



# THE DEFINITIVE GUIDE TO MOBILE PRINTING

---

Printing in the  
21st Century

an ebook from  breezy



# The 21<sup>st</sup> Century Mobile Printing Guide

## **Content**

Team Breezy

## **Graphic Design and Illustrations**

Sarun Pinyarat

## **Terms of Use / Disclaimer**

In creating this ebook, BreezyPrint Corporation (“Breezy”) has attempted to comply with all known legal, ethical, and professional requirements. The information contained in this document is provided for informational purposes only. Given the ever-changing nature of the technologies and products discussed in this document, it may contain information that is not up-to-date. Although a reasonable effort is made to

furnish current information that is up-to-date, use of this document is on an “as is” basis with no warranties as to accuracy, completeness, reliability, or timeliness.

Use of any website links, including those operated and maintained by third parties is entirely at your own risk and discretion. Breezy is not responsible for the content, actions, products, or services of third-party websites.

## **Copyright/Distribution**

Distribution or replication of this e-book’s content is prohibited without prior written consent.

©2014, BreezyPrint Corporation

# TABLE OF CONTENT

---

<b>① Introduction</b>	<b>4</b>
• The Consumerization of IT	7
• What the Analysts Say	8
• Purpose of this ebook	10
<b>② Who Needs Mobile Printing?</b>	<b>11</b>
• Employee Behavior: The Weakest Link	16
• A (Very) Brief History of Mobile Printing	18
<b>③ Types of Mobile Printing Solutions</b>	<b>20</b>
• Shadow IT: When 'Doing the Right Thing' is Wrong	21
• Types of Mobile Printing Solutions	23
• On-Device Encryption: Necessary Protection for Mobile Printing	25
<b>④ Mobile Printing Compliance Issues</b>	<b>28</b>
<b>⑤ Making the Business Case for Secure Mobile Printing</b>	<b>31</b>
• Integration with Existing Infrastructure	32
• Scalability and Functionality	33
<b>⑥ Introducing Breezy, a Gartner 2013 Cool Vendor</b>	<b>35</b>
• The Breezy Advantage	37
• Comparing Solutions	38

# INTRODUCTION

---

# 1

For centuries, printing was a time-consuming, manual process. In the 20th century, computers connected to printers took the drudgery out, and cut costs. In the 21st century, despite predictions of a paperless office, mobile devices connected to company networks have created a new set of security and connectivity problems.

Easy, secure mobile printing remains elusive for many companies. Breezy created this ebook to show companies how to solve the problem of delivering simple, secure mobile printing for tablets and smartphones within IT control.

---

# INTRODUCTION

In the beginning, words and images were created by hand. The process was slow and difficult, and written documents were expensive and highly prized.

A Chinese businessman named Bi Sheng created the first printing press during the Han Dynasty (about 1043), because he wanted a faster way to create documents for the royal court. It took another 400 years for Johannes Gutenberg to bring printing to the western world (1450).

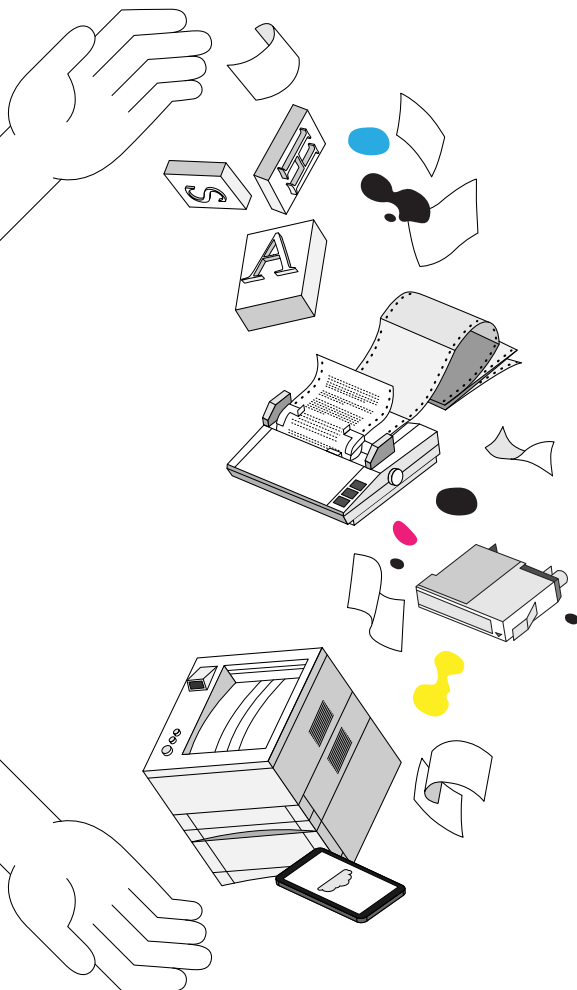
The printing press made things less expensive, but the process was still slow and cumbersome, and printing was the province of specially trained craftsmen – not ordinary business people.

In the 1860's, typewriters began appearing in businesses, and the legions of clerks who had toiled over ledgers and business records were replaced by typing pools. Things didn't change much until computers began to make their appearance in the middle of the 20th century.

Printing technology improved with the onset of dedicated word processing machines and computers.

- Chester Carlson created the first dry-ink printer in 1938
- Remington-Rand Corporation created the first high-speed printer for the Univac computer in 1953
- Digital Equipment Corporation (DEC) launched the first dot matrix printer in 1970
- Hewlett-Packard launched the Laser Jet printer in 1984 – and has shipped more than 200 million of them since

The year before Hewlett-Packard launched the Laser Jet printer, Tandy Corporation launched the world's first notebook computer, the Tandy Model 100. For the first time, people could easily carry a computer around



with them, connect to networks via dial-up modem, and plug the notebook computer into any printer with the right connector.

The early notebook and portable computers became laptops, but like all their predecessors, laptops required a physical connection to a printer in order to turn digital documents into printed text. Then, in 1992, the Australian radio-astronomer [John O'Sullivan](#) created an experiment to detect exploding mini black holes the size of an atomic particle. The experiment failed, but he and his team realized that they had created something new in their attempt, and obtained a patent on a technology they called Wi-Fi. Wi-Fi changed everything. Old barriers to printing, sharing data, and transmitting files between networks and devices vanished quickly.

By the beginning of the 21st century – roughly a thousand years after the printing press made its debut – mobile devices were revolutionizing the way people communicated and worked. Every year in this century has seen huge strides in the capabilities of mobile devices, as the costs and size have plummeted.

The 2014 workforce is more mobile than ever before. More than 2 billion Android, BlackBerry and Apple iOS devices access corporate networks every day. End users want access to desktop functions for all business applications, on any device, anytime, anywhere – and printing is no exception.

# THE CONSUMERIZATION OF IT

The press calls it “the consumerization of IT”. Smartphones, tablets and other devices designed for consumer use have quickly made their way into almost every kind of business. Companies talk in terms of BYOD policies, securing the endpoint, and mobile device management. But employees call their demand for anytime, anywhere access to corporate systems (including printing) an essential part of getting the job done.

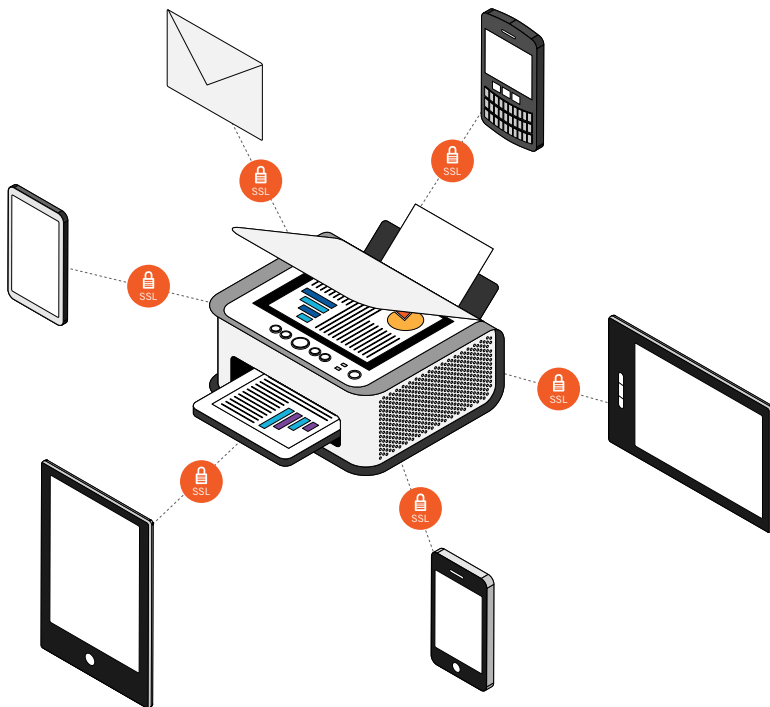
The days when an IT department chose what platforms and services to offer company employees are gone, replaced with the need to support a diverse range of mobile platforms. End users understand the value that the company gets when they use personal devices or extend the workday by using mobile devices provided by the company. So they are becoming increasingly vocal when it comes to demanding the tools they need – and

mobile printing is often on the list.

Despite decades of predictions of a paperless office, businesses continue to rely on printing. Rolling out an enterprise mobile print strategy can seem far from simple, as companies face a wide array of hardware, software and service offerings that vary by platform and printer. IT managers know that they can’t afford to ignore the consumerization of enterprise printing – because if they do, employees will bypass IT and use consumer printing apps

that lack all of the security, compliance, and cost controls IT has put in place.

Like the rest of IT, the future of enterprise printing will increasingly be shaped by consumer trends. The extent to which organizations and vendors

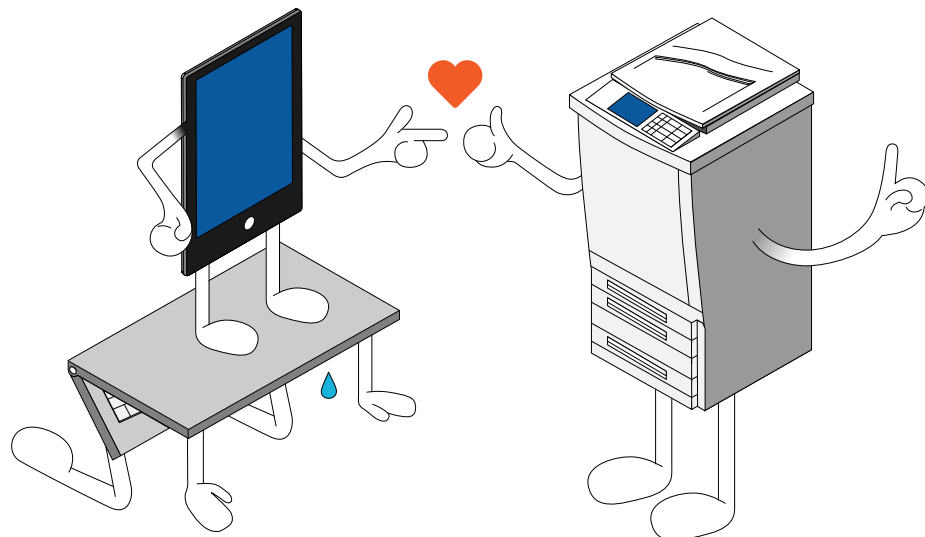


can harness these trends will determine success or failure. Organizations must balance a mobile print strategy with security, cost, business process requirements, user needs and delivery models.

For some companies, secure mobile printing remains a “nice to have” service, but for an increasing number, it’s essential. IT must provide enterprise mobile printing capabilities that are secure, reliable, and in compliance with state and federal rules like the Computer Fraud Act (CFA), HIPAA, FINRA and FERPA. Without it, employees are less productive, and IT can’t track or control what’s being printed, or where.

## WHAT THE ANALYSTS SAY

A recent [IDC report](#) says 75% of tablet and smartphone users expect to increase the number of documents printed from mobile devices, and that smartphone and tablet users are more likely to print than their non-mobile counterparts. By 2016, the total number of pages printed from mobile devices is expected to grow at a compound annual rate of 12%, while the number of pages printed from PCs is expected to decline 5% according to Angèle Boyd, Group VP and General Manager, Imaging/Output Document Solutions at IDC.



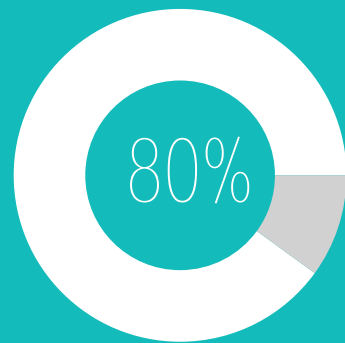


Industry analyst Mary Meeker, at the venture capital firm KPCB, reports that tablet shipments surpassed desktop PCs and notebooks in the fourth quarter of 2012, less than 3 years after the introduction of the original iPad. More than 27.5 million iPads were sold for use in American businesses during 2012.<sup>1</sup>

The tablet takeover is primarily driven by consumers, but it's affecting the IT landscape, too. Mobile security for employee-owned devices is now one of the top headaches for IT managers and CIOs, especially in regulated industries where compliance is a factor.

“Every 15 to 20 years, the IT landscape shifts. The last major shift of this magnitude was the creation of the web”, explains Jared Hansen, CEO of Breezy. “But the shift to mobile is no less disruptive. It's changed the way people work, and the way organizations conduct business. Mobile security is one of the primary initiatives in most IT organizations, whether they purchase company-owned devices or encourage BYOD.”

**2 billion mobile devices** access corporate networks every day.



of mobile devices contain **unsecured** apps that can expose data.

IDC reports that by 2016, employee owned smartphones, tablets and PCs in the workplace will grow from 2 billion to more than 5.25 billion. These users expect IT to support them in accessing corporate databases and applications seamlessly and securely. This expectation creates new demands on the corporate network and can pose risks to the company's customer and employee data.

<sup>1</sup> Number calculated based on U.S. iPad sales in 2012, as reported in the 2012 Annual Report for Apple, Inc. and the percentage of iPads used at work, as reported in the 2012 IDC Survey of iPad use. 33.2 million iPads were sold by Apple in 2012, and 87% of them are used at least in part for work according to IDC.

For example, over 80% of companies are currently at risk of a data breach due to a single gap in their security architecture, and that risk is likely to increase as more tablets and smartphones enter the workplace: companies are taking steps to protect their data, but most existing security solutions leave a gaping security hole when it comes to mobile printing. But it doesn't have to be that way, Hansen says: "That's where Breezy comes in. We secure the 'last mile' for mobile data, with secure on-device encryption that allows employees to print from any mobile device, to internal and external printers, with just a few clicks."

## PURPOSE OF THIS EBOOK

While terms like Bring Your Own Device (BYOD) and Mobile Device Management (MDM) have made headlines, mobile printing has been much less visible even though it is extremely important for businesses and IT managers.


Printing often seems to be forgotten in the rush to deploy mobile devices within the business world. As more and more devices are being shipped with **Print** buttons on them, the problem is compounded because device manufacturers haven't addressed the requirement for security or the range of print functionality.

Sometimes, management becomes aware of the problem only when an employee or a group of employees begins creating their own "work-around" printing solution that circumvents security policies altogether.

Breezy, a 2013 Gartner Cool Vendor in Imaging and Print Services, created this ebook to help IT teams evaluate mobile printing's value for their employees. The ebook addresses critical questions organizations should analyze when the need for mobile printing, and discusses the business case for deploying a secure mobile printing solution.

# WHO NEEDS MOBILE PRINTING?

---



Employees, used to easy printing from their desktops, have their own ideas about the smartphones and tablets they want to use – and how they want to print from those devices. IT has historically focused more on the cost controls, security features, and tracking required, or even on eliminating printing altogether.

As a result, mobile printing can seem like a “nice to have” but not essential feature to IT, while feeling like an essential tool to end users. Bringing the two sides together is the first challenge in deploying a mobile printing solution.

---

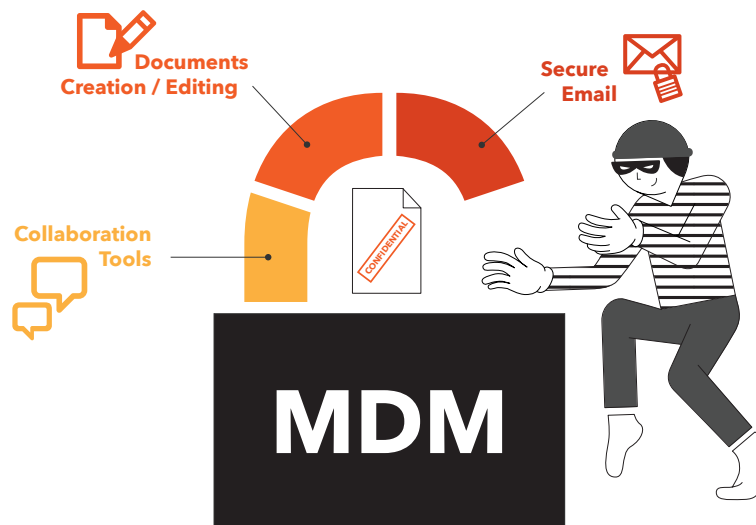
# WHO NEEDS MOBILE PRINTING?

When early adopters first began bringing smartphones and tablets to work, businesses tried to control things by selecting a single device operating system such as BlackBerry to support, and providing the devices that they wanted employees to use.

Employees had their own ideas about what devices they wanted, however, and quickly started bringing their own devices to work and using them without monitoring, security protection, or oversight by IT. As a response, companies created BYOD (bring your own device) policies.

BYOD is now becoming the norm at most businesses, and products designed for consumers and selected by employees will continue to be added to corporate networks in increasing numbers. In fact, a global CIO survey by Gartner<sup>2</sup> estimated that 38% of companies expect to stop providing devices to employees by 2016. For CIOs, that means committing to supporting the “any device, anytime, anywhere” needs of an increasingly mobile workforce, and it definitely includes mobile printing.

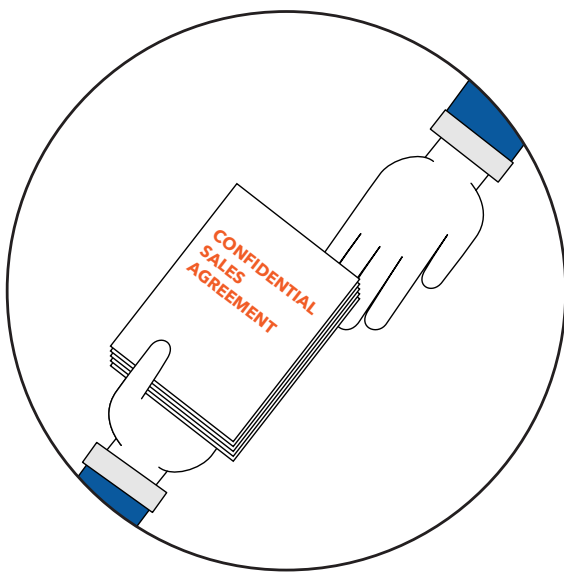
The desire for mobile printing creates a security problem for many companies. Over 63% of the employees surveyed in a Check Point study in



*Unsecured printing creates a security threat.*

June 2013 said that they transferred files from a mobile device to a cloud storage service like Dropbox or Google Drive so that they could print the document from a computer that wasn't connected to the company network – and therefore not protected by the company's security software.

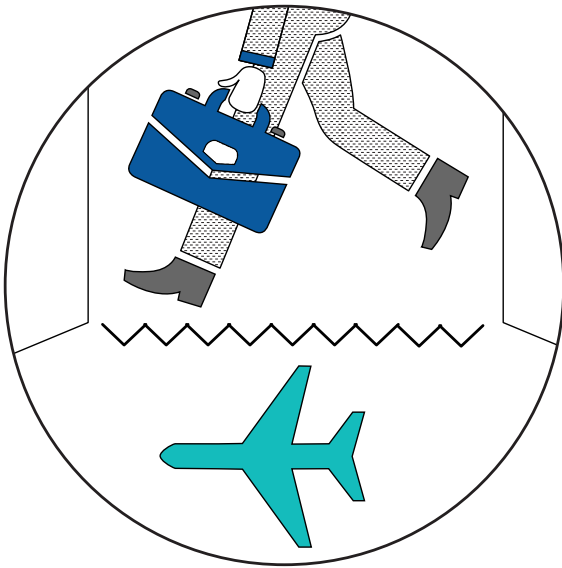
“But isn't printing going away? Doesn't the move to tablets mean people don't need to print anymore anyway?” Not so fast! There are many everyday business applications for printing. Think of these common scenarios:



Every day, **sales people** print collateral, contracts, price lists and more. But they shouldn't need to carry a bulky laptop when a tablet will suffice. Secure mobile printing lets IT meet the sales team's need for print and enables cost savings without compromising on security.

**Real estate agents** know that the ability to print a document anytime, anywhere, can make the difference between getting a deal done – and losing it to another agent. Many of the documents Realtors handle are confidential, so a secure print solution for mobile devices is especially important to them.



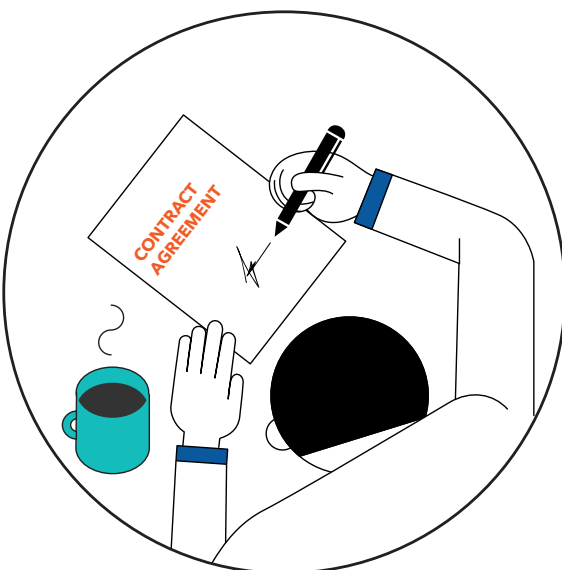


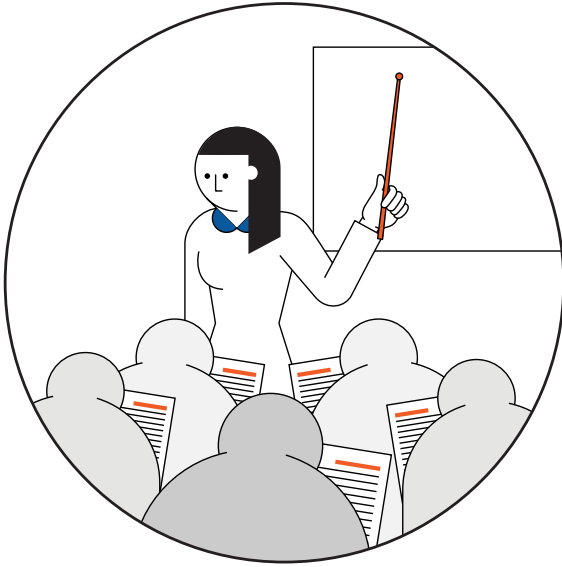
**Traveling consultants** are among the most frequent fliers on the planet. Their need to print documents securely is so important that many travel with their own portable printers. It's a consultant's dream come true: an end to scanning through hundreds of pages of documents on a small screen, or lugging a printer on every flight.

**Hotel staff** can now use tablets to check guests in as soon as they arrive, with printed receipts and passes ready and waiting at reception as soon as the guests arrive. Mobile printing also provides a competitive advantage as well as a new revenue stream for hotels, airport lounges, coffee shops, libraries, and other locations where mobile workers gather.



According to an American Bar Association estimates, **Lawyers** use 20,000 to 100,000 sheets of paper every year – and there's nothing more confidential than the client files entrusted to an attorney. Secure mobile printing allows attorneys to save valuable time and print vital documents from any device, whether in the office, at home or on the road, without compromising their ethical obligations.





**Field trainers** at franchise companies, restaurants, retail stores and many other businesses often travel from city to city conducting staff training and evaluations. These trainers have a constant need to update and print confidential documents such as personnel forms and training materials. Adding a secure mobile print solution to their tool kit saves time, money and headache.

**Insurance agents** meet with prospective policyholders in a range of locations – and many state insurance rules require that applications be hand-signed in front of a witness. Until recently, that meant at least two face-to-face meetings, so that the agent could get the necessary application documents prepared and printed before returning them to the client for signing. With a secure mobile printing capability, insurance agents can modify documents on the fly during a meeting, then print on any printer network, and get the application ready to submit in one meeting instead of two.



Of course, there are many other day-to-day business activities where the ability to print from a mobile device can add convenience or enhance productivity, including:

- Print documents at a remote corporate location without IT assistance
- Receive last-minute updates to a presentation and print the presentation before attending a meeting
- Print from the phone on the way to the office and have documents waiting when you arrive

## EMPLOYEE BEHAVIOR: THE WEAKEST LINK

One of the basic realities facing IT managers is that any security system is only as reliable as the users make it. Employee behavior around mobile printing is a perfect example of this rule in action.



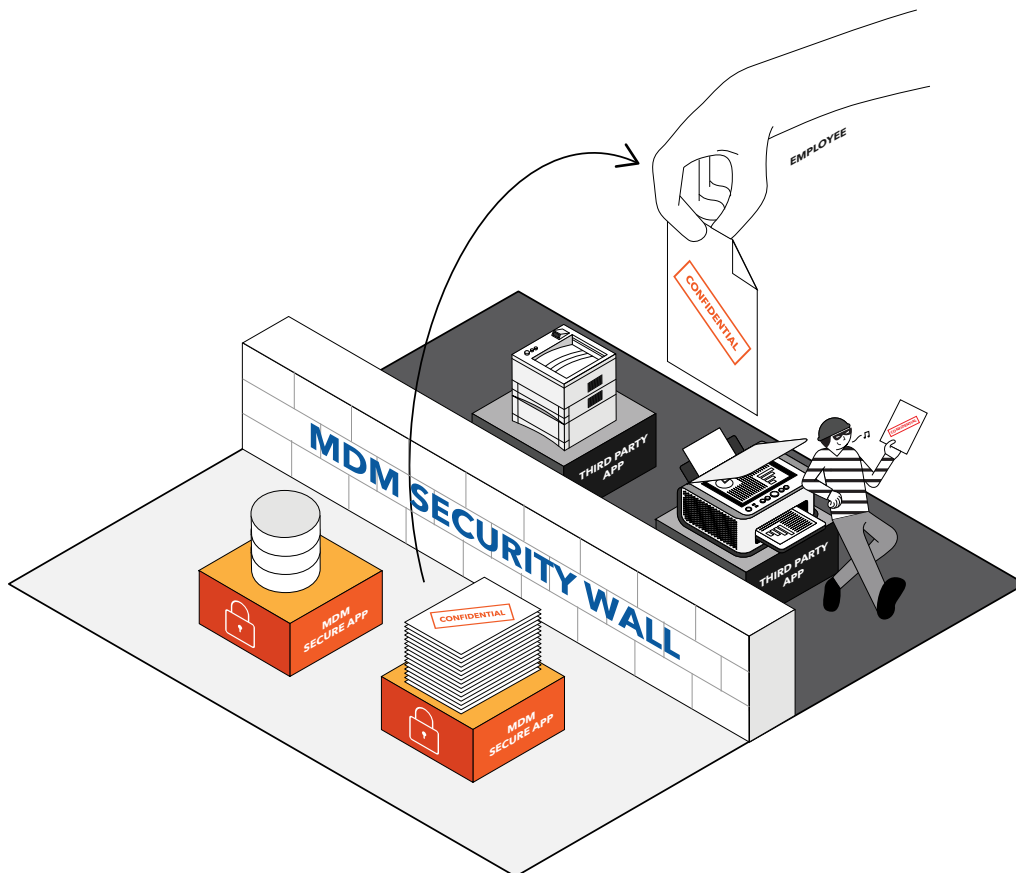
**63% of employees** have transferred company data to an unsecured cloud application or computer for easier mobile printing.



Employees **will** print from their mobile devices. If there's no simple, easy way to do it within the company's secure network, they'll take whatever steps they believe are required to get the job done, including:

- Downloading consumer apps that transmit unencrypted files over the internet, leaving company data exposed.
- Emailing a file to be printed to an unsecured desktop machine at a public print terminal, hotel business center, or home PC.
- Emailing a file to be printed to a personal email account
- Uploading a file to be printed to third-party cloud file sharing services such as Dropbox, then downloading to a computer with access to a printer.

A well-designed secure mobile printing solution should integrate seamlessly with mobile device management (MDM) and mobile application management (MAM) solutions, as well as other existing corporate security risk solutions, remove risk, and give employees the ability to get their jobs done easily – without creating security nightmares for IT.



# A (VERY) BRIEF HISTORY OF MOBILE PRINTING



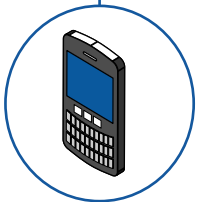
**1984**

The first notebook computer (the Tandy Model 100) is released, creating the first mobile device capable of connecting to a network.



**1992**

Wi-Fi is created out of a failed astrophysics experiment intended to find tiny black holes, and wireless network connections become possible.



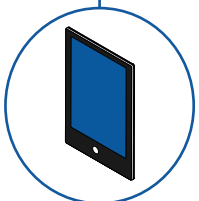
**2000**

With the advent of the 21st century and increasing usage of high-end phones like BlackBerry, the market began to sense some need to help these users print.



**2005**

Hilton became the first hotel chain to make a significant investment in guest printing, deploying printers with email addresses across many of their properties. Other hotels followed suit, giving travelers a way to print boarding passes from their smartphones.



**2010**

The launch of the first iPad starts the tablet takeover – and users soon began asking IT how to print from their tablets.

Breezy launches on BlackBerry as the first app ever to allow printing email attachments to any printer, and the only print solution with on-device encryption.

Apple launches AirPrint, a print subsystem for iOS that allows printing so long as the iOS device and AirPrint-enabled printer are on the same Wi-Fi subnet.

**2011**

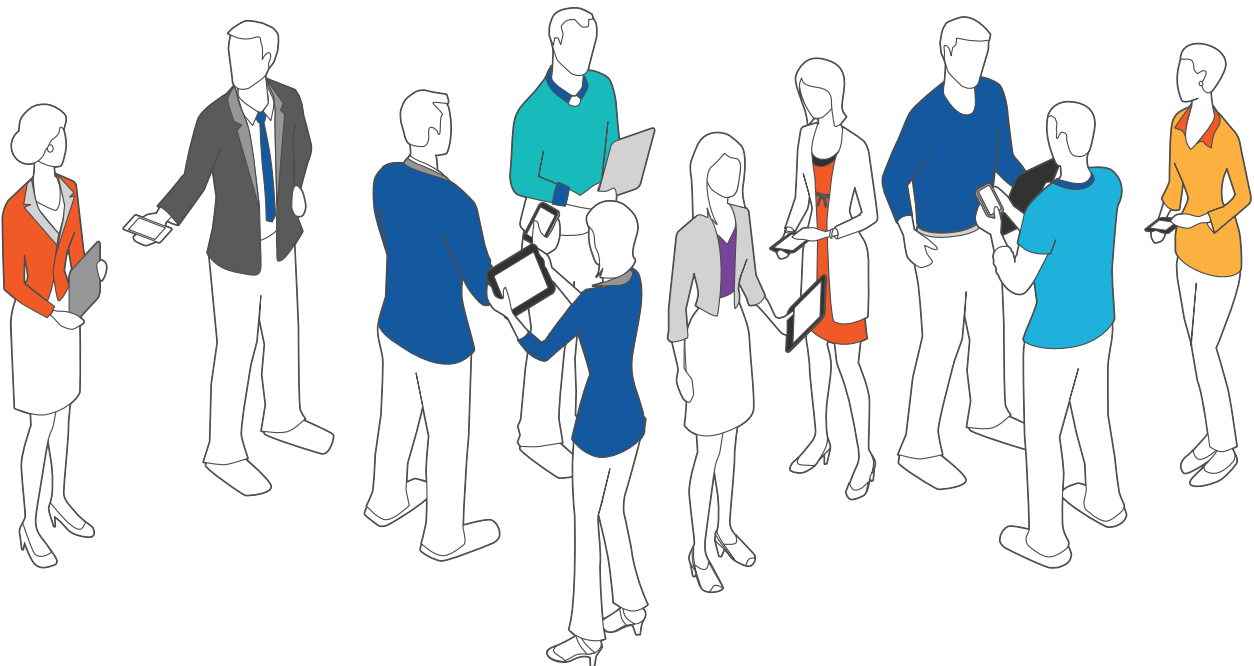
U.S. courts define smartphones, MP3 players, and printers as “computers” under the federal Computer Fraud Act, making it mandatory for all companies to secure data stored or transmitted between those devices.

Breezy come to Android and iOS, launching the industry’s first printer-agnostic, secure mobile printing solution that meets compliance standards and enables secure printing from any mobile device, over a secure partner network of public printers or a company’s printer fleet.

**Present**


Secure mobile printing is a necessity for business, and some features such as on-device encryption have become essential.

An increasing number of vendors offer mobile print solutions, but Breezy remains the only proven solution for enterprises and mid-size businesses that need an easy-to-deploy managed solution that will stand up to a compliance audit.



# TYPES OF MOBILE PRINTING SOLUTIONS

---



Shadow IT – consumer-grade software downloaded by employees – has become a problem for companies as more consumer-owned devices find their way into the enterprise. Many companies have tried a range of mobile printing solutions, including email, Wi-Fi and Cloud.

Most don't include on-device encryption to protect company data, or work with legacy printer fleets or corporate MDM solutions. The ideal mobile printing solution is flexible, built to deliver the ease-of-use employees want while providing the security, reliability, and accountability that IT needs.

---

# SHADOW IT: WHEN 'DOING THE RIGHT THING' IS WRONG

Careless employee behavior has always put company data at risk. Human failings such as lost laptops and passwords jotted on sticky notes have made headlines around the world when data breaches have occurred. But what about when employees are trying to do the right thing by being productive, but inadvertently leaking sensitive data in the process?

Survey after survey shows that if employees can't print from their mobile devices, they will engage in behavior that can seriously compromise security such as transferring files to a cloud storage site, or emailing it outside the network to an unsecured desktop computer (at a business center, for example) where they can print it.

Another common attempt by employees to solve mobile printing problems leads to so-called shadow IT: that is, a situation when an employee reads about or sees an unauthorized app that promised to solve their printing problem, and installs it on a device without IT control or approval.

Shadow IT in the form of third-party consumer apps is the Achilles heel of many mobile deployments. Fewer than one in 10 mobile device users know that there are [malware apps](#) that don't attack the infected device, but lie in wait to attack other computers or networks to which the device subsequently connects. Even fewer, about one in 10,000, realize that many mobile apps are designed with risky behaviors as a core part of the app.

According to [Network World](#), at least 80% of mobile apps have built-in security and privacy holes designed into the app. Some apps request permissions that aren't used by the app, creating a built-in security hole that hackers can exploit to steal unencrypted data.

For example, many unmanaged mobile apps obtain permissions to:

- Access the user contacts (including the contact information that may come from corporate email that syncs to the phone)
- Access the user's calendar information
- Collect or determine a user's location and track the user's movement
- Pass along any or all of this information to ad networks, analytics firms or other third parties

Network World reports that 96% of iOS apps and 84% of Android apps can access at least one of these data risk categories.

With the demand for mobile printing growing every day as users become more mobile, and with so many risks attending many of the ways users solve the problem on their own, it's never been more important for IT to provide a secure, standardized mobile print solution for their organizations.

**80% of employees**  
of employees work  
remotely during the  
week.



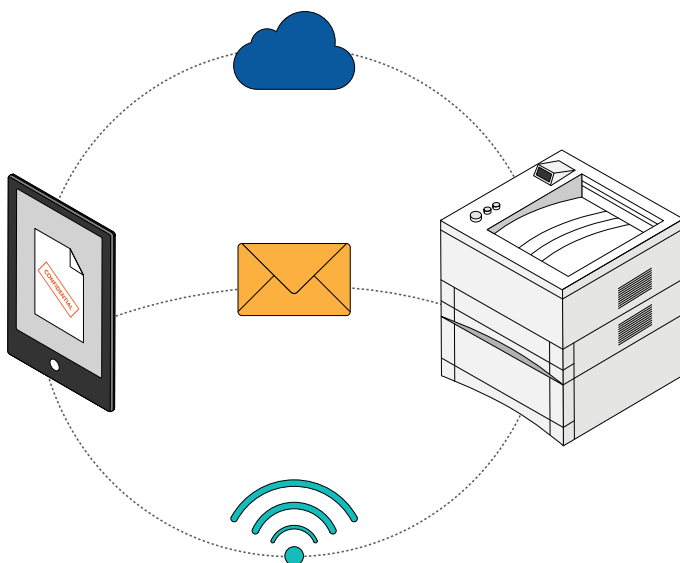
**29% of workers** are fully mobile without a dedicated workspace

# TYPES OF MOBILE PRINTING SOLUTIONS

When businesses first began to formulate policies to integrate mobile devices into corporate IT, printing was, as a rule, completely neglected – either forgotten about altogether, or treated as a mere “nice to have” – but not essential – function.

Users eventually began to give up, and searches for “mobile printing” started trailing off in 2007. That changed dramatically with the invention of the iPad in 2010, which heralded new possibilities for working with mobile devices. No longer satisfied with simply consuming content on a small screen, users expected more. Many began clamoring for printing as part of a complete productivity solution, and when AirPrint was announced in the fall of 2010, Steve Jobs received a standing ovation from a packed auditorium. The “missing print feature” was finally here, or so it seemed.

The optimism was short-lived, as AirPrint turned out to be incomplete. It required a direct Wi-Fi connection between the printer and mobile device, supported only a subset of apps and file types, it couldn’t integrate with enterprise print management systems and of course it worked only with devices running Apple’s iOS.



Meanwhile, multiple vendors continued to develop various kinds of mobile printing solutions, including:

- Email – email the document to a printer on the corporate network or a public print network for printing.
- Wi-Fi – transmit data wirelessly from a mobile device to a printer that is connected to a subnet of the corporate network or a public print network.
- Cloud – public, hybrid, or on-premise clouds (with widely varying security capabilities).

Within these options, different vendors have tried both peer-to-peer and cloud printing solutions. In a peer-to-peer scenario, data is transferred from the mobile device to a PC, or to a print server located on the network. Cloud printing options can render the print job in either a public or private cloud. Cost, complex set-up procedures, access problems and limited rendering fidelity have often been cited as problems in peer-to-peer mobile print solutions, while security concerns and a lack of IT control are usually cited as the problem with cloud solutions for mobile device printing.

The terms “mobile printing” and “cloud printing” are sometimes used interchangeably when the subject of printing from tablets and smart phones is discussed. IDC Vice President Holly Muscolino considers cloud printing a subset of mobile printing since while all cloud printing is mobile printing, not all mobile printing involves a cloud implementation.

Nevertheless, the industry appears to be converging toward a cloud-based approach, with vendors and buyers alike generally recognizing that a cloud approach is the only way to provide the full range of flexibility users require – which means that security has attained critical status as when evaluating mobile print providers.



# ON-DEVICE ENCRYPTION: NECESSARY PROTECTION FOR MOBILE PRINTING

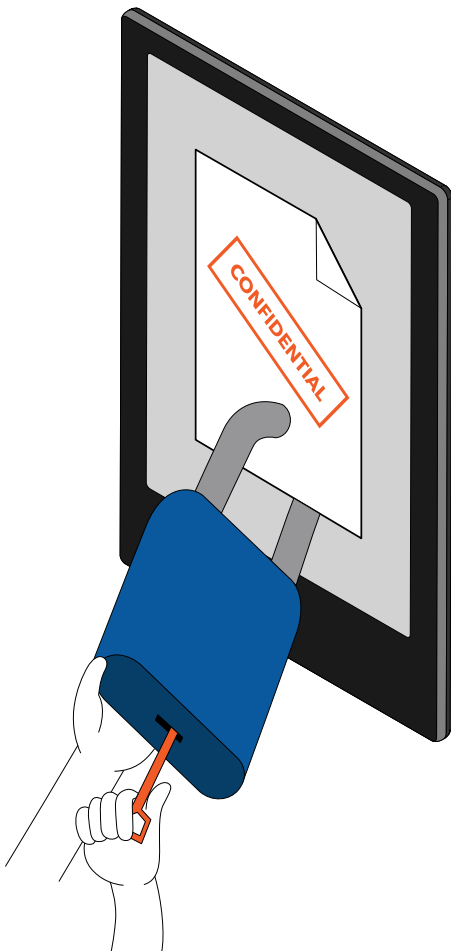
Once a decision is reached to use the Cloud, the first question on the evaluator's mind should be: "How secure is my document as it moves to the printer?" Within the overall category of cloud-based mobile print solutions, there are widely varying methods of document transport, and many different levels of security.

On-device encryption should be considered the Holy Grail of mobile print security for the simple reason that it's the only way to protect sensitive company information both at rest (being stored on the mobile device) and in transit to another device (such as a printer).

Data that isn't encrypted on the mobile device where it is stored is subject to man-in-the-middle attacks when it is "in transit" between the mobile device and the printer. And while nearly every vendor uses some form of encryption, many use only "transport layer" encryption, rather than performing full encryption on the mobile device.

## Defining On-Device Encryption

The term on-device encryption means that the document is encrypted by the mobile device before it is transmitted to the printer.



## How On-Device Encryption Works

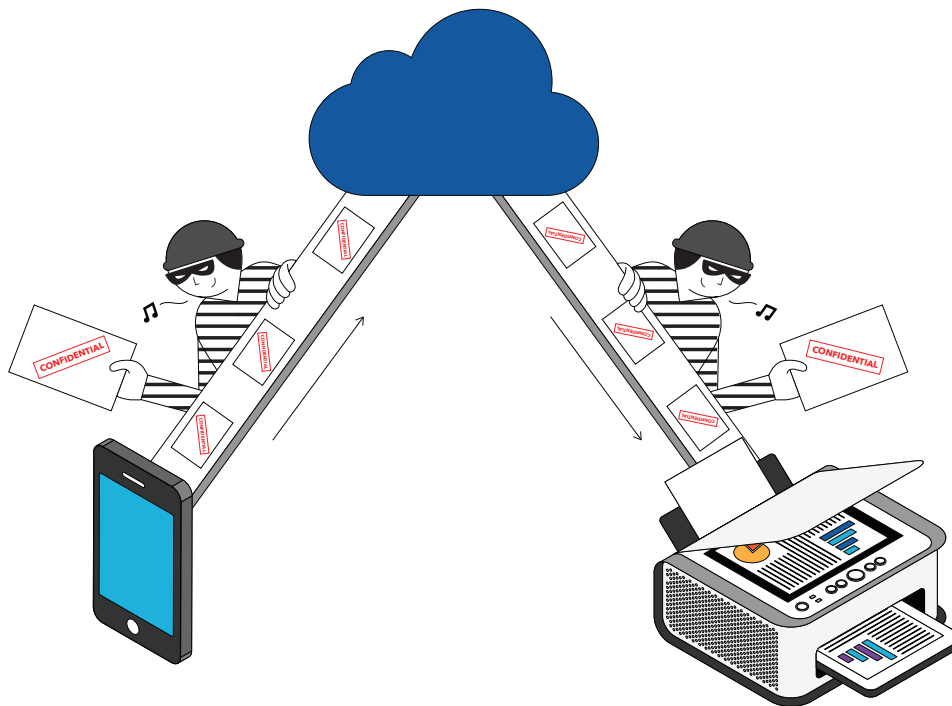
In a cloud printing system employing on-device encryption, each printer will have an associated keypair allowing asymmetric-key encryption. In simple terms, this means that each printer will have a private key that is kept secret, and a public key that can be advertised. The keys are linked such that when an encryption algorithm is applied to a data stream and the public key, the data stream can only be decrypted by an entity in possession of the private key.

Before a document is sent to a printer, an app using on-device encryption will obtain the public key associated with that printer, and use it to encrypt the document before transmission.

## Why On-Device Encryption Should Be Required

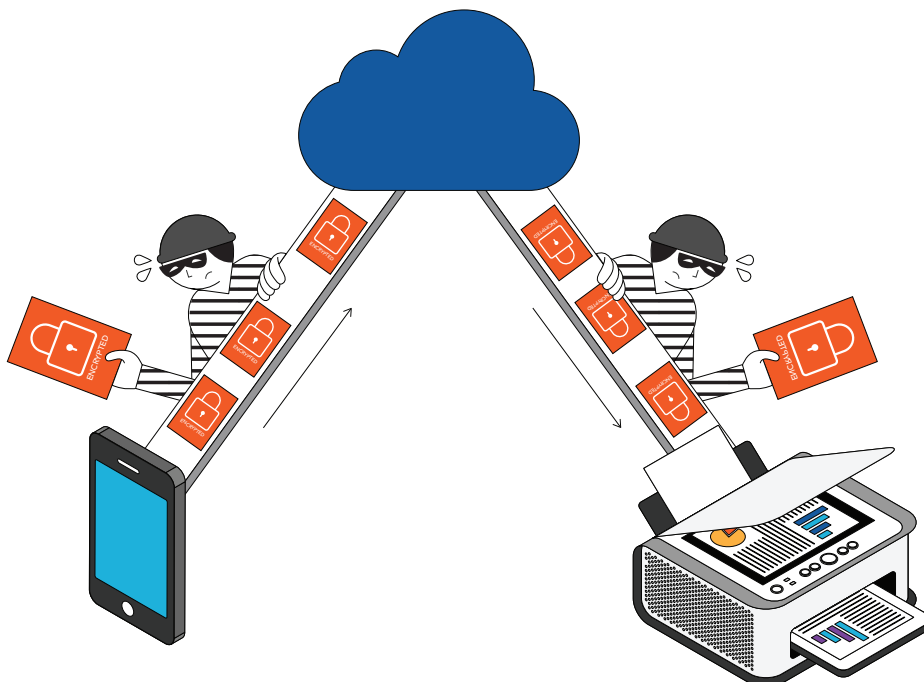
Consider the following scenario:

- 1) A vendor sells a cloud printing app that lacks on-device encryption but touts the app's use of HTTPS as a security measure, possibly using terms such as bank-level encryption or the like. The vendor relies on the HTTPS protocol to protect the document on its transit to the vendor's cloud, and from there to the client's infrastructure (this is known as "transit layer" encryption).
- 2) A user prints a sensitive document using the app. The app dutifully sends the document to the vendor's cloud via HTTPS.
- 3) Even though the app behaved appropriately, there is a surprise: unbeknownst to the vendor or the user, a man-in-the-middle attack has compromised the app's connection to the vendor's cloud – or, worse yet, the vendor's cloud itself has been compromised. In either case, the attacker is able to retrieve the document – and because the document is not encrypted, the attacker has full access to its contents.



Without On-Device Encryption, any compromise of the https tunnel leads to exposure of the document's contents.

On-device encryption protects document confidentiality by ensuring that even if an attacker is somehow able to obtain a copy of the document, he won't be able to decrypt it:

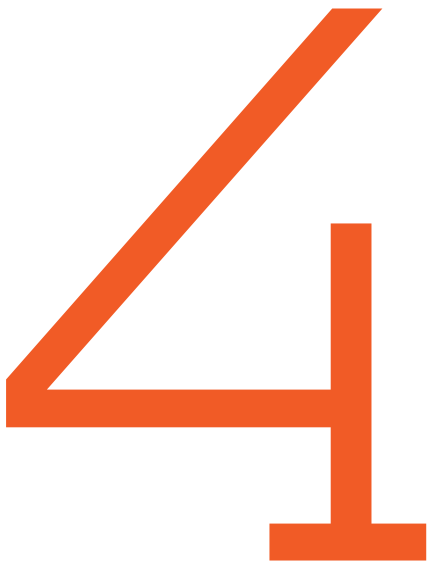


With On-Device Encryption, document confidentiality is protected even in the case of an https breach, because the data itself is encrypted even before it enters the https tunnel.

Though many schemes exist for assuring security as documents transit the cloud, only on-device encryption can ensure document confidentiality even in a “worst-case” security breach scenario.

# MOBILE PRINTING COMPLIANCE ISSUES

---

A large, stylized orange number '4' is centered within a white circle. The circle is positioned on the left side of the page, overlapping the orange background.

Agencies that enforce laws such as the Computer Fraud and Abuse Act or privacy and consumer protection laws like FINRA, FERPA, and HIPAA are taking a close look at mobile printing compliance issues. Many compliance audits now include a section on printing, leaving organizations that are otherwise meeting compliance standards vulnerable because of employee-owned devices with unsecured mobile printing applications. Mobile printing compliance should be built-in to a mobile printing solution, and on-device encryption for sensitive data is a critical part of mobile compliance.

---

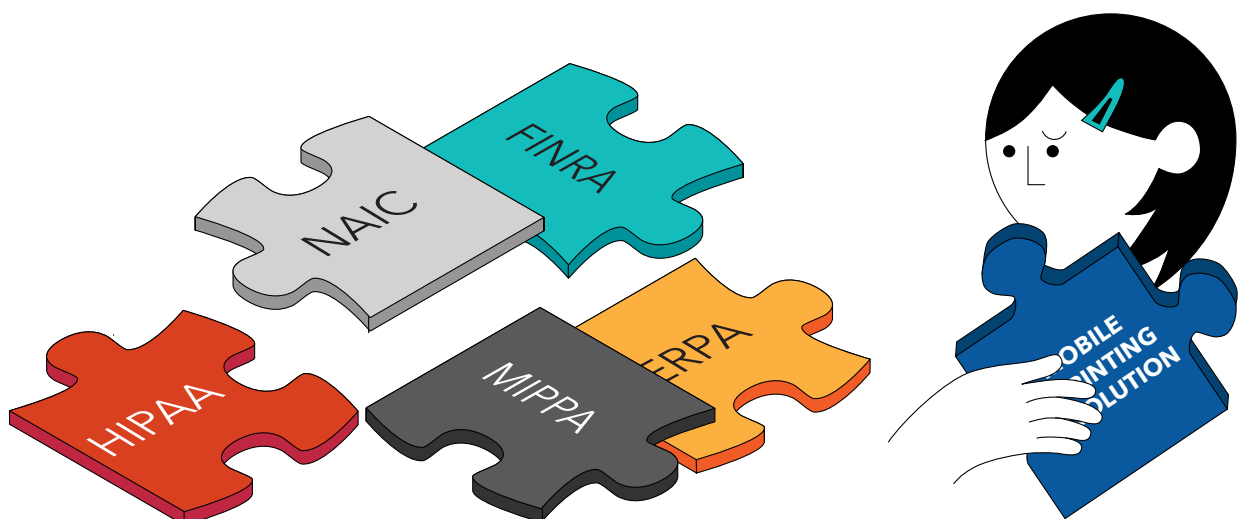
# MOBILE PRINTING COMPLIANCE ISSUES

When IT departments first started thinking about mobile printing several years ago, only companies in some highly regulated industries such as healthcare, financial services, banking and pharmaceuticals had to add compliance to the list of potential mobile printing problems.

That changed in 2011, when the U.S. Eighth Circuit Court of Appeals ruled that any device with storage and processing capabilities could be considered a computer under the Computer Fraud and Abuse Act (18 USC §1030), or CFA. In 2012, in *United States v. Kramer*, the Fourth Circuit Court specifically named both printers and mobile devices like watches, smartphones and MP3 players as being subject to the CFA.

As a result, compliance audits involving FINRA, FERPA, HIPAA, MIPPA, NAIC, PCI and other federal and state agencies are focusing more closely on mobile device security. Since it is clear that mobile devices are covered under the CFA, securing those devices has taken on a new urgency for businesses, schools, hospitals, and other organizations subject to regulatory oversight.

There is no consistent standard for mobile printing compliance. The rules vary depending on what kind of business you work in. But in general, the new rules mean that the security standards for mobile devices and printers are the same as those for any other “computer”.



In a compliance audit, you may be asked to show that:

- Data stored on these devices can be remotely wiped in the event of a data breach
- Data is encrypted both “in transit” and “at rest”
- Access to data stored on these devices – temporarily or permanently – is restricted and monitored, with accessible logs
- You have secured the data on these devices with “appropriate measures” that meet industry standards

If those rules seem general and not completely clear, it’s because they are still evolving. In general, most compliance experts advise businesses to:


- Ensure that software and systems are updated regularly, including installing any recommended patches
- Remediate identified vulnerabilities
- Encrypt data whenever possible
- Establish data surveillance and IT alert policies

Breezy is the only mobile print provider that ensures compliance by securing data on any mobile device – iPhone, iPad, Android tablet or smartphone, or BlackBerry device – with military-grade encryption before transferring the encrypted files safely via SSL to any approved printer or print network. In addition, Breezy has integrated with seven of the [top mobile security platforms](#) (see comparison chart on page 38 for a full list), and is continually adding others.

Recent court rulings make printers and mobile devices subject to the Computer Fraud Act and regulations like HIPAA and FINRA.

# MAKING THE BUSINESS CASE FOR SECURE MOBILE PRINTING

---



IT managers have to make a strong business case before investing in a mobile printing solution. Making the business case for secure mobile printing requires choosing a solution that delivers end user acceptance, integration with existing infrastructure, scalability and functionality, security, and compliance.

End user acceptance is often the hardest part, because users will circumvent any secure mobile printing solution they find too cumbersome. Scalability and functionality are essential, and solutions must stand up to high print volumes and peak times.

---

# MAKING THE BUSINESS CASE FOR SECURE MOBILE PRINTING

When the need for mobile printing in your company moves up the priority list, it's almost certain that you'll be asked to make the business case for the investment in a solution. There are four primary considerations:

- End user acceptance
- Integration with existing infrastructure
- Scalability and functionality
- Security and compliance

## End User Acceptance

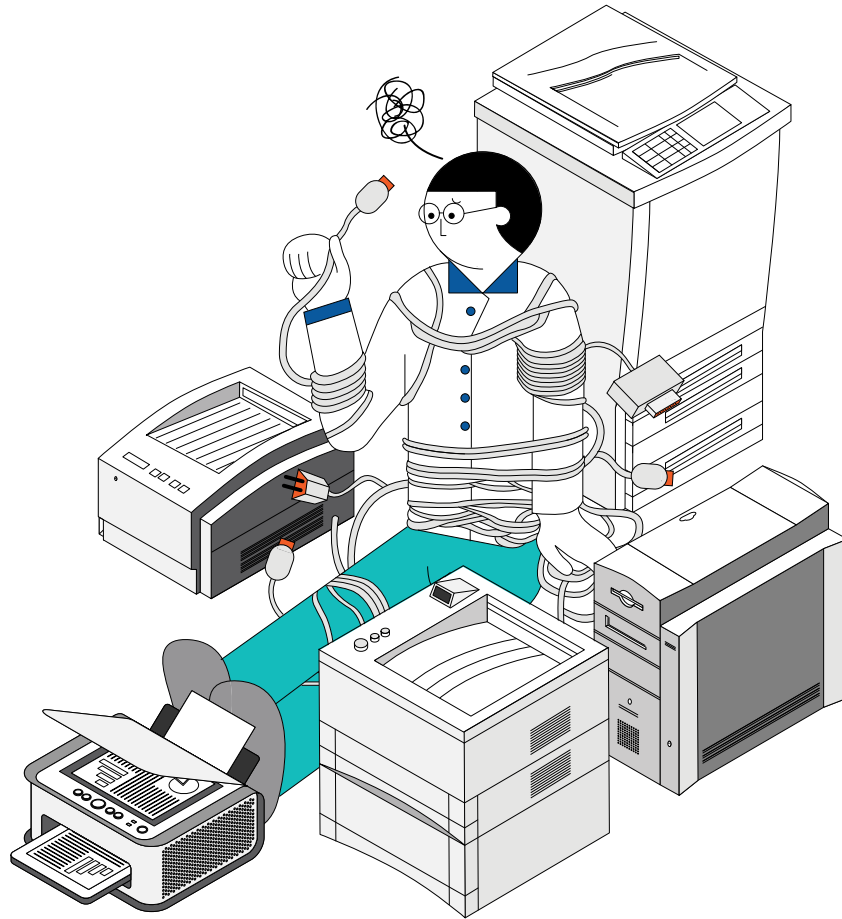
End user acceptance is first on the list, because if users aren't satisfied with the mobile print solution deployed by IT, they will resort to consumer applications that circumvent corporate security and cost controls. Employee behavior is the #1 risk factor in mobile device security. Among the most common risky behaviors are transferring company files to unsecured cloud storage services, sending them to unsecured PCs like the ones in a hotel business center so they can be printed, or installing mobile printing solutions designed for consumers and lacking the kind of control and security features required for a corporate environment.

So the first step in making the business case for a mobile print solution is to talk to end users about their mobile printing needs and desires.

## Integration with Existing Infrastructure

A mobile printing solution can, and should, work with all networked printers within a company, regardless of brand or age. The reality is that very few enterprises standardize on a single brand of printer, so it is important that your printing solution support a mixed printer fleet to avoid additional





hardware costs. In addition, mobile printing software should integrate seamlessly into existing print management infrastructure for added security and convenience.

While solutions from printer manufacturers often give preference to their brand in order to increase device and supply sales, it's both easier and more cost effective to select a printer-agnostic secure print solution.

## Functionality and Scalability

Mobile printing solutions deployed at the enterprise level need to be able to handle many users printing at once. That's because corporate print networks have peaks and valleys as users all access the print network at certain times of the day.

But some mobile print solutions were created for consumers or small businesses, and can't handle the demands of a large volume of simultaneous print requests.

Nothing will light up phones on the IT help desk faster than an application that fails because it can't handle a high demand.

So before you purchase a mobile print solution, make sure that it's been tested under stress.

## Security and Compliance

Your investment in mobile device management (MDM), endpoint and network security, and compliance management tools is probably substantial – especially if your business is in a highly regulated industry like banking, education, financial services, healthcare, insurance, or pharmaceuticals. But not all mobile print solutions meet the high standards you've set for security and compliance.

As part of the search for the right secure mobile print solution for your business, make sure that the mobile print solution you pick integrates with the MDM solution you've already invested in, and can work with the print management controls you have in place. The best solution will integrate with the majority of the leading MDM solutions on the market, so you can keep your secure mobile print solution even if you change MDM vendors.

Last, but certainly not least if your business is subject to federal or state compliance standards, the mobile print solution you select has to meet the security standards imposed by the agencies that regulate your industry. Chances are that means on-device encryption for documents.



# INTRODUCING BREEZY, A GARTNER 2013 COOL VENDOR

---

Breezy is a leader in secure mobile printing for enterprises and mid-size businesses that value ease of use, scalability and security. On-device encryption for documents provides assured compliance and security, and Breezy integrates with all of the most popular MDM platforms. It's the only secure mobile printing solution that is fully printer, device and network-agnostic, and satisfies all of the needs of today's corporate customers. Compare Breezy's secure mobile printing solution with others in the market, and see why Gartner chose Breezy as a [2013 Cool Vendor](#).

---

# INTRODUCING BREEZY, A GARTNER 2013 COOL VENDOR

The market for mobile printing is highly fragmented. Since there are so many different mobile devices and printers, it's hardly surprising that the available mobile printing solutions are equally diverse and fragmented. There are three broad categories of solutions available:

- Hardware manufacturers tend to offer a mobile printing solution that includes hardware, software, and services – and most are brand-specific although some do offer multivendor support. Vendors that offer some form of mobile printing solution include Canon, HP, Lexmark, Konica Minolta, Ricoh, and Xerox.
- Independent software vendors such as Breezy, Cortado, EFI, and PrinterOn offer printer-agnostic mobile print solutions, but approaches vary widely in both usability and flexibility, and most aren't secure enough to meet compliance standards.
- AirPrint on iOS and the print framework in Android 4.4 and above offer direct mobile printing via Wi-Fi to supported printers.

Breezy is a leader in secure mobile printing for enterprises and mid-size businesses that value ease of use, scalability and security. Breezy's modular secure mobile printing solution is:

- Easy to use – easy to install, configure and support
- Highly scalable
- Accurate, with pixel-perfect rendering of a wide variety of file types
- Printer- and device-agnostic
- Integrated with all of the most popular MDM platforms
- Secure – on-device encryption meets or exceeds compliance rules
  - » SSAE 16 / ISAE 3402 SOC 2 Type I security certification
- Flexible – allowing users to print from any device, anywhere



For details about Breezy's products and services, visit the company's website at [www.breezy.com](http://www.breezy.com) – or try it for yourself. Free trials are available for companies considering a mobile print solution, and Breezy's team of solutions architects are available to answer questions anytime.

BYOD requires IT to support more devices and systems than ever before. Breezy is the only solution that works with all devices, printers, and MDM solutions.

## THE BREEZY ADVANTAGE

Breezy is designed from the ground up to be secure, flexible, mobile, and simple to use and deploy. It's the only product that gives IT complete control over what and where users can print, and protects every document with on-device encryption before transfer via secure channels to the intended printer, plus single sign-on (SSO) integration via MDMs and identity federation providers.

**Request A Demo**



## Comparing Solutions

	Breezy	AirPrint	HP ePrint Solutions	Xerox Mobile Print Solution	Cortado	EFI PrintMe Mobile	PrinterOn
Mobile Platform Support							
Android (tablet, smart-phone)	●	○	●	●	●	●	●
Apple iOS (iPad, iPhone)	●	●	●	●	●	●	●
BlackBerry (smartphone)	●	○	●	●	●	●	●
Meets Compliance Standards with On-Device Encryption							
FERPA	●	○	○	○	○	○	○
FINRA	●	○	○	○	○	○	○
HIPAA	●	○	○	○	○	○	○
PCI	●	○	○	○	○	○	○
Integration with MDM Vendors							
AirWatch	●	○	○	○	○	○	○
Appsense/MobileNow	●	○	○	○	○	○	○
Aruba	●	○	○	○	○	○	○
Citrix Worx	●	○	○	○	○	○	○
Good Technology	●	○	●	○	○	○	○
MobileIron	●	○	○	○	○	○	○
Mocana	●	○	○	○	○	○	○
Printer Support							
Printer vendor-agnostic	●	●	○	○	○	●	○
Job Submission							
Native apps	●	●	●	●	●	●	●
Email printing	●	○	●	●	●	●	●
Web browser (Public Cloud, unencrypted)	○	●	○	●	●	●	●
Embeddable print button for in-house apps	●	○	○	○	○	○	○
Centralized IT Management							
Centralized Management Console	●	○	●	●	●	●	●
Detailed Reporting	●	○	Limited	Limited	Limited	Limited	Limited
Native AirPrint Support	●	●	○	○	○	●	○
Secure Public Print or Managed Print Services Partner Network							
Print Partner Network	●	○	●	●	○	●	●

(Table current as of January 2014.)

**Breezy**

160 Franklin Street, Suite 105  
Oakland, CA 94607  
(866) 245-3399  
[sales@breezy.com](mailto:sales@breezy.com)