A UNIFIED APPROACH TO RUGGED DEVICE MANAGEMENT

vmware® airwatch®

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The only thing growing faster today than the volume and variety of mobile devices is the expectation of users and lines of business. Mobility remains a top strategic opportunity, due to the potential to make an enterprise more competitive, whether by making employees more productive or engaging with customers in innovative ways. Today's users are accustomed to a consumer-like experience that is simple and convenient, and they expect to be able to work anywhere, at any time, and from any device. These growing expectations have increased the pressure on IT to deliver the same level of ease when working with corporate-owned devices purpose-built for business-critical operations. This includes ruggedized or enterprise handheld mobile computers designed to withstand harsh work environments such as a warehouse, manufacturing plant, oil rig, or hospital.

Creating a consumer-like experience for remote workers, outside the corporate office, has become more and more complex for organizations that continue to use multiple disconnected tools to manage various rugged deployments. To address these challenges, enterprise IT is shifting towards a unified endpoint management (UEM) approach. This approach for purpose-built deployments gives IT greater visibility, simplified management, increased security, and improved operational efficiency through combined management tools and processes. This whitepaper will delve into the evolution of rugged devices, the management challenges associated with such deployments, and how a UEM solution can address these challenges to enable a fully connected environment that is both manageable and secure.

THE RUGGED DEVICE INDUSTRY IS EVOLVING

Rugged devices, which includes semi- to fully ruggedized laptops, tablets, mobile computers, and handheld barcode scanners, are designed for large-scale business use and are optimized for entering data, navigating line-of-business applications, and interfacing with back-end systems. The ruggedness of a device describes its ability to operate in any exposed working condition for approximately three to five years. The three most common environmental specifications tested include temperature range, military standards, and IP rating. Such devices are typically shared by multiple employees working in shifts and can be found in all industries including healthcare, retail, warehousing, manufacturing, and transportation and logistics.

The rugged device industry is evolving and, in recent years, has seen considerable encroachment from consumer-grade devices thanks to their "curb appeal," increased affordability, popularity among workers, and the introduction of pseudo-rugged features such as water and dust resistance. However, truly ruggedized devices offer unprecedented functionality, performance, durability, connectivity, and cost efficiency across a variety of use cases and industries, as well as significantly lower failure rates and total-cost-of-ownership (TCO). This TCO advantage and the increasing selection of more user-friendly rugged devices have made this device type the most viable option for many enterprises — even those that are customer-facing or lack environmental requirements.

Traditional device manufacturers of ruggedized devices, include Zebra, which makes Symbol and Motorola mobile computers, printers, and scanners; Honeywell, which makes Intermec and LXE barcode scanners and mobile computers; Panasonic, which is best known for ruggedized tablets; Bluebird; and Sonim. Over the past ten years, Microsoft's Windows CE and Windows Embedded Handheld (WEH) 6.5 have been the most popular operating systems for rugged devices. This is due to the large selection of Windows devices and development tools. However, with Windows CE and WEH 6.5 quickly reaching their end of service, organizations have begun upgrading to WEH 8.1 or Windows 10 or, alternatively, migrating to iOS or Android. Android, in particular, has made significant strides when it comes to mission-critical line-of-business (LOB) applications. According to VDC Research, there is no quick or easy solution for migrating but, "doing nothing or pursuing the wrong option can result in performance issues, disruption to operations, and budget overruns[1]."

Historically, device management for purpose-built devices was built into the device. This forced enterprises to either manage a fleet comprised of devices from one manufacturer or administer multiple management systems. Fortunately, now companies can select which solution most effectively manages their deployment. Management solutions that decrease administrative support time and increase device uptime, such as streamlined provisioning and deployment, as well as remote configuration and troubleshooting are invaluable to any organization.

[1] VDC Research, Migrating Legacy Enterprise Mobile Applications, by David Krebs, 2015

TOP USE CASE SCENARIOS FOR RUGGED DEVICES

Rugged devices are most commonly found in healthcare, retail, and logistics, where organizations rely on these devices to improve customer or patient experience and boost operational efficiency and accuracy across the supply chain.

Healthcare
Improve patient safety, streamline clinical work-flow, and deliver patient-centered care

- A nurse scans a patient's ID bracelet with a handheld scanner and is immediately given access to the patient's latest care information, such as lab results and medication changes. This real-time information empowers the nurse to provide the best possible patient care.

- After a medical device is recalled by the FDA, administrative staff ensures none of the recalled devices are used during a patient procedure by quickly locating all recalled devices through their Unique Device Identifier (UDI) number.

- A phlebotomist utilizes a handheld mobile computer and portable printer to immediately label specimens as they are collected at the patient's bedside. Not only are these specimens accurately associated with the right patient, but the lab technician can also use a barcode scanner to easily track specimens throughout lab operations.

Warehousing, Manufacturing, Transportation and Logistics
Gain unprecedented visibility into goods, assets, and workers throughout the supply chain

- A logistics company uses sensors and smart software to monitor fleet vehicles in a variety of ways, from temperature (for vehicles transporting food or precious cargo) to real-time repair alerts. After a delivery truck driver gets an alert that part of his shipment is damaged, he uses his mobile computer to alert the warehouse, who then identifies the fastest way to get the rest of the shipment fulfilled.

- A warehouse drastically reduces picking errors and search time by equipping workers with wearable computers and ring-style scanners. These devices enable workers to scan materials, find them faster with digital navigation, and access context-sensitive information, hands-free. They also improve worker safety by eliminating the need for workers to hold a device or paperwork while handling materials in a potentially hazardous work environment.

- A manufacturing plant operator uses a ruggedized tablet to more effectively and efficiently monitor and repair plant equipment. The tablet enables the operator to act on critical information from control systems, access best-practice content, and collaborate with subject experts in remote locations.

Retail
Gain greater visibility and improve customer experience

- A sales associate at a home décor store assists a customer with a piece of furniture they wish to purchase on the show floor. The associate uses a handheld mobile device to locate the item in inventory, make the purchase, and schedule it for delivery to the customer's house.

- A clothing store uses in-store Bluetooth beacons, thermal sensors, and wireless access points to gain better insight into customer behavior. Each week, the store manager analyzes heat maps, highlighting traffic flow and footfall, to optimize store layout and determine which "low foot traffic" merchandise should go on sale.

- To improve customer satisfaction and inventory management, a retailer utilizes an array of purpose-built mobile computers, barcode scanners, and RFID products to gain accurate and real-time visibility into inventory and decrease the amount of out-of-stock merchandise.

RUGGED DEVICE MANAGEMENT CHALLENGES

While innovation in the rugged industry has driven device performance, connectivity, and usability, purpose-built devices still come with a host of unique management challenges and requirements.

Manageability

When devices are deployed outside of the corporate office, and away from IT, it is essential that enrollment and configuration be low-touch. Upon enrollment, device management of rugged devices in the field needs to be automated or remotely controlled. The ability to remotely manage and maintain as well as support and troubleshoot such devices significantly increases uptime and productivity.

Scalability

As businesses grow and initiatives change, deployments must be able to easily scale to support a growing and diverse fleet, as well as respond to market fluctuations in real-time. Multi-tenancy and scalability capabilities enable organizations to support tens of thousands of devices, regardless of device type, OS, or location.

Security

As the number of purpose-built endpoints increase and become more connected to the Internet and other enterprise systems, they also become more vulnerable to security attacks. Security vulnerability is a potential at every data access point which includes the device itself as well as its applications, services, and connected things. It is imperative that organizations safeguard corporate data at every layer with device restrictions, encryption, passcodes, data loss prevention (DLP) policies, and remote lock, wipe, and troubleshooting.

UNIFIED ENDPOINT MANAGEMENT FOR RUGGED DEVICES

According to Gartner, "The future of endpoint management lies in the consolidation of management tools that manage traditional PCs and mobile devices as a common management framework evolves across the two[2]."

With the proliferation of various endpoints in the enterprise, organizations have begun to reject the traditional bifurcated approach, to managing mobile devices and PCs, and demand a single management tool and process. A UEM approach is a holistic management framework that enables organizations to manage any endpoint to create a fully connected and secure IT environment. This approach is especially critical for purpose-built devices since they require low-touch enrollment, configuration, and application management.

Rapid Deployment and Provisioning

A UEM solution enables organizations to easily onboard devices with out-of-box enrollment options, such as barcode scanning or side loading. Upon enrollment, organizations gain immediate visibility into managed devices by enabling IT to track and collect critical information, such as system diagnostics, network information, certificates, internal and external apps, and IT-defined custom attributes. A UEM also supports an organization's device fleet as it grows and requires different devices and operating systems to fit the needs of varying use cases. In addition, it is able to support organizations maintaining their existing legacy platforms (such as Windows CE or WEH 6.5), migrating to next-generation platforms, or supporting a mix of both.

Device Security and Controls

A multi-layered approach to security encrypts sensitive company data and secures access from the user all the way to the network. A UEM solution enables IT to protect corporate data on ruggedized devices with granular device controls and policies, such as passcode complexity requirements and device encryption. Organizations are also able to restrict functionality on the device such as camera, screen capture, external storage usage, Bluetooth, device tethering and more to prevent data loss. A unified solution also supports advanced user authentication and automated compliance policies that streamline operations and reduce the need for manual intervention.

[2] Gartner, Inc., Mobile and Endpoint Strategies Primer for 2016, by Chris Silva, 2016

App Delivery and User Enablement

Line-of-business applications are an essential part of any organization. They are the tools that allow for the creation of content, processing of work, and serve as the conduit to business growth. In today's dynamic and fluid world, as organizations expand and evolve, so do their application requirements. Mission-critical applications on ruggedized devices need to be available at any time, on any device, and across any network.

A unified endpoint management solution supports the complete app lifecycle, including sourcing or developing, securely deploying, and analyzing metrics. Since employees leveraging rugged devices are typically working in shifts, many organizations configure a single device to be shared by multiple users. A UEM enables IT to customize device configuration by user through user authentication. Upon device check-out or authentication, specific applications and settings for that user are automatically and dynamically deployed to the device. Organizations also have the option to lock down a device to create a customer kiosk or only contain apps required for the job.

Remote Management and Control

Since remote workers do not have easy access to IT or spare devices, nothing is more important than reliable remote support. Remote management capabilities enable IT and support teams to easily remotely manage and maintain as well as support and troubleshoot business-critical devices that remote workers need to do their job, significantly increasing productivity and reducing downtime.

With remote management, a retailer with handheld scanners shared by shift workers, can silently update their inventory management application so workers have the information they need to maintain inventory accuracy. In another scenario, a cable company can provide immediate support to a field technician who is experiencing device issues while on-site with a customer. Tools that allow IT to remotely connect to devices in seconds with little lag time and instantly view device information, such as support session history, system diagnostics, network information, installed applications and profiles are critical.

Support for Industrial IoT Endpoints

In addition to traditional rugged devices, considerable investments in IoT have already been made in healthcare, warehouse management, manufacturing, transportation and logistics, and retail. Unlike standard mobile technologies, things – such as wearables, printers, smart AV, gateways, sensors, and beacons – have the ability to uniquely enable workers with business-critical data or apps in ways that used to be impossible.

For example, wearables are giving operations and field service workers the ability to perform tasks while simultaneously accessing information and applications hands-free. Wearable devices – such as smart watches and smart glasses – have proven particularly valuable across virtually every industry, with Salesforce predicting use of enterprise wearables, will more than triple over the next two years[3]. With these compelling use cases in mind, implementing smart glasses and augmented reality (AR) applications in the workplace will soon be a business imperative. A UEM solution enables organizations to make enterprise-IoT a reality by allowing them to securely manage anything and its data, alongside other purpose-built deployments.

VMWARE AIRWATCH UNIFIED ENDPOINT MANAGEMENT

The VMware AirWatch® Unified Endpoint Management platform provides a simple yet robust solution to manage and support semi- and fully ruggedized laptops, tablets, mobile computers, and handheld scanners. AirWatch has a long history of enabling customers to provision, stage and manage rugged devices, since its start in 2003. In 2013, AirWatch also acquired Motorola Solutions' Mobility Services Platform (MSP) solution and their best-in-class R&D team to further extend management capabilities for rugged devices. AirWatch delivers comprehensive support for purpose-built devices with rapid deployment and provisioning, comprehensive device security and controls, streamlined app delivery and user enablement, and remote management and control.

To learn more about VMware AirWatch® UEM for rugged devices, call +1 404.478.7500 or visit airwatch.com.

Customer Case Study:
The Home Depot

The Home Depot uses AirWatch to equip its employees with hundreds of thousands of ruggedized handheld computers with custom line-of-business apps that enable store associates to manage inventory, check product prices and availability, and complete transactions from anywhere in the store. In a matter of months, The Home Depot was able to deploy all their devices from a central staging facility, ship to hundreds of stores nationwide, and remotely custom-configure devices by store location.

SUMMARY

IDC Research projects that the US mobile worker population
will hit 105.4 million by the year 2020[4].

As the mobile industry evolves, the unprecedented functionality, performance, durability, connectivity, and cost efficiency of rugged devices continues to make them the best option for organizations that require corporate-owned and purpose-built tools for employees. However, such devices and the environments in which they are used often come with a host of unique management challenges and requirements. To address these challenges, enterprise IT can utilize a comprehensive unified endpoint management approach, such as the AirWatch UEM platform, to increase visibility and security, simplify management, and improve operational efficiency through combined management tools and processes. A UEM solution can help support a variety of new-generation and legacy devices and OSs, business-critical applications, and varying use cases across a variety of industries.

[4] IDC, U.S. Mobile Worker Population Forecast, 2016–2020, by Bryan Bassett, 2016