esper

How to develop an ultra-secure, user-first retail device strategy

Best Practices to Secure your
Retail Android Devices

Key Takeaways

While there have never been more options for innovation, growth, and scalability, the stakes for businesses are also higher than ever. Businesses today must provide customers with second-to-none digital experiences that are secure, seamless, and engaging. This requires building powerful applications on APIs that are scalable, flexible, and easy to understand.

If you're a CxO or an IT Director dissatisfied with stock BYOD options and looking to understand how to apply the principles of Orchestration to Dedicated Devices across apps, operating systems and hardware, you've come to the right place. Imagine coupling the world's most popular mobile OS with the best-in-class features of enterprise device fleet management.

Table Of Contents

Introduction

Digital transformation is everywhere. In our homes, jobs, schools, cars, at the grocery store, hospital, or airport, you name it; there's not one place that we don't witness the impact of digital technologies changing the way we live, work and play. This phenomenon is the engine to our modern economy and is creating enormous opportunities and challenges for enterprises everywhere. In fact, one report showed that 86% of CEOs say they have two years to make inroads on digital transformation before suffering financial or competitive consequences. So how are they achieving this?

Touch screens are ubiquitous

Much of this transformation is the result of what's lying in the palm of your hand. The global number of mobile phone users is expected to be more than 5 billion in 2019. Throw into the mix the dominance of consumer voice and the surge in Augmented and Virtual Reality, Internet of Things, and AI over the past 5 years and the breakneck speed of technology change becomes quite dizzying.

Let's take the retail industry for example.

According to retail analyst Joe Skorupa, "Digital transformation in retail is a radical rethinking of how a retailer uses technology to pursue new and improved revenue streams and new business models."

The focal point for this new revenue stream is dedicated devices and their touch screens. On any given day your fingers will interact with a digital device at some point, whether swiping a tablet to pay a restaurant bill, signing a receipt, or ordering your favorite espresso at a kiosk.

Scan-and-Go is the new normal

Devices are slowly replacing human workers and we see this especially in the flurry of cashierless checkout technologies like Amazon Go. By just scanning smartphones at the entrance of the store, customers can grab and go whatever they need. All the transactions and charges are tracked on the Amazon Go app.

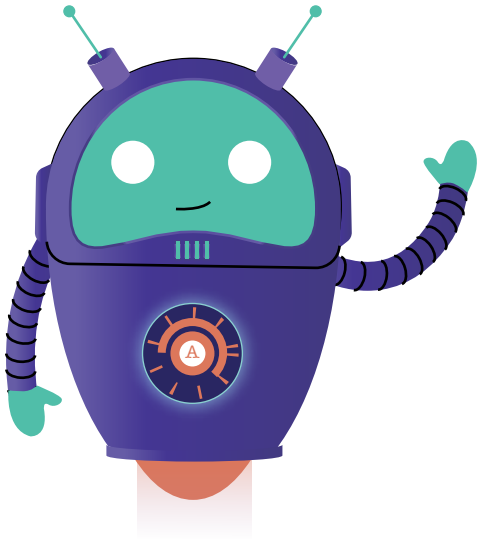
"While all of this new-fangled technology is a great thing and a digital retail strategy is obviously critical for business survival, digital transformation does present significant business and operational challenges. Consider the technology implications of balancing the increasingly complex front-end customer expectations with the backend infrastructure required to run these overlapping technologies. Legacy systems are not equipped to handle the new era of digital transformation, at least not without significant and costly upgrades."

But one of the most frequently overlooked areas of retail technology is perhaps the most critical: retail management and security. More often than not, security is the "elephant in the room" that nobody wants to discuss. The cost of inaction are substantial and there's plenty of data to back it up. A new study by Verizon shows that **33% of companies have suffered a data breach involving a mobile device with major company impact.** And hackers are more ominous than ever, with major data breaches spanning a wide range of enterprises over the past 6 years including brands such as Target, Sony, and Home Depot to name a few.

MDM is not enough

Have you noticed that the Mobile Device Management solutions in the market do not completely address the complex needs of a digital economy? MDM platforms obviously have served a purpose over the years for corporate security and BYOD. But the problem is that they still tend to follow a traditional IT perspective rather than a progressive DevOps one. With locked down policies and protocols, limited range of developer options and APIs, the task of patching and provisioning corporate devices with MDM solutions can be frequently repetitive and time-consuming. The implications are clear.

The rise of retail mobile means that digital companies today must also build corresponding measures to protect, secure, and manage their infrastructure and assets. The days of "winging it" are long over. The CxO team must face the reality about being hacked and manage tirelessly to keep critical company assets protected and secure at all times, on all devices.



The Bottom Line

Survival in today's high-stake retail race means providing your customers with a device management fleet solution that delivers seamless, secure, and elegant customer expriences. Device security is more important than ever and giving this first priority will save your company from data theft and loss of dollars.

In this whitepaper we explore the **latest trends** that impact retail device management and security, and then follow-up with **security tips** that can help you adopt a proactive approach to protecting your retail stack against hacks.

The whitepaper addressess these concerns by showcasing how Esper provides value as the industry's only **Android device fleet management platform** offering device orchestration APIs to enterprises.

The Rise of “Digital” Retail

Technology has been used in the retail space more than ever due to the digitization wave. There are many retailers who have taken this to the next level and here are a few doing a great job at it.

- Sephora’s physical to digital shopping experience is a great example. Customers can add products using NFC cards at the physical store and also through Sephora’s digital platforms for a single check out. To amplify the customer experience, they even have augmented reality mirrors that simulates makeup on customers’ faces, in real time.

- Home furnishing giant IKEA has improved the retail customer experience through AR technology. Their mobile application allows you to design a room using IKEA products via your camera.

- Amazon’s new flagship grocery stores are cashierless. Instead of grabbing a cart, get your phone, scan the “Amazon Go” app in the turnstile and enter the exciting new world of frictionless shopping. No registers, no cashiers, just rows of food items.

With the above examples one thing becomes clear, eCommerce is morphing into mCommerce as mobile is increasingly the preferred form factor for consumer engagement and transactions. Faster delivery time, better customer service, and convenience are the crux behind this revolution. In fact, mCommerce sales in 2019 will reach an estimated 44.7% of total U.S. eCommerce sales, up from 39.6% in 2018.

Adding to the rapid disruption in retail are touchscreens . . . lots of them! Wherever you go today whether Starbucks or Taco Bell, digital kiosks are popping up everywhere. More than likely you will interact with a hardware device at some point, whether paying a bill or ordering your favorite espresso on a kiosk. This is when the question arises.....

Why Retailers Are Not Serious About Device Security

Retail digital transformation is definitely changing the entire shopping experience. Just ask any customer at Lowe's who uses the in-store navigation app to find their products in a timely manner. The influx of POS terminals, kiosks, digital signages, smartphones and tablets are here to build seamless customer experiences leading to enormous changes in how businesses, people, and processes interact and overlap.

"But all of this change is not without its fair share of corporate challenges. Unfortunately, one of the tradeoffs has been a sharp rise in hackers and cyber-attacks in recent years. Retailers today are more vulnerable than ever to phishing, malware, and other infiltrations that can steal millions of financial records in no time."

That's why it is more incumbent for enterprises to pay attention to their customer endpoints in a secure and seamless way that boosts customer confidence and avoids disasters like data breaches and lost financial information.

The two focus areas that often are not stressed by enterprises are device management and security. This especially holds true in the retail industry where attention is placed heavily on the front-end experience and convenience, resulting in the backend security getting overlooked. Ron Schlecht, managing partner at cybersecurity consulting firm BTB Security sums it up this way, ***"The focus is so much on how technology fills or creates business value that security is often an afterthought."***

Unfortunately, this means that corporate management tends to turn a blind eye to security or naively assume that a major hack will never happen to them. Adding to the conundrum is the fact that enterprise mobility is a complex area and the influx of BYOD and smartphones has made security and device management more critical, but also more challenging than ever.

Without security wrappers in place, critical corporate data and assets get compromised in the process. A recent report by technology advisory firm IDC says that, “Greater than 40% of the US enterprises say they’ve had a data loss issue in the past 12-18 months.” And if internal data loss was not enough of a problem, the explosion in retail hacking in recent years ensures it is “not a matter of if, but when” an enterprise will experience a major incident.

Hackers Are Busier Than Ever

Every time we turn around news emerges about another major retail data breach. In fact, some of the most popular companies have been the target for hackers in recent years. Major companies like Chipotle, Equifax and Uber were attacked in 2017.

Chili’s, a well-known food chain believes that in the spring of 2018 malware was used in its restaurant payment systems to gather credit and debit card information.

Who can forget the Target Corporation data breach of 2013? That debacle ended with theft of 40 million card numbers and 70 million personal records. The breach started after a third-party vendor was attacked through a phishing virus. Firstly, the vendor had access to Target’s Ariba external billing system. Next, Target had poor network segmentation and the hackers were able to easily gain unlawful entry to their entire system. From there, it just got worse.

Once the system was breached, a POS malware was installed to finish the job of collecting 11GB of personal records and credit card numbers which were then siphoned via FTP to drop sites in Brazil and Miami. This information was then sent to the black market.

This massive data breach happened primarily because of several reasons:

- Target failed to investigate the initial security warnings.
- Target did not properly isolate sensitive network assets from easily accessed network sections.
- POS terminals were not hardened enough to stop unauthorized software installation and configuration.
- Proper third-party access controls were not implemented.

"If major corporations can fall victim to major data breaches, then no one is immune. Retail devices such as digital tablets, POS, and kiosks are especially vulnerable as they are the conduit for millions of shoppers' names, addresses, emails, credit cards, passwords, or other personal and financial information."

This brings us to the next point, how solid is your current retail device management and security strategy? The sad truth is that it probably will not be able to withstand the tactics of even the most amateur hackers. But there is hope!

13 Best Practices to Secure Your Retail Devices

According to a report, ***"User resistance is the most-cited reason why devices used in business are not enrolled in enterprise mobility management platforms. Among enterprises with EMM deployed, 43% cited this as an issue."*** But the honest truth is that retailers need to manage and secure their device fleet to achieve full operational efficiency, protect assets, and preserve peace of mind. Measures must be implemented to ensure employees are onboard, compliant, and proactive about protecting their BYODs and all dedicated devices against cyber attacks and malware.

Here are 13 best practices for protecting your device fleet that should be taken into account by enterprises.

1. Ensure all device software is known and trusted

Regular compliance checks and updates are critical for ensuring that all software is free of malicious code or malware that can infiltrate the enterprise infrastructure.

2. Encrypted manufacturing protocols

Any type of unsecured manufacturing process is going to create another entry point for hackers to introduce unauthorized code into production runs. Therefore, ensuring strict protocols starts with hardware security modules (HSMs) and other digital certificates to ensure full code authenticity.

3. Secure code signing

Code signing is a critical part of affirming the efficacy of your source code and scripts. Make sure that it comes with the use of a cryptographic hash to validate authenticity and integrity.

4. Secure boot with chain of trust

Secure boot is designed to protect your devices against malicious code by ensuring that only authenticated software runs on it. Secure boot goes hand in hand with chain of trust and is an integral part of any data management and security strategy.

5. Encryption key management

By including encryption key management with other data protection measures companies will be able to manage the primary steps involved in protecting, storing, and backing-up mobile device fleet.

6. Improve login credentials

Weak passwords and login credentials are the most exploited weakness on devices. Adopting long passphrases, two-factor authentication and password encryption are some of the ways to create a robust login.

7. Use an antivirus and/or monitoring

Sophisticated enterprises need security software to protect hardware, emails, cloud environment, IP information and data. What is required today is complete endpoint protection that scans your software to remove problematic files and apps and sends alerts when malware is found.

8. Keep software up-to-date

Most successful computer attacks exploit well-known vulnerabilities for which patches exist. All device software must be updated regularly to install the latest security protocols. Without timely updates, enterprises are at risk of a hack.

9. Restrict internet access

Restricted internet access for IT staff on enterprise devices should be limited to domains they absolutely need for functioning. By restricting inbound and outbound internet connections the threat of an attack is reduced. This also improves the ability to detect when malware is present on devices.

10. Secure remote access

The biggest underlying problems with remote access technologies are poor identity validation and weak authentication. Any type of remote access to field devices, if available, must be made secure with robust credentials and two-step authentication.

11. Lock your system

Devices must have a strict lockdown policy to reduce vulnerabilities and prevent corporate hacks. Another important thing to remember is to add remote wipe feature in case the device is lost or stolen. This protects company assets and reduces the risk of a data breach.

12. Use encryption

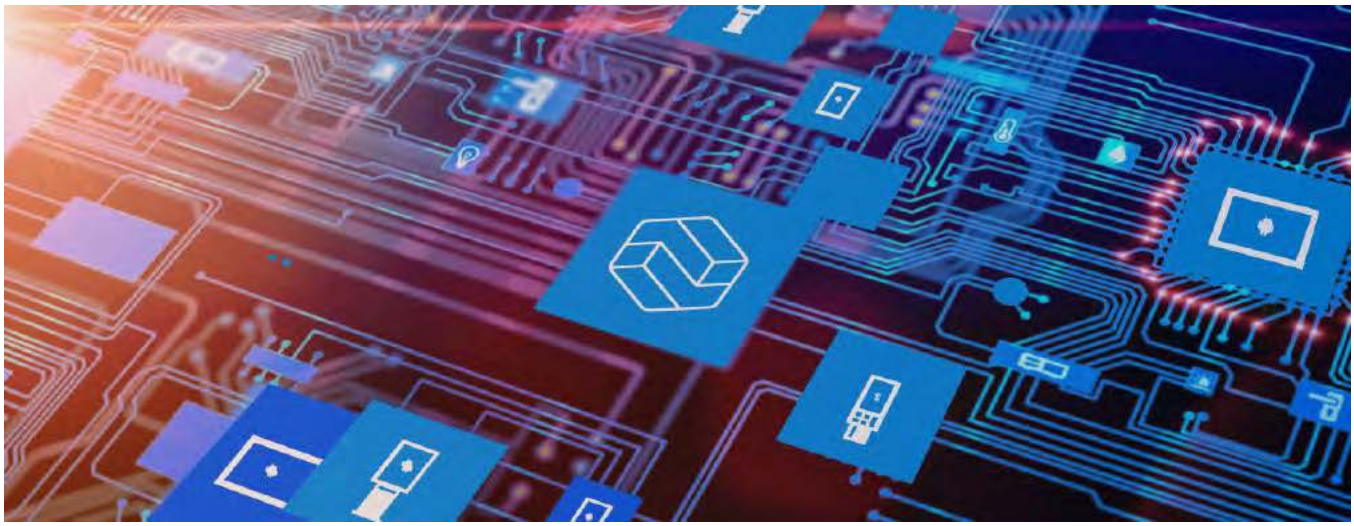
Encryption uses an algorithm to scramble data and then uses a key for the receiving party to unscramble. Adding encryption makes it very difficult for hackers to gain access to important files in case of a data breach.

13. Stay PCI compliant

If your business accepts credit cards then compliance to PCI DSS (Payment Card Industry Data Security Standard) is a must and has to be updated. In the event of a data breach, lack of PCI compliance could result in steep fines by the PCI DSS.

A Smarter (Than MDM) Way to Manage Your Device Fleet

The cloud computing and DevOps revolution over the past decade has fundamentally changed the way enterprises work and how applications get built, deployed and managed. Infrastructure-as-a-Service has migrated a lot of the heavy-lifting of server and data storage to the cloud and reduced the frustration of late-night patches and updates for businesses.



But unfortunately, when it comes to mobile device management a lot of solutions are still oriented towards a traditional IT approach. While there are platforms that contain some technology integrations, the APIs are often less than adequate for the robust requirements of today's digital economy. Developers don't want to be stuck with frequent and repetitive tasks, such as provisioning apps on devices or dealing with OS updates and patches. Instead, they want to focus on what matters to them the most - building and deploying devices at scale, helping to create operational business efficiencies and developing innovative experiences for customers.

At Esper, we give you the freedom to explore that. We're striving to create an epic shift in the way device management works by integrating it with the latest DevOps and orchestration best practices. Rather than time consuming patches and updates, developers on Esper can orchestrate dedicated devices across the full app lifecycle. Imagine defining a policy script in Python and firing it up whenever you're updating deployed devices, interacting with your development devices via API calls, or bolting in your own code to help you run your development cycles.

Esper, Built for Developers by Developers

In today's retail culture where customers expect second-to-none experiences delivered quickly and seamlessly, malfunctioning devices or connectivity issue is not an option. Such high customer demands leave businesses with little tolerance for errors or clunky IT models that don't integrate well with digital application, device management and monitoring frameworks.

What's more, enterprise developers frequently work on code bases that target millions of customers. Juggling this responsibility with periodic scaled deployments and multiple product changes leaves development teams with little time for managing cumbersome MDM policies and protocols.

"Esper provides developers with a dependable deployment pipeline for large-scale code releases that rely on secure, reliable and seamless delivery. Our solutions offer much speedier ways to tackle the big challenges of dedicated device development such as identifying, debugging and resolving issues with their apps and devices in the field."

Here are some of the rich features offered by Esper:

- Zero-touch enrollment
- Critical alerts when devices go offline, have low batteries, or security risks
- Remote viewer and remote control of devices in the field
- Device monitoring

Best-in-Class API Set

As a pioneer in device fleet management, Esper moves beyond static MDM models to provide seamless and secure ways to manage your dedicated devices. And we do this by bringing you a full set of rich API documentation and tools, including SDKs and even a CLI.

Esper APIs are a set of REST-based APIs that helps you programmatically control and monitor Android-based Dedicated Devices running on the Esper platform. With these APIs you can orchestrate and manage devices that have been provisioned by you.

Here are some key benefits of the Esper APIs:

- Develop — Build cutting edge apps using Android Studio. Start with emulation, target an existing device, or use one of our Esper Development Devices to work with Esper Enhanced Android.
- Deploy — Provision your device fleet, create policies, and deploy approved applications; connect these with continuous delivery through automated scaling and rollbacks.
- Manage — Remotely trigger app and device-level actions, as well as obtain device details such as memory, location, battery and more.

Business Use Case: Food Ordering Kiosk

Kevin wanted to add 3 kiosks for his growing food ordering startup but was stuck on finding the right management platform. His expectations were high as he required a clean, seamless platform with solid management and security protocols – along with easy and intuitive developer access and APIs. What's more, he had opted to focus on Android OS for his initial build-out.

After looking around at a few kiosk management systems, Kevin wasn't satisfied. They all seemed to lack sophistication that he was looking for. He wanted a system that was robust and provided enterprise-grade security and management standards that customers would implicitly trust. Kevin had heard too many horror stories of hacked systems and lost data and wasn't about to compromise on security.

After searching for weeks, Kevin was about to give up and even considered switching to Apple iOS when he stumbled upon Esper – industry's only Android based device fleet management platform. It seemed too good to be true and after taking a closer look and signing up for Esper trial version and playing with the APIs, Kevin knew it was a great match.

What particularly drew his attention to Esper was that it's much more than a kiosk management system. Esper is a fully dedicated Android-based device fleet management tool with complete API documentation and even a Python SDK.

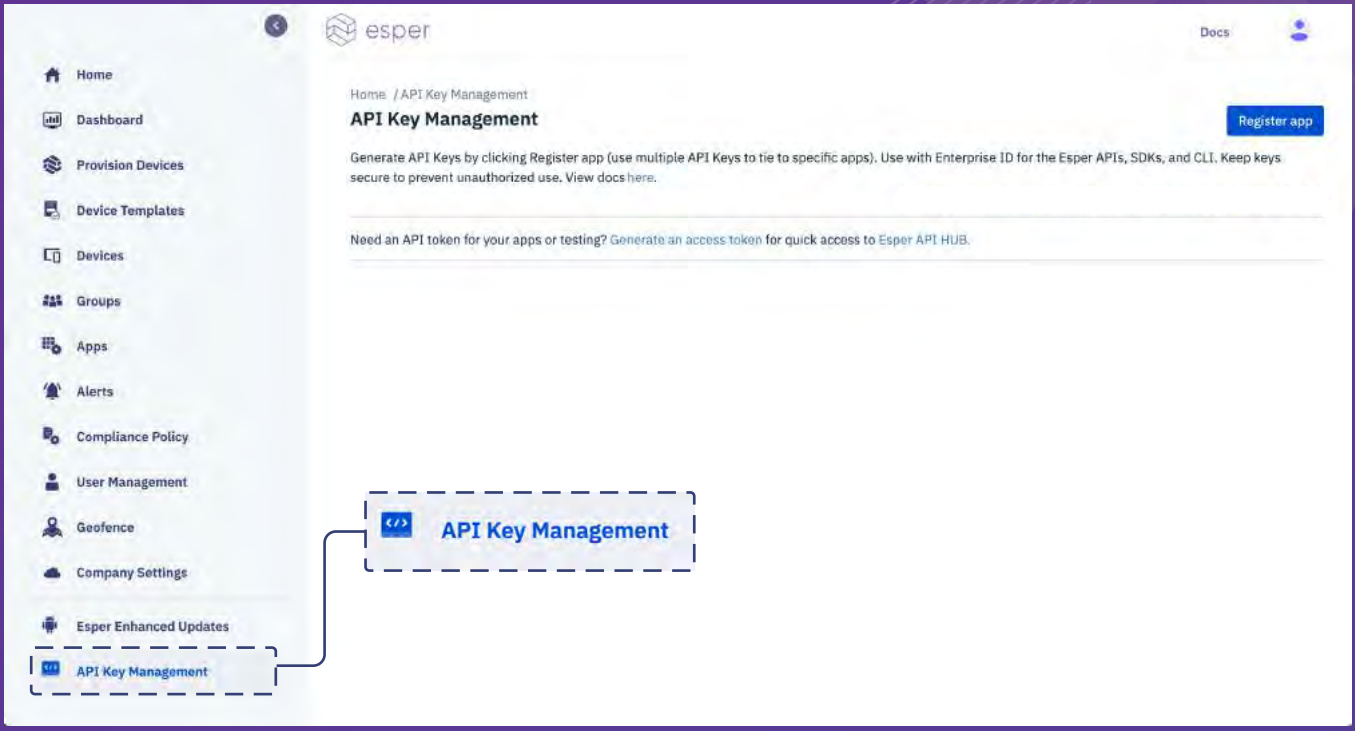
Esper's robust feature set was a dream come true, here's why

- Seamless Enrollment and Bulk Enrollment (QR Code, NFC-based, IMEI)
- Remote View and Remote Control
- Application Lockdown & Management (all the way to the hardwar elayer)
- Device Monitoring, Groups and Graphs
- Device Security State Assessment
- Device and Group Commands and Actions
- Rich Alert Engine
- Android Enterprise Support

- App Install Scheduler
- App Management
- Firmware-over-the-air (FOTA) Android OS Updates (Esper Foundation for Android)

After launching his Esper Console and private Cloud account, Kevin got busy with the intuitive and easy to understand Esper Dashboard. Here he was able to setup Device and Policy Management for his Kiosk, choose which privacy and security controls he wanted, approve applications for user download and more.

The robust options for developers on the Esper Console provided Kevin with a wide range of choices for provisioning and securing his kiosk strategy.



By registering his device, authenticating with oAuth, and setting up API calls for controlling the security and hardware features, Kevin was able to rollout a kiosk strategy which was safe, secure, and that gave him and his team the peace of mind and confidence they needed to grow their business.

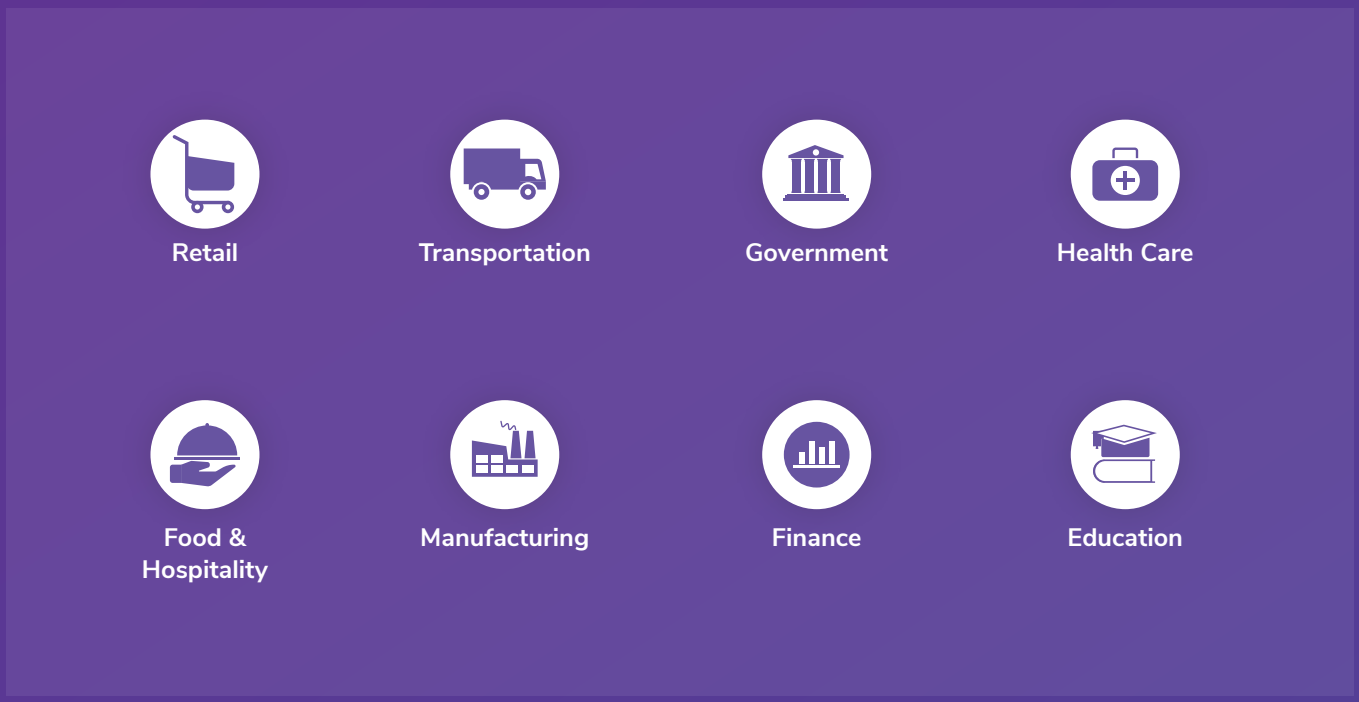
```
Curl  -x GET \
https://DOMAIN.esper.cloud[?]/api/enterprise/<enterprise_id>/
-H 'Authorization: Bearer <ACCESS_TOKEN>' \
-H 'Content-Type: application/json' \
```

What's Next?

The age of digital transformation represents both an opportunity and a challenge for organizations today. While there have never been more options for innovation, growth and scalability the stakes are higher than ever. Businesses today must provide customers with second-to-none digital experiences that are secure, seamless and engaging. And this requires building powerful applications on APIs that are scalable, flexible and easy to understand.

Imagine coupling together the world's most popular mobile OS with the best-in-class features of enterprise device fleet management. At Esper, we offer an intuitive, cloud-based connected device platform for managing all of your Android devices seamlessly and securely. Whether that happens to be a kiosk, POS, or smartphone know that your assets are safe and secure.

Esper has also joined the API economy and as a developer-focused community, we're passionate about changing the way enterprises manage and provision their apps to create secure, seamless customer experiences.



If you're in the process of mapping out your retail device fleet management strategy, then give us a call today. Whether your business consists of a food ordering Kiosk, a hospitality check-in counter, or retail point of sale, we can assist in building a solution that meets your strategic business goals and give your leadership team and employees the peace of mind they deserve.

esper

Esper is the most powerful set of tools for Android device deployment and application management. We deliver operational excellence and a stable, scalable infrastructure that help customers quickly deploy delightful user experiences at scale.

Get in touch with us

sales@esper.io

www.esper.io