A SIMPLE BYOD APPROACH

HOW ZIX GETS IT RIGHT

zix | ONE

A WORLD TRANSFORMED

There has never been a more profound consumer-driven technology craze than mobile devices. In 2013, worldwide sales of smartphones reached 968 million[1], with tablets at 195 million[2]. Mobile devices have changed the way we live and work—and the way we combine the two.

Nowhere is this more apparent, or challenging, than in the healthcare industry.

The healthcare professionals, administrators and staff entering today's workforce grew up with mobile devices. While they may be willing to take the late call, respond to the after-hours email and work the weekends at home, they want to do so on their own mobile devices. And they want to stay connected to their private lives when reentering the workplace for their next shift. They want to use their own phones and tablets at work to access personal information as well as healthcare data, the security of which is regulated by HIPAA, the HITECH Act and possibly state regulatory or PCI requirements.

But the desire of healthcare workers to use their own mobile devices is also for a greater cause. In one recent study, nurses stated that the ability to use their own mobile devices—the devices with which they are most familiar and efficient, not a different brand or model provided by the employer—allowed them to improve patient safety, more quickly communicate with other clinicians and reduce the risk of medical errors.[3] But like all workers, doctors and nurses do not want to be smothered by inconvenient security. In fact, a 2012 Enterasys Networks survey reported that 91% of mobile-device users had disabled the auto-lock on their tablet and 75% did the same on their smartphone.

Companies across all industries have had to accept this reality, otherwise known as bring-your-own-device (BYOD). Six out of 10 companies already have BYOD programs, and another three out of 10 companies plan to move to BYOD programs soon.[4] Now, it is IT's uphill battle to manage BYOD.

> "There's nothing hotter for consumers than tablet devices and smart phones. There's also nothing more terrifying for IT than tablet devices and smartphones."
>
> —Mark Fidelman
> Forbes

THE CHALLENGES OF BYOD

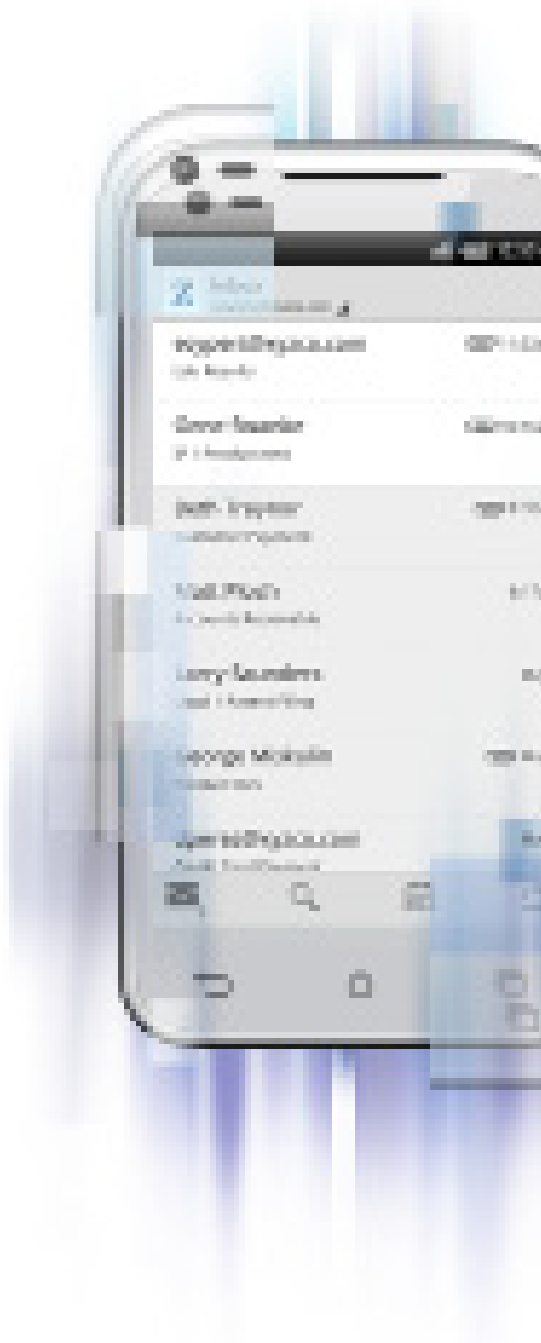
With 81% of employees using their phones at work,[5] businesses have stopped asking: "Is sensitive data leaking from personal devices?" and started asking: "How do we effectively prevent sensitive data from leaking from personal devices?" Although the answer is not simple, the cost of breaching electronic PCI is too high to ignore. Even one breach could result in government fines, legal fees and costs associated with notification and personal protection. And the resulting loss of trust—with both patients and partners—could impact your organization long-term.

Mobile Device Management (MDM) monitors employee devices and wipes all data when devices are lost or stolen. But MDM solutions are complicated and costly for business and do not fully address the regulatory issue of protecting healthcare data. MDM solutions leave data on the device. When a device is lost or stolen, the business can disconnect access to the data if the device is online. However, if the device is offline, all sensitive data is jeopardized.

And for employees, MDM is a nightmare. The user experience is beyond frustrating, requiring password protection on every function, whether employees want to call a friend or take a photo of their kids. Add on the idea that all personal data, from messages to photos, could be erased by the employer without a moment's notice, and it's easy to understand why employees would be upset when forced to use an MDM solution on their devices.

Policy controls with native devices, such as connections to Exchange ActiveSync, are a type of MDM. They secure specific functions but offer fewer management capabilities with the same employee frustrations. Again, because policy controls allow data to reside on the device, any stolen or lost devices are vulnerable and unprotected if taken offline.

Containerization offers a modicum of the user experience employees demand—a separation of work life and personal life. However, the user experience has flaws. Container solutions do not automatically integrate corporate contacts into the phone, so if you receive a call or text, your phone can't identify the person. In addition, some container solutions lack the ability to notify users about upcoming events or inbound email and can only provide access to the most recent corporate emails.



THE CHALLENGES OF BYOD

The worst flaw of containerization, however, is the most significant for the healthcare industry. Similar to MDM solutions, containerization leaves regulated sensitive data on the device and vulnerable. If stolen or lost devices are taken offline, the data is left unprotected.

Virtualization can be an effective manner of managing corporate data, but there are tradeoffs. The solution enables the employee's whole desktop to be accessible on their device. If a device is lost or stolen, the connection is broken, and the data is secured. However, those occasions are overshadowed by the impairment of everyday use. A desktop is easy enough to navigate on a laptop; placed on a tablet or a smartphone where screen real estate is limited, the virtual desktop becomes an overwhelming experience for employees.

Browser-based services, such as Outlook Web Access, are another method of managing corporate data. However, similar to virtualization, they too offer a poor experience for employees. They require full credentials, making access to corporate data inconvenient and cumbersome, which discourages employee enablement. In addition, like MDM and containerization, browser-based services expose companies to vulnerabilities, leaving unprotected sensitive data cached on the device.

None of these approaches are truly effective. None of them truly secure regulated healthcare data or provide a solid user experience. If sensitive data is unsecure, then you risk regulation non-compliance—and the BYOD approach is useless. If the user experience is poor, then the success of the solution will be impaired. "Many organizations have learned from BYOD projects that the success or failure of IT choices hinges upon user acceptance of the solution and whether it's perceived as having a productive and pleasant user experience," said Trent Henry, Vice President, Identity and Security for Gartner Research.[6]

> "Many organizations have learned from BYOD projects that the success or failure of IT choices hinges upon user acceptance of the solution..."
>
> —Trent Henry
> Vice President,
> Gartner Research

THE CHALLENGES OF BYOD

A UNIQUE COMPARISON

Our home is a safe place where we keep our most valuable possessions. To fully comprehend the BYOD challenge and current solutions, we'll use the metaphor of working from home as compared to BYOD solutions.

MOBILE DEVICE MANAGEMENT, INCLUDING NATIVE POLICY CONTROLS

Monitors your employees' devices and can wipe all data. In work-from-home terms, MDM installs the locks and security system on your employee's whole house. Their every move is monitored, and all their personal belongings are destroyed when the company decides it needs to remove its files from the home. Think your employees would be upset if they lost all their furniture, clothes and family photos?

CONTAINERIZATION

A local key secures data: In work-from-home terms, containers would put a lock and security system on your employee's home office. When they leave, they always lock up, but the key has to stay under the mat. If thieves look where they need to, all sensitive data is vulnerable.

VIRTUALIZATION AND BROWSER-BASED SERVICES

Like hitting a nail with a sledge hammer: In work-from-home terms, your employee's office is crammed into a small bin and buried in a coat closet. Ever have a hard time finding something in a packed closet?

It may seem inappropriate to compare a home to a mobile device, but to most users, their device is their next most valuable possession. It houses photos, videos and personal data, and it enables connections to bank accounts, social media and the office. Clearly we wouldn't expect employees to tolerate either of these intrusions or inconveniences in other business contexts, so it's no surprise they won't tolerate it in a BYOD setting.

A SIMPLE SOLUTION THAT BALANCES WORK AND LIFE

Zix simplifies the BYOD challenge. We recognize that easy, secure mobile access to sensitive data is powerful for your organization and more convenient and productive for doctors, nurses and other healthcare workers. We also recognize that employee buy-in is critical to the solution's success. ZixOne is a BYOD solution that both business and employees can accept with ease.

ZixOne enables easy access in a simple environment to the most used business application on mobile devices—email. Of all activities performed on mobile devices, email still remains the most popular (79% for smartphones and 72% for tablets[7]). In comparison, mobile users spent less time on every other function, including phone calls, text messages, social media, Internet browsing and shopping. And that trend isn't going away. Forrester Research forecasts 78% of all U.S. active email users will also access their emails through mobile email clients by 2017.[8]

ZixOne is a mobile app that enables corporate email access without allowing the data to reside on the device where it has greater potential for compromise. Most importantly, ZixOne provides the ultimate BYOD solution—uncompromised benefits for both employees and companies.

AN UNRIVALED USER EXPERIENCE

ZixOne does not offer mobile email in the same way your employees know it today. With ZixOne, mobile email is better. It combines a consistent look and feel with greater speed and security. After entering a simple passcode, employees read, compose, reply and forward corporate email as usual. Their calendar and contacts are intact. Best yet, attachments will no longer slow them down. Attachments are viewed instantly from the exchange server instead of watching the ticker as the whole attachment is downloaded to their device. Thankfully for you, the attachment can't be stored on the device either.

A SIMPLE SOLUTION THAT BALANCES WORK AND LIFE

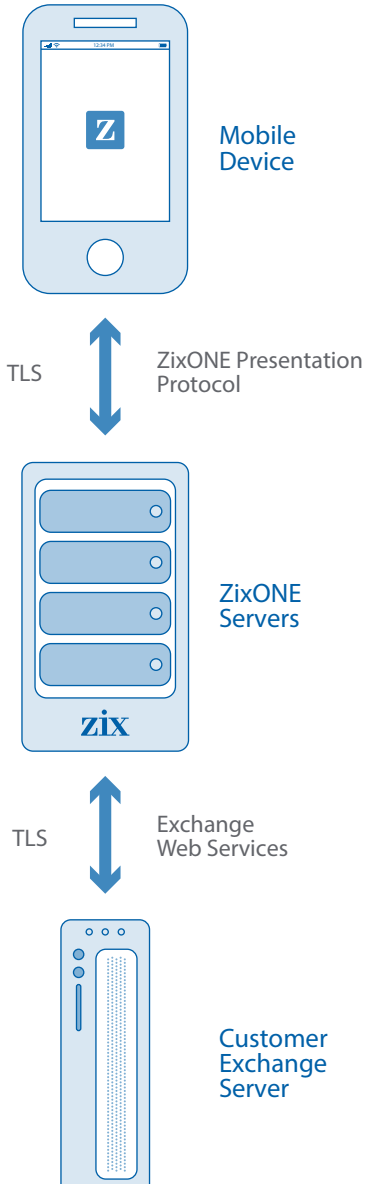
Your employees will appreciate that their corporate email looks the same and operates quicker, but not nearly as much as they'll appreciate that the added security does not impact the other functions of their device. Their apps and data remain under their control. They can switch to other apps, take a phone call or browse the Internet with ease. More importantly, their privacy is never jeopardized, because their company only controls access to their corporate email.

HEALTHCARE DATA PROTECTION WITHOUT THE DOWNFALLS

The benefits of other BYOD solutions are overshadowed by their shortcomings. With ZixOne, your organization does not have to compromise. ZixOne solves the greatest BYOD risk exposure by protecting the most-used mobile app—email. ZixOne raises the bar on BYOD security by not allowing email data to reside on the device. Through a secure, mobile environment, employees interact with their mobile email as usual. If the device is lost or stolen, companies disable access. Because sensitive and regulated data does not reside on the device, companies do not have to manage or worry about thousands of copies of emails and attachments.

ZixOne delivers all this security in an easy user experience. The user experience may not be the first need that comes to mind for all companies, but it is certainly essential. After all, this whole BYOD movement started due to user demand. With an easy experience, ZixOne will be accepted by even your most demanding employees.

An additional benefit of ZixOne is the avoidance of corporate legal liability. By enabling access to corporate email, companies are merely presenting their data. Without access to other aspects of the personal device, ZixOne eliminates any legal liability in the event employees or contractors want to sue their company for illegal actions associated with monitoring personal data.



A SIMPLE SOLUTION THAT BALANCES WORK AND LIFE

OTHER BYOD APPROACHES COMPARED TO ZIXONE

To fully realize how ZixOne best solves the BYOD challenge, please compare how each BYOD approach manages all the needs and demands of your company and your employees.

		MDM	CONTAINERIZATION	NATIVE CONTROLS	VIRTUALIZATION	BROWSER-BASED SERVICES	ZIXONE
CORPORATE NEEDS	Corporate Data Protection Corporate data does not reside on mobile devices and is not in jeopardy when offline.				✓		✓
	Employee Work Enablement Employees have simple, full access to the most used mobile application—email.	✓		✓			✓
	Prevent Legal Claims Liability is removed, because businesses cannot access personal data.		✓		✓	✓	✓
EMPLOYEE NEEDS	Employee Convenience Easy connection to life and work on the devices they choose without any impediments.						✓
	Employee Control Employees control their devices, their apps and their personal data.		✓		✓	✓	✓
	Employee Privacy Personal activities and data cannot be monitored by their company.		✓		✓	✓	✓

WELL POSITIONED TO OFFER THE LEADING BYOD SOLUTION

Zix has gained the trust of the nation's most influential organizations by providing easy-to-use, reliable secure email through encryption services and The Power of Everyone, a community of tens of millions of users. If you don't use Zix, odds are you know someone that does.

Zix is used by one in every five U.S. hospitals, more thn 30 Blue Cross Blue Shield organizations, all the U.S. federal financial regulators, the SEC, FINRA, divisions of the U.S. Treasury and one in every five U.S. banks.

We understand secure email, and we understand why finding the right BYOD solution has been so challenging. Other solutions don't offer an approach that meets all your regulatory needs and your employees' demands. If you compromise, your BYOD solution will be useless.

ZixOne is designed to offer a simple solution that meets every need and demand and provides benefits beyond industry standards. Bring Your Own Zix and see how easy BYOD can be.

NOTES

1. "Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013." Gartner Research. February 2014.
2. "Gartner Says Worldwide Tablet Sales Grew 68 Percent in 2013, With Android Capturing 62 Percent of the Market." Gartner Newsroom. March 2014.
3. "BYOD To Work—Tech Trend Helps Nurses Provide Improved Patient Care." Health IT Outcomes. August 2013.
4. "Consumerization Drives Smartphone Proliferation." Forrester Research. December 2011.
5. Research conducted by Harris Interactive.
6. "How to Achieve Single Sign-On With Mobile Devices." Gartner Research. March 2013.
7. Adobe Digital Publishing Report. January 2013.
8. "Email Marketing Forecast, 2012 To 2017." Forrester Research. October 2012.