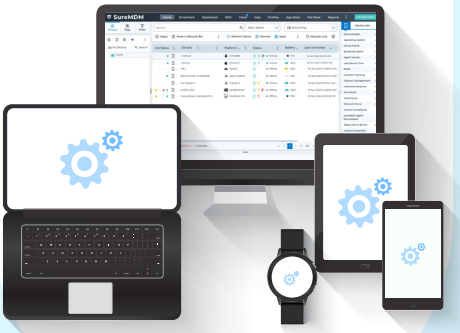
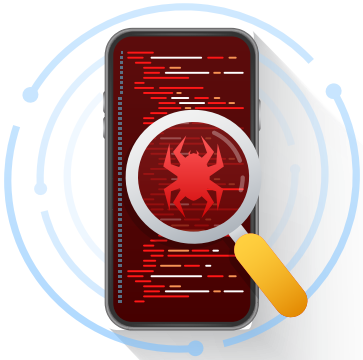
Risiken des Fehlens einer effizienten dedizierten MDM-Lösung

Mobile Device Management ist eine Softwareanwendung, mit der IT-Administratoren mobile Geräte aus der Ferne sichern, steuern und verwalten können. Mithilfe einer MDM-Lösung können Administratoren Geräte mit den erforderlichen Einstellungen und Anwendungen bereitstellen, verschiedene Richtlinien konfigurieren, Kioskfunktionen implementieren und die Leistung und Integrität der Geräte überwachen. Ohne Mobile Device Management (MDM) fällt es Unternehmen schwer, ihre Mobilgeräte zu verwalten und zu sichern. Dieser Mangel an Kontrolle kann sich auf die Produktivität, Sicherheit und Einhaltung von Branchenvorschriften auswirken.

Werfen wir einen detaillierten Blick auf die Risiken, die entstehen, wenn IT-Teams keine dedizierte MDM-Lösung einsetzen, im Gegensatz zu denen, die eine solche Lösung einsetzen:

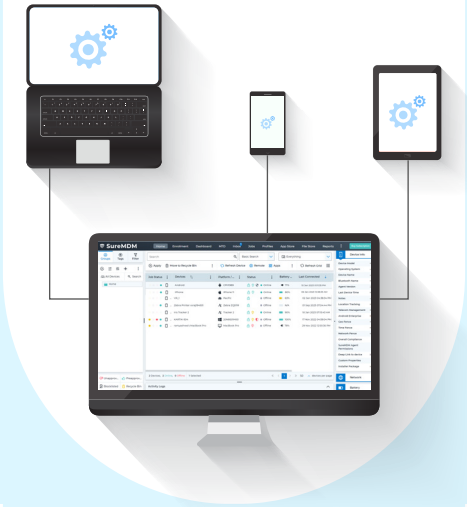
Risiken, die entstehen, wenn keine effiziente dedizierte MDM-Lösung vorhanden ist	Funktionen und Vorteile von SureMDM
Erhöhte MDM-Komplexität Verwenden Sie mehrere MDM-Lösungen, um unterschiedliche Gerätetypen zu verwalten? Die Bereitstellung unterschiedlicher Gerätetypen in unterschiedlichen Lösungen ist für IT-Teams mühsam und zeitaufwändig. Die Schulung und Wartung mehrerer Systeme können kostspielig sein.	 **Registrieren und konfigurieren Sie verschiedene Gerätetypen** wie Mobiltelefone, Tablets, PCs, Wearables, VR- und IoT-Geräte in SureMDM. Verwalten und überwachen Sie verschiedene Geräte von einer zentralen Konsole aus, um den IT-Aufwand und zusätzliche Kosten zu reduzieren.
Abgelenkte Mitarbeiter: Kosten in Milliardenhöhe **Mangelndes Engagement der Mitarbeiter führt zu einem jährlichen Produktivitätsverlust von $8,8 Billionen,** der größtenteils auf Gerätemissbrauch und unkontrollierte Internetnutzung zurückzuführen ist.	 Beschränken Sie den Benutzerzugriff **auf ausschließlich genehmigte Anwendungen und URLs** und verfolgen Sie Nutzungsmuster, um eine höhere Produktivität sicherzustellen.
Cyberbedrohungen (schädliche Apps und Phishing-Angriffe) CloudSEK stellte fest, dass 193 Apps im Google Play Store mit Malware infiziert waren. Ohne eine MDM-Lösung mit dem integrierten MTD (Mobile Threat Defense) sind Unternehmen anfällig für Cybersicherheitsbedrohungen und Datenlecks.	 **Scannen Sie mobile Anwendungen kontinuierlich** auf Malware und überprüfen Sie Links auf schädliche Fishing-URLs, um sich vor den neuesten Cyberangriffen zu schützen.

Risiken, die entstehen, wenn keine effiziente dedizierte MDM-Lösung vorhanden ist

Funktionen und Vorteile von SureMDM

Ungesicherter Zugriff und Netzwerkangriff

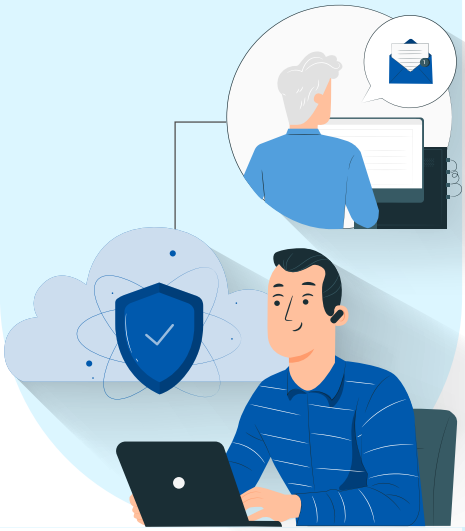
Über 50 % der Unternehmen sind anfällig für ungesicherte WLAN-Bedrohungen. Ungesicherter Fernzugriff und veraltete Schutzmaßnahmen machen Ihr Unternehmen anfällig für netzwerkbasierte Angriffe.



Konfigurieren Sie einen sicheren und bequemen Fernzugriff zwischen Unternehmensressourcen und verwalteten Geräten mithilfe einer in SureMDM integrierten Zero-Trust-Lösung.

Stillstand bei der Arbeit und Gemeinkosten

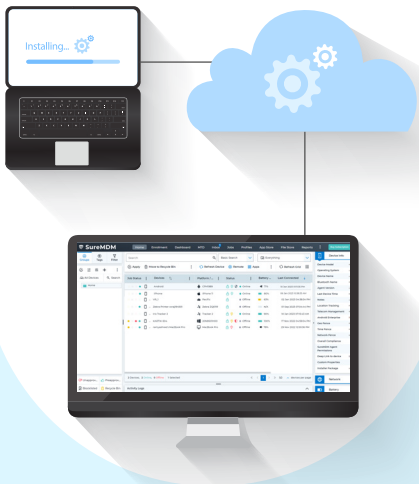
Betriebsstörungen oder Ausfallzeiten aufgrund von Gerätefehlern führen zu einer geringeren Produktivität und höheren Gemeinkosten. Darüber hinaus verursachen der Versand von Geräten und die Bereitstellung von Support vor Ort sowohl finanzielle als auch zeitliche Kosten.



Zeigen Sie das Gerät aus der Ferne an und steuern Sie es, um Probleme schnell zu lösen. So sparen Sie Versandkosten und Produktivitätsverluste.

Zeitaufwändige App-Verwaltung

Die manuelle Installation und Aktualisierung aller Geschäftsanwendungen auf mehreren Unternehmensgeräten ist sehr zeitaufwändig und wirkt sich negativ auf die Produktivität der IT-Teams aus.



Installieren, deinstallieren und aktualisieren Sie geschäftsbezogene Anwendungen aus der Ferne und verwalten Sie interne Apps nahtlos, um die Geschäftsbereitschaft sicherzustellen.

Risiken, die entstehen, wenn keine effiziente dedizierte MDM-Lösung vorhanden ist

Funktionen und Vorteile von SureMDM

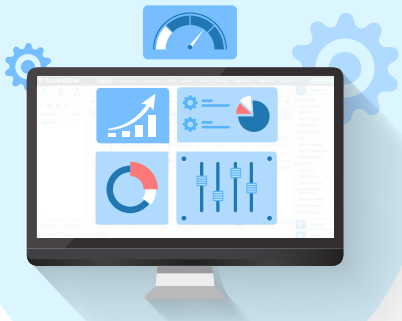
Verlorene Vermögenswerte, Lieferverzögerungen auf der letzten Meile

27% der Lieferkettenunternehmen gaben an, jedes Jahr 10% ihrer Geräte zu verlegen. Der Verlust von Geräten sowohl im Freien als auch in Innenräumen führt zu finanziellen Verlusten und Datenschutzverletzungen. Lieferungen auf der letzten Meile führen zu Zeitverschwendung und übermäßigen Kraftstoffkosten.

Lokalisieren Sie Ihre Vermögenswerte im Innen- und Außenbereich mit Echtzeit-Tracking. Erhalten Sie Einblicke in vergangene Routen und ermitteln Sie optimale Lieferwege, um pünktliche Lieferungen zu gewährleisten.

Eingeschränkte Sichtbarkeit des Gerätezustands

Schwachstellen bei der Überwachung des Gerätezustands und der Geräteleistung können zu potenziellen Geräteproblemen führen.



Erhalten Sie Echtzeiteinblicke in den Gerätestatus, die Integrität, Leistung und App-Nutzungsmuster usw., **um fundierte Entscheidungen zu treffen und die Leistung zu optimieren.**

Ineffiziente BYOD-Implementierung

Einem Bericht zufolge sind 63 % der Cybersicherheitsexperten besorgt über Datenlecks als ihr größtes Sicherheitsrisiko bei BYOD (Bring Your Own Device). BYOD bietet Komfort, wirft jedoch ernsthafte Bedenken hinsichtlich Datenschutzes und Sicherheit auf.

Verwalten Sie BYOD-Geräte effizient, indem Sie separate Container für arbeitsbezogene Anwendungen und Daten erstellen.

Risiken, die entstehen, wenn keine effiziente dedizierte MDM-Lösung vorhanden ist

Sicherheitsrisiken, versteckte Kosten

Die weltweiten Durchschnittskosten eines Datenschutzverstoßes beliefen sich im Jahr 2023 auf 4,45 Millionen US-Dollar, was einer Steigerung von 15 % innerhalb von drei Jahren entspricht. Ihr Unternehmen könnte potenziellen Sicherheitsrisiken ausgesetzt sein, wenn Geräte schwache Passwörter und Daten auf verlorenen Geräten haben, und mangelnde Kontrolle über die Firewall-Richtlinie und die Peripherieeinstellungen können zu potenziellen Sicherheitsrisiken führen.

Funktionen und Vorteile von SureMDM

Setzen Sie strenge Richtlinien wie komplexe Passwörter durch, und konfigurieren Sie Firewall- und Peripherieeinstellungen wie WLAN, mobilen Hotspot, GPS usw. Löschen Sie Unternehmensdaten auf verlorenen Geräten.