X Platform

Security

WHITEPAPER

HARDWARE

SOFTWARE

IoT PLATFORM

EXOR JMobile CORVINA

HOLDEX EXOR JMobile CORVINA ONE DIGIBELT Next-Stel Solutions AXEL FACTORYAL

Index

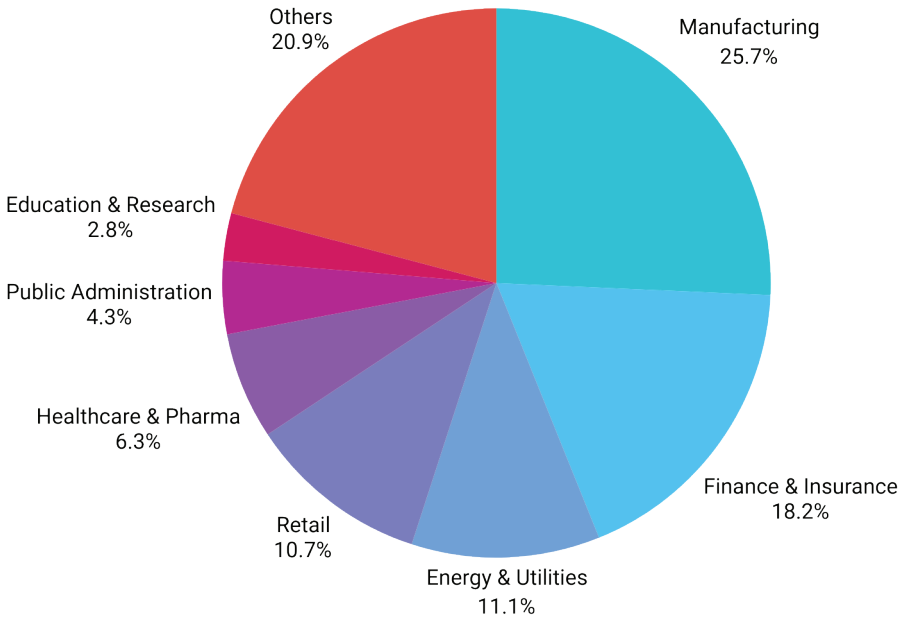
1.0 Premises

The industrial sector is a prime target for cybercriminals, experiencing frequent and severe attacks.
Key statistics reveal a significant portion of all cyberattacks target this sector, with substantial costs associated with data breaches and ransomware incidents. Supply chain attacks have also increased dramatically.

The sector's sensitive data, including intellectual property, and increasing reliance on interconnected systems and IoT devices make it particularly vulnerable. Robust cybersecurity measures, including technology investments, employee training, and incident response plans, are crucial for protecting operations, reputation, and financial stability.
However, Cloud technology is essential for modern industry, driving efficiency, agility, and innovation.
It optimizes operations through real-time production visibility and predictive maintenance, leading to reduced costs and downtime. Cloud-based solutions enhance collaboration and communication across the supply chain, accelerating time-to-market.

Scalability and flexibility allow manufacturers to adapt to changing demands, while access to advanced technologies like AI and ML fuels innovation. While security concerns exist, reputable cloud providers offer robust security, often exceeding in-house capabilities. Ultimately, cloud adoption is crucial for industrial organizations to thrive in the digital age.

Share of cyberattacks by industry



According to the 2024 X-Force Threat Intelligence Index by IBM Security

2.0 X Platform Introduction

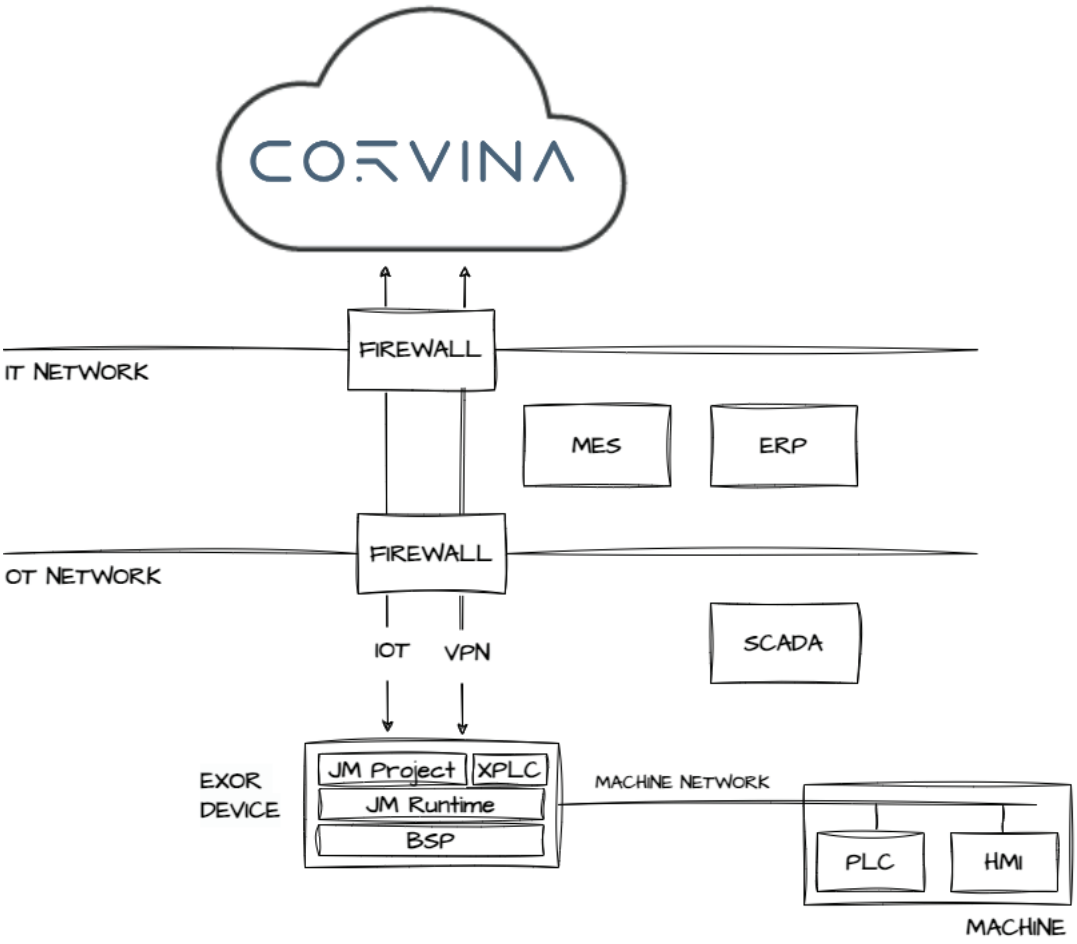
The All-in-One Industrial Automation Platform.

X Platform is an all-in-one platform designed to seamlessly integrate every aspect of industrial automation. The X Platform, a quietly confident presence, bridges the gap between the complex aspirations of machine builders and the practical necessities of factory operations.

X Platform merges unparalleled software, firmware, and hardware experiences. Whether it's at the component level with impressively aesthetic and functional data interfaces, or at the factory level with multi-protocol data visualization, the X Platform offers an unmatched solution. Our long-standing experience ensures that even when challenges present themselves, we provide the expertise to overcome them. With the X Platform, machine builders not only meet but redefine industry benchmarks.

3.0 X Platform Architecture

Exor's X Platform is a comprehensive industrial automation solution that seamlessly integrates hardware, software, cloud services, and data analytics to enhance efficiency and security in manufacturing environments. Designed with an open architecture, it ensures interoperability across diverse devices and systems.



The Components of the X Platform

Software

Communication across multi-vendor, multi-protocol and multi-device environments and then sending this data to local or cloud storage is a requirement for manufacturing efficiency.

JMobile suite of software offers this with unmatched level of user experience based on nearly 50 years of Industrial automation experience.

Hardware

The evolution of EXOR from a traditional HMI hardware designer and manufacturer to a complete IIoT solution provider is most evident in the hardware offering.

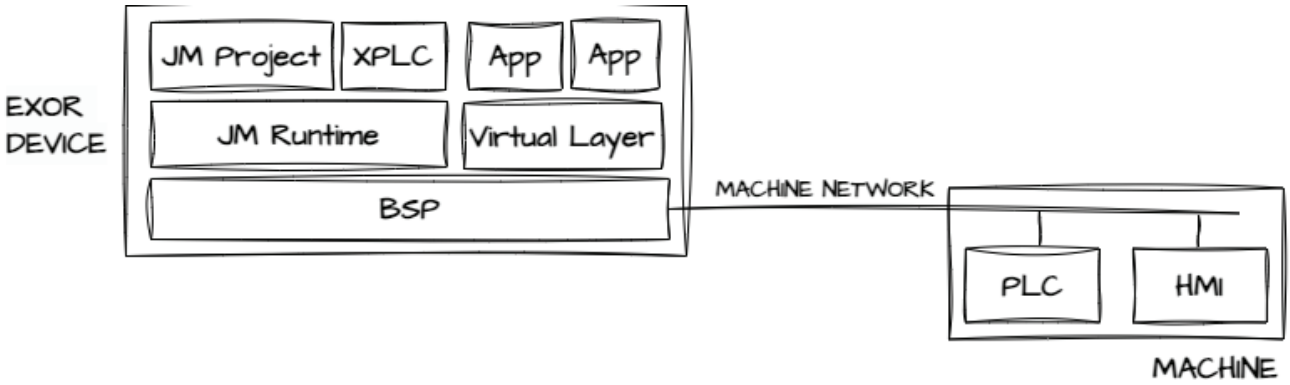
From the very basic component of IIoT, at the SOM level, through field and then up to SCADA and Master level panels, EXOR covers all the current and future market needs.

Cloud based

Built for Industry with all the particular requirements for this sector.
Born from Operation Technology speaking the language of the factory.

Corvina is constructed with state-of-the-art technology specifically mapped for scalability, reliability and fault tolerance and offered as on premises behind your firewall.

4.0 EXOR Device



Exor Device is the OT/IT bridge, it integrates the OT of the machine and enable the IT Integration of the Machine.
Acting as a bridge, the exor device be they an HMI or a Gateway/Edge it integrates all the feature and function that can warranty the security of the machinery.

4.1 EXOR Device structure

Exor Device Architecture is composed by 2 main level:

- **BSP**
- **JMobile** that is logically divided in:
  - o JM Runtime
  - o JM Project /XPLC

4.2 BSP

Board Support Package (BSP) is a collection of software components that enable our Linux operating system to run on a specific hardware platform. Think of it as the bridge between the operating system and the hardware. It contains all the necessary drivers, libraries, and configuration files that the OS needs to interact with the hardware.
As well of this it contains all the necessary function to preserve the security of the Device:

- A/B Updates (release expected in later 2025)
  - o Support for rollack on update fail
  - o Redundancy (double OS)
  - o iMX8 with Secureboot OS platforms only
- Support for TLS 1.2 & 1.3
- Keyring support for storing applications & services sensitive data (passwords, certificates, private keys etc)
- Inactivity timeouts on services
- Countermeasures for Brute Force attacks configurable
- Multiple users on BSP supported with roles configurables

BSP Security Functions in details

Firewall

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a barrier between a trusted internal network and untrusted external networks. It provides the possibility to block incoming connections for specific ports / protocols and allow the specified domains to be whitelisted or blacklisted.

NAT and Port forwarding

NAT allows multiple devices on a private network to share a single public IP, conserving IPv4 addresses and improving security. Types include:
Port forwarding directs external traffic on a specific port to a device inside a private network, enabling remote access to services like web servers, gaming, or security cameras.

Whitelist and Blacklist

Configurable via System Settings allows to limit the access to defined website passing through the device. Whitelist (Allowlist) is list of approved entities (IP addresses or websites, etc.) that are granted access to a system or network.
Blacklist (Blocklist) is a list of denied entities that are blocked from accessing a system or network.

Apps executed as user «app» by default

Running apps as the “app” user instead of root follows the least privilege principle, enhancing security, limiting system access, preventing unauthorized changes, and improving stability.

Support for Docker Containers (Exor provides Docker Engine as an installable application)

Enables running applications in isolated, lightweight environments, improving portability, security, efficiency, and scalability.

Limited resources for services

Limiting as example SSH and VNC connections improves security, Security preventing brute-force attacks and unauthorized access, Performance reducing system resource usage (CPU/RAM), Privacy ensuring only intended users connect and Bandwidth avoiding network congestion.

Persistent logging of critical security operations on dedicated log file with log size configurable

All essential security-related actions (e.g., login attempts, configuration changes, access control modifications) are continuously recorded in a dedicated log file. Administrators can configure the log file size to manage storage efficiently while ensuring detailed records are maintained for auditing, troubleshooting, and compliance purposes.

Device reset via TAP TAP or via USBb stick option in system settings (cleanup entire HMI content)

A factory restores and data cleanup enhances security, improves performance, ensures compliance, and prepares the system for a fresh start by removing sensitive and unnecessary files.

Secureboot Option (Not yet available on all BSPs)

Secure Boot is a security feature that ensures only trusted and digitally signed software runs during system startup. It helps prevent malware, rootkits, and unauthorized software from compromising the boot process.

Implemented tokens anti CSRF (Cross-site request forgery)

CSRF tokens are unique values dynamically generated by a server-side application and sent to the client. Since these values are unique for every request, and constantly changing, it is nearly impossible for an attacker to pre-create the URLs/ requests for an attack.

Enforced security with HTTP headers and options

enhances web security by using protective headers like CSP, HSTS, X-Frame-Options, and others to prevent XSS, click-jacking, and other attacks, ensuring safer user interactions.

CORS options configurable now via system settings

Cross-Origin Resource Sharing is an HTTP-header based mechanism that allows a server to indicate any origins (domain, scheme, or port) other than its own from which a browser should permit loading resources.

Certificate configuration for VNC Server (not yet available for all BSPs)

Enables SSL/TLS encryption to secure remote connections, ensuring authentication, data protection, and compliance with security standards.

Force passwords change at first access

Forcing a password change at first access enhances security by preventing default password vulnerabilities, ensuring compliance with industry standards (e.g., GDPR, NIST, ISO 27001), and promoting user accountability. It protects against insider threats and encourages strong password practices, reducing the risk of unauthorized access.

Strong password rules

Enforcing strong password rules prevents unauthorized access, defends against cyber threats, ensures compliance with security standards, reduces credential leaks, and promotes better security practices.

Configurable rules

Configurable rules for users are customizable policies that define how users interact with a system. These rules allow administrators to tailor user permissions, access controls, and behaviors to meet specific organizational requirements. For example, configurable rules can specify login restrictions, data access levels, and trigger notifications or actions based on user activities. This flexibility enhances both security and usability, ensuring the system adapts to unique business needs.

Passwords expire configurable

Allows administrators to set a custom password expiration period, enhancing security by requiring regular password changes and ensuring compliance with security policies.

System user notification message supported

System user notification message supported" means that the system has built-in functionality to deliver messages—such as alerts, updates, or warnings—directly to its users. This feature ensures that users receive timely notifications about important events, system changes, or required actions, thereby improving communication and overall system responsiveness.

Hardening supported for USB/SD

Hardening for USB/SD involves implementing security measures—such as disabling auto-run features, enforcing access restrictions (e.g., whitelisting), and applying encryption and strict usage policies—to safeguard against vulnerabilities and prevent unauthorized access, malware infections or code execution.

Whitelisting for USB devices

Whitelisting for USB devices is a security measure that only allows pre-approved USB devices to connect to a system. Administrators create a list of authorized devices, and any USB device not on that list is blocked. This helps prevent malware infections, data breaches, and unauthorized access that can occur when unknown or malicious devices are connected.

Rate Limiter agains DOS attacks

Rate limiting is essential for mitigating Denial-of-Service (DoS) attacks because it restricts the number of requests a user can make within a set time frame. This helps prevent system overload, protects critical resources, and maintains service availability even under heavy or malicious traffic conditions.

Manifest file inside System Setting for SBOM and OSS

Including a manifest file for SBOM and OSS in system settings provides transparency, enhances security by tracking vulnerabilities, ensures licensing compliance, and simplifies audits and software maintenance. This improves the overall integrity of your software ecosystem.

4.3 JMobile

Exor JMobile is a powerful and versatile software suite designed for industrial automation and HMI (Human Machine Interface) development. It provides a comprehensive set of tools for create graphical interfaces, connecting to industrial devices, and managing data.
Here's a breakdown of its key features and capabilities:

- **JMobile Studio**: This is the core development environment where you design and build your HMI applications. It offers a user-friendly graphical interface with drag-and-drop functionality, a rich library of objects and widgets, and powerful scripting capabilities using JavaScript.
- **Connectivity**: JMobile supports a wide range of communication protocols, allowing you to connect to various PLCs, sensors, and other industrial devices. This ensures seamless data exchange and integration within your automation system.
- **Visualization**: JMobile enables you to create visually appealing and intuitive user interfaces with advanced graphics, animations, and customizable layouts. This allows operators to easily monitor and control processes.
- **Runtime Environments**: JMobile applications can run on various platforms, including Windows, Linux, and even HTML5-compatible devices. This provides flexibility and allows you to deploy your applications on the most suitable hardware.
- **Remote Access and Monitoring**: JMobile facilitates remote access to your HMI applications, enabling you to monitor and control your systems from anywhere with an internet connection or through Corvina. This is crucial for remote maintenance and troubleshooting.
- **Data Management**: JMobile offers tools for managing and visualizing data, including historical data logging, trending, and alarm management. This helps you gain insights into your processes and make informed decisions.
- **IIoT Capabilities**: JMobile is designed to support Industrial Internet of Things (IIoT) applications. It enables seamless connectivity to cloud platforms and allows you to leverage data for analytics, predictive maintenance, and other advanced applications.

JMobile Security Functions

User Management

User management in JMobile provides a flexible and secure approach to access control. Roles can be defined with specific permissions for both graphical and logical content, ensuring precise control over user interactions. Local users can be managed dynamically at runtime, allowing for seamless administration. Additionally, the LDAP Connector (4.7) enables the mapping of online users within the JMobile project, streamlining authentication and integration with external directories. Notably, user management is unified across both local and remote access, supporting both native and web technologies for a consistent and secure experience.

Audit Trail

The system enables comprehensive tracking of human activity, generating signed CSV or PDF reports to ensure reliable traceability.
To provide a clear and structured overview of events, audit trails include session ID references for each explicit web session, allowing for precise identification of actions taken.
Additionally, for critical parameters, the system requires password confirmation via digital signature, with a configurable timeout to enhance security and prevent unauthorized modifications.

Project security

The system offers the ability to encrypt the entire project using a strong, complex password, ensuring maximum protection.

Additionally, the project can be digitally signed with a certificate, allowing it to run in runtime only on devices that match the assigned project certificate, enhancing security and preventing unauthorized execution).

BSP password [cross topic BSP-JMobile]

JMobile utilizes BSP password protection to secure project uploads and downloads between JMobile Studio and JMobile Runtime. This ensures that only authorized users can transfer projects, preventing unauthorized uploads to your device or accidental downloads of incorrect projects.

Secured protocols

JMobile Studio uses FTPS protocol to transfer the project from IDE to Runtime. JM4Web, the web server that hosts JMobile html pages is reachable via HTTPS protocol. It can rely to the x509 Certificate that can be installed in the BSP.

TLS

JMobile uses TLS protocol in interfaces such as OPC UA and LDAP. Same protocol is supported for sending emails from JMobile Runtime.

4.4 Support

Keep informed about security events, updates and changes.

EXOR Technical Support: support.it@exorint.com - **EXOR FAQs, Example project, etc**: www.exorint.com/support

4.5 Certifications

Exor is committed to delivering the highest standards of safety across all aspects of machine installation, ensuring reliability and protection in every environment. To guarantee compliance with international regulations and industry best practices, our products undergo rigorous testing and hold a comprehensive range of certifications, including CE, UL, DNV, ATEX, and more. These certifications confirm our dedication to quality, performance, and safety, making Exor a trusted choice for diverse applications in various industries. You can view the matrix of Devices and Certifications at the following link: www.exorint.com/products/certifications

IEC62443 Roadmap (TUV Sud)

- Apr 2025: Compliance 4.1
- Q3 2025: Compliance 4.2 (products based on iMX8 Only for 2025)
  - o eX700M, JSmart700M, eX200, MicroEdge Plus
- Q4 2025: Compliance 4.2 (product based on iMX6)
  - o MicroEdge Basic

Cyber Resilience Act (CRA)

Regulation (EU) 2024/2847 of the European Parliament and of the Council
Publication date: 20 Nov 2024
Date of entry into force: 11 Dec 2027

From the initial analysis, it appears that all products placed on the market before 11/12/2027 are subject to the requirements of the regulation only if a substantial modification is foreseen for them starting from that date. They are, however, subject to the obligations referred to in Article 14 (various reports to be made to the designated national CSIRT and

ENISA), the entry into force of which is scheduled for 11/09/2026. The obligation to comply with the CRA remains for new devices placed on the market after the date of 11/12/2027. However, some devices manufactured by Exor International S.p.A. will be certified according to the IEC 62443-4-2 standard, and considering the requirements of this standard and those specified in Annex I (ESSENTIAL CYBERSECURITY REQUIREMENTS) Part I (Cybersecurity requirements relating to the properties of products with digital elements) and Part II (Vulnerability handling requirements) of the CRA, we can declare future compliance with the European regulation.

Network and Information Security Directive 2 (NIS2)

Legislative Decree 04/09/2024, n. 138
Reception of Directive (EU) 2022/2555, concerning measures for a high common level of cybersecurity within the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

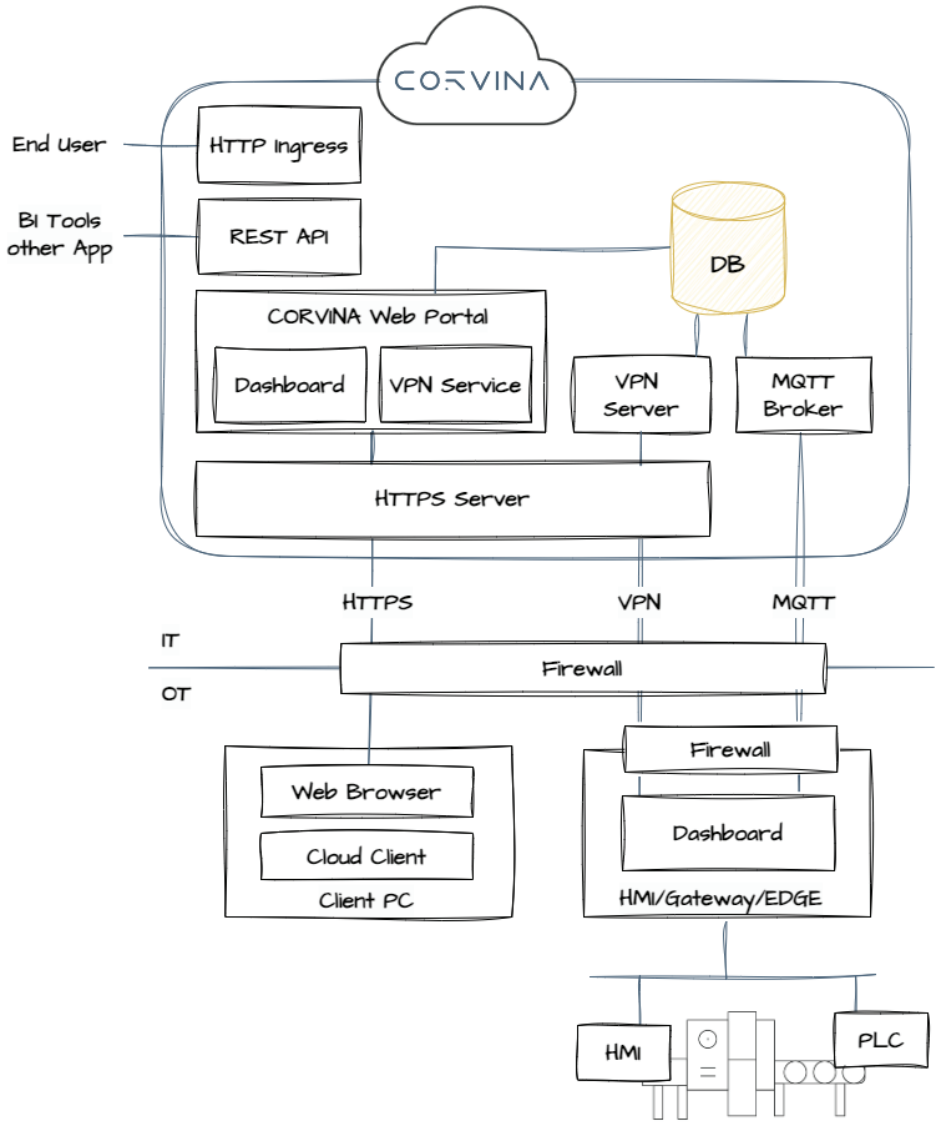
With this legislative decree, Italy has transposed into national law Directive (EU) 2022/2555 (NIS 2), which aims to ensure an increase in the common level of cybersecurity by harmonizing the rules applicable to various operators in different Member States and strengthening the standard security levels compared to those provided by the current regulations. In Italy, the National Cybersecurity Agency (ACN) has been designated as the competent NIS authority, tasked with overseeing the implementation and enforcement of the decree. By April 2025, the ACN will regulate, through its own determination, the basic obligations of Article 25 (obligations regarding incident notification) of the decree. Regarding these obligations, entities that fall under one of the sectors/subsectors/types defined by NIS 2 are required to register on the designated software platform by February 28, 2025. After reviewing the registrations, ACN will create the list of NIS entities by mid-April 2025, providing confirmation or exclusion notifications to the registered companies. By January 2026, the confirmed NIS entities must comply with the basic incident notification obligations, and by October 2026, they will have to meet the basic cybersecurity obligations.

From the internal analysis conducted, Exor International, together with its subsidiaries Holdex S.r.l., Exor EMS S.r.l., and Corvina S.r.l., has registered on the designated platform, as it recognizes itself as a service provider with respect to Corvina S.r.l., which is among the essential entities listed in Annex I of the mentioned decree. The determinations from the competent authority are awaited.

5.0 Corvina

Corvina allows you to connect industrial devices (such as PLCs, sensors, actuators) to a centralized cloud-based system, allowing users to view and control data in real-time, perform remote maintenance, receive alarms and notifications in case of anomalies, and much more.

5.1 Corvina Architecture



Kubernetes Cluster

Corvina leverages Kubernetes to manage its microservices architecture. This is a strategic choice for modern, scalable applications. Corvina's platform is composed of numerous independent microservices, each handling a specific function within the overall platform (e.g., data collection, device management, user authentication, visualization, etc.). this allows to:

- **Enabled independent** development and deployment of microservices, accelerating release cycles and minimizing deployment risks.
- **Designed and implemented scalable microservices**, optimizing resource utilization and ensuring responsiveness under varying workloads.

- **Implemented fault isolation strategies**, significantly reducing the impact of individual service failures on overall platform stability.

In Corvina we leverage the power of Kubernetes and microservices to build a robust, scalable, and reliable platform for industrial market. This allows us to focus on delivering value to our customers while Kubernetes handles the complexities of managing the underlying infrastructure.

Time series database cluster

Machine data is efficiently collected and transmitted by connected devices (Edge/HMI) to Corvina via MQTT. Corvina stores this data in a time series database to provide users with rapid access to historical data. This allows for querying large time ranges in fast time and performing calculations like mean values with high efficiency. Furthermore, the database supports advanced data lifecycle management to optimize data storage and analysis.

5.2 Device and Corvina Communications

Rest API

Corvina Rest API is a programming interface (API) that allows developers to interact with the Corvina Cloud platform programmatically. By using the Corvina Rest API, you can access the platform's features, such as data collection and analysis, device monitoring and remote control, and integrate them into custom applications or existing systems.

In practice, the Corvina Rest API allows you to (as examples):

- **Read data**: retrieve data from connected devices, such as sensor values, machine states, process parameters, etc.
- **Write data**: send commands to devices to control them remotely, change settings, start or stop processes, etc.
- **Manage devices**: add new devices to the platform, configure settings, monitor connection status, etc.
- **Manage users**: create and manage user accounts, assign access permissions, etc.
- **Receive notifications** be notified in real-time of specific events, such as alarms, anomalies, or changes in device status.

To use it, you need a Corvina Cloud account and the appropriate authentication credentials.

MQTT broker services

Corvina's **MQTT broker service** is a critical component in the platform's **communication architecture**, providing reliable, efficient, and secure message transmission between devices and the central system.

The MQTT broker serve multiple key functions:

1. **Pushing Device Configurations**: The broker enables seamless configuration updates to devices in the field. By sending configuration messages, it ensures that devices are running the correct settings and parameters, allowing for easy device management and adjustments in real-time.
2. **Sending Commands for Data Transmission**: The MQTT broker facilitates the sending of commands to devices, instructing them to transmit data logs. This ensures that critical data is securely and efficiently transmitted to the central system for processing, analysis, and storage.
3. **Alarm Notifications**: The service also handles the transmission of alarm notifications, ensuring that if an issue or anomaly is detected, immediate alerts are sent to the appropriate parties. This real-time messaging capability enables rapid response times to prevent or mitigate problems.
4. **Updating Mapping Configurations**: The broker also supports the dynamic updating of Mapping Configurations. When changes are required, such as new device placements or re-mapping of the system's architecture, the broker ensures these changes are reflected across the relevant devices, ensuring consistency and accuracy.

Overall, Corvina's **MQTT broker service** plays a pivotal role in maintaining seamless communication, efficient data transmission, and real-time alerts, while ensuring compliance with regional data protection standards.

VPN servers

Corvina's geographically distributed VPN cluster are a vital component for providing secure, **high-performance, and reliable** remote access to the devices.

This architecture ensures that users around the world can efficiently monitor, manage, and control their industrial equipment, regardless of their location. The Configuration is transparent for the user as the connection of the device to the VPN Servers are automatically managed by Corvina. A lightweight VPN client running on your computer establishes a secure connection, enabling your PC to remotely manage your machines.

Remote Connection on HTTPS

Even if a computer doesn't have a VPN client installed, access to the machines or web-based controls is still possible. Corvina's Web Access feature allows this by routing machine data through the edge gateway. This gateway uses the existing VPN connection to communicate with the VPN server. The data is then securely streamed to the user's web browser via HTTPS or a secure WebSocket connection.

Corvina EDGE Manager (CEM) and Artifact Registry

CEM is an advanced **Edge and Industrial Fleet Management** solution designed to optimize the device lifecycle, covering provisioning, monitoring, updates, and security. Using a **software-defined approach**, CEM enables businesses to efficiently deploy, configure, and maintain large fleets of edge devices, **ensuring consistency, efficiency, and enterprise-grade security**. By treating device provisioning as code, CEM ensures repeatable, versioned, and trackable deployments, reducing manual intervention and errors. It supports **bulk over-the-air (OTA)** updates with flexible deployment strategies, ensuring minimal downtime and high cybersecurity standards.

The **Artifact Registry** securely stores containers, BSP (firmware), software packages, and configurations, providing verified, versioned artifacts for controlled and secure updates.
It integrates with **CI/CD pipelines**, ensuring only thoroughly tested software versions are deployed.

CEM automates the update process, reducing errors, streamlining operations, and minimizing downtime, all while maintaining software security on edge devices.
In summary, CEM simplifies edge device management, enhancing **security** and operational efficiency through **automated processes, version control, and continuous delivery practices**, ensuring that businesses can manage and scale their device fleets effectively.

5.3 Corvina Security Functions

Authentication

The initial login to Corvina utilizes Basic Authentication to verify user credentials securely. Upon successful authentication, users are granted a Bearer token, which serves as a secure access key for the duration of their session, ensuring seamless and protected interactions within the platform.

In Corvina, each user is uniquely identified by their email address, ensuring a distinct and secure login for every account. To enhance security, Corvina enforces strong password policies, requiring robust password strength to protect user credentials and prevent unauthorized access.

User Role Configuration

Corvina offers granular user and role management, which means you can precisely control access to your connected devices, applications and services. This is a crucial feature for security and efficient management, especially in industrial settings. Here's a breakdown of what it entails:

Granular User Management

- **Individual Accounts**: You must create individual accounts for each user who needs access to the Corvina platform. This ensures accountability and allows you to track user activity.
- **Access Control**: You can define what each user can see and do within the platform. This includes which devices they can access, which applications they can use, and what actions they can perform (e.g., monitoring, controlling, configuring).
- **Organization and Domain Structure**: Corvina allows you to organize users and devices into different organizations and domains (tenant). This is useful for managing access across different departments, locations, or clients.

Role-Based Access Control

- **Predefined Roles**: Corvina comes with predefined roles that have specific sets of permissions. Examples might include "Administrator," "Editor," or "Viewer."
- **Custom Roles**: You can also create custom roles to match your specific needs. This allows you to define very granular permissions for different user groups.
- **These permissions can grant full access to all devices**, limit access to specific ones or restrict certain device services.

Two Factor Authentication

Corvina's use of 2FA (Two-Factor Authentication) is a crucial security measure, especially in the context of industrial IoT where sensitive data and critical infrastructure are involved.

2FA adds an extra layer of security to the login process. Instead of just entering a username and password, users are required to provide a second form of verification.

This makes it much harder for unauthorized individuals to gain access, even if they have stolen or guessed a password.

Corvina supports the following services for 2FA:

- FreeOTP
- Google Authenticator
- Microsoft Authenticator

Audit Trail

Corvina's Audit Trail is a crucial feature for maintaining security, accountability, and compliance within your industrial operations. It meticulously logs and records user activities within the Corvina platform, providing a comprehensive history of events like login, logout, and any actions performed within the system. This includes changes to device configurations, user creation or modification, and any other modifications.

5.4 Communication

Corvina

- Corvina Changelog document the changes, updates, and bug fixes implemented in different versions of the Corvina software or platform. It's a valuable resource for users to understand what's new, improved, or fixed in each release.
- EU: app.corvina.io/changelog
- DE: app.corvina-de.io/changelog
- US: app.corvina-us.io/changelog

- Corvina Monitoring tool: is an internal service that provides status info about Corvina. These status pages communicate the current operational status of the service, informing users about any outages, disruptions, maintenance or unscheduled downtime via email notification.
- EU: corvina.instatus.com
- DE: corvina-de.instatus.com
- US: corvina-us.instatus.com

- Corvina Technical Support: support.corvina.io

- FAQs, Videos and more: corvina.io/support

5.5 Certifications

ISO27001 (TuV Sud)

2025: Certification for CORVINA s.r.l

Netrwork and Information Security Directive 2 (NIS2)

Legislative Decree 04/09/2024, n. 138
Reception of Directive (EU) 2022/2555, concerning measures for a high common level of cybersecurity within the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

With this legislative decree, Italy has transposed into national law Directive (EU) 2022/2555 (NIS 2), which aims to ensure an increase in the common level of cybersecurity by harmonizing the rules applicable to various operators in different Member States and strengthening the standard security levels compared to those provided by the current regulations.

In Italy, the National Cybersecurity Agency (ACN) has been designated as the competent NIS authority, tasked with overseeing the implementation and enforcement of the decree. By April 2025, the ACN will regulate, through its own determination, the basic obligations of Article 25 (obligations regarding incident notification) of the decree. Regarding these obligations, entities that fall under one of the sectors/subsectors/types defined by NIS 2 are required to register on the designated software platform by February 28, 2025. After reviewing the registrations, ACN will create the list of NIS entities by mid-April 2025, providing confirmation or exclusion notifications to the registered companies. By January 2026, the confirmed NIS entities must comply with the basic incident notification obligations, and by October 2026, they will have to meet the basic cybersecurity obligations.

From the internal analysis conducted, Exor International, together with its subsidiaries Holdex S.r.l., Exor EMS S.r.l., and Corvina S.r.l., has registered on the designated platform, as it recognizes itself as a service provider with respect to Corvina S.r.l., which is among the essential entities listed in Annex I of the mentioned decree. The determinations from the competent authority are awaited.

5.6 Technical and Organizational Measures

Security at Corvina relies on a combination of **technical and organizational measures** to protect your infrastructure and data. Technically, Corvina employs advanced tools like **encryption, firewalls, and intrusion detection systems,** along with **regular vulnerability assessments** and **access controls**.
Organizationally, clear **roles and responsibilities** are established, and **employee training and security audits** ensure compliance with industry standards and data protection regulations. This integrated approach offers **multi-layered protection** and ensures a secure and resilient environment.

Cluster information

Corvina is an independent **cloud cluster-based solution** designed for **global distribution** and is hosted exclusively on one of the top cloud providers, **Google Cloud Platform (GCP)**.
By leveraging **GCP's robust infrastructure**, Corvina ensures **high availability, scalability, and security**, meeting the most stringent **data center management and security standards**. Google Cloud's **state-of-the-art facilities and multi-layered security protocols** provide strong protection against cyber threats while ensuring compliance with international regulations.
In addition to this, Corvina utilizes **premium-quality networking**, minimizing exposure to the public internet. This approach enhances **network performance, reduces latency, and increases security, ensuring fast and reliable connectivity** for users worldwide.
By relying on **private, high-speed interconnections**, Corvina guarantees a **seamless, low-latency experience**, making it an optimal choice for businesses requiring a **secure and efficient cloud infrastructure**.

Cluster access

Only **authorized Corvina personnel**, including developers and administrators, have access to the servers, ensuring a high level of security and controlled management of the infrastructure.
Access is strictly regulated through **unique usernames and Google Authenticator-based multi-factor authentication (MFA)**, adding an extra layer of protection against unauthorized entry. This approach guarantees that only verified personnel can interact with the system, reducing the risk of security breaches.
Furthermore, all **access-related activities**—such as login attempts, configuration changes, and administrative actions—are **logged and audited in real time**.
These logs are continuously monitored and reviewed to detect any unusual activity, **ensuring full traceability and compliance** with industry best practices and security standards.
By implementing these strict access control measures, Corvina maintains a **secure and transparent operational environment**, protecting sensitive data and ensuring the integrity of its cloud infrastructure.

Service monitoring

Corvina's services are **continuously monitored** using a comprehensive system that combines **industry-standard and custom-built checks** to ensure performance, reliability, and security.
By analyzing **key internal metrics such as system health, resource usage, network performance, and security events, Corvina can detect and address issues proactively before they impact users.**
An automated alert system notifies relevant personnel in **real time ensuring rapid response and resolution**.
This **proactive monitoring approach** guarantees high availability, minimal downtime, and consistent service quality, making Corvina a secure, resilient, and efficient cloud solution for users worldwide

Server configuration

Corvina is a **flexible and scalable Software-Defined Infrastructure (SDI)** that enables seamless management of **compute, storage, networking, and security resources** through software, eliminating traditional hardware dependencies.
Its **replicability** makes it ideal for organizations looking to **deploy their own cloud-based infrastructure**, offering **a customizable and modular architecture** while ensuring high availability, security, and performance.
With automation, orchestration, and centralized management, Corvina supports rapid deployment, simplified maintenance, and seamless scalability, making it a **cost-effective solution for on-premises, hybrid, and fully managed cloud environments.**

Inter-Cluster service communications

Corvina cloud architecture operates within a secure, private internal network, **ensuring isolated communications** between servers, free from public internet exposure. This approach enhances **security, performance, and reliability, protecting against cyberattacks, data breaches, and unauthorized access.**
Utilizing private networking and dedicated communication channels, Corvina **ensures low-latency, high-speed data exchange, while minimizing risks.** With **strict access controls, encryption, and network segmentation, only authorized personnel** and services can interact within the infrastructure, aligning with industry standards and compliance, making Corvina a **trusted, resilient cloud solution for businesses.**

Privacy by design

Any change in data management, such as **software updates, subcontractor changes, or internal process adjustments, undergoes a Privacy Impact Assessment (PIA) to ensure data privacy is upheld**. The PIA evaluates potential risks and identifies impacts on sensitive data, allowing for appropriate **mitigation measures**.
For instance, software updates are assessed for potential vulnerabilities, subcontractor changes are reviewed to ensure compliance with privacy standards, and internal process adjustments are checked for alignment with data protection regulations.
This careful evaluation ensures that **data privacy** is always prioritized and that any changes do not compromise data security or confidentiality.

Data ownership

All personal and machine data stored or created in Corvina **remains your property**. Corvina guarantees that your data **will not be misused, distributed, or sold** in any way. It is securely stored with **advanced encryption and strict access controls**. Your data is handled with the utmost **confidentiality and integrity**, and Corvina will not share it with third parties without your consent, ensuring it remains protected and under your control.

Data retention

With an **active Corvina subscription**, your data never expires and remains accessible. If you choose to **delete your account**, your data will be retained for 6 months, during which you can request a **bulk download of your data**. After this period, your data **will be permanently deleted,** ensuring proper data management and compliance with privacy policies.

Data Encryption

HTTPS and MQTT connections in Corvina use **TLS 1.2 or higher for secure encryption**. Only **strong encryption algorithms** that support **Perfect Forward Secrecy (PFS)** are allowed, ensuring that past communications remain secure even if keys are compromised. Corvina utilizes **ECC and RSA keys** for encryption, offering high security with efficient performance. This approach guarantees that **all data transmissions are robustly protected against unauthorized access**.

Vulnerability scanning

Corvina Cloud Services undergo **continuous monitoring for vulnerabilities**, using a **combination of automated tools and manual audits** to detect potential security risks such as **software flaws, misconfigurations, and unauthorized access**. If a vulnerability is found, **automated alerts** notify the relevant teams **for quick resolution**, such as **patching or reconfiguring security settings**. This proactive approach ensures the cloud environment remains **secure and resilient**, safeguarding users' data and services against potential threats.

Penetration testing

The **Corvina platform undergoes continuous internal penetration testing** to proactively identify and address potential vulnerabilities. Security experts simulate real-world cyberattacks to assess the platform's defenses against both **external and internal threats**. Regular tests are followed by thorough analysis and **remediation** to fix any issues, including patching software and reinforcing access control. This ongoing process ensures that Corvina maintains a **robust, secure, and resilient platform**, meeting the **highest security standards** and offering users a trusted environment.

Incident notification

Impacted parties and users are **notified promptly** about a security incident via email (previous registration). We strive to be as transparent as possible in our communication.

Business continuity plan

A comprehensive plan is in place to ensure **business operations continue without interruption during man-made or natural events such as disasters, cyberattacks, or supply chain disruptions**. It includes disaster **recovery procedures, data backup strategies, and emergency protocols to maintain critical services.** The plan also defines team roles and responsibilities to quickly resume normal operations, **minimizing downtime, and protecting productivity and customer satisfaction**.

Brute force protection

Corvina **protects against brute-force attacks by blocking access after 10 failed login attempts**. The initial block lasts 1 minute, with the duration increasing incrementally after each subsequent failure. **This system prevents attackers from bypassing security** through repeated attempts. Additionally, **failed login events are logged and monitored**, and security teams are alerted if suspicious patterns are detected. This multi-layered defense ensures that user accounts and data remain secure from unauthorized access.

Audit trails

The Corvina Platform **provides device-specific and subscription-wide audit trails**, offering users a comprehensive record of all actions taken on the platform. **Device-specific trails** track individual device activities, while **subscription-wide trails** log events across the entire organization. These logs are **immutable and tamper-proof,** ensuring secure tracking for **security investigations**, **compliance**. By offering detailed tracking at both levels, **Corvina ensures transparency, accountability, and regulatory compliance**.

Security by design

The Corvina platform is secure by design, with **security requirements** established before development begins. These requirements must be met before any changes are deployed, ensuring that **security is prioritized in every stage of the development process**.

Staged deployment

We use distinct environments to ensure secure and stable code deployment:

- **Development**: Runs locally on developers' systems, allowing for code modifications and automated testing.
- **Testing**: Hosts completed features for rigorous manual testing to identify bugs and vulnerabilities.
- **Staging**: Mirrors the production environment, used for integration and stress testing to ensure code performs under load before deployment.
- **Production**: Once the changes pass the previous stages, they are deployed to production. This may be done gradually, starting with a small group of users and expanding over time to monitor for any issues.

This approach minimizes the risk of insecure or faulty code reaching production.

6 Summary

In today's hyper-connected industrial landscape, **security** is no longer an afterthought—it's the **foundation upon which successful operations are built**.
Holdex Group, in collaboration with Exor International and Corvina, delivers an **Industrial IoT platform designed with a security-first philosophy**, ensuring that your operations remain not only efficient but resilient against ever-evolving cyber threats.

Our **globally redundant infrastructure** is strengthened with **multi-layered security protocols**, offering **unmatched data protection** across all touchpoints. From **encrypted data streams to advanced threat detection**, we take a proactive approach in safeguarding your most valuable assets, ensuring that every transaction and piece of data remains secure. This commitment goes far beyond just meeting compliance; it's about **fostering trust, ensuring business continuity**, and protecting the integrity of your entire operation.

At Exor International and Corvina, **we understand that data is your most valuable asset**. That's **why security is deeply embedded in every layer of our solutions**—from initial design through to **continuous monitoring**. Our unwavering commitment to **robust security** provides you with the peace of mind to scale your operations confidently, knowing that your business is protected by the highest standards of **integrity, confidentiality, and resilience**.

EXOR International S.p.A.
Via Monte Fiorino, 9
37057 San Giovanni Lupatoto VR (Italy)
Mail: info.it@exorint.com
Website: www.exorint.com

CORVINA S.r.l.
Via Monte Fiorino, 13
37057 San Giovanni Lupatoto VR (Italy)
Mail: info@corvina.io
Website: corvina.io