DeviceOps 101

From Managing to Monetizing Connected Products

EBOOK

EDGEIQ

Introduction

The purpose of this eBook is to shine a bright light on DeviceOps, an often overlooked, yet foundational part of the Connected Product Economy. DeviceOps is a framework of processes, people and tools employed in the lifecycle management of connected devices and their data as well as the orchestration of workflows and integration of all this into a company's broader value chain.

DeviceOps is not new.

Legacy versions of DeviceOps have been with us for years and touch hundreds of millions of mobile devices (MDM), IT endpoints (ITSM, UEM) and even operational endpoints (EAM). The advent of Connected Products (drones, digital signs and dialysis machines), however, represent an entirely different class of endpoints to manage. For a variety of reasons, legacy endpoint management offerings are not well suited for Connected Products - but all of these connected endpoints benefit from an integrated DeviceOps framework.

This eBook focuses on DeviceOps for Connected Product businesses and how the philosophy is simplifying and accelerating their digital and business transformation.

DeviceOps is a framework of processes, people and tools employed in the lifecycle management of connected devices and their data as well as the orchestration of workflows and integration of all this into a company's broader value chain.

What Is DeviceOps?

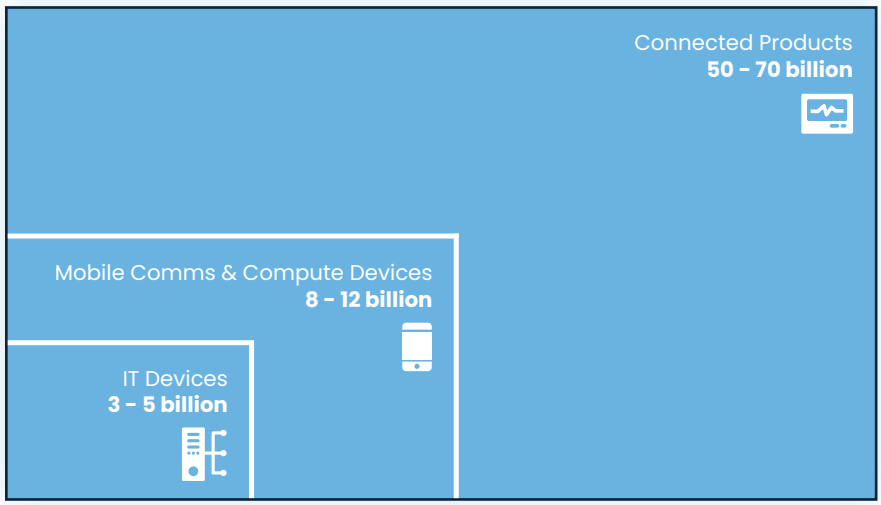
Prior to the formalization of DevOps in 2009, stakeholders were increasingly frustrated over the lack of process and technology that tie together software development and the operations of deploying, securing and supporting it. Hence the birth of DevOps and its ubiquitous infinity loop.

Soon after DevOps, the world realized that these integrated frameworks apply to many disciplines - RevOps, DataOps, PeopleOps, SecOps, DevSecOps, AIOps and so on. With the proliferation of billions of connected devices - IT and Connected Product - organizations needed a way to scale device lifecycle management. This is not a siloed operation, but one that involves a number of discrete processes, multiple organizational pillars and a set of software tools to simplify, automate and scale - giving birth to DeviceOps.

Organizations needed a way to scale device lifecycle management.

Billions and Billions of Connected Devices

While the term DeviceOps is relatively new, the reality of managing connected devices is anything but new. Billions of dollars are spent managing billions of IT endpoints, mobile communications devices and connected products. While enterprise endpoint management has garnered the most attention from third party vendors, it actually only makes up a fraction of the connected devices deployed globally.



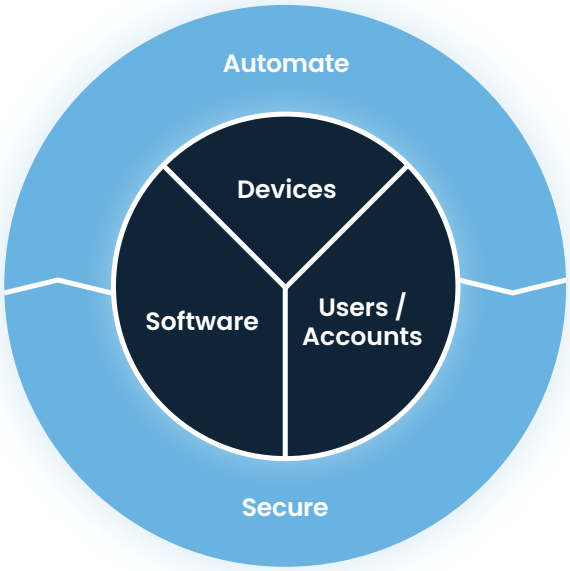
Early DeviceOps - MDM, ITSM, UEM

The first wave of DeviceOps adoption took the form of IT service Management (ITSM) and Mobile Device Management (MDM). Each of these frameworks are still essential for deploying, securing and managing enterprise compute resources: phones, laptops, desktops, tablets and servers. For mid- to larger organizations deploying hundreds, thousands or even millions of IT devices, MDM is an essential tool.

Early MDM vendors (Airwatch, now VMware, IBM MaaS360, Microsoft InTune, Mobile Iron, now Ivanti, SOTI, Sophos, etc.) focused on the traditional handset and laptop market. Now that Apple and Android have taken over mobile and portable computing, there are a new set of innovators dominating the MDM market. Fleetsmith was already acquired by Apple, JAMF went public, and Kandji and Esper are gaining enormous traction with compelling offerings. These providers simplify the lifecycle management of mobile devices, ensuring they are properly configured, secured, only running sanctioned applications and can be removed for service if necessary. Integration with a wide range of other IT tools (identity management, network and application security, etc.) ensures that DeviceOps is integrated more broadly into Enterprise IT, SecOps and PeopleOps.

These providers simplify the lifecycle management of mobile devices, ensuring they are properly configured, secured, only running sanctioned applications and can be removed for service if necessary.

DeviceOps for Mobile and IT Devices



DeviceOps for Connected Products

Connected products are a completely different kind of device - and not just from a technology perspective. Connected products are systems that perform business critical functions for their customers. Within these devices, there are compute and communication capabilities equal to or greater than a mobile phone or tablet. But that technology is embedded in systems like cars, drones, medical devices, security systems, robots, elevators, satellites and the other billions of connected products. Compared to the connected products segment, the mobile device domain looks fairly homogenous - a limited number of OSes all tightly controlled by their providers. MDM vendors are able to leverage powerful and well documented management tools provided by Apple, Google and Microsoft.

In the connected product domain, on the other hand, there are hundreds of variations of Linux, real time operating systems (RTOS) and embedded Windows that are implemented based on the unique needs of each product manufacturer. On top of the OS/RTOS layer is where custom firmware is deployed - unique for every device profile and product SKU. Unlike the MDM world, these underlying OSes provide very limited tooling that can be leveraged in the DeviceOps user experience layer.

In the connected product domain, on the other hand, there are hundreds of variations of Linux, real time operating systems (RTOS) and embedded Windows that are implemented based on the unique needs of each product manufacturer.

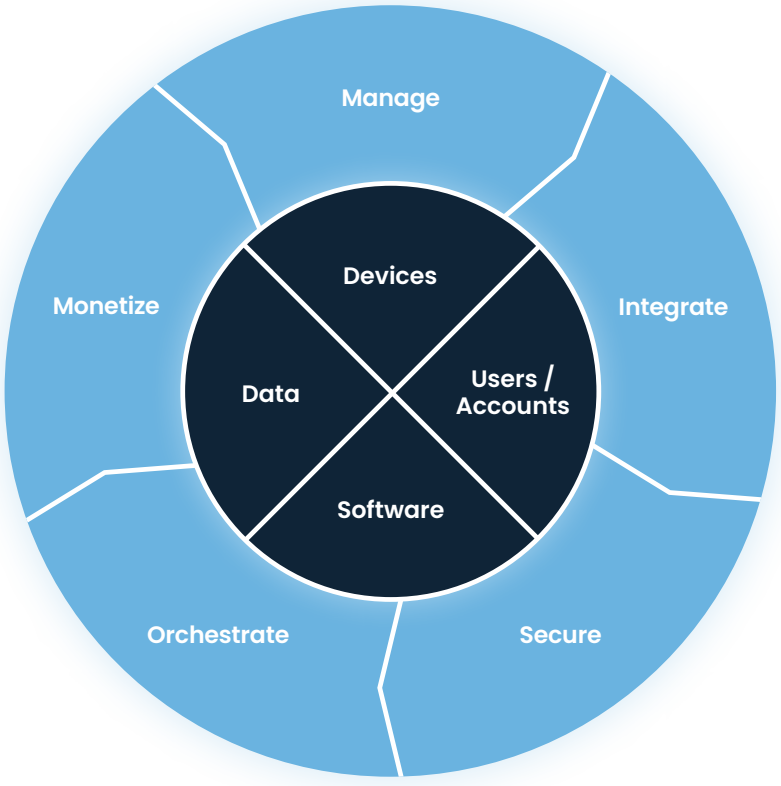
Connected Products are the Business

Mobile communications and compute devices are tools for business. Connected products **are** the business.

Connected Products not only require the baseline lifecycle management features that MDM tools provide, they must deliver more complex network configuration capabilities, customer- and region-specific provisioning profiles and policies, virtually unlimited upstream application and service integrations and more complex workflow orchestration. Beyond these complexities, the two most important differences in Connected Product DeviceOps are the need to operate in the data layer and ultimately provide device entitlements and monetization capabilities.

Beyond these complexities, the two most important differences in Connected Product DeviceOps are the need to operate in the data layer and ultimately provide device entitlements and monetization capabilities.

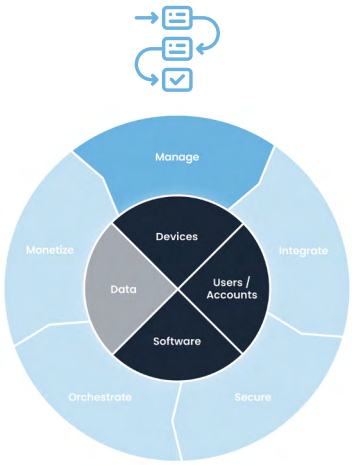
DeviceOps for Connected Products



DeviceOps for Connected Products - A Closer Look

In the Connected Product domain, DeviceOps is much more than device management, but that is where it begins. The following are key capabilities included within any technology platform focused on DeviceOps for Connected Products:

Device Management



Device Profile Management

Define the unique attributes and capabilities for each device type. This becomes the internal catalog and tells the system what devices can and cannot do, how they connect, report and what their associations may be with other devices.

Fleet Management and Onboarding

Create and manage a unified source of truth for all your connected products, onboard individual devices or load in bulk. Devices should automatically associate with their unique profiles and capabilities once onboarded.

Device Provisioning

Enable zero-touch provisioning at power up and initial connection. Send updated configurations, software updates and policies for wellness reporting and data federation. Unique provisioning templates can be created by type or account.

Wellness Monitoring, Alerts and Notifications

Configure devices to send periodic heartbeats with specific payload data. Automate alerts and notifications on any device or data parameter.

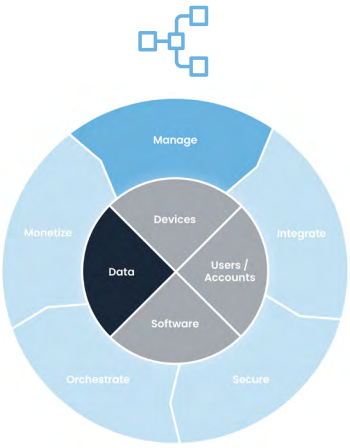
Software and Configuration Management

A service that will update any device software - from the OS to firmware, applications and even AI/ML models. Ideally, updates can be scheduled and audited with retry management.

User and Account Management

Granular, multi-tier support for user role-based permissions and access. The same should apply to the account or organization level.

Data Management



Data consumption

Configure and manage an ingest and translation service that will normalize data from devices and, optionally, operational payload data from sensors and the product's environment.

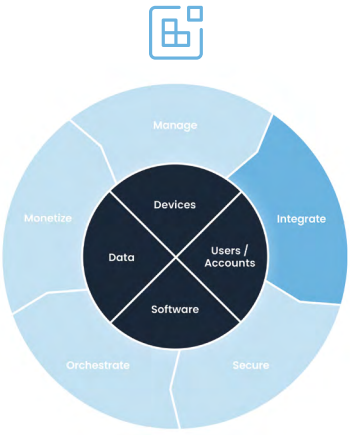
Data federation

A policy-based service for sending normalized data to predefined endpoints, applications and databases. This should support multiple, simultaneous threads.

Analytics and Visualization

Allow customers and internal users to store, analyze and visualize data around specific devices, device profiles, accounts, locations and more.

Integration



Bring Your Own Cloud Infrastructure

Abstract the core DeviceOps service from the primary cloud infrastructure - leverage key services from AWS, Microsoft and Google.

Bring Your Own Enterprise Applications

Organizations should be able to use their own CRM, Field Service, ERP and of course device or business specific services that can interact directly with devices and their data.

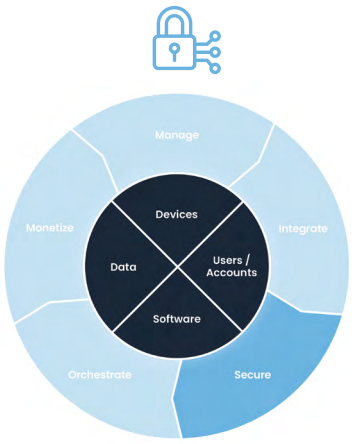
Bring Your Own IAM Service

Leverage a third party identity and access management system to manage user permissions within the DeviceOps platform.

Business and Product Specific Applications

Integrate existing CRM, field service, supply chain, ERP and other enterprise applications to your DeviceOps service.

Security



Security at the Edge

Edge compute services should operate in such a way that there is no local programmatic control. Configurations should be provided externally via secure connections. Connections between the edge and cloud should be via TLS and on specified, secured brokers (MQTT, MQTTS). The DeviceOps service should not require specific, dedicated ports and all communication should be initiated by the device at the edge.

Role and Account Based Security

All actions and access should be restricted to the individual role of the user and further restricted by the organization that a user is part of. This should apply to basic create, read, update, delete and critical changes to devices, their configurations and data.

Separation of Command Creation vs. Execution

DeviceOps frameworks should always separate the creation of commands and updates from the execution of commands and updates.

Encryption

A DeviceOps software platform should encrypt device updates at rest and in transit. Data from devices should be encrypted in transit. Encrypting data and files at rest at the edge is part of best practices for the device owner.

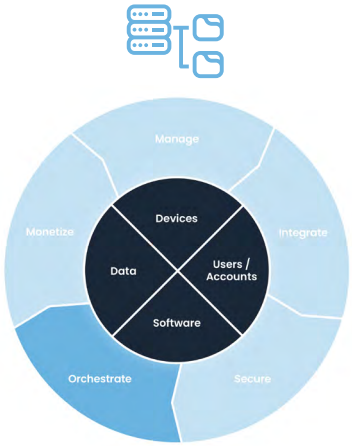
Secrets

DeviceOps best practices should provide that organizations can store sensitive credentials securely that can be invoked in complex but automated workflows.

Certificate Management

Organizations must be allowed to leverage certificates at various levels of the DeviceOps solution - at the device registration level up to cloud service access.

Orchestration



Orchestration is primarily about the creation and management of workflows that tie various DeviceOps system elements together. By definition, the number of workflows that can be orchestrated is limitless. Some examples include:

State Management

Automating the promotion of a device from Escrow state to Active, or Discovered to Active, or assigning configuration and data policies to devices that are put in service in place of devices in Maintenance mode.

Complex Zero Touch Use Cases

Beyond zero touch configuration, orchestration services allow organizations to configure devices with specific heartbeat policies, tie notifications to specific third party alerting services, routing data from specific devices to specific applications and accounts.

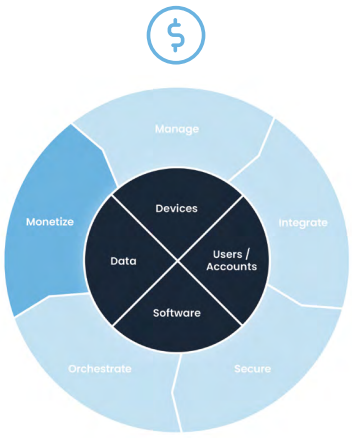
Complex Data and Event Orchestration

Either manually triggered or automated based on an event, a workflow can send data to or initiate an event in one or more upstream services by using credentials stored in a data vault.

Automatically Create Support Tickets

A common workflow that connected product companies will require to create is the ability to automatically create support tickets, log errors, etc. within different systems when an event is detected on the device or network.

Monetization and Rights Entitlement



Monetize Physical Devices as a Service

Completely alter a business model based by converting a one time hardware purchase to an ongoing service offering that comes with specified hardware.

Enhanced Monitoring and Management Services

End customers value (pay for) higher levels of service that includes remote monitoring, management, automated event management, etc.

Device Data Analytics

Analytics is not only a powerful tool for the connected product manufacturer, but it provides invaluable operational insight for the end user organization.

Rights and Feature Entitlement

An increasingly popular and valuable capability is delivering new features as software updates and providing these on a by-account or by-customer basis. DeviceOps frameworks allow an organization to be highly targeted with enhancements from features to integrations.

Connected Products and DeviceOps: What to Build, What to Buy?

Your products are your business so deciding what elements to build versus buy is important. However, the decision criteria are really straightforward. Organizations should focus internal resources - research, design and development - on those product elements that are strategically differentiated. Physical and mechanical design is entirely unique to each product, so that should be done internally. Likewise, firmware is written for the unique capabilities of every device and should be written and maintained by internal experts.

Application layer software and business/domain-specific software are proprietary to your products - they should be designed, created and maintained internally. But you would never design and build commoditized components - processors, memory, sensors, connectivity, displays, etc. Likewise, almost no organization would write their own database software, operating systems or cloud infrastructure.

The same is true for DeviceOps software - which is just a layer of undifferentiated infrastructure software. It operates in the management and orchestration plane between the proprietary elements of connected products. Ultimately, every minute and every dollar spent on undifferentiated layers of your product are a distraction from the elements that truly set it apart. It's a matter of strategic focus.

Ultimately, every minute and every dollar spent on undifferentiated layers of your product are a distraction from the elements that truly set it apart. It's a matter of strategic focus.

About EdgeIQ

EdgeIQ is accelerating the growth of the Connected Product Economy. Our API-first DeviceOps platform helps organizations simplify and scale the management of connected products, their data and the orchestration of essential workflows throughout the product's value chain. Visit EdgeIQ at https://www.edgeiq.ai/ or follow us on LinkedIn at https://www.linkedin.com/company/edgeiq

EDGEIQ