance. Data center doors have alarms that report being opened or when they remain open beyond an acceptable length of time, and they are programmed to display the live CCTV image when a door alarm is triggered. The data centers have security operations desks located in reception areas and are in the line of sight of the single entry point. Addi- tionally, the control room supervisor monitors a live feed of camera views from high-security and high-traffic areas. Data center physical access logs for authorized individuals are retained for 90 days.

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Ports and Services	PR.DS-1	Cognite's cloud provider network security is deny-by-default, which means allowing only connection and communication that is necessary for systems to operate, blocking all other ports, protocols, and connections by default. Access to devices connected to serial and USB ports is not possible since there are no corresponding drivers. Cognite manages connections at the system boundary using cloud providers networking boundary protection devices like IP filtering and firewalls. Cognite also utilizes 3rd party tools to detect configuration issues and observing network connectivity between Cognite Data Fusion® container workloads. Cognite continuosly monitors API activity, network traffic, running workloads, and to alert on anomalous behaviour and known threats.
Recovery Plan Implementation and Testing	PR.IP-4	The CSP Disaster Recovery Plan (DRP) team schedules end-to-end recovery tests, drives test execution, identifies recovery gaps, and communicates test results. At least one major end-to-end scenario is tested annually.

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Recovery Plan Specifications	PR.IP-10 PR.IP-5 PR.IP-6 PR.IP-7 PR.IP-8 PR.IP-9 RC.CO-1 RC.CO-2 RC.CO-3 RC.IM-1 RC.IM-2 RC.RP-1	Cloud Service Providers Disaster Recovery Plans (DRP) provides detailed processes for contingency planning for related cloud infrastructure. These documents serve as a guide for Cloud Service Providers to respond, recover and resume operations during a serious adverse event. The DRP covers the key personnel, resources, services, and actions required to continue critical technology processes and operations. This plan is intended to address extended service disruptions. Cloud Service Providers monitor backups of system OS and customer image(s) using system generated alerts that notify operations team of any failed or incomplete backups. The integrity of data is automatically confirmed upon completion of the backup. Restoration tests are captured and stored to generate reports and perform root-cause analysis, as needed. Protection of audit information is restricted to the centralized audit collection system. Only authorized personnel are allowed access to audit records; their assigned rights prohibit authorized personnel from modifying or deleting audit information. All disks are securely maintained in datacenters. Backup disks are moved to off-site facilities for long term storage. Disk backup libraries, encryption devices and servers are located in datacenters. Facility security teams monitor access to media (disks) and the disk back up libraries. All disks are placed in off-site containers and locked during off-site transport to secure storage facilities. Disks are stored in open racks and can be recalled by a single disk. Cognite's Data Retention, Archiving and Destruction policy sets out the principles for retaining and destroying specified categories of data. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory, or contractual obligations. Disposal of records are carried out in accordance with the relevant retention and disposal schedule. Confidential information is destroyed by a method that ensures reconstruction of the contents is impossible. Archived documents are retained for seven years. Approved destruction methods appropriate for each type of information are required. Proper digital media and computer hard drive disposal methods include, but are not limited to, destroying electronic media by shredding, incineration, melting or pulverizing.

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Secure Development Life Cycle	ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6 ID.RM-1 ID.RM-2 ID.RM-3 PR.IP-2	Cognite's Secure SDLC practices is an established methodology and process to ensure a systematic and secure software development lifecycle (SSDL). This agile process framework incorporates security into the development cycle. Awareness sessions from internal and external threat intelligence sources provides input to the solution architecture, threat modeling, and requirements. Implementation f security testing and vulnerability management using static and dynamic code analysis builds security into all processes of the development.
Security Awareness Program	PR.AT-1	An information security awareness program has been established in line with Cognite's information security policies and relevant procedures, considering the information to be protected and the controls that have been implemented to protect the information. Cognite's security awareness program is updated regularly to ensure alignment with Cognite policies and procedures. This program is built on lessons learned from information security incidents.
Security Event Monitoring	DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5 DE.CM-1 DE.CM-2 DE.CM-3 DE.DP-3 DE.DP-4 DE.DP-5 PR.PT-1	Cognite leverages the cloud provider's extensive monitoring and logging of events at the platform level to protect the platform from intrusions and malicious code using the latest threat telemetry. Audit log review occurs at least weekly or can be triggered at any time by a security incident, customer request or escalation, or any other incident impacting production functionality. Logs are retained in a central repository for at least 90 days to support investigations of security incidents and to meet regulatory retention requirements. Cognite has 24x7 support and monitoring, in addition there is an on-call engineer rotation for escalation. Automated solution for scrambling on call engineer outside business hours is implemented for critical alerts. On call engineers are pre-selected and assigned roles to perform the required operations to identify, contain and restore. Additional resources, either internally or at the cloud provider side, are engaged by on call engineer when needed.

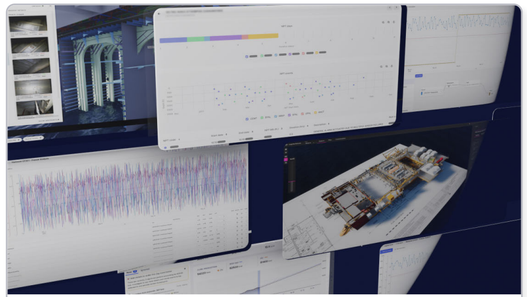
Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Security Patch Management	DE.CM-8 PR.IP-12	Cognite Data Fusion® is a SaaS platform with no planned downtime or patch installations. Vulnerability detection and remediation is continuously executed. Vulnerability management covers activities including network scanning, container scanning, and penetration testing. Scanning is used to detect and remediate vulnerable dependencies and exposed secrets. Detected vulnerabilities are evaluated and ranked, and mitigation activities are agreed upon with developers. Vulnerabilities such as issues and bugs are tracked and kept open until they have been mitigated. Changes are tested and deployed using an automated CI/CD process and can be rolled back within minutes if server metrics, request logs analysis, or support tickets indicate a problem. Static application security testing (SAST) is part of the CI/CD pipeline, as a prerequisite to production release approval. Cognite also runs dynamic application security testing (DAST) in security penetration tests for both authenticated and unauthenticated requests.
Supply Chain Cyber Security Risk Management Plan	ID.AM-4 ID.BE-1 ID.BE-2 ID.BE-3 ID.BE-4 ID.BE-5 ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 ID.SC-5	Cognite's Supplier Relationships Security Policy ensures that information security objectives are established for third parties providing components for Cognite Data Fusion® solutions. Cognite exercises due diligence to gather a complete understanding of all suppliers' information security approach and controls. Arrangements with suppliers that involve accessing, processing, storing, communicating, or managing Cognite information, information systems, or information processing facilities are based on a formal agree- ment containing necessary security requirements. CSP infrastructure enforces case-sensitive passwords with a minimum password length of 14 characters and at least one uppercase letter, lowercase letter, number, and special character. Additional risk miti- gating measures include mandatory two-factor authentication. In addition to implementing these forms of dual- or multifactor authentication, an account password policy is enforced for the domains including strong password complexity, password expiration, password history, and minimum password length. Third-party suppliers are reviewed based on classification and planned use. Reviews result in one of three outcomes: (1) acceptable, (2) request for improvement, or (3) vendor or solution not acceptable. Sources used for supplier review includes ISO SOC 2 Type 2 reports, supplier provided documentation, standard industry certifications, and questions and answers.

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
System Access Control	PR.AC-1	Customers are responsible for managing end-user accounts. Cognite's CSPs use identity repositories for account management. The local administrator account is renamed and disabled. Default passwords are changed for the local admin account and root accounts for network devices. Account owners are required to rotate shared account credentials at least every 70 days. Additionally, account owners are required to rotate shared account credentials whenever there are changes to personnel. CSP infrastructure enforces case-sensitive passwords with a minimum password length of 14 characters and at least one uppercase letter, lowercase letter, number, and special character. Additional risk mitigating measures include mandatory two-factor authentication. In addition to implementing these forms of dual- or multifactor authentication, an account password policy is enforced for the domains including strong password complexity, password expiration, password history, and minimum password length. CSPs alert security personnel to instances where brute force password guessing is attempted and apply addi- tional authentication mechanisms to reduce account privileges for the account associated with the password acquired through brute force.
Transient Cyber Assets and Removable Media	DE.CM-5 PR.PT-2	Cognite's Acceptable Use Policy and Bring Your Own Device Policy governs the overall use of informa- tion, elec- tronic data, computing devices, and network resources. The policies prohibit the use of Cognite information systems or assets in a manner that is deliberately malicious or detrimental to their security, performance, capacity or integrity, or that poses a threat or liability to either Cognite, its employees, its customers, or the public at large.

Control area	CSF Sub Control ID	Cognite support of NIST CSF control
Vulnerability Assessment	DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5 DE.CM-1 DE.CM-2 DE.CM-3 ID.RA-1 PR.IP-12	Cognite uses the Security Audit Logging and Monitoring Policy to monitor the infrastructure, services, accounts, and logs for vulnerabilities and irregular activities. Using standard third-party tools and custom built tools and solutions that provide reporting data based on a number of existing industry-accepted open standards that item- ize software flaws, security configurations, and various product names, including the Common Vulnerabilities and Exposures (CVE). In addition, Cognite uses internal and third-party security specialists and auditors to test, evaluate, and audit operations and environments on an annual basis. Issues and vulnerabilities that are reported or detected are logged, tracked, and prioritized. Prior changes being implemented, information security impact analysis is performed and reviewed. Changes are analyzed as part of the standard change manage- ment process, both prior to and after implementation, to verify that modifications provided the expected output. All items have a named owner, priority, and management visibility and tracking.

Want to know more about our product?

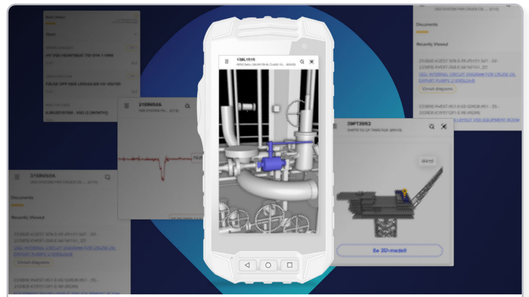
Explore more insights from Cognite



PRODUCT TOUR

Learn from Cognite customers and product managers how Cognite Data Fusion® simplifies and streamlines the data experience of a subject matter expert.

WATCH NOW →



CUSTOMER STORIES

Discover how Cognite Data Fusion® makes data more accessible and meaningful, driving insights that unlock opportunities in real-time, reduce costs, and improve the integrity and sustainability of your operations.

GO TO STORIES →

ANALYST REPORT

Customer interviews and financial analysis reveal an ROI of 400% and total benefits of $21.56M over three years for the Cognite Data Fusion® platform.

READ THE REPORT →

BLOG

Discover our rich catalog of industry insights and technology deep dives.

READ OUR NEWEST BLOGS →

WHY COGNITE DATA FUSION® → BENEFITS FOR YOUR TEAMS → CONTACT SALES →

COGNITE

COGNITE.COM →