When Manufacturers Go Mobile:

Managing Devices, Apps and Documents
# When Manufacturers Go Mobile: Managing Devices, Apps and Documents

## Table of Contents

- The Common Manufacturing Scenario ........................................... 4
- Security and Compliance: Not Your Average Worker’s First Thought ........ 5
- There’s an App for That—or Just Create One ................................. 5
- What Mobility Means for IT ....................................................... 6
- Pulling It All Together .................................................................. 6
- Push Security to All Mobile Devices from a Single Console ............... 7
- Secure, Distribute and Manage All Mobile Apps .............................. 8
- Secure, Distribute and Control Documents on Mobile Devices ............ 8
- World’s Most Certified MDM Cloud Security ................................. 9
- Smartly Lead—Not Follow—Evolving Manufacturing Trends .............. 9
Mobile computing offers manufacturers many new ways to improve productivity and bottom line performance in every area of their business. Smartphones and tablets are becoming natural extensions to core operational systems, including ERP, CRM, BI, MES and WMS, as well as for logistics management, mobile procurement and financial applications. Stronger, more rugged devices are hitting the market for use in factories and harsh manufacturing environments. Most experts agree that the number of manufacturers adopting enterprise mobility is accelerating in the quest of improving costs, product development cycles, manufacturing throughput, supply chain efficiency and customer focus.

Transitioning to a mobile enterprise, however, brings its own set of challenges. Some are common to all organizations taken aback by the rapid emergence of mobility and BYOD; others are unique to manufacturing sectors, including Mill Products; High Tech; Oil, Gas and Chemicals; Aerospace and Defense; Industrial Machinery; Automotive; and Natural Resources.

The Common Manufacturing Scenario

Forrester Research shows that most manufacturing sectors lag other industries in adopting mobility, but the tide is turning. More companies are following the path of Arizona Chemical, the world’s leading bio-refiner of pine chemicals for the adhesives, tire and rubber, fuel additives, mining and oleochemicals markets.

A year ago, Arizona Chemical followed its sector’s “Fortress” grouping in Forrester’s Bring Your Own Technology (BYOT) adoption matrix, with mobility restricted to tightly-controlled, company-owned BlackBerry devices.

Employees began clamoring for IT to change the company-issued devices from BlackBerry to iPhones, iPads and Androids, so Arizona Chemical decided to conduct a practical cost/benefit trial. It also began to weigh the benefits of offering a Bring Your Own Device (BYOD) policy. Providing employees who are not eligible for a company-issued smartphone with the option to connect to corporate email, apps and mobile messaging would increase both productivity and satisfaction. It would also provide users who do receive a company phone the opportunity to select the devices that best meets their needs, and they wouldn’t have to carry both a corporate and personal device.

“Once we decided to make the switch to corporate iOS devices and present a BYOD option, several questions about how we would manage the new devices arose,” said Lars Leuchter, Director, Global IT Infrastructure Services. “How do we restrict usage? How do we ensure our intellectual property is not in danger?”

Company-owned devices may be easier to control, but with so many choices IT must be prepared to enforce security policies on multiple mobile platforms. The BYOD policies that thrive in other industries are gaining momentum in manufacturing as well.
Security and Compliance: Not Your Average Worker’s First Thought

Expanded mobility creates gaps in manufacturers’ information security and regulatory compliance programs. They need to be plugged. Sensitive information is more susceptible to being compromised if a mobile device is unsecured, lost or stolen. Web browsing and targeted mobile malware pose new risks, increasing security vulnerabilities.

The exposure of confidential customer data, product plans, undisclosed operational and financial data, intellectual property and trade secrets is at stake, as well as the higher risk of data breaches and financial penalties for non-conformance with governing regulations.

When it comes to being smartphone-savvy, curious and innovative, manufacturing workers are no different than those in other industries—as many companies learn to their surprise. Employees could be—and most likely are—using personal devices on the job undetected. Security is never their first thought, whether the mobility comes from a company-owned or personal device. IT needs visibility into what devices connect to the corporate network to even begin to investigate who, how and why. Only then can IT think about policies and tools to bring rogue devices into compliance with security and regulatory programs, or to block their access to the corporate network.

There’s an App for That—or Just Create One

Mobile apps for manufacturing are plentiful and cover nearly every area of business. At the very least, IT must manage trimmed-down mobile versions of familiar apps already supported for PCs and laptops. Each manufacturing sector is different, however, and companies getting the most out of mobility take the initiative to develop their own custom apps.

Manufacturers wearing the hat of an app developer can focus apps for specific users on specific devices for specific needs, which can make enterprise mobility all that more efficient and productive. Apps with simple user interfaces that require minimal effort to access or enter data not only can replace paper-based processes or more expensive computing equipment, but speed up decision making and information-driven tasks:

- A worker on the production floor can quickly check the ERP system for parts to avoid a shortage that would stop an assembly line.
- Inspectors and maintenance staff can document and upload work on the spot.
- Shipping and receiving can track up-to-the-minute information about the location and status of shipments, improving inbound and outbound supply chains.
- Sales reps can check production scheduling when negotiating with a customer from the office, the customer’s site or any other location.
Employees with mobile devices can act on information more quickly, so the accuracy of data is important. "The good news is that mobile workers are entering data on the spot, so hopefully that means it’s more accurate than if they are trying to read their notes and enter the information later—or when information is never entered in the first place," says Kimberly Knickle, practice director for IDC Manufacturing Insights.

**What Mobility Means for IT**

If not handled properly, enterprise mobility could suffocate a manufacturer’s IT department. Mobile device OS, security and application updates need to be frequently managed for each platform in use. “You’re going to have new devices that continually get updated,” says Jeffrey Hammond, principal analyst at Forrester. “There is a constant drumbeat of new device capability. There are more hardened devices, more smart sensors on factory floors. If you can’t move fast, your competitiveness will lag.” And whether apps are acquired through a vendor or developed in-house, IT should plan for multiple releases and version tracking.

**Pulling It All Together**

An entire new industry for Mobile Device Management (MDM) and Mobile Application Management (MAM) emerged to address the challenges surrounding mobile users, devices and applications. Offerings include both on-premises solutions and cloud services.

The drawbacks of on-premises solutions are no better for MDM and MAM than they are for other IT capabilities—in fact, they’re worse. In addition to the outlays for servers, software licensing and maintenance, and long implementation times, total cost of ownership (TCO) is driven up by the IT resource requirements to continually update the software and each mobile platform supported. This has led several vendors to offer a cloud service option—running the software themselves or through a third-party partner to tap into companies’ strategic shifts to cloud computing.

Arizona Chemical eliminated on-premises options after realizing that they would require $2-5K in additional hardware alone, extend their initial deployment time and require ongoing maintenance resources. The same is true for Eastman Chemical, a global specialty chemicals company, who didn’t want to spend time continually updating platforms for iOS, Android and Windows Phones. Both were among the latest manufacturers to choose the “pure cloud” MaaS360 solution from Fiberlink—joining the ranks of companies like Actuant, Briggs & Stratton, Fluor, General Motors, and Novelis. “To Fiberlink’s advantage, their sole focus on a cloud solution allows them to do a better job with it than vendors that offer both on-premises and cloud solutions,” said Eric Peterson, a systems associate and member of the IT team responsible for the mobility initiative at Eastman Chemical.
Analysts agree on the benefits of MaaS360’s pure cloud model:

“With a fully cloud-based product and a 30-day free trial, there is little reason not to try MaaS360 when deciding on an MDM vendor,” says InfoTech Research Group.

“We’re big fans of Fiberlink’s delivery model, product and pricing structure. Fiberlink can be up and running in a matter of minutes within an enterprise,” says the 451 Group.

“Fiberlink’s performance with clients is rated highly, as proven by excellent reference client feedback. Clients greatly appreciate its presales and postsales support, smooth and uneventful implementations, and technical assistance during installations. Smooth integration of MaaS360 with third-party cloud email services is commonly reported,” says Gartner.

Push Security to All Mobile Devices from a Single Console

A major reason why manufacturers have been laggards in adopting enterprise mobility is trepidation about information security. Security policies for mobile devices must be defined, implemented and enforced, while “best devices” will differ for front-office, back-office, supply chain and production applications, even in a non-BYOD environment. The more device types, operating systems and security updates that entails, the greater the support required of IT.

MaaS360 simplifies these tasks in a variety of ways, all of which make mobile security a much less formidable challenge. In fact, a 2012 Customer Experience Survey of MaaS360 users revealed security and compliance features to be their most important reason for choosing MaaS360 as their MDM solution.

**Feature 1:** Manufacturers have many options to build their security policies quickly by selecting their preferred passcode strength, levels of encryption, and information about devices they want to see. All devices and OS platforms are supported from a single console. All security options are already tested in the MaaS360 cloud. Once IT defines their choices, the system automatically implements them as part of device enrollment right over-the-air (OTA). Weeks of security set up and testing are reduced to minutes!

**Feature 2:** Frequent updates are made to the MaaS360 platform at Fiberlink and pushed to devices to ensure that the latest security features and corporate policies are enforced. Immediate support of major mobile OS releases is provided as soon as they are available. When users independently upgrade to a new OS release deemed too risky, network access can be automatically blocked, ensuring the manufacturer retains full control of security.

**Feature 3:** Instant discovery of all devices connecting to the corporate network. Unauthorized, jailbroken and rooted devices can be blocked until brought into compliance with a manufacturer’s corporate security policies and device feature restrictions.

**Feature 4:** Compliance rules engine and alerts give manufacturers complete visibility and control of devices, applications and documents over their entire lifecycles.

**Feature 5:** Manufacturers can perform selective and remote wipes of corporate data from devices that are unsecured, lost or stolen, while leaving personal data intact.
Secure, Distribute and Manage All Mobile Apps

MaaS360 simplifies mobile application management by delivering an easy-to-use enterprise app catalog with full operational and security lifecycle management of apps across mobile device platforms. “Our people especially like the MaaS360 app catalog because they no longer need to search and choose from 20 different apps that are basically all doing the same thing. From our expense management and CRM apps to independent apps from our preferred travel vendors, everything is immediately available in the app catalog once a new device is enrolled,” says Leuchter at Arizona Chemical.

Using the catalog, a manufacturer’s mobile workers can instantly view apps available to them, install apps, and be alerted to updates. IT manages and distributes apps from a secure web-based console where the manufacturer can see which users have downloaded and installed apps, and can enforce security policies defined for apps and data. Features include app lifecycle management with real-time inventory reports, app distribution and installation tracking, update publishing, and provisioning profile management.

As with mobile devices, manufacturers can set mobile app security policies with MaaS360, such as whitelisting required business apps, blacklisting disallowed apps, and limiting native apps that come with devices. The system also adds extra layers of security by authenticating users before installing the manufacturer’s downloads and reporting on app compliance events, as well as tracking remediation actions performed for any non-compliant devices.

MaaS360 Application Security is a solution that wraps a mobile app container around enterprise apps with full operational and security management. Available as a simple app wrapper or Software Development Kit (SDK), manufacturers can protect their sensitive data in mobile apps developed in-house. The app container enables authentication, authorization and device compliance checks before access is given. It provides enhanced data protection such as blocking copy and paste, and limiting backups. Real-time alerting of app compliance violations and automated enforcement actions can be configured. And it secures access to corporate data through an app-level VPN tunnel with no device VPN needed.

Secure, Distribute and Control Documents on Mobile Devices

The need to securely distribute corporate information to mobile employees has become essential for manufacturers. With MaaS360, it’s easy to set up and control how documents are distributed and managed, allowing employees to work on the go while protecting corporate information.

Manufacturers can provide access to business documents on mobile devices with total control. Each document can have its own security policy and be distributed to all users, groups, or individual devices, creating a highly personalized experience for each employee while enforcing device compliance. And with workgroup-oriented roles, it’s easy for Marketing, Sales, Product Development, Supply Chain, Manufacturing, Warehousing, Distribution and Finance to use MaaS360’s secure mobile document sharing capabilities with optimized workflows and reporting.
World’s Most Certified MDM Cloud Security

The same concerns about information security that delayed manufacturers’ adoption of mobility once applied to cloud computing as well. Fiberlink is one of the cloud leaders that changed those perceptions.

With a decade of experience, Fiberlink has been defining and delivering the rules of cloud security for years. “By committing to a pure cloud delivery model for MDM with MaaS360, Fiberlink strategically emphasized cloud infrastructure security from the start,” says Christopher Clark, President and COO.

This focus has led to Fiberlink’s leadership in MDM cloud security, as evidenced by MaaS360 being:

- The first and only MDM cloud with AICPA SOC-2 Type II certification (since 2007), validating MaaS360’s security, availability, processing integrity, confidentiality and privacy
- The first and only MDM cloud with authority to operate under the Federal Security Information Act (FISMA)—and Fiberlink being the first and only MDM cloud vendor certified for CyberScope data feeds to the Federal Government
- TRUSTe EU Safe Harbor certified for online privacy and trust in services in compliance with the Safe Harbor Framework developed by the U.S. Department of Commerce and the European Commission for the EU Directive on Data Protection
- The first and only MDM provider to be listed on the Cloud Security Alliance’s Security, Trust and Assurance Registry (CSA STAR), confirming the highest levels of security, transparency and reliability in the industry

Smartly Lead—Not Follow—Evolving Manufacturing Trends

Manufacturers today must lead in trends that result in faster innovation, productive customer engagements, operational efficiency, and bottom-line benefits—or they’ll be left behind. Recognizing that mobility provides new opportunities to achieve these goals is only the start. Mobile devices and the apps, data and business documents on them must be managed and controlled to reap the promised benefits while preserving information security. MaaS360 provides the easiest, fastest, and most secure platform for manufacturers to set up, evaluate and deploy MDM, MAM and Document Management. Based on the highly successful experiences of MaaS360 users across manufacturing sectors, enterprises can maintain information governance in the age of enterprise mobility with multiple types of devices whether owned by the company or employees.