Microsoft

Evaluating Frontline Workforce security & access needs

Over 2 billion people worldwide are Frontline Workers. From interacting with customers to handling new products to executing organizational strategies, frontline workers move your business forward.

To do their work efficiently and effectively, frontline workers require the appropriate technology and digital resources for their specific roles and tasks. At the same time, IT is expected to provide not only seamless, expedient access to critical apps and devices, but also ensure these experiences are completely secure and meet evolving compliance standards.

65% of IT executives have called out security and compliance as their greatest challenges. *

As the profile of a frontline worker varies between organizations, so do their specific needs and requirements to do their jobs. Azure Active Directory (AD) is the identity and access management solution that adapts to your Frontline Workers' specific needs, while taking a strong security and compliance approach by design.

To get started on your identity and access journey for frontline workers, begin by asking these key questions.

*Equip Firstline Workers with Better Tools to Drive Engagement, Forrester Opportunity Snapshot: A Customer Study Commissioned by Microsoft, December 2018

What devices does the frontline worker use?

Who owns the device?

Is it a personal device?

Restricting frontline worker access to applications on personal devices when on the clock is necessary for many organizations.

Other organizations may need the flexibility of allowing frontline workers to securely use their personal device ("bring your own device") to complete time-sensitive tasks.

36% of IT executives allow frontline workers to use a personal device for work-related tasks*

Is it a corporate-assigned device?

Your organization may have specific devices assigned to individual frontline workers.

Devices specifically supplied by an organization can have pre-defined controls and permissions that make user management more streamlined.

64% of companies assign a device to their employees*

Is it an assigned device shared between multiple frontline workers?

Frontline workers may have different applications they access on shared devices, which IT must configure and customize.

Shared device mode can help: Microsoft Endpoint Manager enables provisioning of shared devices at scale, as well as customization of Conditional Access policies and customized sign-in experiences with Managed Home Screen. Frontline workers easily sign out of shared devices with shared device sign-out for Android and iOS.

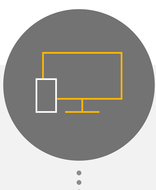
About 59% of frontline workers with assigned devices share them between coworkers in some capacity*

*Microsoft internal research, 2020

How are identities and devices being managed?

What policies are in place for the device?

Depending on the level of security needed, more specific device authentication policies may be necessary, including Conditional Access, Multi-factor authentication (MFA), and Terms and Conditions controls.



Does IT delegate any management to Frontline Managers?

Some IT teams may choose to delegate common identity management tasks to Frontline Managers. Delegated user management through the My Staff portal can equip managers and supervisors to assist frontline workers with password resets or SMS sign-in set up, saving time and resources without having to contact a central IT help desk.

68% of IT teams would delegate some basic identity management decisions to Frontline Managers, while 10% would retain all identity management responsibility*

*Microsoft internal research, 2020

What work is being done on the device?

Is it critical to map the individual to a specific task?

A frontline worker may be responsible for a particular task, requiring their actions on a device to be associated with a specific user. For example, a retailer may want to designate specific frontline workers that have access to the cash till.

How data sensitive is the work being performed?

Highly regulated industries, such as medical organizations working with sensitive patient information, may require additional Conditional Access policies to restrict access to only specific frontline workers using approved devices inspecific locations.

What's the frequency of the work being done on the device?

Frontline workers may only work with an organization for a given amount of time. For instance, they may take part in a single training, while others work on a project within an organization for years.

How time sensitive is the work being done on the device?

Highly time sensitive tasks, such as checking out a customer on a device, require a more seamless sign-on experience that may choose to prioritize ease of access over strict security. Depending on the sensitivity to time or data, organizations may choose to adjust authentication methods and security policies accordingly.

End-to-end security for frontline workers

Security is at the heart of Microsoft's solutions for frontline workers, starting with a strong identity foundation. Azure Active Directory leverages the breadth and depth of Microsoft intelligent security to constantly improve your security posture:

- **8 trillion** threat signals analyzed daily
- **5 billion** device threats detected each month
- **630 billion** monthly authentications
- More than **1 billion** Azure user accounts

Learn more about how Azure Active Directory can support frontline workers: aka.ms/frontlineidentity