theEMPLOYEEapp®

MAKING THE CASE TO IT:

An Internal Communicator's Guide to Evaluating Technology Vendors

MAKING THE CASE TO IT:

An Internal Communicator's Guide to Evaluating Technology Vendors

Contents

Introduction

What would you do if your company's website, intranet, mobile app, or technology systems were compromised? How would a cybersecurity attack aimed at your company affect you and your employees? What kind of liability would your company face in the event that employees' personal information was exposed as a result of a data breach?

As an internal communicator, you probably don't spend a lot of time thinking about these scenarios—aside from the few times a year you send communications about phishing scams. You are likely to be more focused on pushing out important information to your company's employees and measuring the results of your outbound messages to ensure success. However, your co-workers, in the IT, information security, and compliance departments, think of these "what ifs" constantly.

The technology tools that you bring into an organization can have a profound impact on your fellow employees — in a positive or negative way. They can foster collaboration, keep employees connected and informed, and help reinforce your company's unique culture. But these tools can also present significant security and compliance risks, creating more work and problems for your IT department.

Cyberattacks on the Rise

The larger and more successful a company becomes, the bigger the target on their backs. Cybercriminals know that enterprises generate and store all kinds of valuable data, and they'll stop at nothing to gain access to it. According to a 2020 report by cyber insurance and security firm, Coalition, **ransomware attacks against companies have increased by a staggering 100%** from the end of 2019 to Q1 of 2020.[1] We've also seen a **67% spike in the number of email attacks** in the first half of 2020.[2] And the cost to a company's bottom line after a breach is devastating. IBM and Ponemon calculate that the median cost of a data breach for an enterprise is $3.86 million.[3]

With cybercrime on the rise, IT teams have no choice but to clamp down on requests for technology tools that don't meet the organization's security standards. Sure, these tools might make employees' lives easier, but in the long run, they often present a myriad of security and compliance risks that simply aren't worth it.

As a result, many line-of-business managers are finding work-around solutions behind the scenes, secretly downloading apps that might not meet the company's data security and privacy requirements. This is also known as shadow IT — and we *don't* recommend it.

Avoid the Risks of Shadow IT

One unfortunate side effect of the ongoing battle between IT and frontline managers, such as HR and internal comms, is the rise of so-called shadow IT. Shadow IT is defined as any infrastructure, tools, and technologies that are used by employees outside of the control of the organization's IT team. This could be employees using their personal accounts, personal hardware, unsanctioned SaaS services, or applications for corporate communication and data-sharing, both inside and outside the corporate network perimeters. In fact, a sobering 80% of workers admit to using SaaS applications at work without getting approval from IT.[4] But doing so comes with a great deal of risk for the company. A study from EMC reveals that data loss and downtime cost a total of $1.7 trillion each year due to shadow IT-induced security breaches.[5]

To avoid these risks, frontline managers, HR, and internal communicators need two things: approved tools that don't force them to choose unsanctioned apps, and greater support from IT. They want to know what options are available to them and which pitfalls to avoid. But open communication lines with IT are a must. It's not uncommon for internal communications teams to come into conflict with their IT counterparts. A 2019 survey by Ragan found that 36% of internal communicators said their biggest barrier to properly measuring their employee engagement initiatives was a "lack of technology support."[6]

So, what can communicators do to win the trust of IT security professionals when it comes to employee engagement and communication tools?

1. **Get a sense of the bigger picture when it comes to security and risk.** Turning to shadow IT increases the chances of a data breach (which are already high), along with penalties for non-compliance with laws and regulations, and increased reputational risk for your organization. COVID-19 makes this impact even worse, given the number of employees working remotely, including the security team itself.

2. **Offer transparency and visibility into the tools you're evaluating.** The number-one request from your company's security team is visibility. It's important for IT to have access to information about the security policies and data protection features of any technology that you're considering. That includes proof-of-concepts, mobile apps, or any digital asset that customers and employees are engaging with. Trustworthy vendors will be able to provide this for you.

3. **Create an IT-approved security checklist for your third-party vendor partners.** Whether you're conducting a formal RFP (request for proposals) or still in the early information-gathering stages of investing in an employee communications tool, you will have questions for vendors. Be sure that you're asking the right ones on the topic of cybersecurity by creating a checklist. Have your IT department review it for accuracy.

Creating a Cybersecurity Checklist

Now that you've got the basics down on data privacy, cybersecurity, and the dangers of bringing unsanctioned apps into the enterprise, let's talk about how to use your new knowledge when evaluating technology partners and software vendors. We mentioned earlier in this ebook the idea of creating a security checklist.

Here are a few simple steps your internal comms team can take to ensure you are following best practices:

- Perform your own communications risk audit by making a list of any proof-of-concepts, mobile apps, cloud-based software, vendors, programs, subscriptions, and digital assets that customers and employees are engaging with.
- Report any potential shadow IT threats to IT and ask them to review for security concerns.
- Ask any new technology vendors you're considering to provide you with a list of their security policies and data protection features.
- Ask IT to review those new technology vendors, along with their security policies and data protection features, for any security or data risk concerns.

These basic questions for any potential technology vendors can help you get started with the vetting process:

- How often do you conduct vulnerability testing on your product? Can you share the results of these audits?
- If your solution is cloud-based, which cloud service provider are you using, and can you share their security and privacy policies?
- How does your content management system protect employee data? Will third parties ever have access to it?
- Is your solution compliant with data privacy regulations such as GDPR and any state privacy laws where we do business?
- How will the data about our employees be encrypted, both at rest and in-motion?
- How and where will data be stored, and will it be encrypted?
- Who has access to our data, and do the control mechanisms in place meet our company's IT security policies?
- How will you dispose of our data when it's no longer needed?
- What kind of data backup and recovery services are in place in the event of an IT infrastructure incident?

Depending on their responses to your questions, you may need to dig even deeper. For example, your vendor partner may help you store data internally, or they may store it on their own system or in the cloud. If the system is cloud-based, it's important to know the physical location of the cloud servers. Keep in mind that data is not always hosted in the same country as the vendor. This can be an issue if your organization has strict confidentiality rules.

Satisfying IT's Security Requirements Benefits Everyone

At theEMPLOYEEapp, we believe that the right internal communications tools should meet and exceed your needs as an internal communicator, while also satisfying the security requirements of your enterprise IT team. IT and internal communications should be allies in the battle against cyberattacks. As a member of the internal communications team, it's important to set the right example for the rest of the workforce when it comes to good cyber hygiene.

Cybersecurity incidents do have a direct impact on your role. Data breaches have a demoralizing physical and psychological effect on the workplace and can erode trust between a company and both its internal and external stakeholders. Convenience and ease-of-use of a technology solution should never come at the expense of safety and security. No matter your role within an organization, data security should be a top priority, as it ultimately benefits the company's bottom line and all who work there.

The key is to select tools and platforms that make it easy for your IT team to say yes. The tools you use should offer two key attributes: (1) they must meet the organization's security policies and regulatory mandates, and (2) they also should lighten the load on your IT team. It's certain that your company's IT team is already doing too much, and probably without the proper budget and manpower.

By demonstrating that you empathize with your IT team and understand their core requirements when evaluating any new technology or tool, you can bridge the gap between IT and internal comms and ensure that the solution you choose will not put the company at greater cybersecurity risk.

Data Security Terms and Protocols: An Internal Comms Cheat Sheet

To help internal communicators better understand where their IT team is coming from, we've defined some of the key technology concepts you should know when creating your checklist. Taking the time to learn about these concepts will go a long way towards fostering smoother collaboration between internal comms and IT. Knowing these basic IT security terms will also help guide you when evaluating vendors and tools.

Data Encryption: Encryption is a method of scrambling plain text in emails, stored files, and in the cloud, until it is just a vague alphabet soup with no meaning to anyone except those who have the encryption key to decode the data. This means that even if data is stolen, there's nothing criminals can read and misuse — provided that they don't also steal the encryption keys on their way out. There are several different encryption types commonly used in the enterprise today.

Data Retention Policy: A data retention policy is documentation showing that your business has a process to follow when data collected about customers, employees, and partners needs to be stored or deleted. This includes retaining data and records for a specified period of time, and also promptly deleting or destroying records once the retention policy is up.

Incident Response: Incident response is a term used to describe how a business will handle a data breach or cyberattack. This includes the way the organization discloses a breach to the impacted parties and possibly to the public, and how it manages the consequences of the attack. All businesses need to have a clear incident response plan in place, and it's likely that your IT team already has one. Your vendor should also have one in place regarding your data.

Native App: A native app is one that is installed directly onto the smartphone and can work, in most cases, with no internet connectivity, depending on the nature of the app. Native apps are installed digitally on a smartphone through an application store (such as Google Play or Apple's App Store).

Penetration Testing: A type of security testing that involves a simulated cyberattack to uncover any weaknesses in an application. Penetration testing helps security professionals understand how an app will behave in the real world if a hacker is poking around for a way to gain access to it.

Cheat Sheet
CONTINUED

Privacy Policy: A public statement for an online business that states how the company will collect data on users. This includes what kind of information is gathered, how data will be used, managed, and protected, and whether any of this information will be shared with third parties. If a website or mobile app collects personal data from users, including your employees, that company is required by law to post a public privacy policy in most countries.

REST API: An API, or application programming interface, is a piece of software code that allows software programs to interact with each other. REST, short for REpresentational State Transfer, is a commonly used API for enterprise-grade applications.

Single Sign-On (SSO): SSO is an authentication method that enables users to securely sign in to multiple applications and websites by using just one set of credentials, such as an email address or social media account. SSO authenticates the end user for all the applications the user has been given rights to, and eliminates future password prompts for individual applications during the same session.

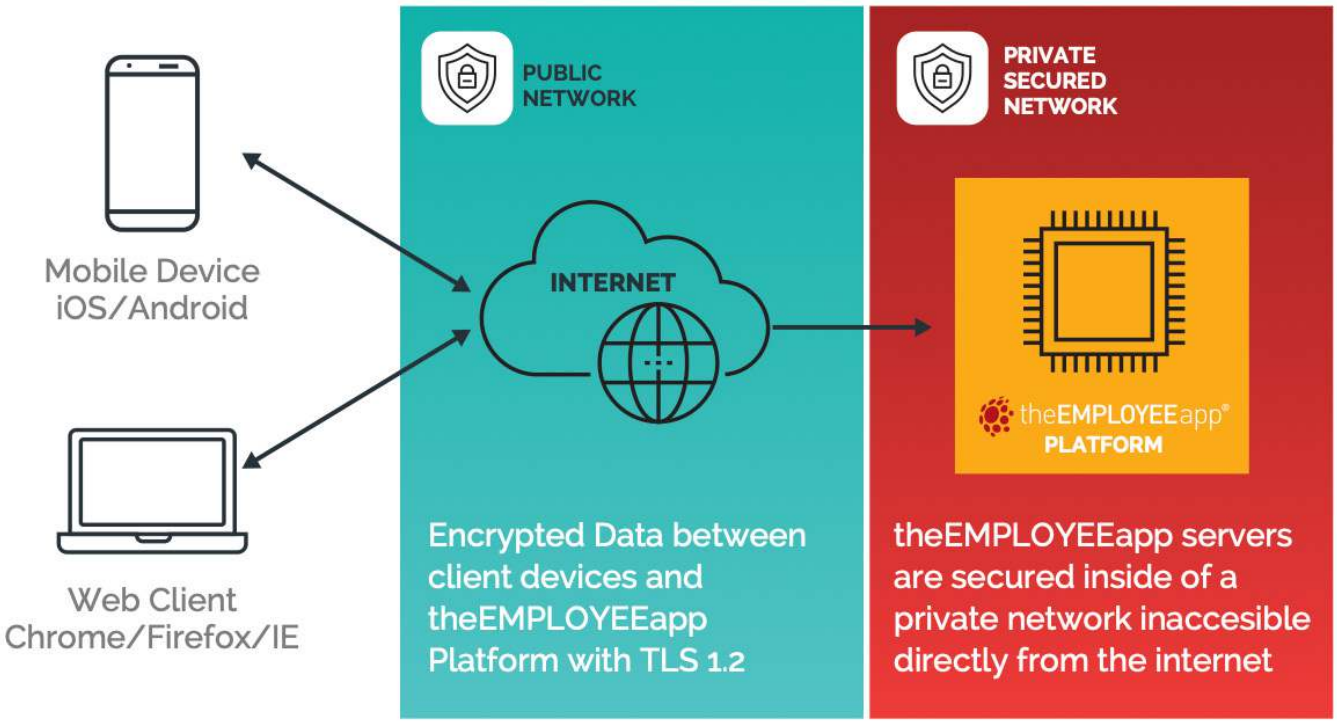
SOC 2 Type II Compliance: Many enterprises who work with cloud-based vendors consider SOC 2 Type II compliance a requirement for doing business with them. Passing the Service Organization Control (SOC) 2 Type II examination shows that an organization has had an independent auditing firm review and certify their security controls. A company that has achieved SOC 2 Type II certification has proven its system is designed to keep its clients' sensitive data secure.

Vulnerability Testing: Vulnerability assessments are most often performed by using an off-the-shelf software package to scan for known vulnerabilities, such as malicious software bugs or missing software patches that can increase your app's risk. After the scan, vulnerability testing software can generate a comprehensive report that lists discovered vulnerabilities. Some solutions even offer enterprises an indication of the severity of the vulnerability and basic remediation steps.

Web App: Technically, web apps are not real applications. Instead, they are websites designed to look and feel like a corresponding native app. Web apps run over a browser and are typically written in HTML. Users access them as they would any web page. Like websites, web apps are subject to cyberattacks, such as phishing, in which hackers build a highly convincing "fake" version of the web app. The victim is redirected to the phony web app and unwittingly enters their login and password data, and voila. The hacker has succeeded.

Peace of Mind, Light Load for IT

Give your IT security team the peace of mind that comes with knowing an application won't create more headaches for them. With theEMPLOYEEapp, internal communicators can find common ground with IT and feel confident in the security of sensitive data.



Here are seven reasons why your decision to partner with the EMPLOYEEapp will be welcome news to your IT department:

1. **Annual vulnerability assessments from industry leader, Veracode.** theEMPLOYEEapp conducts annual vulnerability testing of its entire platform and an extra assessment upon completing any major platform upgrade. We utilize the services of independent, reputable, third-party testing firm, Veracode. In our most recent comprehensive vulnerability assessment, theEMPLOYEEapp received a score of 100 — the highest score given by Veracode for any third-party application testing.

2. **A cloud-based platform, delivered via Amazon Web Services, ensures data integrity.** theEMPLOYEEapp's data aggregation engine utilizes a virtual private server (VPN) and is hosted in a SOC 2 Type II-compliant, off-site data center controlled by Amazon Web Services. This ensures that your data is backed up in a state-of-the-art, secure facility. Snapshot backups are performed every six hours, and are saved for two days. A single daily snapshot is kept for seven days, a single weekly snapshot is kept for four weeks, and a single monthly snapshot is kept for 13 months.

Peace of Mind
CONTINUED

3. **Easy but secure content management via our mobile app.** theEMPLOYEEapp content management system (CMS) is custom-built for our clients to easily manage all internal communications content for their branded app. It is built on the MERN (Mongo/Express/React/Node.js) stack of technologies and incorporates Secure Sockets Layer (SSL). Internal communications teams can confidently upload content to the CMS via an Internet browser and completely control how it appears in the app. Further, there is less third-party risk, because theEMPLOYEEapp does not manage your company's app content (except for hard-coded graphic images).

4. **Integration with all of the leading HRIS tools you're already using.** theEMPLOYEEapp supports many integrations to various systems, including the leading Human Resources Information Systems (HRIS) such as ADP, Workday, UltiPro, Kronos, and SuccessFactors. We also integrate with survey platforms like SurveyMonkey, Jebbit, or Qualtrics. And we can link out to Wellness Portals, Self-Service, Timekeeping, and much more.

5. **A strong security policy.** We're happy to share theEMPLOYEEapp's company security policy with our customers and prospects. Our security policy explains theEMPLOYEEapp's written guidelines that apply to our employees and any third-party partners who govern data security and have access to our data.

6. **A robust disaster recovery plan.** The disaster recovery plan includes a contingency plan, in the event that service through AWS is interrupted, to ensure application uptime and continued data protection. Our customers and prospects are welcome to review it at any time on request.

7. **SLA-backed security.** theEMPLOYEEapp stands behind a detailed service level agreement (SLA) with our customers that clearly communicates all the ways in which we protect your data. Most SLAs focus primarily on application uptime, but theEMPLOYEEapp goes beyond that to also ensure that our software meets regulatory compliance and the most current security standards, as set by the Apple App Store and Android Store.

Mobile devices and apps are now a major part of the enterprise tech experience. Mobile devices and customized apps have gained more appeal as a way to engage with all employees, especially those who do not sit at a desk or access a corporate email address. Many of these apps collect, share and store large volumes of data — both customer and employee information. It's important for line-of-business managers to work closely with their IT departments to ensure that the technology tools they bring into the organization to achieve their goals don't end up becoming weak links in the security chain.

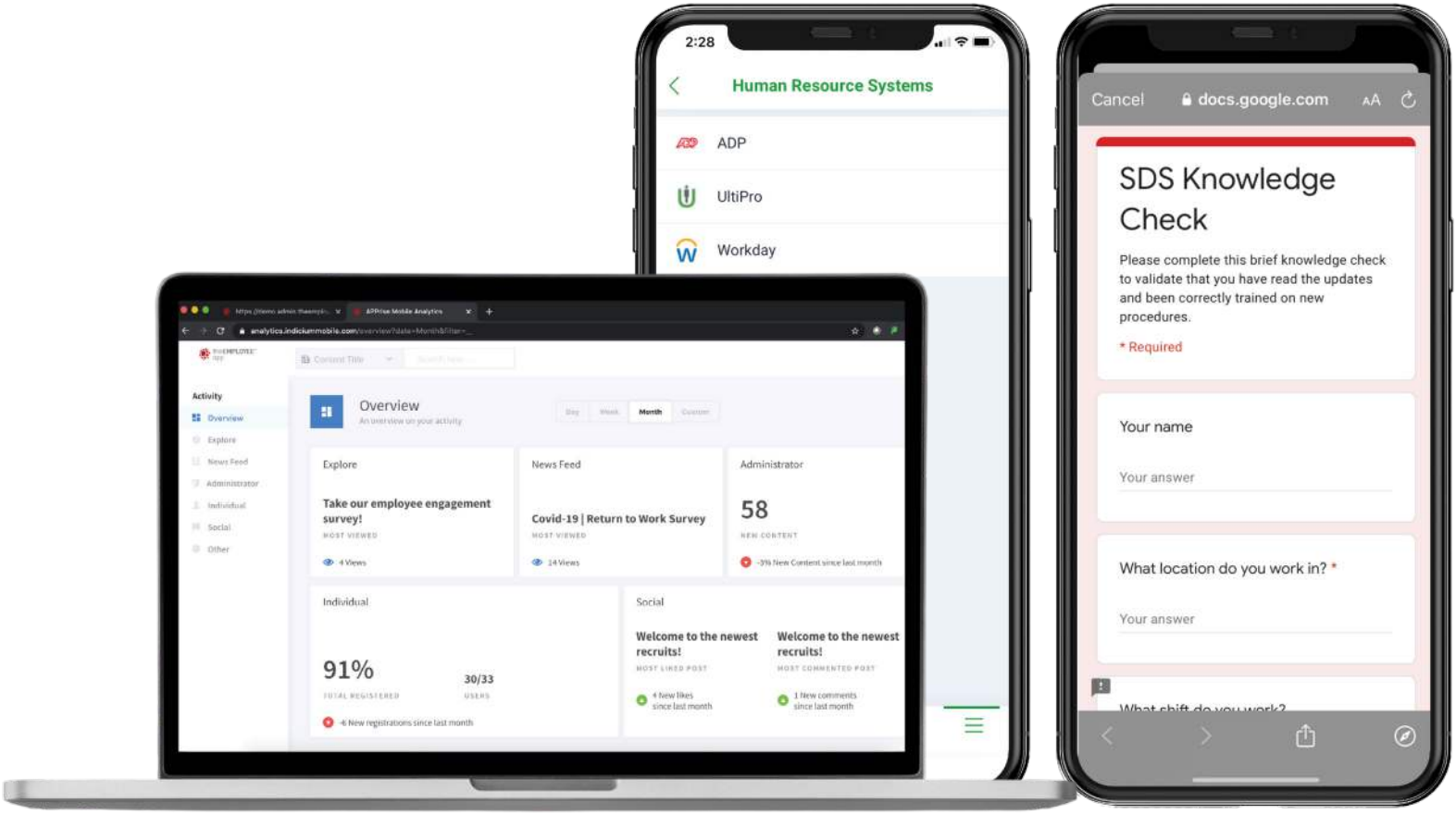
We hope this ebook helps you advance the conversation with your IT team about internal communications mobile apps that meet your company's productivity and security needs. theEMPLOYEEapp experts are also available to provide more detail on how seriously we take data security. Contact us today for more information.

About theEMPLOYEEapp

theEMPLOYEEapp was created by communications and HR professionals to address the challenges organizations face communicating with a dispersed and deskless workforce. theEMPLOYEEapp is an internal communication and engagement solution that allows workers to have fast and easy access to the information, documents, and resources they need to succeed in their work.

Our app allows you to target information to your employees when and where they need it on their smartphone, tablet, or computer, and empowers leaders and frontline managers to engage and activate employees across the organization. Unlike most traditional communications channels, theEMPLOYEEapp creates a customized, branded experience for employees, encouraging your workforce to join together in a single, centralized channel.

To learn more about theEMPLOYEEapp, request a demo. You can also stay informed on the latest trends and issues impacting the internal communications industry by following us on LinkedIn.



References

[1] Insurance Business Magazine, Cyberattacks on the Rise Amid Covid-19 - Report," September 2020

[2] Insurance Business Magazine, Cyberattacks on the Rise Amid Covid-19 - Report," September 2020

[3] IBM/Ponemon, Cost of a Data Breach 2020

[4] G2, 21 Shadow IT Management Statistics You Need to Know, October 2020

[5] Forbes, "Shadow IT," February 2017

[6] Ragan, 2019 Internal Communications Measurement Survey Results

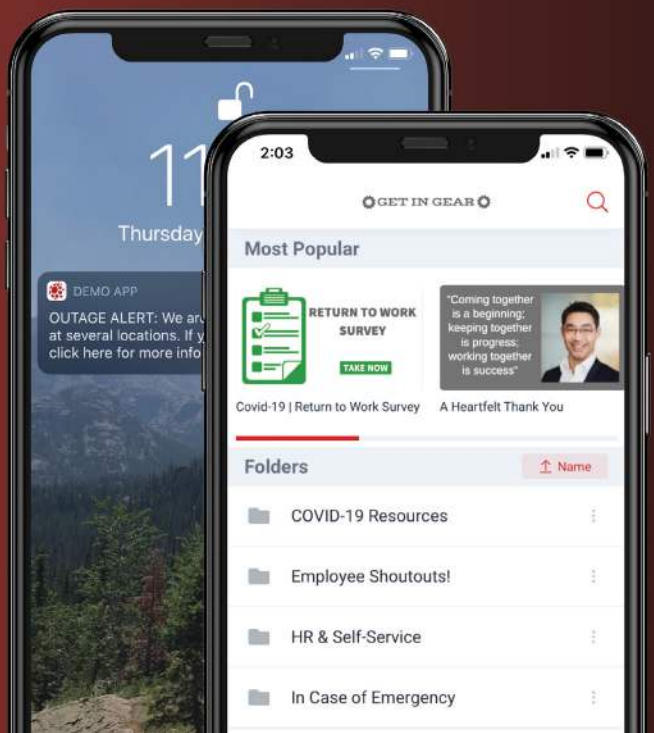
About theEMPLOYEEapp

theEMPLOYEEapp was created by communications and HR professionals to address the challenges organizations face communicating with a dispersed and deskless workforce. theEMPLOYEEapp is an internal communication and engagement solution that allows workers to have fast and easy access to the information, documents, and resources they need to succeed in their work.

Our app allows you to target information to your employees when and where they need it on their smartphone, tablet, or computer, and empower leaders and frontline managers to engage and activate employees across the organization. Unlike most traditional communications channels, theEMPLOYEEapp creates a customized, branded experience for employees, encouraging your workforce to join together in a single, centralized channel.

Our Mission is to enable the effortless flow of meaningful information for organizations driven by frontline workers.

Request a Demo



theEMPLOYEEapp®