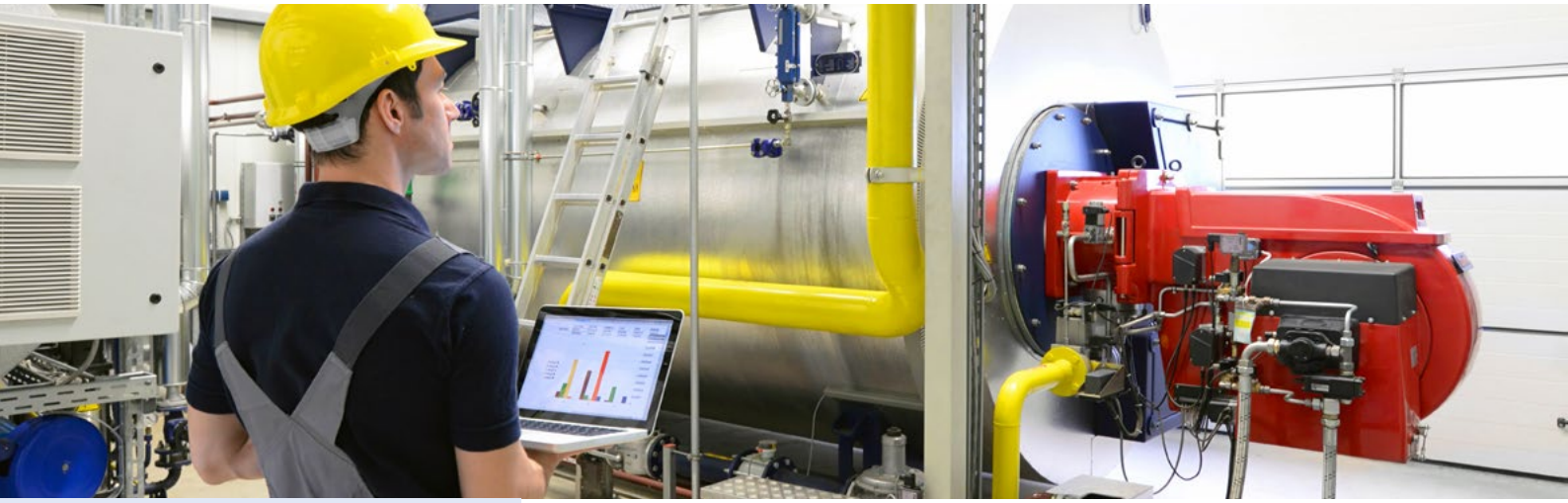
opentext™

Lösungsübersicht

Sicheres Device Management für das Internet of Things

Die Integration und Erweiterung von Geschäfts-anwendungen beginnt mit einem identitätszentrierten Fokus auf Menschen, Systeme und Geräte



31 Millionen verwaltete digitale Identitäten - bewährte Skalierbarkeit

Daten haben keinen Kompass - geben Sie Ihren IoT-Daten eine klare Richtung vor

Transparenz und dezidierte Geräteverwaltung für präzise Steuerung

Die Zahl der vernetzten Geräte wird bis 2025 weltweit wahrscheinlich 41,5 Milliarden übersteigen.[1] Damit verdoppelt sich die Zahl aus der ersten Schätzung für 2020.[2] Nach Ansicht von OpenText wird die Menge der Identitäten parallel dazu wachsen. Für einen Hersteller bedeutet ein vernetztes Produkt, ein besseres oder wertvolleres Gerät zu bauen und neue servicebasierte Umsatzmodelle zu erschließen. Für einen Eigentümer/ Betreiber bedeutet ein vernetztes Gerät die Verbesserung der betrieblichen Effizienz und der Services durch eine optimierte Nutzung.

Die Herausforderung besteht darin, vielen wichtigen Akteuren vertrauenswürdige Informationen zu liefern. Eigentümer und Betreiber von Produkt-Ecosystemen müssen ein Netzwerk von physischen Objekten schaffen und verwalten. Diese Objekte müssen sicher miteinander vernetzt und koordiniert sein. Sie müssen Daten sammeln und intelligent verteilen, um nützlich zu sein. Ohne eine sichere Geräteverwaltung sind die Daten des Internets of Things (IoT) und die darauf basierenden Prozesse gefährdet.

Führungskräfte wissen, dass die Vernetzung der unzähligen Menschen, Systeme und Geräte aus der Wertschöpfungskette eine sehr positive Wirkung haben kann. Sie

[1] Worldwide Global DataSphere IoT Device and Data Forecast, 2019-2023, May 2019.
[2] Gartner, Leading the IoT: Gartner Insights on How to Lead in a Connected World, 2017. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

opentext™

Ein digitaler Zwilling ist ein digitaler Repräsentant eines physischen Objekts, dargestellt als ein Software-Objekt, das die Eigenschaften und den Zustand eines eindeutigen physischen Objekts widerspiegelt.

wissen auch, dass das Zusammenstellen einer Lösung mit mehreren eigenständigen Komponenten oder der Aufbau einer Lösung selbst eine beträchtliche Menge an Zeit und Ressourcen erfordern würde. Dies würde oft mehr Zeit und Ressourcen in Anspruch nehmen, als sie tatsächlich aufbringen können und würde zu einer fehleranfälligen Lösung führen, die schwer zu verwalten und nicht leicht skalierbar ist.

Die Lösung besteht darin, dem IoT die gleiche Aufmerksamkeit und den gleichen Fokus zu widmen wie anderen Unternehmensanwendungen, die Innovationen vorantreiben und zeitnahe Geschäftsentscheidungen ermöglichen.

Ein vernetztes Ecosystem aus Menschen, Systemen und Geräten erfordert in jedem dieser Bereiche fundiertes Wissen und Expertise. Dazu gehört auch die Fähigkeit, eine Reihe von Komponenten zu erwerben, zu programmieren und zu warten. Genau wie Unternehmen haben Menschen, Anwendungen und Geräte ein breites Spektrum an Eigenschaften. Diese Einheiten und ihre Beziehungen müssen sorgsam verwaltet werden. Secure Device Management von OpenText standardisiert die Darstellung dieser Geräteidentitäten und stellt so sicher, dass die höchste Integritätsstufe skalierbar bleibt. Einheitliche Definitionen von Entitäten ermöglichen ein konsistentes Verhalten von Identitätsbeziehungen, Versionierung und Erweiterbarkeit.

OpenText: Den Informationsvorsprung nutzen

Als Grundlage einer digitalen Transformationsstrategie hilft das Enterprise Information Management (EIM), Informationen intern über Silos und Anwendungen hinweg zu konsolidieren und Prozesse von Anfang bis Ende zu digitalisieren. Prozesse lassen sich in einem Ecosystem mit digitalisierten Kunden leichter koordinieren und rationalisieren. In jeder Phase des Produkt-Lebenszyklus können Abläufe automatisiert und analysiert werden. Dies führt zu tieferen Einblicken, um die Effizienz und den Output sowie die Collaboration mit Kunden, Partnern und Lieferanten zu verbessern. Dank des „Information Advantage“ aus dem IoT können Unternehmen flexibel agieren, sich an Marktveränderungen anpassen und auf Wachstumschancen reagieren.

Cyber-Sicherheits-bedrohungen in verschiedenen Branchen durch die sichere Bereitstellung von Geräten verhindern

31+ Millionen digitale Identitäten bei bewährter Skalierbarkeit

OpenText, der Marktführer im Bereich EIM, ist bestens gerüstet, um mit der OpenText Internet of Things-Plattform Lösungen zu liefern, die das agile Unternehmen ermöglichen und stärken. Die OpenText IoT-Plattform verwaltet mehr als 31 Millionen digitale Identitäten und verfügt über eine nachgewiesene Skalierbarkeit. Sie bietet ein sicheres Gerätemanagement, das für die komplexen Ecosysteme von Menschen, Systemen und Geräten unerlässlich ist. Es ist dieser identitätszentrierte Ansatz für IoT und Secure Device Management, der die Erweiterung und Integration von Unternehmensanwendungen ermöglicht.

Daten haben keinen Kompass - geben Sie Ihren IoT-Daten eine klare Richtung vor

Die Verwaltung, Steuerung und Prüfung von Daten, insbesondere von IoT-Daten, ist nicht einfach. Doch der Einstieg kann durchaus gelingen. Mit Secure Device Management von OpenText können Sie Templates für Geräte, Ereignisse, Befehle und sogar ganze Lösungen erstellen. Diese digitalen Zwillinge physischer Objekte machen es einfach, kontextbezogene Daten zu visualisieren, unabhängig davon, wo sich das Gerät befindet. Die Templates erleichtern auch das schnelle Einbinden neuer Geräte und katalogisieren Attribute für die zukünftige Nutzung. So können Anwender ganze Lösungen auf der Grundlage früherer und bewährter Modelle erstellen.

opentext™

Gewinnen Sie Transparenz und eine dezidierte Geräteverwaltung für eine genauere Steuerung

Da IoT-Bereitstellungen von einfacher Überwachung und Fehlerwarnungen zu komplexeren und anspruchsvolleren Lösungen wie digitalen Zwillingen übergehen, müssen Unternehmen einen identitätsorientierten Ansatz verfolgen. Nur so kann sichergestellt werden, dass die Daten und Geräte nicht gefährdet sind. Wenn das IoT-Gerät nicht angemessen überprüft und verifiziert wird, könnte dies zu einem zu umfangreichen oder zu eingeschränkten Zugriff führen, die Integration behindern oder möglicherweise Daten oder das Gerät Cyberangriffen aussetzen.

Die OpenText IoT-Plattform ermöglicht eine granulare Steuerung von IoT-Geräten und -Daten, wenn neue Funktionen entwickelt und eingesetzt werden. Ein Beispiel hierfür ist die Entwicklung, der Betrieb und die Erweiterung eines gefertigten Produkts durch einen digitalen Zwilling. Wenn sich ein Produkt in der Entwurfsphase befindet, können die Daten gesammelt, verwaltet und analysiert werden. Diese delegierte Geräteverwaltung ermöglicht es, bestimmte Datenströme dorthin zu leiten, wo sie die erwarteten Ergebnisse liefern, ohne die Daten auf breiter Basis zu erweitern. Durch die klare Definition der IoT-Datenpfade des Produkts wird sichergestellt, dass der Datenzugriff nicht von Unbeteiligten als Rauschen oder als Sicherheitsrisiko betrachtet wird, das für nicht-qualifizierte Personen sichtbar ist.

Eine identitätszentrierte Plattform, die auf Sicherheit und Skalierbarkeit ausgelegt ist

Der identitätszentrierte Ansatz von OpenText für IoT macht diese IoT-Plattform einzigartig und bereit für die Integration mit Unternehmensanwendungen. Die OpenText IoT-Plattform verfügt über ausgereifte, sofort einsatzbereite Identitäts- und Zugriffsmanagement-Funktionen, die sonst von Grund auf neu erstellt werden müssten. Dies wäre mit einem hohen Entwicklungsaufwand verbunden und würde das IT-Budget strapazieren.

Möglich wird dies durch Beziehungs- und Lebenszyklusmanagement. Damit können Unternehmen alle Interaktionen über den gesamten Lebenszyklus von Menschen, Systemen und Geräten erfassen, authentifizieren und autorisieren. Die Fähigkeit, die Identität eines Geräts während seines gesamten Lebenszyklus zu verwalten, ist entscheidend für die Sicherheit im gesamten Ecosystem. Die Verwaltung der Beziehung, die ein Gerät mit irgendjemandem oder irgendetwas hat, macht die OpenText IoT-Plattform einzigartig. Sie ist in der Lage, IoT-Initiativen zu unterstützen, die ein Höchstmaß an Sicherheit erfordern.

Identity of Things kurz erklärt

Identity of Things (IDoT) ordnet Dingen, Geräten und Objekten eindeutige Identifikatoren und Metadaten zu.

Holen Sie sich den Leitfaden *Identity of Things Explained* und erfahren Sie mehr über das Identitätsproblem beim IoT und wie eine starke IDoT-Basis IoT-Verbindungen identifiziert und verwaltet, um dieses Problem zu beheben.

The Identity of Things (IDoT) erweitert das bisherige Identitäts- und Zugangsmanagement (IAM) für das Internet-Zeitalter. Es identifiziert alle IoT-Infrastrukturkomponenten, um eine sichere Verbindung und das Vertrauen in die Daten von IoT-Geräten zu gewährleisten.

Der Leitfaden gibt eine Einführung in das IDoT und verrät, wie man dem IoT eine Identität hinzufügt. Darunter finden Sie Kapitel zu den Themen

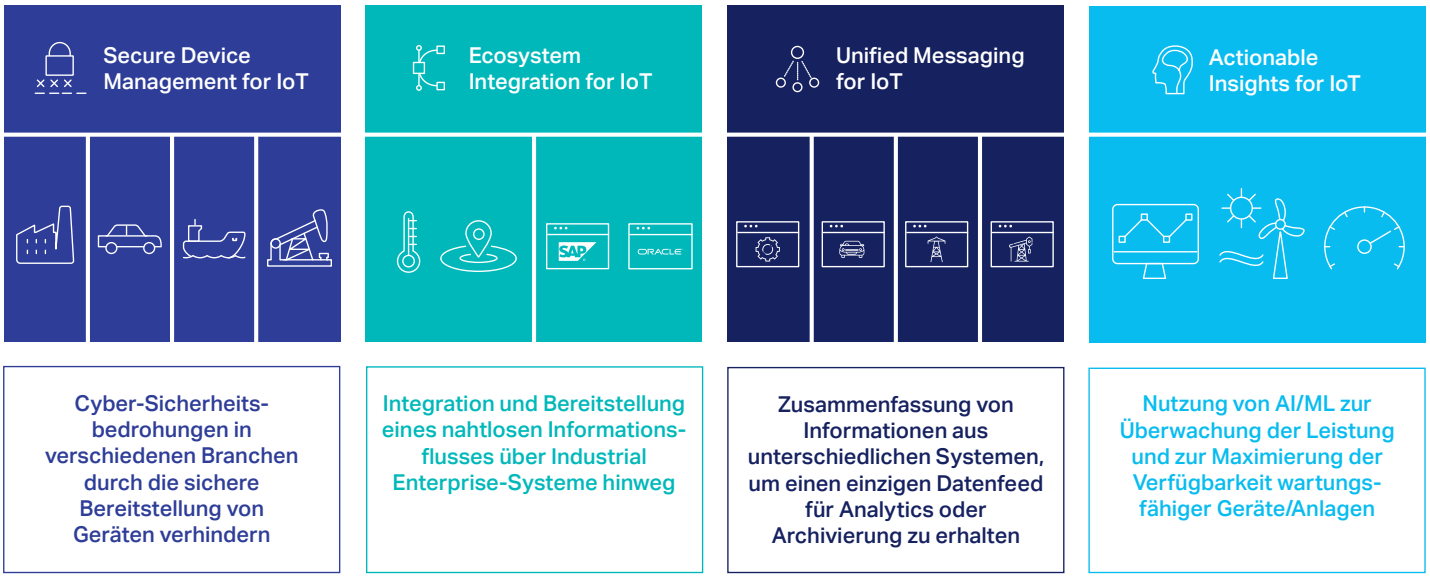
- Die wichtigsten Funktionen einer identitätsgesteuerten IoT-Plattform
- Die 10 wichtigsten Aspekte, die bei der Implementierung von Identitätsmanagement im IoT zu beachten sind
- Auswahl des geeigneten Providers für IDoT

opentext™

Holen Sie sich noch heute den Leitfaden

opentext™ | IoT

Umfassende, erweiterte Unternehmensanwendungen vernetzen Menschen, Systeme und Geräte durch einen identitätsbasierten Ansatz



Secure Device Management for IoT	Ecosystem Integration for IoT	Unified Messaging for IoT	Actionable Insights for IoT
Cyber-Sicherheits-bedrohungen in verschiedenen Branchen durch die sichere Bereitstellung von Geräten verhindern	Integration und Bereitstellung eines nahtlosen Informations-flusses über Industrial Enterprise-Systeme hinweg	Zusammenfassung von Informationen aus unterschiedlichen Systemen, um einen einzigen Datenfeed für Analytics oder Archivierung zu erhalten	Nutzung von AI/ML zur Überwachung der Leistung und zur Maximierung der Verfügbarkeit wartungs-fähiger Geräte/Anlagen

Zusätzlich zum Secure Device Management für IoT kann die OpenText IoT-Plattform auch Ecosystem-Integration, Unified Messaging und umsetzbare Informationen liefern

Bieten Sie eine außergewöhnliche Kundenerfahrung

Die Hersteller von heute sitzen auf einer Goldmine von IoT-Daten, die automatisch von Maschinen oder angeschlossenen Produkten an zahlreiche Entitäten gesendet werden können. Ziel ist es, das Angebot zu erweitern und die Customer Experience (CX) zu verbessern. Durch eine Kombination aus KI, IoT und Analytics können z.B. Automobilhersteller und Service Provider diese Daten für Folgendes nutzen:

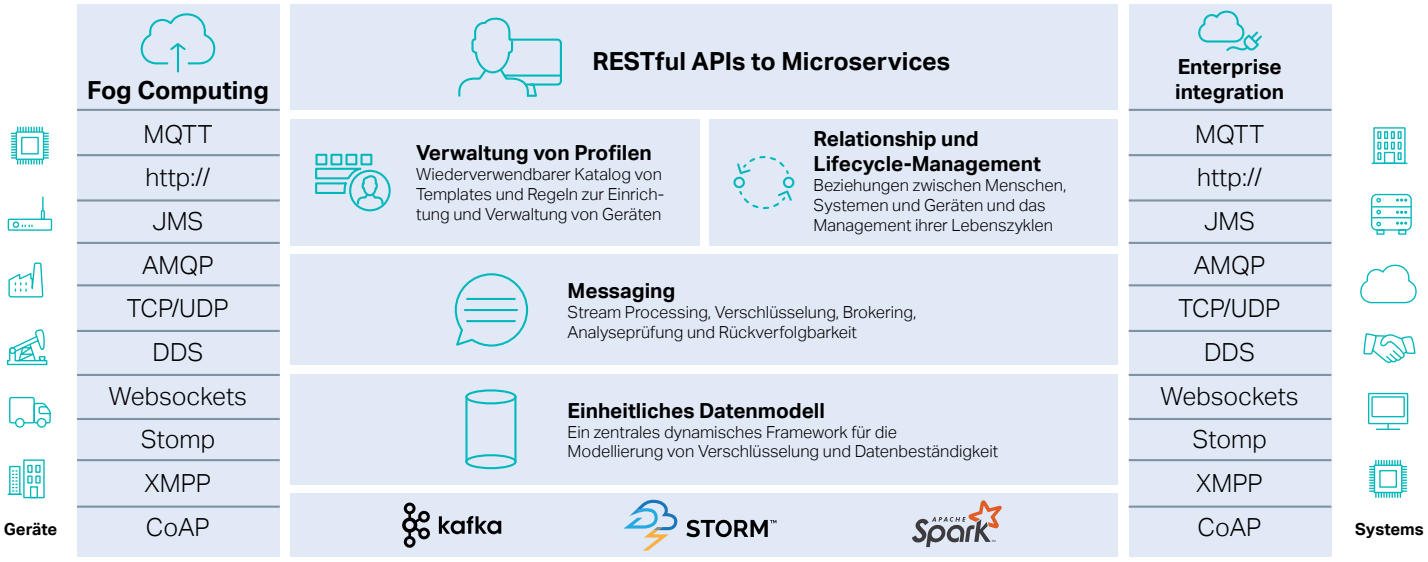
- Ermöglichen Sie OEMs das schnelle Onboarding von Partnern und Drittanbietern von Anwendungen und Systemen, die mit dem vernetzten Fahrzeug interagieren.
- Erlauben Sie den OEMs, wichtige Daten über die vernetzten Fahrzeuge für CRM-, CX- und Qualitätsüberwachung zu zentralisieren.
- Sorgen Sie für die Sicherheit des Datenstroms, der zum und vom Fahrzeug übertragen wird und fördern Sie so die Sicherheit und Loyalität der Kunden.
- Prognostizieren Sie potenzielle Fehlerquellen und installieren Sie proaktive Warnhinweise, die die Ausfallzeiten der Fahrzeuge reduzieren und so die Kundenzufriedenheit verbessern.

Laden Sie den Leitfaden herunter

opentext™

Komponenten des Secure Device Management

Verwaltung von Profilen	Ein wiederverwendbarer Katalog von Templates und Regeln zur Einrichtung und Verwaltung von Geräten
Relationship und Lifecycle-Management	Beziehungen zwischen Menschen, Systemen und Geräten und das Management ihrer Lebenszyklen
Messaging	Stream Processing, Verschlüsselung, Brokering, Analyseprüfung und Rückverfolgbarkeit
Einheitliches Datenmodell	Ein zentrales dynamisches Framework für die Modellierung von Verschlüsselung und Datenbeständigkeit



OpenText IoT Architektur

Mehr erfahren

OpenText Internet of Things »

Secure IoT Network–
OpenText Industrial Grid »

opentext.de/Kontakt Twitter | LinkedIn