

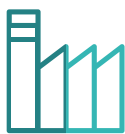


A secure Remote Access Platform made easy for industrial environments

WL Digital Doorman

Connecting manufacturing and critical infrastructures to the internet

In today's Industry 4.0 revolution, enterprises operating production lines and critical assets evolve in a fast-paced environment, where air-gapped systems which are typically isolated from unsecured networks are now connecting to the internet. The blending of physical and digital worlds has enabled innovative digital services with data playing a key role in driving efficiency and optimisation. As an essential part of the enterprise supply chain, suppliers are now given the opportunity to remotely access these critical infrastructures and maximise the Overall Equipment Effectiveness (OEE). However, providing this type of remote connectivity raises challenges about security and business continuity. It is essential to have the right tools in place to keep operations secure and prevent companies from being exposed to any unexpected events.



"NEVER TRUST, ALWAYS VERIFY" ACCESS TO YOUR CRITICAL ASSETS

Traditional VPN (virtual private network) connections for third-party vendors provide limited levels of security against cyberattacks, as granting potential full access to the company network expands the attack surface for hackers.

With WL Digital Doorman, sensitive industrial environments such as factories and other industrial sites can securely benefit from the new generation of digital services offered by suppliers. As a connectivity hub, WL Digital Doorman allows the production manager or plant IT to easily and securely manage all remote users of relevant critical systems, while keeping full transparency and control over the accessed data and machines.



TURN CYBERSECURITY RISKS INTO BUSINESS OPPORTUNITIES

Do you really know your vendors?

Do you really know what is being done remotely on your machines or with your data?

Are you concerned that your remote access solution compromises your corporate security policy?

Do you think securing remote access is complex and time-consuming?

Are you struggling to keep up with the fast pace of change?

If any of the above concerns apply to your business, WL Digital Doorman could be the ideal solution to enhancing the efficiency of your IT security by providing full transparency as well as control of remote machine actions.



PROVIDING A RICH SET OF SERVICES TO CONTROL ANY REMOTE CONNECTIVITY

WL Digital Doorman is a unique offering which enables multiple security-enhancing use scenarios.

Fast connect

Connecting any machine to known suppliers is fast and straight forward.

Authorise

Fine-grained access control policies by local IT for each supplier and abstraction of security network parameters.

Collaborate

Seamless collaboration between local maintenance and remote technicians.

Audit

Audit Trail features provide full insight into data flows and user credentials to local IT.

Red button

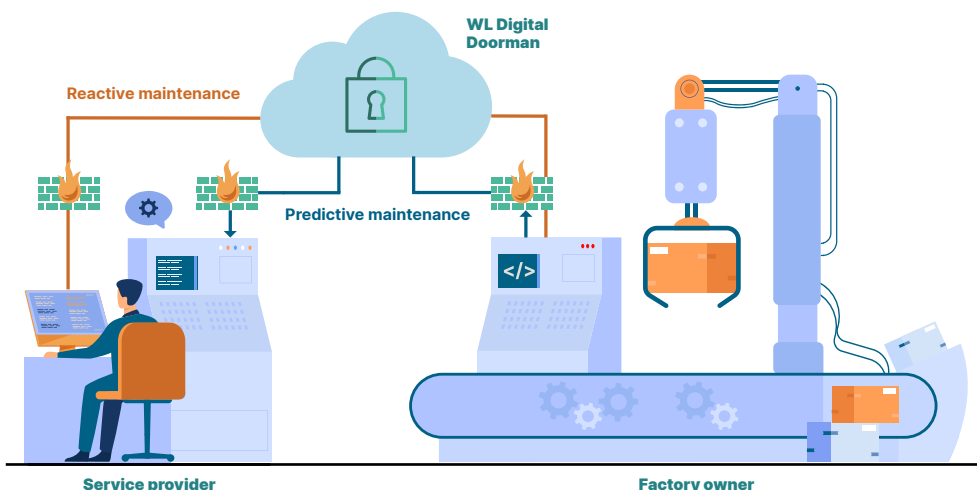
Instant blocking by local IT in case of data infringement.

Integration

Connect without coding

Flexible APIs to integrate Enterprise IT & IoT/Data Analytics platform

Supports also RDP, VNC, HTTPS, File Update & TeamViewer





The highest level of cybersecurity with the least effort.

State-of-the-art security mechanisms form the foundation of WL Digital Doorman.

The solution, compliant with the ISA/IEC 62443* standards, follows Zero Trust principles to protect industrial environments against cybersecurity threats and ensure business continuity. While doing so, it solves multiple challenges that industrial plants and critical infrastructures face today, and even more so in the coming years:

- Removing the complexity of setting up a remote secure data tunnel without the need for IT experts to do so.
- Decreasing the attack surface with no extra routes to maintain.
- Enabling the right individuals to access the right resources at the right times for the right reasons.
- Providing full transparency on sessions carried out with the integrated audit trail.
- Reducing operational costs significantly due to the improved processes.
- Optimising maintenance with faster diagnosis and repair while reducing travel costs.

** The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), provide a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACS).*

PROVEN TRACK RECORD

Developed for over a decade to meet the highest security and machine management expectations of our industrial customers.

15+

years

600K+

machines connected

190

countries

20M

remote sessions/month

25TB+

telemetry data/month

30K+

users

5M+

user access/month

8TB+

downloaded machine data/month

About Worldline

Worldline [Euronext: WLN] is the European leader in the payments and transactional services industry and #4 player worldwide. With its global reach and its commitment to innovation, Worldline is the technology partner of choice for merchants, banks and third-party acquirers as well as public transport operators, government agencies and industrial companies in all sectors. Powered by over 20,000 employees in more than 50 countries, Worldline provides its clients with sustainable, trusted and secure solutions across the payment value chain, fostering their business growth wherever they are. Services offered by Worldline in the areas of Merchant Services; Terminals, Solutions & Services; Financial Services and Mobility & e-Transactional Services include domestic and cross-border commercial acquiring, both in-store and online, highly-secure payment transaction processing, a broad portfolio of payment terminals as well as e-ticketing and digital services in the industrial environment. In 2020 Worldline generated a proforma revenue of 4.8 billion euros.

worldline.com



For further information
WL-marketing@worldline.com



Worldline is a registered trademark
of Worldline SA. August 2021
© 2021 Worldline.