

Securing the digitally connected processing floor

JBT Marel
Software

Digital systems are bringing food processors incredible opportunities to improve yields and operational oversight. But, the shift away from manual and paper-based systems also means processors have to think about security in a new way, one that goes beyond the physical processing environment and into the cyber environment.

The age of cyber security

Processors stepping into or developing digital systems must examine the safety and continuity of data, and choose a digital partner that protects businesses, supply chains, and customers from unnecessary risks.

JBT Marel Software's AXIN Solutions portfolio connects machine, process, and business level data to provide insight and oversight of operations not possible with only manual monitoring. It helps food processors of any size meet industry challenges and remain competitive by making more from raw materials, keeping lines flexible, and meeting increasingly stringent regulatory compliance needs.

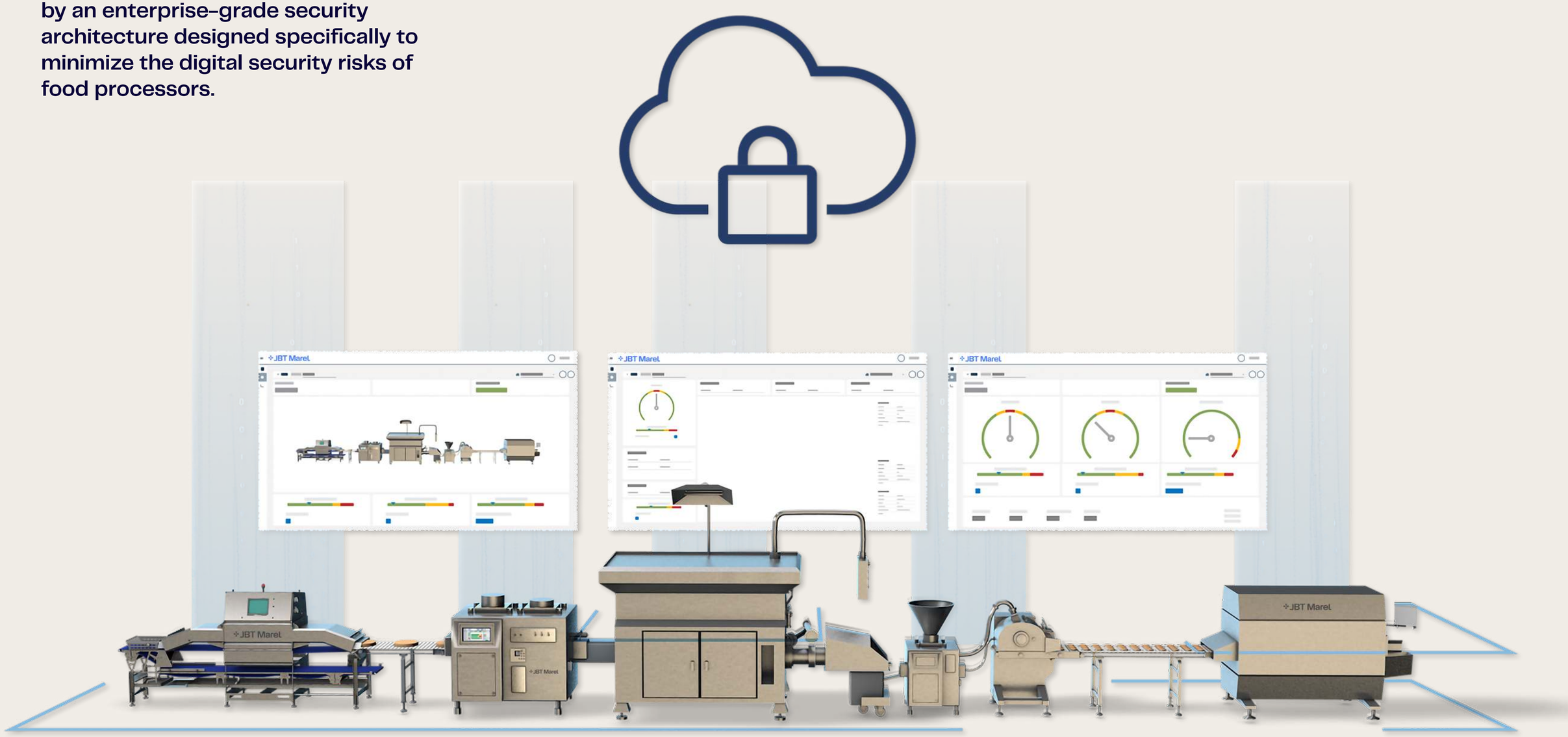
The rise of digital connectivity has come with the rise of cyber-attacks. To keep operations safe, food processors should feel confident in the security of the systems invested in, checking providers meet global cyber security regulations and guidelines, keep your data within your control, and ensure data remain secure as digital environments and your businesses evolve.

Digital connections on the processing floor

Digital systems at a machine level provide processors with access to information about machine health and performance, which extends operational uptime and equipment lifetimes, and lowers cost of ownership.

AXIN Machine Solutions is JBT Marel Software's brand for machine-level digital connectivity. Powered by AXIN Machine Solutions, Connected Services links machine data and consultancy tools and service to deliver coordinated planning, proactive maintenance, and responsive support that enables continuous improvement of operations.

AXIN Machine Solutions and Connected Services are underpinned by an enterprise-grade security architecture designed specifically to minimize the digital security risks of food processors.



Data discretion for data security

Embedded into each JBT Marel machine with AXIN Machine Solutions is a digital engine that links machine, process and production data to the JBT Marel Cloud. Data is referenced and separated into a discreet customer database.

When considering data security, knowing what information is not collected is just as important as what is collected. No personally sensitive information, including personally identifiable information, financial or recipes, is collected, stored, or accessible on the JBT Marel Cloud. This ensures processors gain the benefits of a digital connection, without risking the safety of employees, customers, suppliers, or businesses.

Data sent to the JBT Marel Cloud remains within a customer-specific environment on the server and is not accessible to our service layer without clear separation and agreement.

The importance of isolation

Isolating digital systems works the way walls in a house do. It creates a barrier between one data ‘room’ and another, mitigating risk by limiting the attack surface. If a cyber–attack does occur, the malicious actor cannot move from one room to the other.

Isolation with a two–port network

A critical element of AXIN Machine Solutions security is physical and logical network separation.

Each digital engine (DE) operates with two separate network ports:

- **Port 1** – external – connects to the machine controller. Here, communication is restricted to the machine and its digital engine
- **Port 2** – internal – faces the customer network and cloud. This port permits only outbound connections it has initiated. Unsolicited inbound traffic from the internet is blocked by design

The digital engine can send information between the two ports, but it does not bridge them.
Because data has no way to travel back and forth between internal and external ports, the risk of a malicious actor entering from the internet or other external source and accessing the machine controller is significantly reduced.

The deliberate separation of internal and external networks means your machine controllers remain isolated from the internet, even while your performance data flows securely to the Cloud.

Looking both inward and outward

While collecting and storing data on an on-site hard drive may seem inherently more secure than a Cloud, in reality the risk profiles are just different.

For food processors, the security of an on-site hard drive is dependent on the quality of internal IT and physical security practices. Aging systems, no monitoring, and no offsite backups, are found in a large portion of food processing facilities today, and these are exactly the things ransomware groups target.

External parties are not the only security risk; breaches can also come from inside a business, accidentally or maliciously. For example, uploading a virus from a USB stick or poor log security with multiple people using the same details creates unnecessary risk to your digital system, data, and operations.

AXIN Machine Solutions aggregate logs of which user has accessed what and when. This provides evidence if an incident occurs – malicious or otherwise. With this detail, it is easy to see if a program or recipe has been changed and fix it before damage has been done to production. It also helps improve security by revealing where businesses may have access weaknesses.

The Cloud is structurally strong with enterprise-grade security by default. JBT Marel Cloud is hosted on Microsoft Azure, layering redundancy between Azure's standard infrastructure and our own resilient application architecture. In Cloud storage, identity and account management—weak passwords and misassigned permissions—become your biggest weakness.

JBT Marel Cloud services are certified to ISO/IEC 27001:2022, within the defined scope*. This certification demonstrates that our cloud-based systems meet rigorous security requirements and are continuously improved to stay ahead of evolving threats.

* The scope definition is: Delivery of the JBT Marel AXIN Cloud infrastructure and the applications hosted therein as part of the JBT Marel offering to support the AXIN-Cloud-enabled equipment, as defined by management and in accordance with the Statement of Applicability version 29-01-2024.

Good security comes from every side

Data security is achieved by both internal and external systems being robust, regularly reviewed, and, of course, having a software partner who can offer industry specific expertise to guide and support processors with best security practices.

For example, using multi-factor authentication (MFA), role-based access control (RBAC), and security awareness training for staff are three practices easy to implement that have a high impact on system security.

A digital partner gives you access to an IT team whose job is to keep on top of security; reviewing and implementing industry best practices, providing automatic updates and patches, continuous monitoring for breaches, and faster breach detection.

JBT Marel provides partnership, not just products. Our experts work with you from day one to design, advise, and implement digital security systems that meet your business's specific needs.

Protecting and function, the best in digital possibilities

Data is more than just security. When visible, it is the key to continuously improving operations. Which is why at JBT Marel we take both so seriously.

By enabling machines with AXIN Machines Solutions, we're ensuring processors can see information on the health, after performance and production of equipment. By building a Cloud product with security at its core, we're keeping our customer's digital data safe. When both are combined, processors have the insights and peace-of-mind to make strong data-driven decisions that drive a profitable, future-ready business.

JBT Marel
Software

SO26_015_EN_July