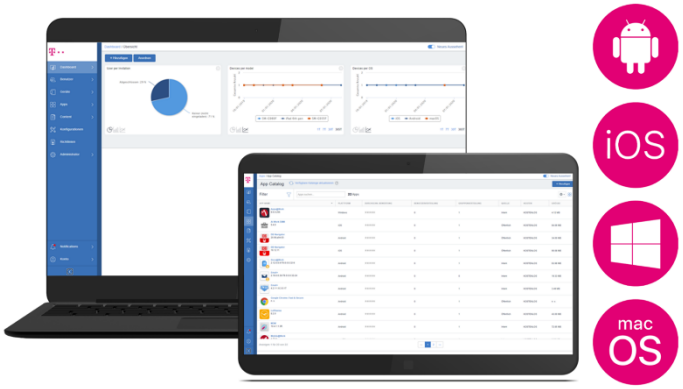
Wesentliche Funktionen von Unified Endpoint Management (UEM) im Überblick

Mobile Device Management und Mobile App Catalog

Schaffen Sie die Grundlagen des Unified Endpoint Management indem Sie mit Mobile Device Management Sicherheits- und Verwaltungsrichtlinien auch für Applikationen und Inhalte definieren.

Durch eine Verwaltungskonsole ist es möglich, verschiedene Konfigurationen für Endgeräte festzulegen. Bildschirmaufnahmen von internen Dokumenten und Applikationen können beispielsweise unterbunden werden. Bei Verlust oder Diebstahl können Geräte gesperrt werden.

Der App Catalog legt fest, welche Applikationen im Arbeitsumfeld genutzt werden dürfen auch in Bezug auf den Schutz von sensiblen Unternehmensdaten.



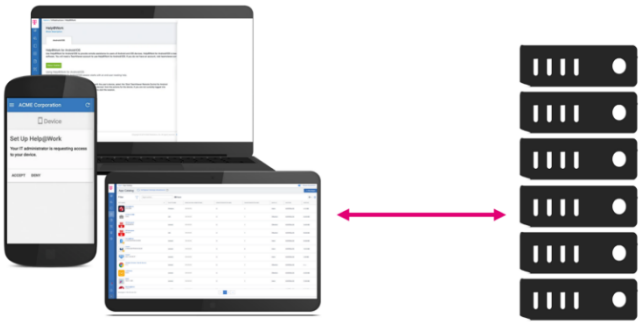
Desktop Management (ab Secure UEM)

Profitieren Sie nicht nur bei mobilen Endgeräten von den Vorteilen des Device Managements und managen sie zusätzlich auch Notebooks und Desktops mit MacOS oder Windows10.

Alles zentral und einheitlich mit einem System auf einer Plattform.

Unternehmensanbindung

Schützen Sie mit dem erweiterten Funktionsumfang in den Editionen Secure UEM und Secure UEM Premium Unternehmensdaten und persönliche Daten Ihrer Mitarbeiter und Kunden durch eine sichere Anbindung zwischen Ihrem Unternehmensnetz und den Endgeräten.



Eine Sentry (Gateway) verschlüsselt, verwaltet und sichert den Datenverkehr zwischen Endgeräten und Backend-Systemen im Unternehmen.

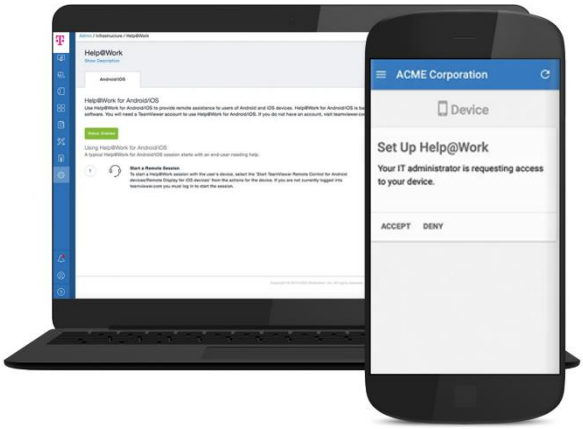
Ein LDAP Connector ist ein Gateway zur Anbindung an Unternehmensverzeichnisse zur Verwaltung und Authentifizierung der Nutzer. So werden beispielsweise E-Mails und E-Mail Anhänge, aber auch Zugriffe auf z.B. SAP oder SharePoint verschlüsselt und gesichert.

Produktivitätswerkzeuge

Mit den Editionen Secure UEM und Secure UEM Premium erhöhen Sie ihre Produktivität, indem sie Geschäftsprozesse mobilisieren. Grundlage hierfür bildet die Bereitstellung, Verteilung und Konfiguration von Applikationen sowie das rasche Lösen technischer Probleme.

Apps@Work

Der AppStore Apps@Work erleichtert die Verteilung und Konfiguration mobiler Applikationen. Unternehmenseigene Applikationen, beispielsweise zum Einreichen von Krankmeldungen oder Urlaubsanträge, können in einen AppCatalog aufgenommen und mit diesem verwaltet werden. So kann der Arbeitsalltag von Nutzern nachhaltig erleichtert werden.

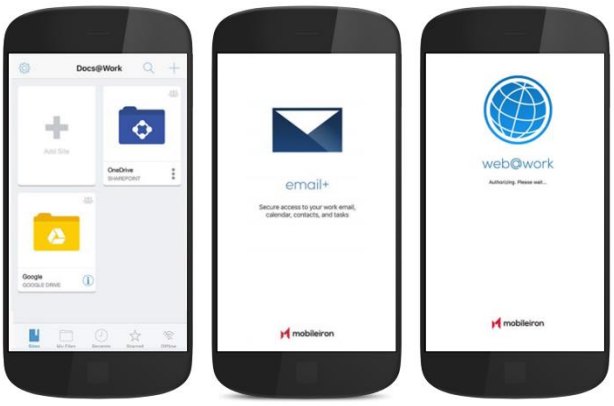


Help@Work

Sollten technische Probleme auftreten, ermöglicht die Help@Work Funktion Helpdesk-Mitarbeitern einen unkomplizierten Remote-Zugriff auf das Gerät. Das betroffene Gerät des Nutzers ist schnell wieder einsatzfähig.

Erweitere Produktivitätswerkzeuge

Unterstützen Sie Ihre Mitarbeiter mit Secure UEM Premium durch Applikationen die sowohl auf Produktivitätssteigerungen als auch Erhöhung der Sicherheit ausgelegt sind.



Docs@Work

Ermöglichen Sie eine sichere Zusammenarbeit: Mit Docs@Work können Nutzer sicher auf Inhalte aus Repositorien wie SharePoint, Box, Google Drive usw. zugreifen, diese erstellen, bearbeiten, markieren und gemeinsam nutzen.

Email+

Durch E-Mail+ bietet Unified Endpoint Management eine sichere Personal Information Management (PIM) – Applikation zum Zugriff auf E-Mail, Kontakte oder Kalender. Die Sicherheitskontrollen umfassen u. a. eine starke, für Verwaltungsbehörden geeignete Verschlüsselung. Email+ ist intuitiv aufgebaut, so dass die Produktivität des Nutzers nicht durch die Sicherheitsvorkehrungen beeinträchtigt wird.

Web@Work

Sicheres surfen sowohl im Internet als auch im Intranet.

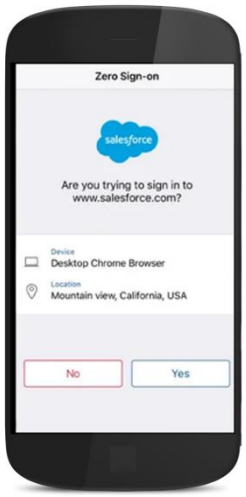
Erweiterte Sicherheitsfunktionen

AppConnect

AppConnect sorgt für eine sichere Trennung zwischen dienstlicher und privater Nutzung eines Gerätes, durch Kapselung von Applikationen in Containern. Im Container sind die Daten verschlüsselt und vor unberechtigtem Zugriff geschützt. Alle dienstlichen Container-Anwendungen sind untereinander verbunden. Auf diese Weise lassen sich Richtlinien, beispielsweise Single Sign-On und Dokumenten teilen.

Conditional Access

Conditional Access bietet den Nutzern einen sicheren Zugriff auf interne und externe Dienste (z.B. Box, Office 365, Salesforce). Der Zugriff wird nur gewährleistet, wenn der Nutzer autorisiert, das genutzte Endgerät richtlinienkonform ist und die Applikationen abgesichert bzw. für den Zugriff freigegeben sind. Der Access-Service unterstützt Single Sign-On (SSO), so dass der Nutzer sich nur einmal autorisieren muss, um Zugriff auf alle für ihn freigegebenen Clouddienste zu erhalten. Das Endgerät kann zusätzlich als Multi Faktor Authentifizierungsmethode bei anderen Diensten dienen.



Zero Sign-On (one)

Mit Zero Sign-On wird die Sicherheit des Zugriffs eines Clouddienstes noch einmal erhöht, da hier biometrische Merkmale des Nutzers, wie beispielweise ein Fingerabdruck oder Face-ID zur Autorisierung herangezogen werden. Die Eingabe eines Passwortes entfällt und es wird keine Angriffsfläche für einen Passwortdiebstahl geboten.

Tunnel

Ivanti Tunnel (AppTunnel) bietet sicheres Tunneling und Zugriffskontrolle, um übertragene Applikationsdaten zu kontrollieren und zu schützen, ohne dass dafür ein alle Applikationen umfassendes VPN benötigt wird. So ermöglicht AppTunnel granulare Sicherheit für jede einzelne Applikation, um jeden App-Container mit dem Unternehmensnetz zu verbinden.

Die Funktionen im Überblick

Mit Unified Endpoint Management (UEM) verwalten Sie über eine zentrale Plattform einfach eine Vielzahl unterschiedlicher Endgeräte wie Smartphones, Tablets, Notebooks und Desktops.

Transparent, effizient und sicher – für Endgeräte unter Android & iOS und jetzt auch für Windows 10 und macOS Rechner.

	UEM Classic	Secure UEM	Secure UEM Premium
Mobile Device Management	✓	✓	✓
Mobile App Catalogue	✓	✓	✓
Desktop Management	x	✓	✓
Sentry	✓	✓	✓
Apps@Work	✓	✓	✓
Help@Work	x	✓	✓
AppConnect	x	x	✓
Email+	x	x	✓
Docs@Work	x	x	✓
Web@Work	x	x	✓
Tunnel	x	x	✓
Conditional Access	x	x	✓
Zero Sign-On (one)	x	x	✓