



Frontline Worker Endpoint Decisions that Unlock the Value of Your Infrastructure Investments

Understand where to place your
bets for higher **ROI**

A vertical bar on the left side of the image, composed of a teal segment on top and a green segment on the bottom.

Focus Your Strategy for Maximum Effect





What You Target Affects Operational Outcomes

[Gartner estimates](#) there are some 2.7 billion frontline workers—more than twice the number of desk-based workers. These are the people who directly interact with customers, products, or services outside a traditional office setting. What they do is essential to the daily operations of industries like healthcare, retail, manufacturing, logistics, and hospitality. Examples include nurses, delivery drivers, retail associates, factory workers, and restaurant staff, and they rely heavily on mobile technology and tools to perform their duties efficiently.



that data and coming AI-driven workflows that will drive higher revenue. Without those tools, organizations can't unlock an adequate return on their infrastructure investments.

As organizations shop for endpoint solutions, there are some key considerations that should be factored in to ensure the right outcomes. Based on our decades of experience providing and supporting mobile technology solutions for frontline workers at some of the world's biggest companies, we recommend concentrating on these five key areas:

Security

Flexibility

Utilization

Business Continuity

Subsidized Transformation

That means that for a huge number of companies, getting technology right for frontline workers is critical. Employees need the right devices and fast access to information to efficiently deliver services and products to customers. If they don't, the success of the organization suffers.

Many companies have invested heavily in infrastructure like data centers, but now they need to put powerful endpoints in the hands of frontline employees to leverage faster access to

“ Employees need the right devices and fast access to information to efficiently deliver services and products to customers. If they don't, the success of the organization suffers.

Read on as we explain each challenge and explore the solutions.

Security



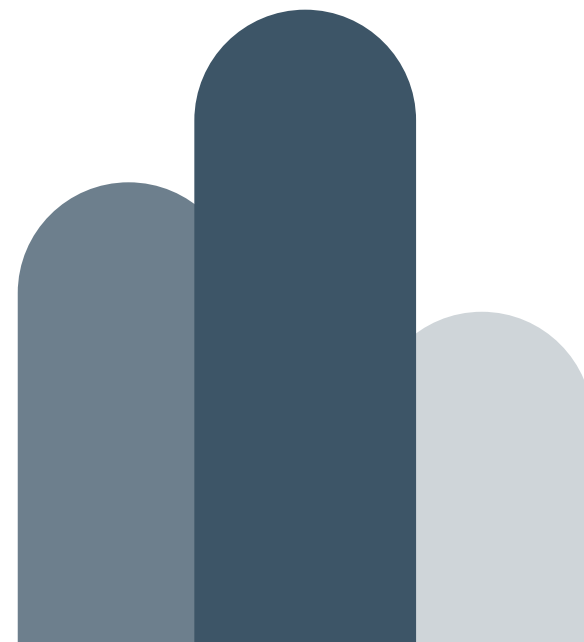


The Challenge: Distributed Workforces are More Vulnerable

Frontline workers often operate outside the secure boundaries of a corporate office, using mobile devices in various locations, such as homes, retail stores, warehouses, or customer sites. These decentralized environments increase exposure to unsecured networks and devices. For example, home healthcare workers work with highly sensitive electronic medical records and use their devices for all aspects of clinical workflows in wide geographic areas.

In some industries, frontline workers share devices or use them for both work and personal activities. This increases the risk of cross-contamination between personal and professional data and creates opportunities for security breaches.

Because frontline workers' mobile devices are usually on the move, they're more prone to being lost or stolen, which could lead to unauthorized access to sensitive data if devices are not secured with encryption or remote wipe capabilities.



The Solution:

Combine the Right Devices with Rigorous Endpoint Management That's User-Centric

To mitigate frontline workers' vulnerabilities, organizations should implement strong mobile security measures, such as endpoint management, device encryption, secure authentication (e.g., biometrics), regular security updates, and comprehensive training for employees. The key is to find the right balance between adequate protection and user-friendliness. Security measures shouldn't be so onerous they affect productivity.

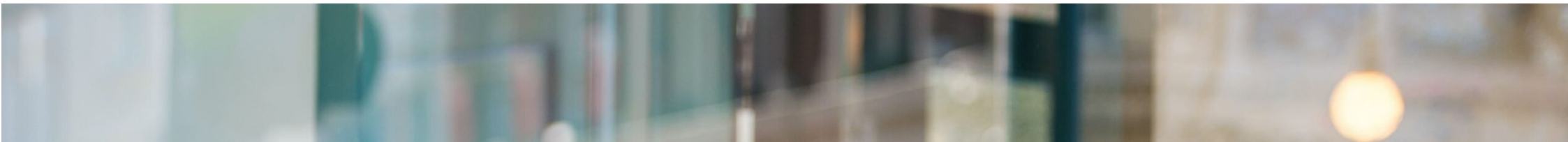
For example, Apple devices support strong endpoint security by incorporating robust security features directly into the hardware and operating system, including end-to-end encryption for data, secure boot processes,

biometric authentication (Face ID/Touch ID), strong access controls, and a dedicated endpoint security API that allows third-party security solutions to monitor and manage devices effectively—all while maintaining user privacy as a core design principle.

Stratix Unified Endpoint Management (UEM) uses containerization that separates personal information and applications from ones used for work on corporate-owned personally enabled (COPE) and BYOD devices to prevent cross-contamination while still giving the user a great experience.

This enables workers to securely access the sensitive information they need, such as medical records, payment processing, or inventory management on devices with minimal risk of data breaches.

The bottom line: IT leaders should be looking for the complete package of devices with robust and user-friendly security features and a comprehensive endpoint management strategy that layers on additional security while also automating routine IT team tasks for increased overall efficiency.



A vertical bar with a green top half and a blue bottom half, located to the left of the word "Flexibility".

Flexibility



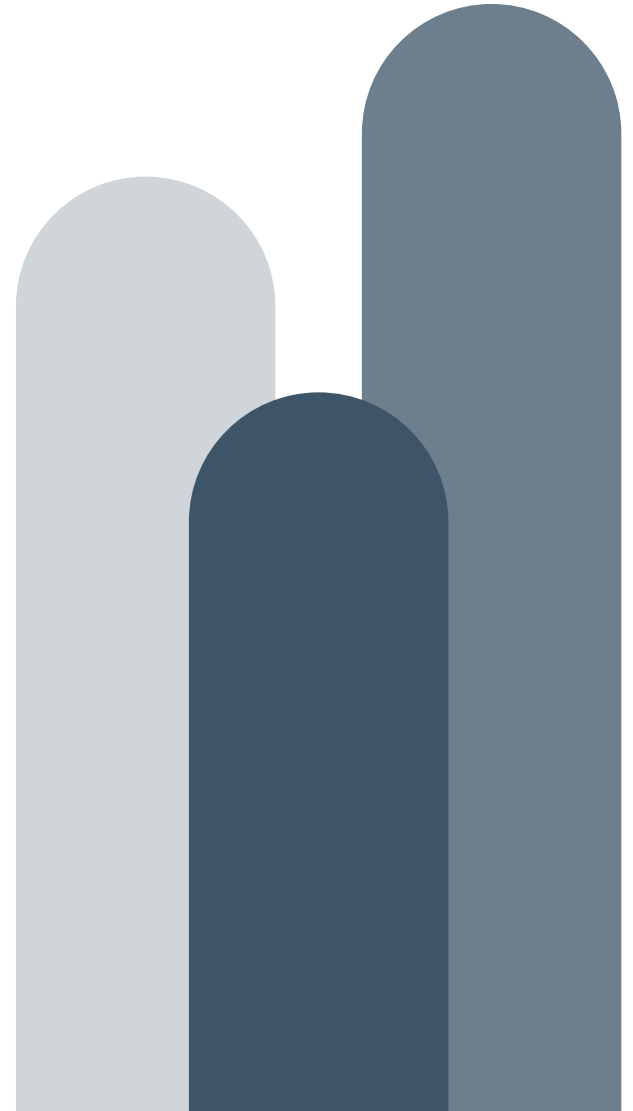
The Challenge: Purpose-Built Can Be Limiting

For many years, enterprise organizations thought that purpose-built devices for specific workflows were the way to go. In retail, for example, a completely different device for inventory scanning than what associates use for point of sale. But now, it's time to shift that paradigm.

In the past, purpose-built devices often made sense because they did the job for that use case well, and utilizing a multi-use device often involved workarounds or clunky peripherals that slowed productivity and weren't reliable. That isn't the case anymore, and buying and supporting a wide range of devices isn't a smart business practice.

Take the example of a restaurant. With specialized devices for table management, inventory and food safety, ordering and tableside payments, etc., you quickly run into a scenario where there are more devices than employees on a shift to accommodate peak capacity for each use case.

With purpose-built devices you're committed to managing separate technology solutions (procurement, lifecycle management, support, etc.) and that equates to higher costs and lower efficiency when employees can't seamlessly move between different workflows.



The Solution: Go Omni-Use

Mobile devices like smartphones and tablets are so good now—and offer such powerful apps—that the same device can easily handle different workflows quickly and efficiently. For example, the camera on iPhone or iPad paired with the right app is a highly effective barcode scanner for inventory management in retail. The same device is a user-friendly customer service tool that associates can carry with them and help shoppers anywhere in a store. You not only benefit from the simplification of your technology stack, but you empower employees to seamlessly move between workflows so they can do more—potentially lowering labor costs.

Endpoint management solutions can also be used to create different experiences for different users on shared devices when they log in—for example, showing the apps that a particular user typically needs more prominently on the home screen or completely blocking apps and information that are not relevant to what they do. In a restaurant, for example, a host or server gets one set of apps on login, while cooks get applications for kitchen management.

Your investment in the total number of devices goes down—per store, per employee—and that's amplified as you look across your organization.

Stratix services not only keep those devices supported, repaired, and working, but our UEM team consultants can build login profiles for you that are tailored to employee types and needs.

The bottom line: shifting from purpose-built devices to flexible, multi-use mobile devices streamlines workflows, reduces costs, and improves efficiency—enabling employees to seamlessly handle various tasks while simplifying technology management across the organization.



The word "Utilization" is written in a large, white, sans-serif font. To the left of the text is a vertical bar with a green top half and a blue bottom half.

Utilization



The Challenge:

Tech Often Isn't Aligned with How Employees Actually Work

For frontline workers, mobile devices, applications, and peripherals are the critical tools that they use continuously throughout their day. While most organizations recognize that, and have mobile technology solutions, a great many aren't as effective as they could be simply because leaders and developers didn't take the time to understand how their people do their jobs at a granular level.

For users, tools and platforms may feel cumbersome, unintuitive, or disconnected from daily tasks. This can lead to low adoption rates, frustration, and inefficiencies that undermine the intended benefits.

Examples include:

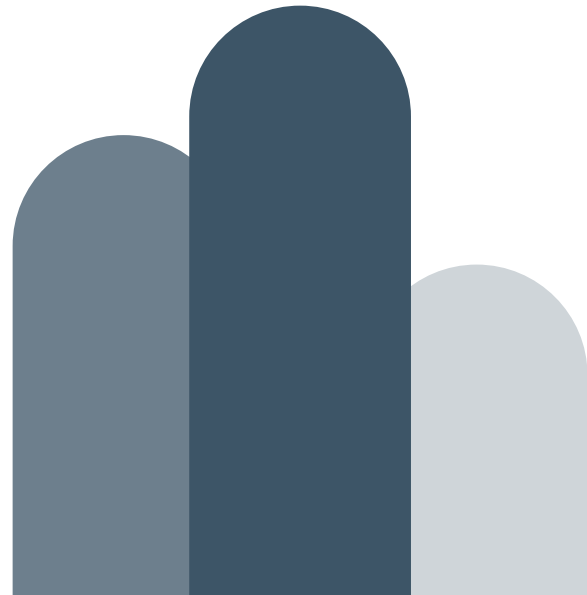
- Clunky interfaces that require excessive scrolling or tapping
- Logins that require multiple steps and passwords
- Constantly having to switch between apps in one workflow
- Manually entering data multiple times because systems aren't integrated
- Slow loading times and frequent app crashes



The Solution: Listen First & Then Build



It goes beyond listening sessions with employees. It's important to establish a group of beta testers who will try out demo solutions and give feedback.



Before running out and buying a solution "off the shelf," organizations need to do their homework. They must have an understanding of how frontline workers will use devices and what those workflows will look like step by step. How will they communicate, enter data, write, print, and access information? The goal is to make those tasks as seamless and easy as possible.

It goes beyond listening sessions with employees. It's important to establish a group of beta testers who will try out demo solutions and give feedback. While it can be challenging and feel time-consuming, the payoff is enormous

Stratix solution architects are experts in this area. Our team does the research and puts together beta solutions featuring different device and software combinations for "bake-offs" done by your testers.

With their familiar operating system and user-friendly features, Apple devices break through utilization challenges. Purpose-built applications can reduce the number of peripherals frontline workers require, and the simple, consistent

interface reduces the learning curve for employees and improves efficiency.

Because frontline workers frequently work in areas with poor cell service, Stratix offers our Connectivity service, which features SmartSIM technology. Users are automatically connected with the strongest carrier signal where they are. It not only reduces frustration and boosts productivity but there are cost savings because data is pooled among users—instead of organizations being billed for individual lines.

The bottom line: to maximize frontline productivity, businesses must align mobile technology with employees' actual workflows by involving users in solution design, simplifying interfaces, integrating systems, and ensuring reliable connectivity. This reduces inefficiencies and improves adoption.

Business Continuity



The Challenge:

Downtime Has an Immediate Effect on the Bottom Line

Technology downtime can be disastrous for businesses, as it disrupts operations, reduces productivity, and negatively impacts customer satisfaction. When systems go offline, employees may be unable to access essential tools, data, or communication channels, halting workflows and delaying critical tasks. For customer-facing roles, downtime can lead to missed sales opportunities, frustrated clients, and damaged brand reputation. Additionally, downtime can incur significant financial costs. In July 2024, the [Crowdstrike outage cost the average organization \\$44M, and the total impact was \\$5.4B](#). In February 2024, an AT&T outage took many frontline workers down and left them unable to work due to a technical error.

While both episodes are extreme examples of downtime, organizations do have to think about business continuity—especially IT and operations—from a national, local, and individual employee level because if devices aren't working, employees aren't working.





The Solution: Be Prepared

To mitigate the risk and consequences of downtime, businesses must invest in reliable technology, proactive maintenance, and robust contingency plans to ensure minimal disruption and swift recovery.

Stratix prevents and mitigates downtime in various ways. We offer customers a spare pool of preconfigured devices that can be deployed overnight. Our Connectivity service can also be used as a wireless failover to automatically switch to another cellular network in the event of wireless or fiber optic connection disruption.

The bottom line: businesses should invest in reliable devices, proactive maintenance, and contingency plans to ensure seamless continuity and swift recovery.



Subsidized Transformation



The Challenge: Budgets are Tight

Financial constraints are significantly slowing the pace of IT projects in businesses, as limited budgets force organizations to prioritize short-term needs over long-term digital transformation goals. Rising costs for hardware, software, and skilled IT personnel, combined with economic uncertainty, make it challenging to secure the funding needed for ambitious projects. As a result, critical upgrades, system migrations, or automation initiatives are delayed, leaving businesses to operate with outdated or inefficient technology.



The Solution: Find Money Where You Can

Money doesn't grow on trees, but there are ways to realize savings that will fund IT projects. At Stratix, our Telecom Expense Management (TEM) service saves customers an average of 4 percent on connectivity costs. In one case, we saved a customer over a million dollars in one year. That's money that can be reinvested in digital transformation initiatives.

Apple devices also have higher residual values—meaning devices can be traded in to fund new devices or factored into financing payments to make devices more affordable.

Another way to offset costs is what you do with old technology when it reaches end of life. Stratix partners with [Jonathan's Landing for IT Asset Disposition \(ITAD\)](#). The nonprofit group helps create a life of dignity, purpose, and belonging for neurodiverse adults through careers in IT. Instead of selling old devices or scrapping them, companies can donate and get maximum value for them—even after they've been fully depreciated. It's a win-win where companies recoup more of their technology investments while helping a good cause.

The bottom line: businesses can help fund digital transformation by leveraging cost-saving strategies like Telecom Expense Management and strategic IT Asset disposition to reinvest in critical technology upgrades.



Conclusion



Empower Frontline Workers with the Right Technology to Maximize ROI and Drive Business Growth

In today's fast-paced and digitally-driven world, organizations must prioritize frontline worker technology to unlock the full value of their infrastructure investments. By focusing on robust security, flexible multi-use devices, user-friendly design, reliable business continuity, and creative cost-saving strategies, businesses can empower their frontline teams to drive efficiency, enhance customer experiences, and contribute to organizational growth.

Investing in the right tools and strategies ensures that frontline workers are equipped to seamlessly perform critical tasks, leverage AI-driven workflows, and maintain productivity even in challenging conditions. With solutions like Apple's secure and versatile platform and Stratix's comprehensive support services, organizations can achieve higher ROI while positioning themselves for sustained success in a competitive landscape.



Want more insights?

Stay Up to Date
with **Mobile Tech**