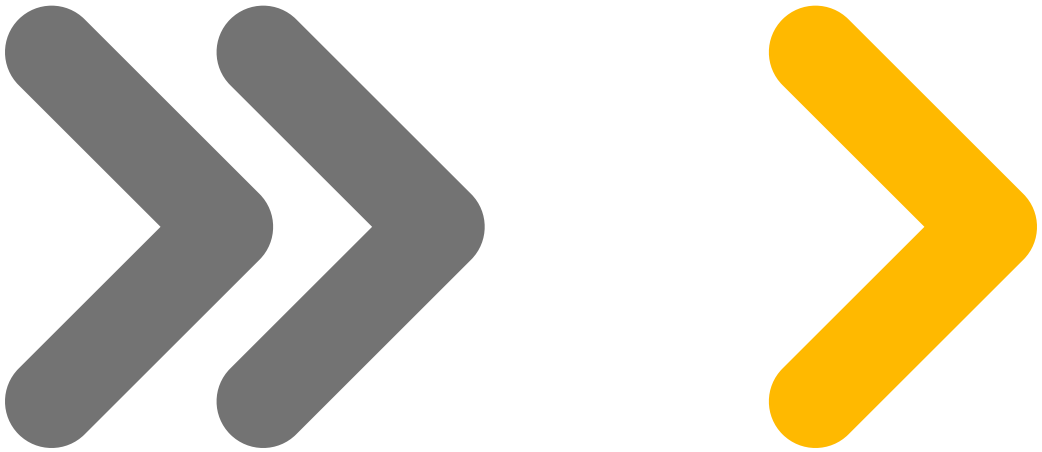
Microsoft Security

Microsoft Azure Active Directory

Empowering and securing your Frontline Workforce



Introduction

IT leaders face many challenges in uncovering the use of unsanctioned technology — or 'shadow IT' — and mitigating their potential security risks. According to Microsoft internal data from November 2019, there is an average of 181 or more software as a service (SaaS) apps in use at every organization. However, the shadow IT footprint of your organization extends beyond corporate knowledge workers.

Across every industry, Frontline Workers make up a massive segment of the workforce. This worldwide workforce includes more than two billion retail associates, factory line workers, customer service representatives, first responders and healthcare practitioners, housekeeping staff, call center teams, support technicians, field service workers, and many more. These workers are the backbone of your business—the first to engage customers, the first to see products and services in action, and the first to represent your brand.

According to Microsoft research powered by Pulse in February 2020,

65% of IT executives identify security and compliance as their greatest challenges when introducing technology to Frontline Workers.

Because frontline workers have often been left behind when it comes to digital transformation, many lack seamless access to the tools and data they need to be productive. They often don't have any form of credential or identity in organizational IT systems. Many frontline workers resort to using manual systems and consumer technology that may be unknown to IT, Business Operations, Communications, or Legal, and every unrecognized app or device introduces new levels of risk to your already complex environment.

Our investments in Azure Active Directory (Azure AD) reflect Microsoft's commitment to frontline workers. By proactively equipping frontline workers with access to the tools and technology they need on day one, IT leaders can accelerate productivity while protecting the organization with a strong identity foundation.

When it comes to Frontline technology,

the top priority for 74% of IT leaders is ensuring the security of company and customer data,

followed by providing relevant technology tools (66%) and boosting productivity (59%).

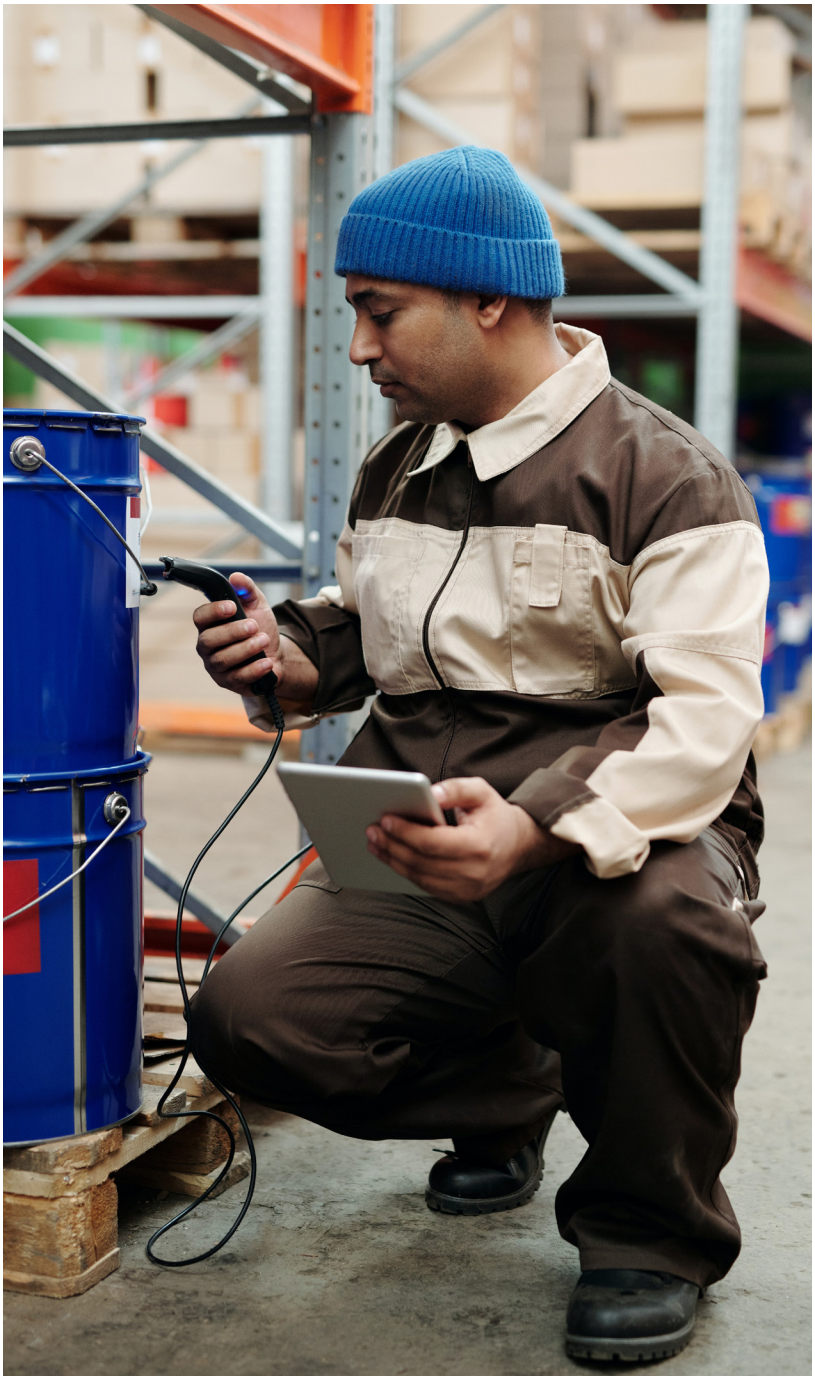
Determining sign-in methods based on risk

Each application that IT is unable to manage and secure exposes your organization to security and compliance risks, especially as frontline workers encounter sensitive data or are subjected to evolving regulatory standards.

It can be a struggle to balance seamless user experiences and security. When should you prioritize a low-friction method of authentication to encourage ease of use, and when should you enforce strong authentication policies? The answer depends on what access and data your frontline workers need.

Many organizations recognize that frontline workers use unsanctioned technology as a workaround to communicate with teammates, check their shift schedules, record information or look up data, and plan. When a user no longer needs to create their own solution to fit their needs, they're less likely to use outside apps — and more likely to increase productivity.

54% of IT executives suspect that frontline workers use a variety of unsanctioned shadow IT, including document - or file - sharing tools and social messaging apps.



In the contexts frontline workers most often operate in, any additional friction to accessing technology results in lost productivity and poor customer experiences, or encourages the proliferation of lightweight shadow IT solutions.

Reducing some friction in authentication enables frontline workers to onboard and quickly access the productivity apps and tools they need. For example, enabling SMS sign-in allows frontline workers to sign in with one-time passcodes sent to their phone via SMS or text, eliminating the need to remember a username and password for Microsoft Teams, custom line-of-business (LoB), or other SaaS apps.

Highly regulated industries where frontline workers encounter sensitive data, such as patient information, may require stronger phishing-resistant options. For these scenarios, IT leaders may consider using FIDO2 security keys—a Fast Identity Online (FIDO) standards-based passwordless authentication method that can come in any form factor, such as an external security key or a platform key built into a device. Microsoft offers Windows Hello as a biometrics-enabled platform key, and also integrates with several FIDO2-compliant security keys from partners.

97% of IT teams agree or strongly agree that reducing sign-in friction for your frontline workers would improve their productivity.

Scaling identity management for Frontline Workers

Given the scale of the frontline workforce across many businesses, IT leaders must scale their ability to manage many new users and identities.

Some organizations assign common, tactical identity management tasks to frontline managers to free IT teams to address more strategic objectives. Additionally, this delegation of basic IT controls can help frontline managers develop stronger relationships with their direct reports.

With delegated user management, frontline managers can be granted access to a lightweight portal called 'My Staff' that offers a simpler, user-friendly admin experience. From the My Staff portal, managers can unblock staff issues such as resetting passwords or enabling SMS sign-in by adding phone numbers without needing to call a corporate IT help desk. This capability not only reduces the burden on IT to support hundreds of thousands of users, but also keeps employees connected to the apps they need on the job.

Putting these steps into action can pay off in big ways. By moving to Azure AD, Mattress Firm's IT department went from 12 associates managing identity and access for the company's 10,000 retail associates down to just 2, freeing up 10 IT employees to work on more strategic projects.

Given the opportunity, 68% of IT teams would delegate some basic identity management decision making to their frontline managers. Only 10% would retain all identity management responsibility.

"It's simple to assign permissions for associates to access content, instead of going to IT to establish access rights for people. We don't need to waste time with setting up the team to get things done."

- Tony Miller, Senior Vice President of ITS and Supply Chain at Mattress Firm, "Mattress Firm Hero case study"

Managing devices for Frontline Workers

Lastly, organizations must evolve their strategy to manage not only frontline workers' access to apps but also the devices they use, whether these are personal, shared, or dedicated company-owned devices.

Although 64% of companies assign a device to their employees, up to 36% of IT executives allow frontline workers to use their own personal device for work-related tasks.

Some questions to consider when evaluating device security and management:

- Are users assigned devices by the organization or are they using their personal devices?
- Are users assigned their own device or are they sharing with others?
- Do users take their devices home or leave them in a secure location at the office or store?

Today, many frontline workers use personal devices on the job. As organizations adapt to evolving regulations on the use of personal devices, many IT executives expect to change their policies as well. In the meantime, many rely on capabilities such as off-shift access controls built into Microsoft Teams, which restrict access to the application when frontline workers use their personal device off the clock. Simple notifications and access controls help employers comply with labor regulations and protect company data.

Many frontline workers share devices with multiple employees across shifts or locations, posing unique operational and security challenges. Employees may have varying levels of access to applications and data that should not be available to others using that same device. With the shared device sign-out capability in the Microsoft Authentication Library (MSAL), IT administrators can mark devices as shared to manage this device scenario. This enables users to sign out of all their apps and browser sessions on a device with just one click, protecting both their personal data and company data before handing off the device to a teammate or returning it to a hub.

About 59% of frontline workers that are assigned devices share them with coworkers in some capacity.

Partner across your business to empower Frontline Workers

Balancing ease of use and access to technology with security continues to be a challenge, particularly for executives who must adapt to unique operational, legal, and regulatory circumstances that govern frontline worker use cases. Microsoft's approach to streamlining the user experience across apps and devices can significantly help reduce the shadow IT footprint and strengthen the security posture of the organization.

Although IT leaders drive decision making for technology requirements, getting buy-in from partners within your organization is crucial for success. Working with HR, Operations, and other parts of your business will contribute to a more robust strategy for frontline workers technology.

Learn more about how Microsoft 365 for Firstline Workers can help you empower your frontline workforce