

The how and why of rugged device management



Great enterprises are often built on efficient employee networks. They act as the roots stabilizing the enterprises. So, it's obvious why providing suitable conditions for the efficient functioning of the workforce remains at the top of the enterprise priority list. And that's precisely where rugged devices and rugged device management play a significant role.

“

According to *reports*, the global market for Rugged Devices is estimated to reach US\$8 billion by 2027.

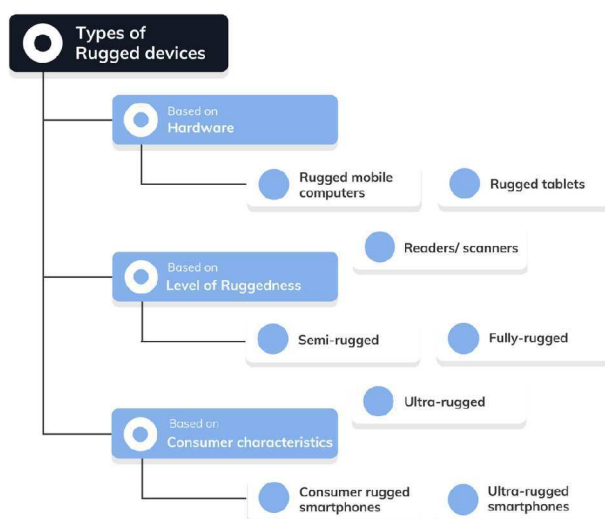
Workspaces have undergone major transformations from those well-defined spaces, hosting massive computers. We hardly find such bulky devices; laptops have replaced the desktop computers in offices, while in industries, ruggedized devices have substituted them all.

New entities in the enterprise world - Rugged devices

Rugged devices are being widely sought in the enterprise world. Its rigid nature and other advantages over consumer-grade devices have made it suitable for industrial use cases.

What are rugged devices?

Rugged devices are industry-grade devices equipped with all the functionalities of consumer devices and the added benefit of withstanding extreme conditions. These devices are built from the inside out to tolerate far more hazards than consumer devices. They can tolerate conditions ranging from extreme temperatures to wet or dusty environments. These can be further extended to include exposure to fluid contaminants and vibrations, which are often experienced by workers in industries like manufacturing, transportation, construction etc.



Some well-known vendors of rugged devices:

- Zebra Technologies
- Datalogic
- Getac
- Honeywell International
- Panasonic
- Kyocera
- Sonim
- Bullitt
- Urovo
- Bluebird
- Spectralink
- Armel
- Dell
- Lenovo
- Samsung

Addressing the myth- Why consumer devices with protective cases can't be called rugged?

Rugged devices are called rugged for a reason! There is a common misconception among industry outsiders to treat rugged devices as consumer devices with protective cases. Well, there are definitely many more aspects that need attribution for their ruggedness. These devices need to satisfy some quality criteria to gain entry into the rugged category.

These devices undergo rigorous testing. A US military standard- MIL-STD-810 is used to test whether these devices will remain operational under conditions like low pressure, high and low temperatures, temperature shocks, random vibration, humidity, rain etc. during their lifetime. These tests mainly aim to create an environment that simulates the same level of stress these devices will experience during their operational period.

For a handheld computer to qualify as a rugged device, five factors are taken into consideration. These include the outer shell, the keypad, the display, the internal components, and the accessories. Each of these shells serves specific purposes like preventing penetration by a certain extent of contaminants depending on the exposure of these surfaces.

Each of these shells carries Ingress protection (IP) consisting of two digits that denote their tolerance to substances. The first digit indicates protection against solid objects, while the second digit indicates its tolerance to liquids.

A “fully-rugged” device must have a minimum rating of IP54, which means it offers a tough layer of water protection and dust protection capable of preventing all minor interactions in a typical working environment from becoming a major challenge.

Essential aspects of rugged devices

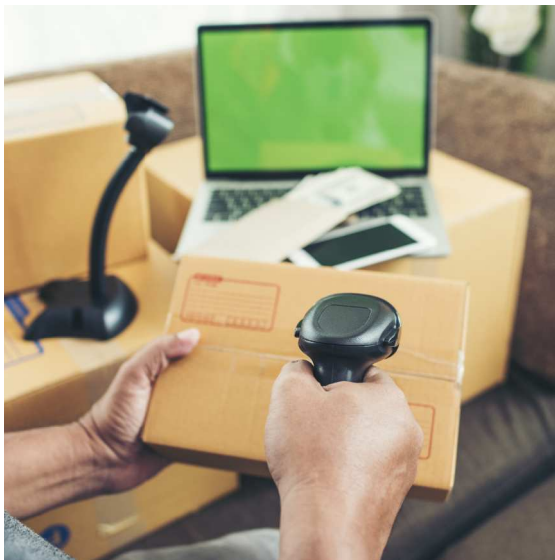
Rugged devices are best equipped with features for the efficient functioning of an enterprise workforce. They are built with an emphasis on aspects like:

- Capacity to tolerate the harshest weather and environmental conditions
- Higher battery life of over 30 hours or more
- Larger screens with better visibility
- Integrated with GPS, RFID, barcode readers, voice recorders, cameras and even industrial-grade miniature scan engines
- Have over the air data transmission capabilities
- Equipped with multi-touch capabilities

But, why a rugged device?

Rugged devices offer a lot of benefits compared to their consumer-grade counterparts. Some of these include:

Reduced total ownership cost



Rugged devices are often more expensive compared to consumer-grade devices. These devices, however, suffer fewer damages and other issues like breakages, thereby minimizing device support and repair costs. Further, as their longevity is also greater, less is spent on device replacement which is often more frequently required for consumer devices. So, in summing up, with rugged devices, businesses can save on support and repair costs in addition to recurring expenses resulting in a reduced total ownership cost compared to consumer devices.

Guaranteed performance even in harsh conditions

Rugged devices are designed to withstand harsh conditions. As these devices undergo rigorous testing, they perform well even in the most demanding working conditions. These devices are rated as per their effectiveness in tolerating harsh conditions, ensuring that they exhibit high performance in the conditions in which these devices are tailored to work.

High-performance processing

Rugged devices aren't just meant to withstand harsh conditions; in fact, they also have a much greater processing power. These can be particularly beneficial for companies that have specific programs or systems. As these devices can easily incorporate these programs, there is no need for employees to get used to different systems depending on the devices being used. Further, with reduced chances of devices crashing or running slow, customer satisfaction is also increased.

Greater durability

Rugged devices can be dropped, subjected to extreme temperatures and even submerged in water without damaging the device. Even though there is a limit to this, they are definitely far more durable than consumer devices.

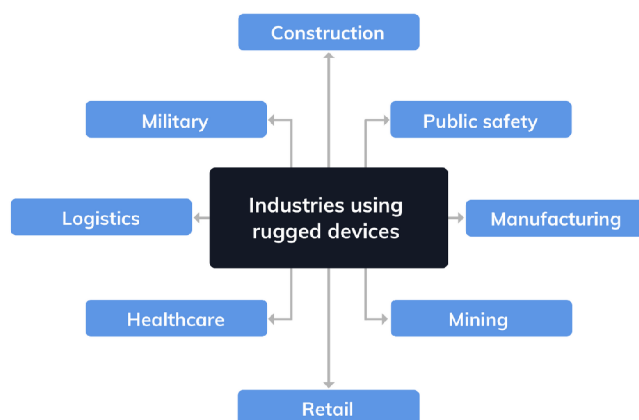
The typical lifespan of ruggedized handheld computers ranges from three to six years. Despite this, it's often found that these devices remain operational even after six years of around-the-clock usage. There have been many instances of these devices running strong even after 15 years of use.

Nearly zero downtime and enhanced employee productivity

Device downtime is one of the prime aspects leading to long-term losses for enterprises. With rugged devices, the chances of device failure are significantly reduced. Even if there arises a need for repair, its modular design greatly simplifies its repair process. With a high-performing system backing it, chances of the device running slower or crashing are further checked, reducing downtime to nearly zero.

Not just that, zero downtime has other perks as well. As there is reduced wastage of employee time due to device issues, they can focus more on things that matter, which implies a more productive workforce.

Usability features specifically built for industries



As rugged devices are specially built for enterprises, many additional features are beneficial for the workers. Some of these are:

- Sunlight readability feature for reducing the glare on the screen even when the device is under direct sunlight.
- It enables touch input with wet or gloved fingers.
- Highly tolerant to faults making it reliable.
- Focusing on usability aspects like providing docks for when tablets need placement on counters
- Integrated functionalities along with built-in support for peripheral features built-in for enterprise operations

Need for rugged device management

Though rugged devices are definitely rugged physically, it also has its less-rugged areas that need attention. Hence, consideration is needed before implementing these devices in an enterprise environment.

Security issues

Just like consumer devices, rugged devices also have a lot of security concerns. As these devices are often parts of enterprises, even slight negligence in security can have an ever-lasting impact. For ensuring security, it's often necessary to focus on different levels like device, data and network security.

Device-level

As rugged devices are often used outside the offices, keeping track of where and how the device is used is essential. So, a mechanism to keep track of the device needs to be implemented to eliminate the chances of the device being misused or misplaced.

Data security

Rugged devices being industry-specific requires data storage which is often critical to the organizations. If these devices fall into the wrong hands, they can be threatening for the organizations. Hence, implementing efficient mechanisms ensuring that data remains safe even if they fall into unsafe hands is essential.

Network levels

Unsecure networks are the root cause of most security vulnerabilities. When the mobility of devices increases, their chances of being subjected to networks outside the organizations also increase. Hence, it's crucial to either restrict these enterprise devices to networks that the organization trusts or ensure a VPN.

Issues due to legacy OS rugged devices

Cybercriminals are constantly on the lookout for vulnerabilities. This existing security threat is compounded if your company is using an outdated OS for rugged devices. Some of the primary reasons for this concern are as follows:

- No OS updates, which means no security patch protecting your device from attacks
- No OS-level encryption, which means unprotected data on devices
- Obsolete cryptographic methods which the hackers can crack easily
- No OS feature to prevent device misuses like remote lock or ring

Restricting device to a single or a set of applications



This is particularly important in industries where users in different shifts make use of the same device. This restricts the device to a single or a group of applications that the users require preventing chances of unauthorized access.

Need for remotely configuring settings and troubleshooting

As these are routinely used by employees who spend most of their time in fields, remotely configuring settings and troubleshooting are beneficial. A lot of time can be saved by automating enrollment and device provisioning and remotely configuring the required settings like apps, content, Wi-Fi, and VPN settings.

With remote troubleshooting in place, we can reduce device downtime by solving device issues in real-time and eliminating any need for commuting.

Need to manage devices of different operating systems

An industry may have devices with different operating systems depending on the environment where it's used, the time they acquired the device or the job requirements. So, a unified system capable of managing all these devices from a single console like [Hexnode](#) can be advantageous.

How Hexnode aids rugged device management

Even though many device management features target platforms like Android, it is often difficult to find features specifically designed for rugged devices. OEMConfig and Android enterprise recommended are two such management mechanisms that evolved for easier rugged device management.

OEMConfig

Android enterprise provides a set of features specific to **BYOD devices**, enabling those devices to accommodate both work and personal data while ensuring work-data security at the same time. While android enterprise provides a basic set of management APIs, with OEMs, it is further possible for enterprises to develop their own management strategies and implement them on top of that, incorporating features beyond the scope of UEMs.

UEM vendors had to manage devices by incorporating the APIs offered by device manufacturers into their UEMs. This used to be a complex process. However, with **OEMConfig**, the UEM vendors can now get all the required features without integrations, making the process a no-brainer.

Android Enterprise Recommended

Android Enterprise Recommended is Google's validation program to find out and deploy quality devices for the various enterprise use cases. Submitted devices often go through thorough examination like hardware, support for bulk or zero-touch deployment etc. Additionally, it ensures IP64 certification for rugged devices and delivery of security patches within 90 days of release for a minimum of 5 years for rugged devices.

Hexnode being an Android Enterprise EMM, provides device and app management solutions, device and work profile management, along with kiosk management features. It also offers many Android Enterprise Recommended features like transferring setup details via QR code, setting lock screen restrictions, and silently distributing work apps, among others.

Hexnode's multitude of features for easier rugged device management

Rapid deployment



Gone are the times when the IT department enrolled each device separately and deployed it. We are now in this zero-touch era where Hexnode has simplified the enrollment process, making it possible in a click with features like **ZTE**, **KME**, **Android ROM/OEM**, among others like **open**, **QR code**, **email** and **SMS** enrollment.

Device and data security

Enterprise device security is one of the prime focuses of enterprises at any level. With robust security features ranging from password policies and encryption mechanisms to aspects like forced compliance and root detections, Hexnode has got everything covered.

Endpoint management

With Hexnode, you can now manage the device throughout its lifecycle. With provision for application, network, content, kiosk and expense management, all the aspects of the devices can be easily managed from a single console.

Remote commands

Managing devices without actually touching the device is no more a distant dream. With Hexnode's features like screen sharing, remote view and control, we can quickly troubleshoot field devices in real-time and reduce the chances of device downtime. With commands like corporate wipe, we can easily wipe sensitive data in case of any device loss.