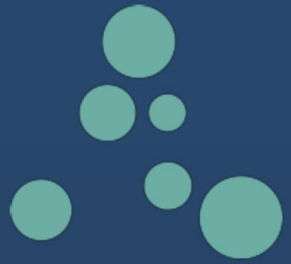
Introducing



AUGMATE

The world's leading IoT and Wearable Device Management Platform

Connecting your employees, customers, devices and data.

The Problem

Smart devices are connected to the internet, but not to each other.

No single platform connects disparate protocols and ecosystems.

Security in centralized systems is easily compromised.

Existing systems focus on the technology, not the user.

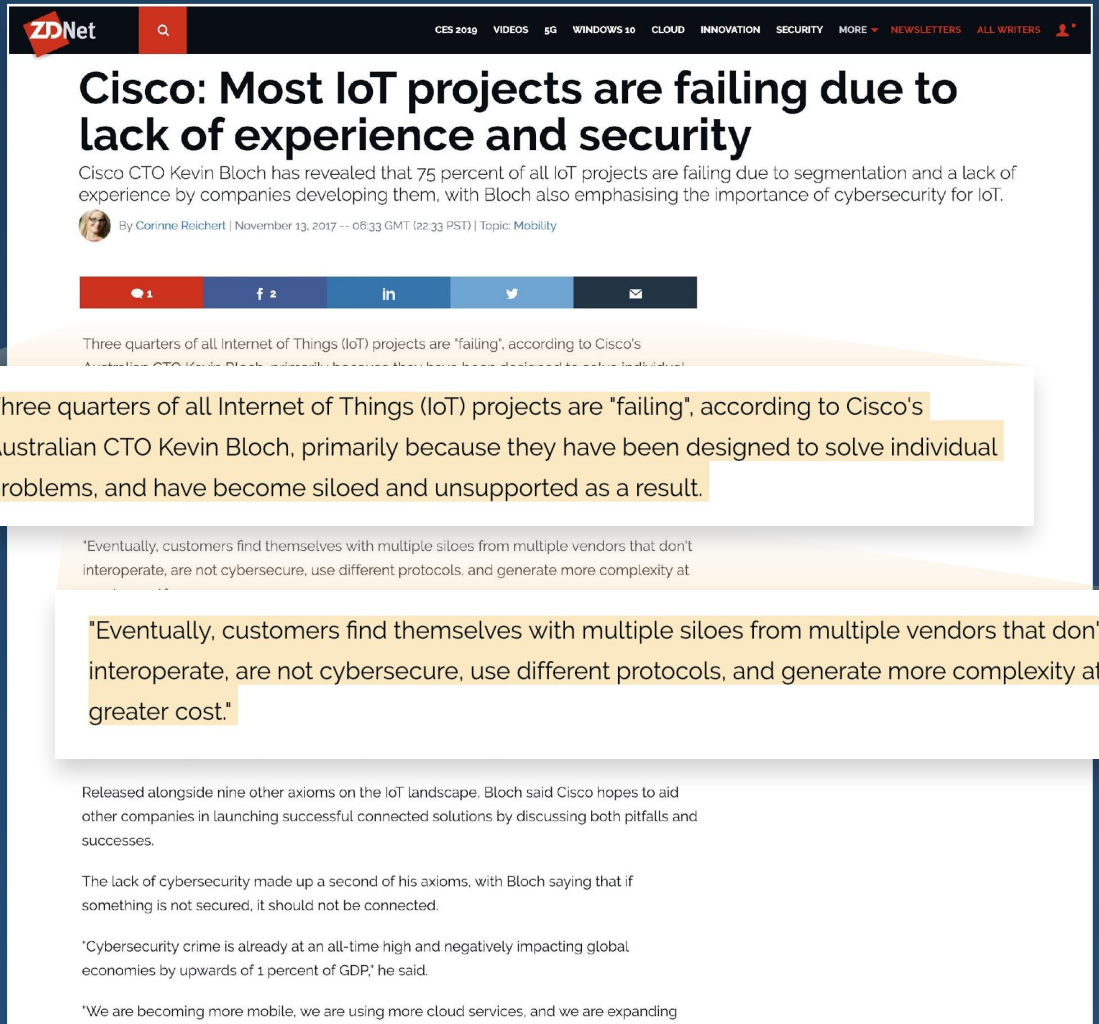
MDMs and policies lock down devices rather than enabling them.

No easy way exists to manage multiple users and devices at scale.

Complexity and low ROI have impacted enterprise adoption of IoT devices

Three quarters of all Internet of Things (IoT) projects are "failing."

– CISCO



ZDNet

CES 2019 VIDEOS 5G WINDOWS 10 CLOUD INNOVATION SECURITY MORE NEWSLETTERS ALL WRITERS

Cisco: Most IoT projects are failing due to lack of experience and security

Cisco CTO Kevin Bloch has revealed that 75 percent of all IoT projects are failing due to segmentation and a lack of experience by companies developing them, with Bloch also emphasising the importance of cybersecurity for IoT.

By Corinne Reichert | November 13, 2017 -- 08:33 GMT (22:33 PST) | Topic: Mobility

1 2

Three quarters of all Internet of Things (IoT) projects are "failing", according to Cisco's

Three quarters of all Internet of Things (IoT) projects are "failing", according to Cisco's Australian CTO Kevin Bloch, primarily because they have been designed to solve individual problems, and have become siloed and unsupported as a result.

"Eventually, customers find themselves with multiple siloes from multiple vendors that don't interoperate, are not cybersecure, use different protocols, and generate more complexity at

"Eventually, customers find themselves with multiple siloes from multiple vendors that don't interoperate, are not cybersecure, use different protocols, and generate more complexity at greater cost."

Released alongside nine other axioms on the IoT landscape, Bloch said Cisco hopes to aid other companies in launching successful connected solutions by discussing both pitfalls and successes.

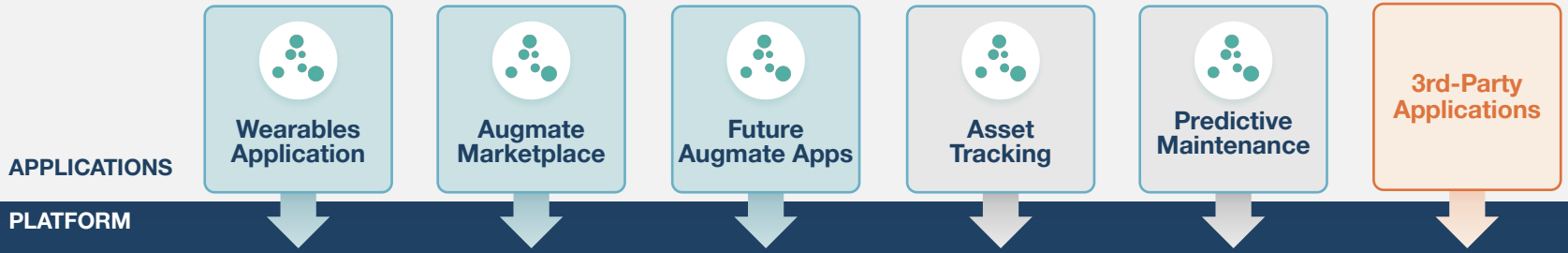
The lack of cybersecurity made up a second of his axioms, with Bloch saying that if something is not secured, it should not be connected.

"Cybersecurity crime is already at an all-time high and negatively impacting global economies by upwards of 1 percent of GDP," he said.

"We are becoming more mobile, we are using more cloud services, and we are expanding

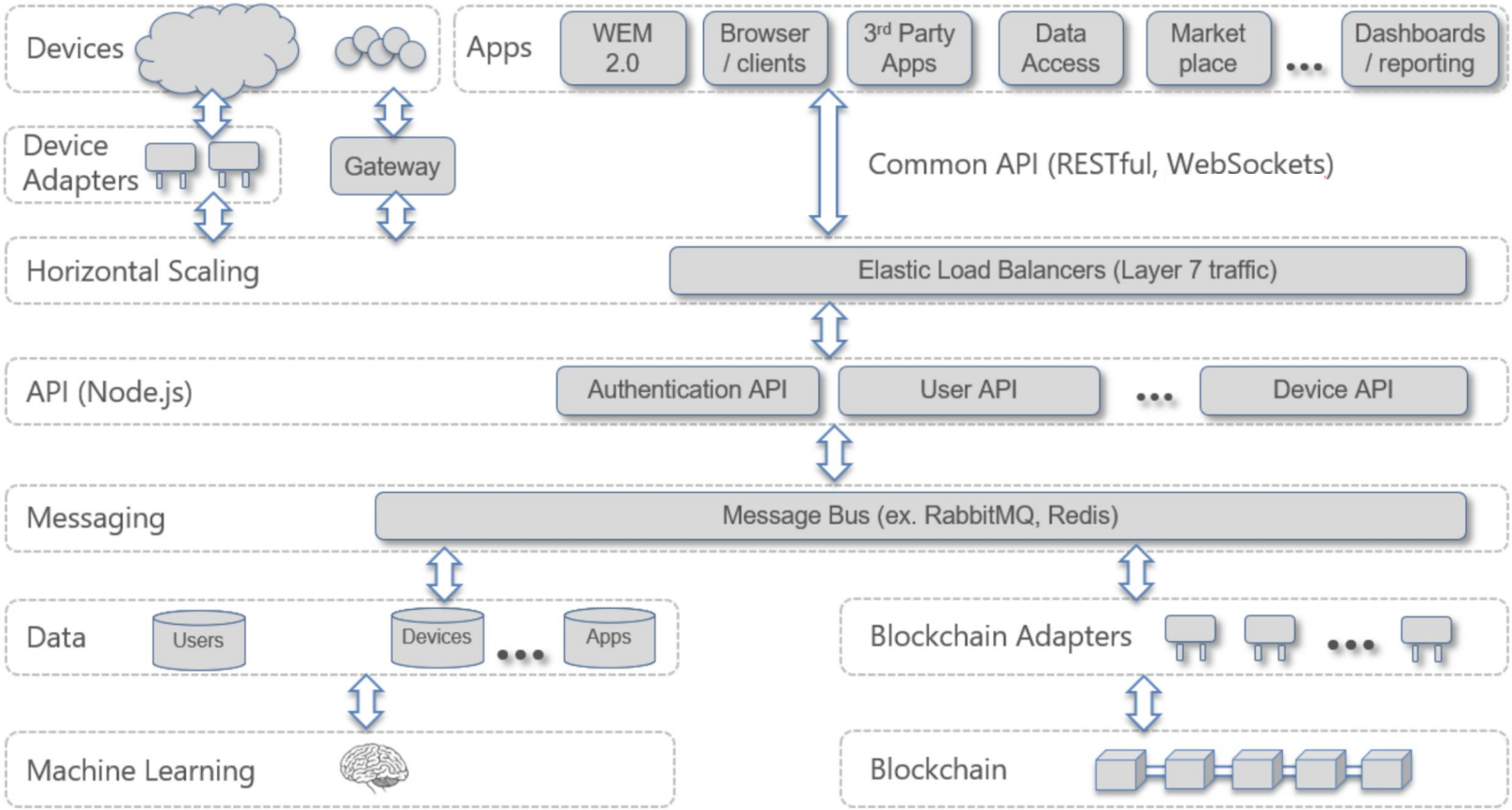
The Solution

Augmate Connect™ *is the Leading Solution for Managing High-Value IoT Devices*



AUGMATE CONNECT™

Augmate Connect Platform Architecture



Device Naming Architecture (DNA) Overview:

INVENTORY OF THINGS

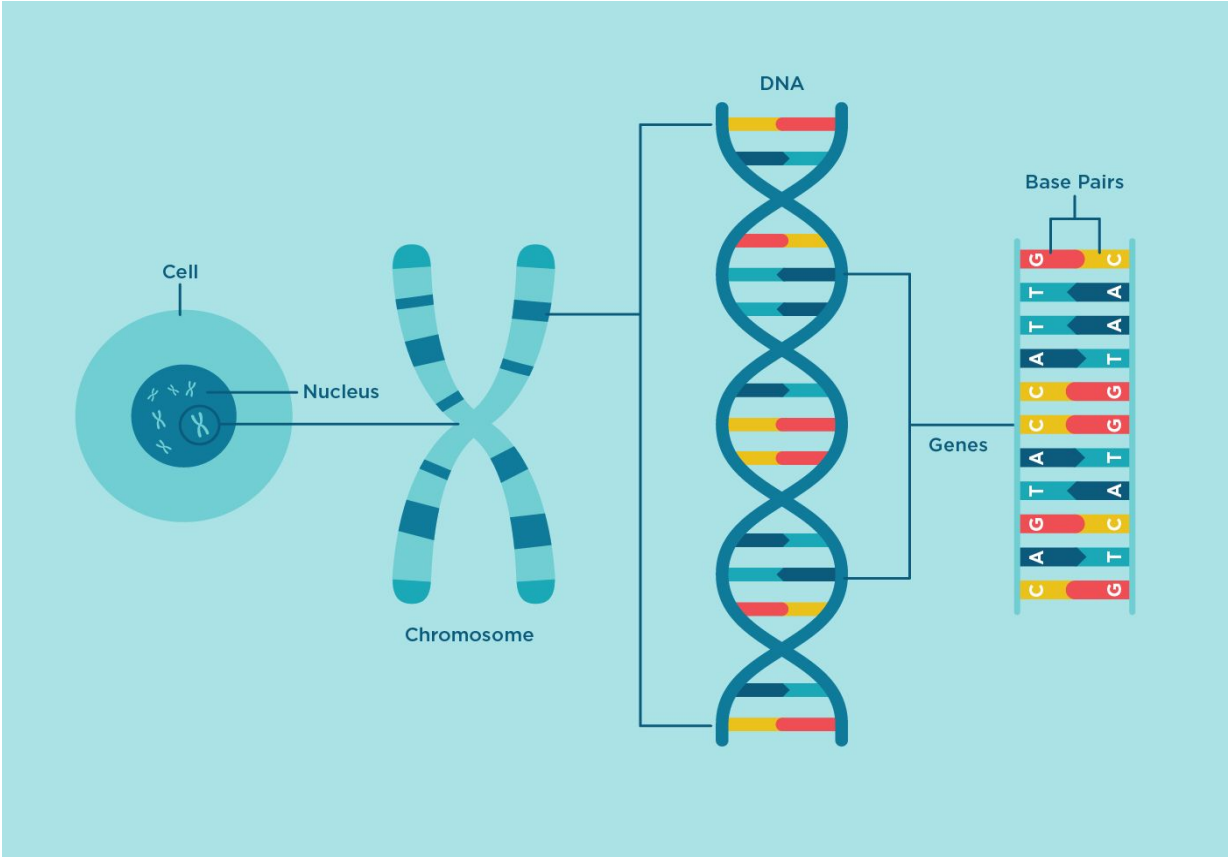
Device Properties:
Sensors
Location
Interaction Mechanism

UUID:
A universally unique identifier (UUID) is a 128-bit number used to identify information in computer systems.

Blockchain:
Ethereum
Hyperledger

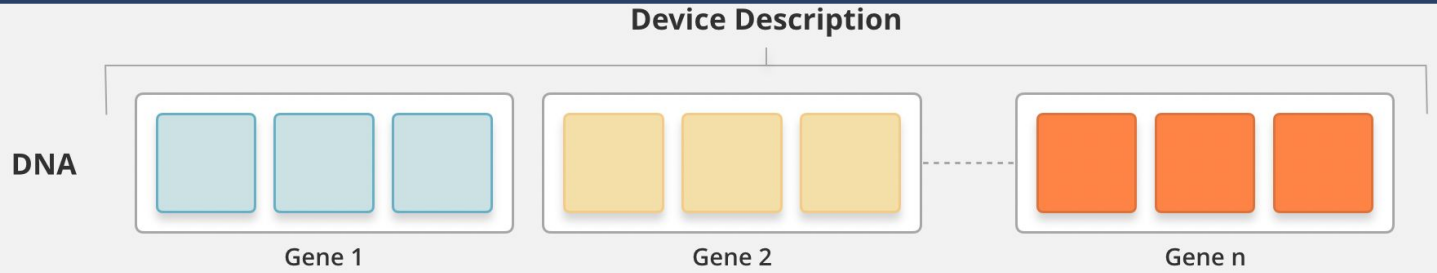
Markup Language:
Making it easy to work with.

Tools:
Augmate Smart Contracts



AUGMATE

Device Naming Architecture (DNA) Details:



- A hierarchical, scalable taxonomy that describes Things in a human- and machine-readable format
- Modular, object-oriented model; uses “genes” to modularize definitions
- Designed for Blockchain; Immutable, trusted

- Ideal input for Smart Contracts as device structure is well-defined and standardized
- Can describe a real-world thing and render the attributes for a digital twin
- Structured input to automatically render a UI

- DNA is stored on the blockchain for device capability immutability
- Allows for devices to be self-describing, even devices that don’t yet exist

A definition and registry for the Internet of Things:

Augmate’s innovative contribution to IoT standards

Solving the Infrastructure Problem

Overcoming Issues

Wearable Device technology has proven ROI in many industries including manufacturing, aerospace, logistics and healthcare, but needs proper infrastructure to support it in a secure enterprise environment.

PROBLEMS WE SOLVE

ISSUE 01

SECURITY

Protect data and prevent unintended usage of devices

ISSUE 02

SCALABILITY

Monitor and manage a fleet of devices, data, and usage

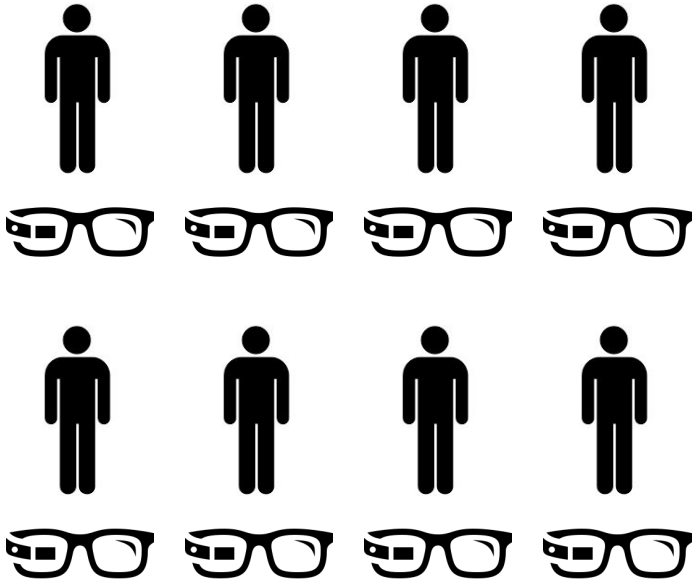
ISSUE 03

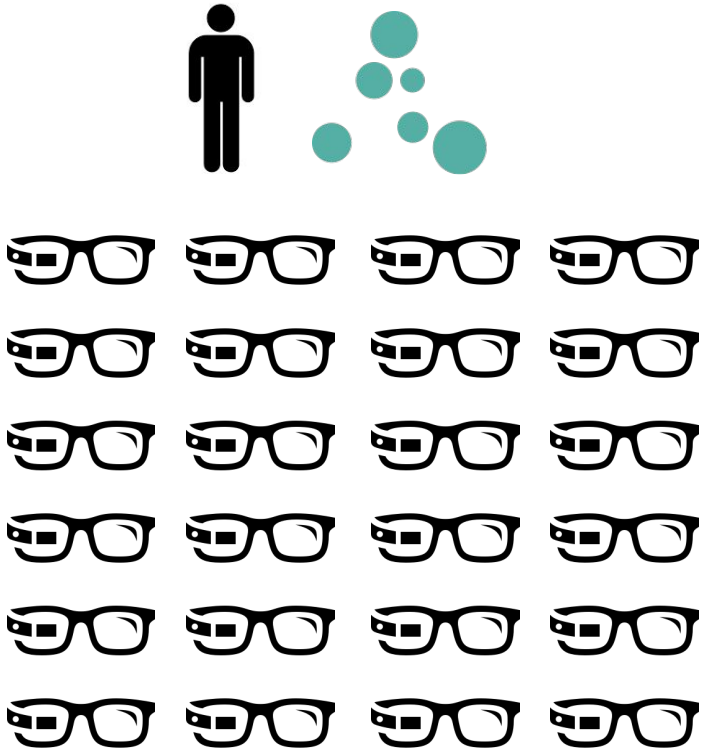
INTEGRATION

Get hardware and software systems to work together

AUGMATE

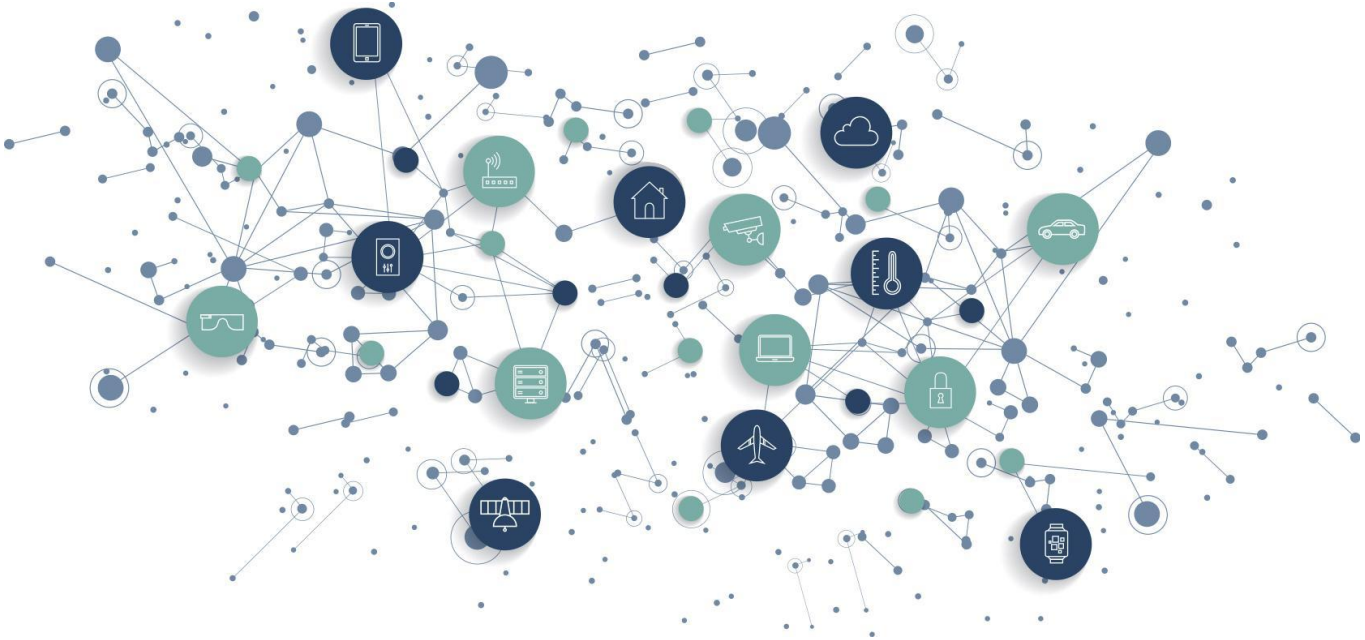
Solution: Device Management





IoT Device Management

- IoT Network Health Check
- Securely Connect to a Device
- Ensure Proper User Authentication
- Pass Appropriate Device Data
- Device Policy Based on Organization
- Remote Device Management
- Centralized Device Monitoring
- Over The Air Updates
- Full IoT Device Control



AUGMATE

Product Roadmap

2017

- WEM 1.0

2018

- Connect dev
- Marketplace dev
- Pilot / AR dev
- Asset Tracking POC

2019

- Connect platform launch with WEM 2.0
- MDM expansion
- Marketplace launch
- Pilot in a Box launch
- Blockchain development
- SSO
- Rule engine dev
- Support

2020

- Blockchain Protocol 1
- Open APIs
- Broader set of IoT devices supported
- App Developer dev
- Rule engine
- Developer Portal
- Data Analytics / Reporting

2021

- App Developer v1
- Blockchain Protocol 2, 3
- Data Strategy
- Machine Learning Modules

2022

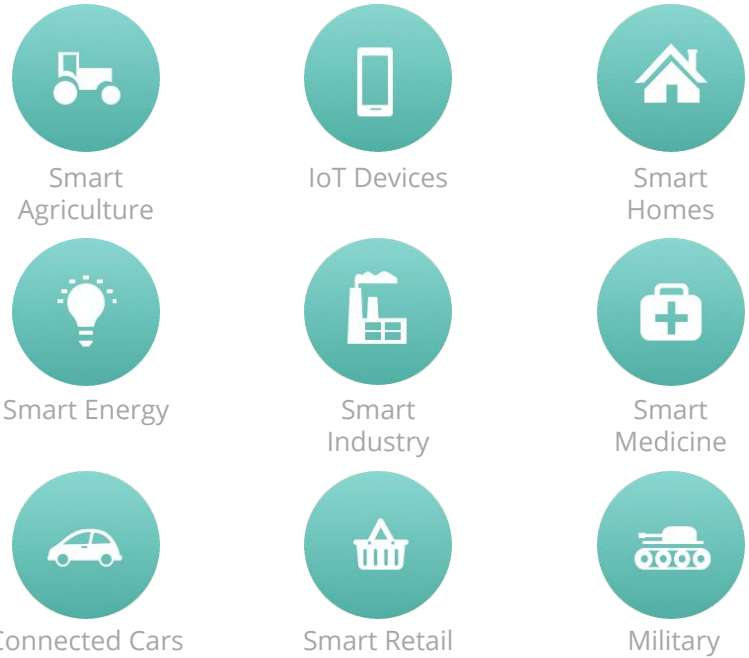
- App Developer v2
- Predictive ML modules
- Anomaly detection
- Blockchain Protocol 4+

2023

- Market expansion

AUGMATE

Verticals



Building for a connected world, but focusing on industry, field services and supply chain.

Learn more
augmate.io/learn/resources

Competitive Advantage

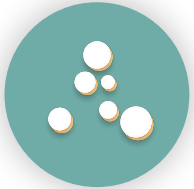
First to Market
Wearable Device Management

Product Ecosystem
Cross-promotion across product line

Platform vs App
3rd parties build on our platform with a simple, common toolset

Open Architecture
API and SDK support

Built for IoT & Blockchain
Using best-in-class technology, not retrofitted

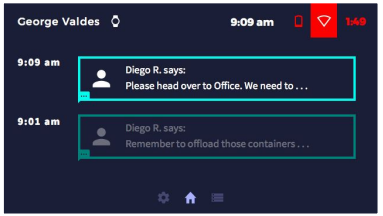


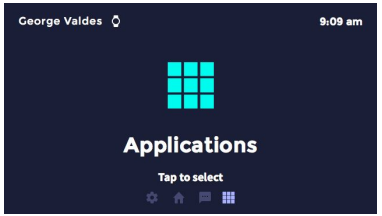
Augmate Brand
Well known in enterprise wearables, easy extension to IoT

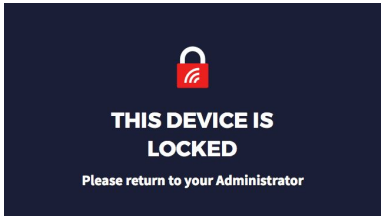
A Proven Solution

Wearable Environment Manager™ (WEM) enables enterprise IT administrators, application developers, ERP, and SI's to efficiently manage fleets of wearable devices.

ADMIN PORTAL







WEARABLE INTERFACE

AUGMATE

Select Clients & Partners

Device List

Realwear
Realwear HTM-1

Vuzix
Vuzix M100
Vuzix M300
Vuzix M300XL
Vuzix Blade

Epson
Epson BT-2000
Epson BT-350

Google
Google Glass 2.0
Google Glass

Pico
G2

ReconJet
ReconJet Pro

Optivent
Optinvent ORA-1

ODG
ODG R-7

COMING SOON

Microsoft
Hololens

Apple
iPhone
iPad

Android
Smartphones
Tablets

AUGMATE

Competition… or Strategic Partners

MDM

MobileIron

airwatch by vmware

SOTI

Centralized

C3 IoT

Windows IoT

CISCO

GE

Blockchain

FILAMENT

Atonomi

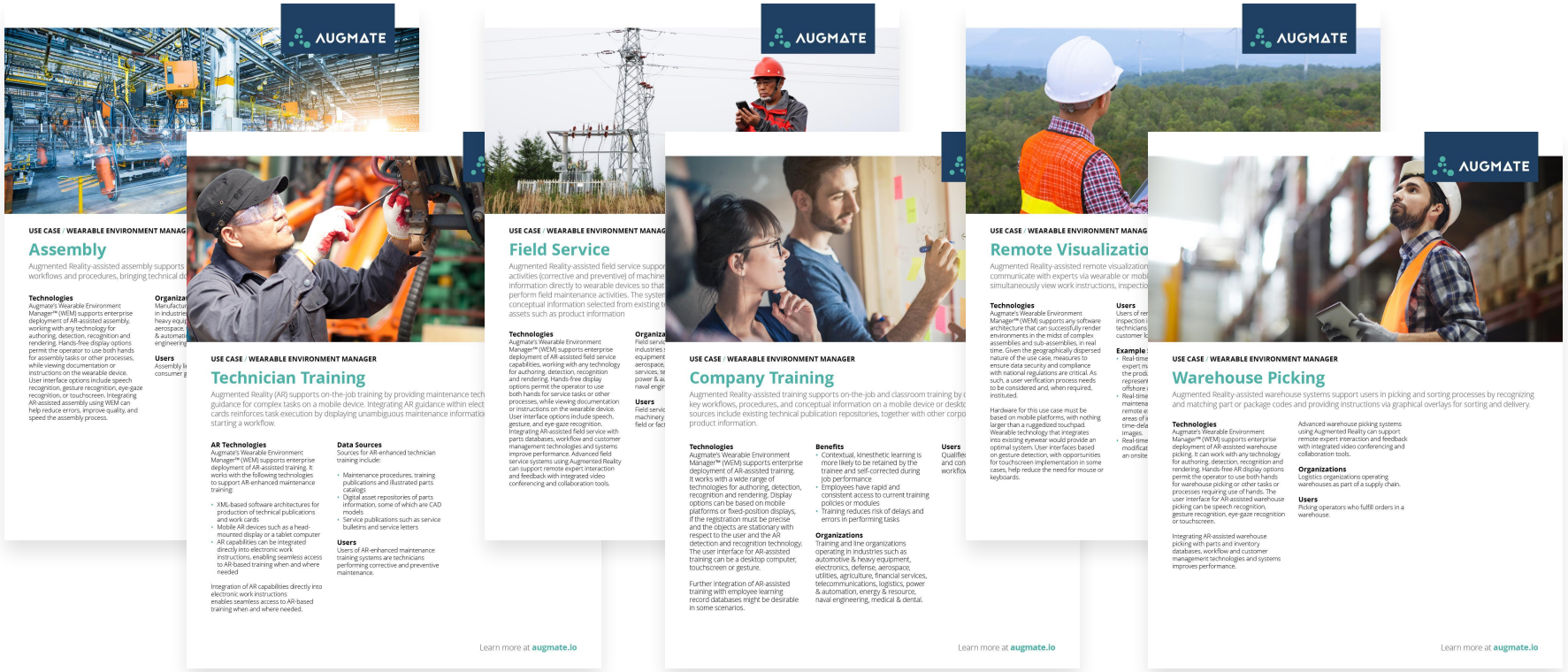
CONSENSYS

HYPERLEDGER

IoT + Blockchain + AI

AUGMATE

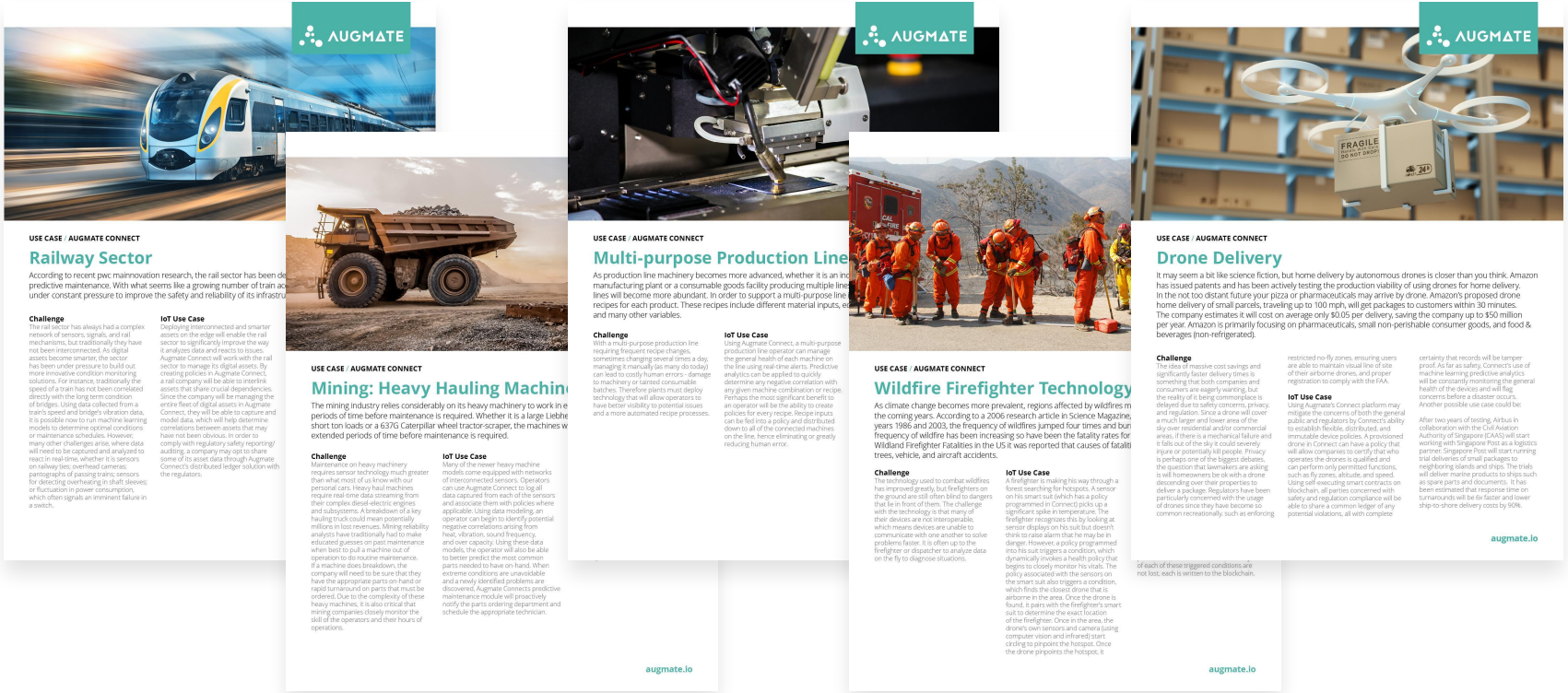
Use Cases / WEM



Learn more

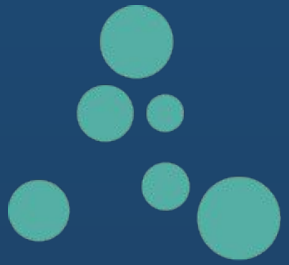
augmate.io/learn/resources

Use Cases / Connect



Learn more

augmate.io/learn/resources



AUGMATE

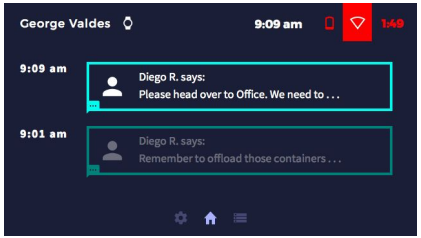
augmate.io

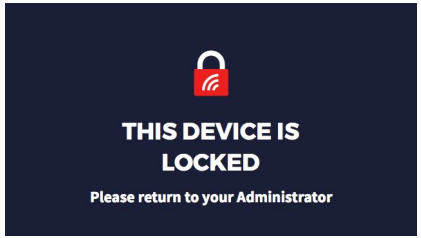
Appendix

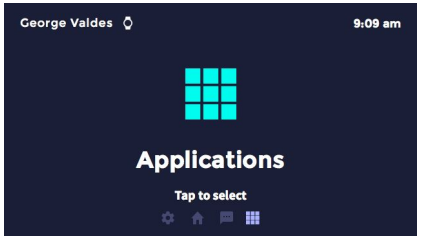
Augmate WEM

Wearable Environment Manager (WEM)™

Augmate provides complete HMD management by allowing administrators to operate devices through a Wearable Environment Manager (WEM) portal. Our enterprise platform handles device and user management, security, policies, and over-the-air application deployments.





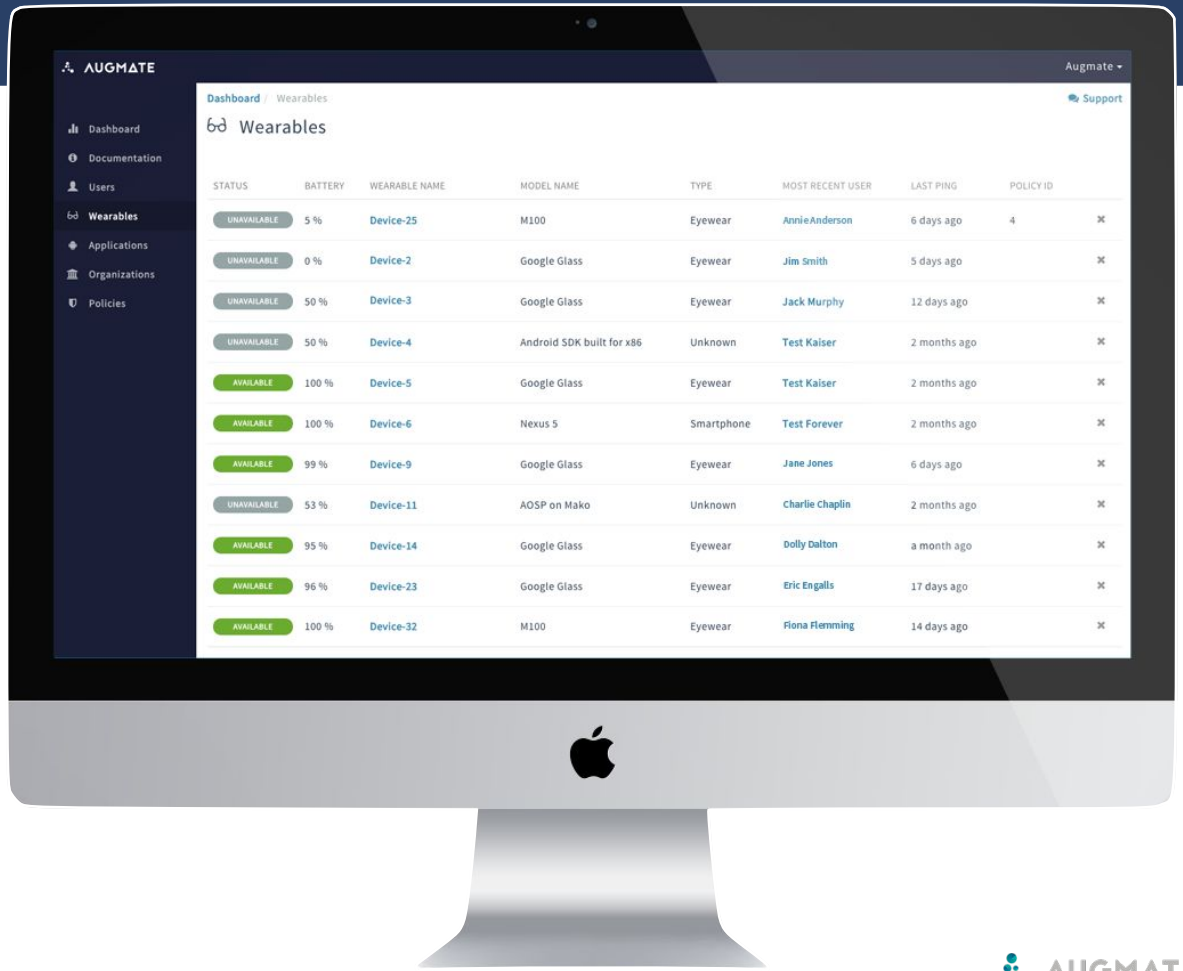


AUGMATE

WEM platform

Augmate's **Wearable Environment Manager (WEM**) platform enables enterprise IT administrators application developers, ERP, and SI's to efficiently manage fleets of wearable environments.

Our platform enhances device security, while providing policy management tools that enable application and connectivity management, user and device tracking, real-time communications, sensor data collection, and beacon management—all done securely and remotely from a single management portal.



AUGMATE

Competition

We do provide MDM-like functionality, however MDM companies have not entered this space. We not only have a first mover advantage, we have a deep knowledge of customer needs and strong network ties within this ecosystem.

FEATURES	Augmate	Airwatch	Mobileiron	SOTi
Wearable-first platform posture	X			
Remote Application Management for Smart Glasses	X			
Remote Connectivity Management	X	X	X	X
Privileged System level device Access for complete lock down of device access by end user	X	X		X
Common UI for Normalized navigation across different smartglasses	X			
Remote lockout of device	X	X	X	
Real Time Battery Life Monitoring	X			
User Authentication	X		X	X
Shared Device Tracking/History	X	X		
Real Time Messaging to Smartglass end user	X			
Parent Child Hierarchy for separating environment by customer, use case, or region	X	X	X	X
Shared Environment Pilot/production management control between application developers and end customers	X	X	X	X
Choice of auto-app launch on each device	X			
Security GeoFencing	X	X	X	
Beacon integration	X			
Device Sensor data collection, BPM	X			

AUGMATE

Augmate Platform Solution Overview

POLICY

Wifi Credentials

Static Files

Applications

Security Settings

Selected Devices

USERS

Password Credentials

Usage Analytics

SMS Notifications

DEVICES

Application History

Device Properties

Current User Profile

SMS Notifications

Usage Analytics

Augmate WEM Architecture

Launcher
User Interface for Smart Eyewear

Secure Login
Wearable users sign into the device by entering a 4-digit PIN. User accounts and passwords are created and managed via the Augmate Portal.

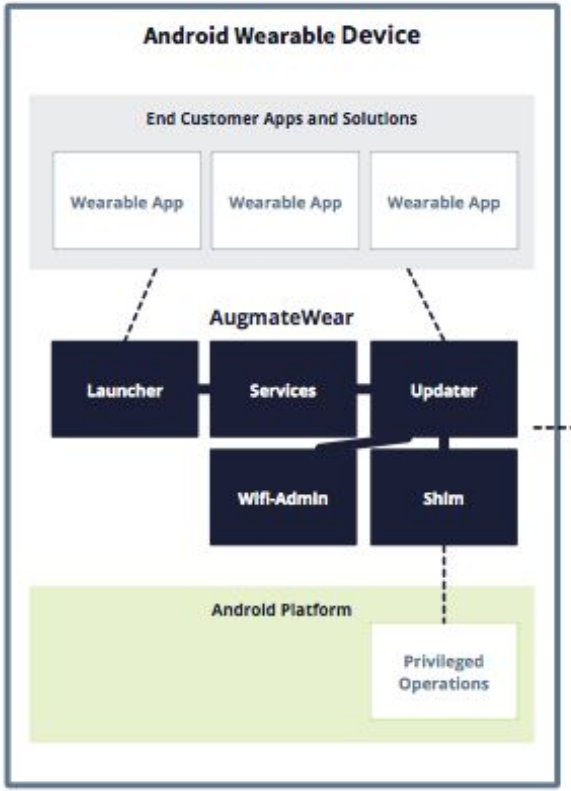
Kiosk Mode
Limits user access to only specific, pre-determined applications.

Messaging
Wearable Users can receive messages sent by network admins via the Augmate web portal.

Services
Real-time background services

Device data collection
Services tracks the device's battery status and usage, granting users of the Augmate web portal a real-time snapshot of their organizations' wearables.
By implementing *AugmateWear* in combination with Internet-of-Things technologies like locational beacons, Augmate web portal users can visualize device locations in a graphical floorplan.

Wifi Admin
Network Accessibility Management



Easy Enrollment
Devices are provisioned onto customer networks wirelessly through a web browser for a simple and speedy rollout process.

Multiple Wi-Fi Networks
Set up multiple Wi-Fi networks to allow devices to move without losing connectivity.

Updater
System-level OTA Updates

Over-the-air (OTA) Updates
Updater remotely installs and uninstalls applications, configures hardware permissions, and manages system-level settings on the wearable.

Policies
Admins can establish policies via the Augmate web portal and ascribe them to specified devices. This allows customers to manage devices according to various business needs.

Shim
System-privileged Library

Admin/Root-level Access
By installing the Shim—Augmate's system-privileged library—customers are able to perform various admin/root-level operations like installing applications and configuring hardware permissions.

AUGMATE

Augmate / Device Features

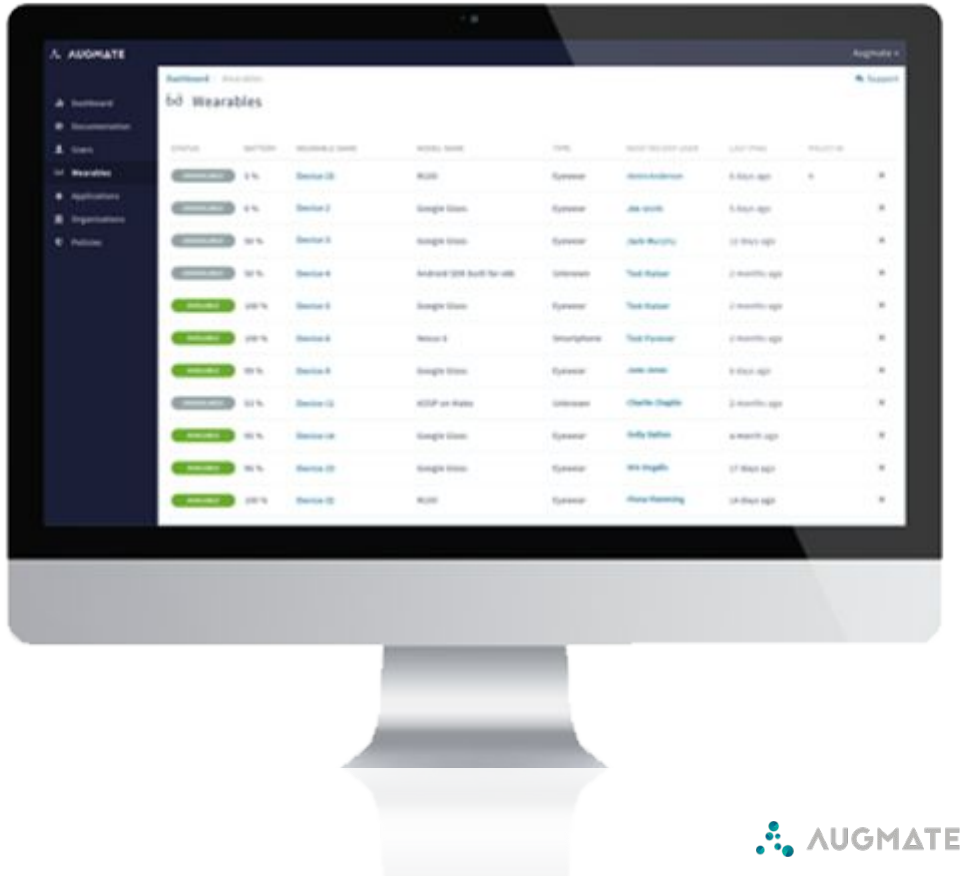
Key Features

- Augmate software at hardware layer
- Device Agnostic
- Common Menu across devices
- Provisioning Software signed by OEM
- Receive Text Messages

Augmate / Portal Features

Key Features

- Create and administer wearable users and devices
- Install/uninstall apps
- Send system-wide messages and notifications
- Establish policies to facilitate whitelisting of software applications
- Lock devices remotely
- Enable devices to seamlessly connect to multiple wifi networks
- Organize devices and users by team or customer

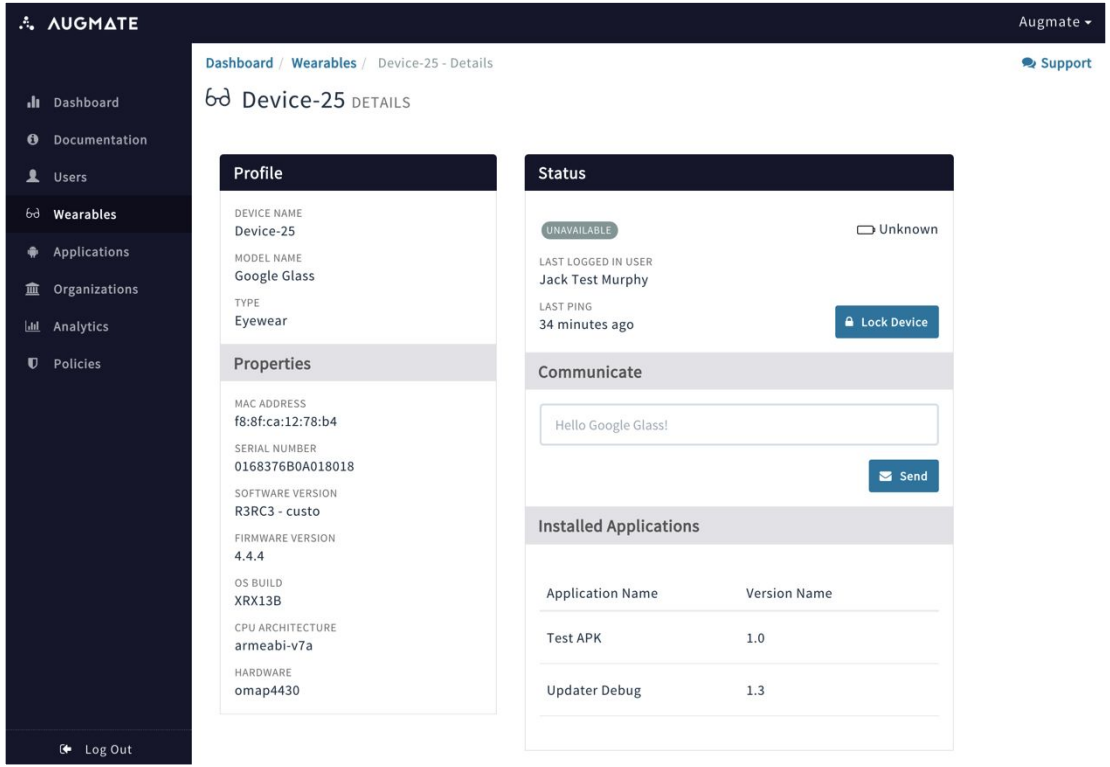


Manage each wearable across your entire organization from our portal.

AUGMATE

Portal / Wearables

Augmate gives enterprises complete control over the management of smart glasses by allowing IT administrators to operate the devices through a WEM portal. Our infrastructure platform handles device management, user management, security, policies, and over the air application deployments from the Augmate platform.



[Augmate Platform Demo](https://goo.gl/PGCmaK)

https://goo.gl/PGCmaK

AUGMATE

Augmate Technical Security Details

Mobile security incidents are expensive causing half of all medium to large companies over $100,000 per year

Device Management	Infrastructure	Database Level	Android Device Level
Security kiosk mode prevents unintended usage of devices	Immutable infrastructure for our web, API, and data ingest	SQL injection prevention	Security kiosk mode enforced by system level operations
Prevent access by remotely locking device	Managed database with periodic backups	SQL level multi-tenancy	Privileged shim that only tals with our OTA updater
Restrict device usage to Wi-Fi and Bluetooth based geofences	Multi-factor authentication to access Augmate infrastructure	Periodic backups and point-in-time recovery	APK Encryption In Transfer and at Rest
Audit applications to detect modifications installed on device	Segmented access keys to limit access between cloud resources		Wifi Credential Encryption In Transfer and at Rest
Ensure latest software is delivered to device	HTTPS encryption everywhere using only strong protocols (TLS)		
Respond quickly to security vulnerabilities	Per-organization isolation of all data		

- 52% of large companies say cost of mobile security incidents last year exceeded $500,000
- 45% of businesses with less than 1,000 employees reported mobile security incident costs exceeding $100,000

Source: dimensional research

Department of Homeland Security Selects Augmate Platform

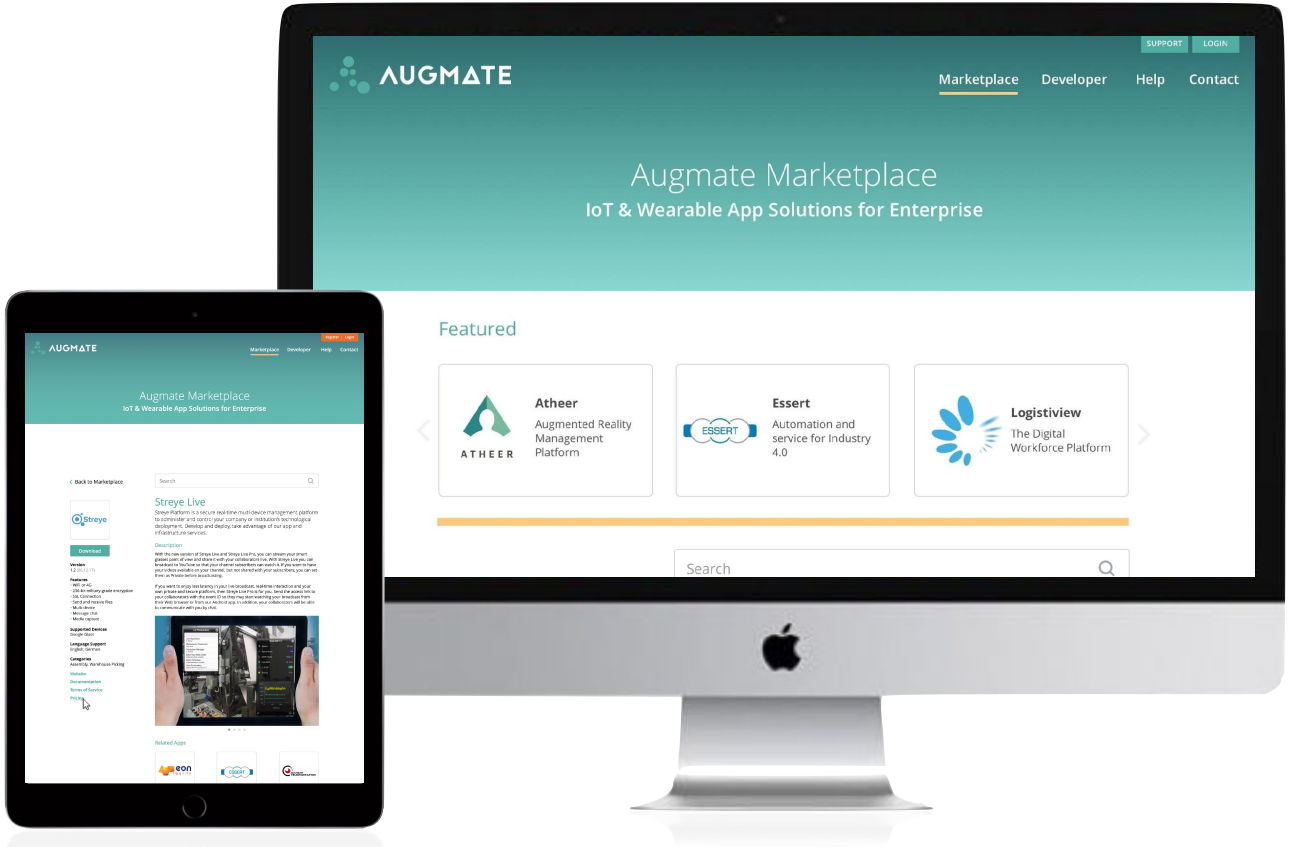
https://www.dhs.gov/science-and-technology/news/2016/10/06/news-release-dhs-st-selects-10-start-ups-first-responder

AUGMATE

Marketplace

One Stop Shop for IoT & Wearable App Buyers

- Simple, intuitive interface
- New and featured apps
- Advanced application and device filtering
- Developer admin tools
- Dashboard & Analytics
- Payments via Stripe
- ZenDesk support



Press & Awards

Gartner Cool Vendor 2017
in Enterprise Wearable
and Immersive Technologies

Thank You

AUGMATE

335 Madison Ave, 16th Fl
New York, NY 10017
info@augmate.com

/augmate
/augmate
/augmate

www.augmate.com