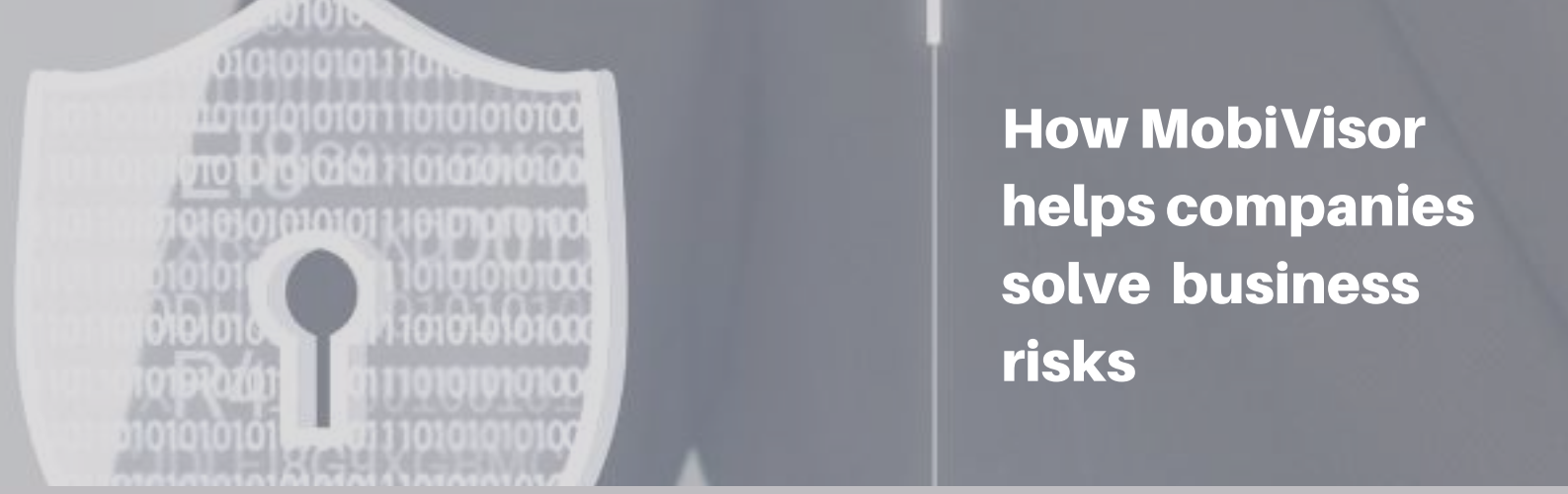
Risk Management with MOBIVISOR

Administering a business is accompanied by many different challenges. Now, risk management is not difficult anymore thanks to MobiVisor!



How MobiVisor helps companies solve business risks

RISKS

Security Breach

When an employee leaves the office with their device, this might give access to security breaches, data leakages, etc.

Lost Devices

The usage of mobile devices in public places poses the risk of these devices getting stolen.

Data Ownership

On accounts of the Bring Your Own Device method in workplaces, corporate data is held in the same device as the employee's private data. Private and corporate Data in the same place may be dangerous. For example, employees may accidentally compromise corporate information on their own devices, or an employee-owned device with corporate data might get lost or stolen, which then leads to data leakage.

Untrusted Mobile Devices

Using a device from a brand that is not really known well or with a model that is too old to be equipped with an MDM may create doubt among employees.

Untrusted Apps

Some well-known apps may seem reliable at first, but for company devices, they are quite unsuitable, since they are open to the public. Some have small advertisements that may be dangerous if you click on them – sometimes ad links can direct you to a page that asks for your private info to keep on shopping, stealing your private info. This way, corporate data might get stolen.

Open Wi-Fi Networks

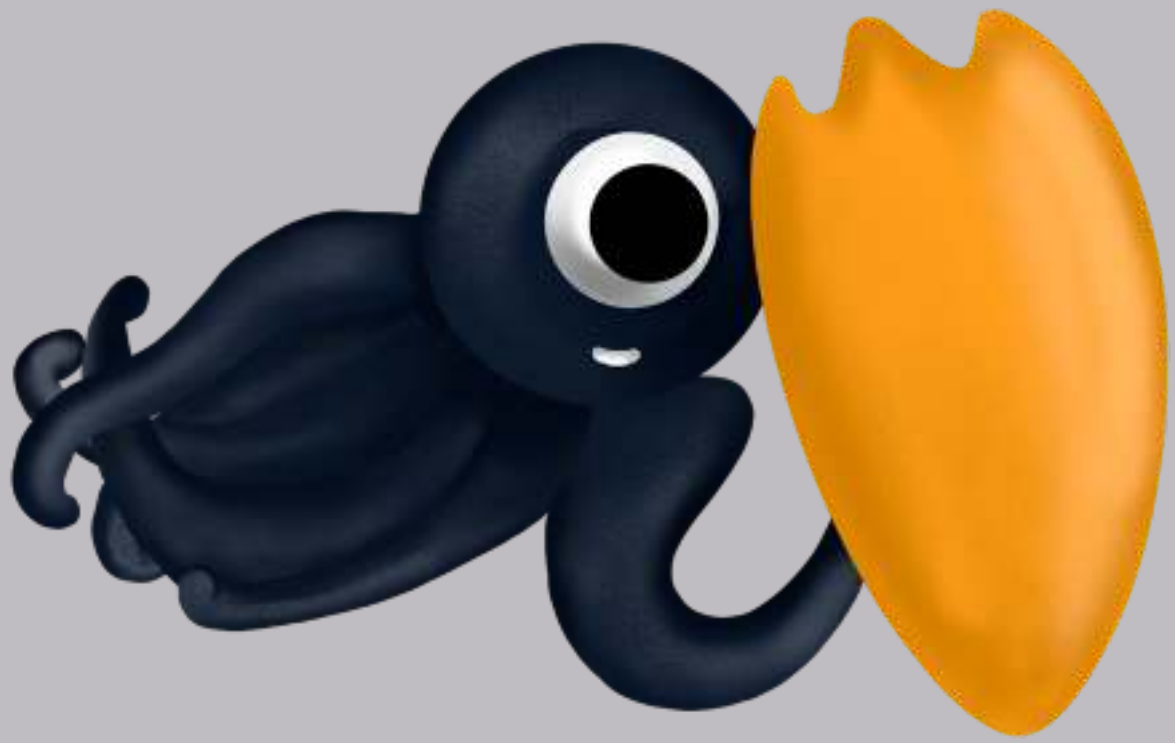
Connecting to a Wi-Fi connection that has no password or is used by everyone in the company building is harmful to important data. Common Wi-Fi for all includes the risks of theft of corporate data, cyber-attacks, malware distribution, and more.

Outdated Software

Old software lacks new improvements in security features and encryption from the manufacturer. If you are affected by a cyberattack, your device will be inefficient as it will slow down and not be able to fight viruses and attacks quicker than the attack's distribution velocity.

Phishing

Phishing is a cybercriminal's effort to acquire a victim's trust by convincing them to click a link or making them provide sensitive information. Phishers send emails that appear just like those from official banks or other well-known sources. They also create websites that resemble or replicate trusted sites.



SOLUTIONS WITH MOBIVISOR

Deactivating Access

Employers should put timed restrictions on access for out-of-office hours in order to prevent security breaches.

Passcode & Encryption

The MDM can enable complex passwords along with face-ID and touch-ID options that go beyond simple numeric passcodes to keep your device safe.

Isolation

Companies can isolate corporate data from private data by using a special cloud computing system. This way, company-related data can be backed up in a specific cloud with a special password.

Common Device

Determining a standard device like iPhone, iPad, Samsung, Casper,... for all employees is beneficial in terms of avoiding the challenges of any old or smuggled device.

App Monitoring:

With MobiVisor, you can update, delete or lock apps on your devices - Anything to do with control and management.

- Company-specific application catalog
- Update installed apps
- Individual permission and prohibition of apps
- Install and delete apps remotely
- App-protection through backups

Per-App-VPN

You define certain apps and Internet domains. When a defined app or domain is accessed, the VPN connection activates automatically and your data is protected.

Wi-Fi Monitoring:

MDM solutions enable administrators to change Wi-Fi settings and configurations on devices, to automatically connect devices to defined Wi-Fi networks, to prohibit users from connecting to illegitimate Wi-Fi networks and even to prevent them from turning off the Wi-Fi connection altogether.

Automated Updates:

MDM keeps your device updated instead of manually confirming updates according to employees' interests. Advancements in privacy policies and cybersecurity operations of the device will help you stay dynamic in case of any virus attack, or cyber damage.

Blocking Scam Numbers:

By blocking numbers such as the ones beginning with 0850, the MDM can trap advertiser-looking cyber trickers in workplaces. Additionally, MDM can provide special email servers for companies so that employees will not be subject to commercial fake emails whose goal is phishing.

Do you want to know more?

Do you have questions about how MobiVisor and our extensions work, or are you unsure whether MobiVisor MDM fits your company and its challenges?

We are happy to assist you with advice and support! Just contact us by phone or e-mail.
We would also be happy to arrange a personal presentation appointment with you and provide you with a test environment of MobiVisor without obligation.

Toni Voß
toni@iotiq.de
+49 1578 3020995

Saskia Riechers
saskia@iotiq.de
+49 176 1500 6080