ivanti

The Ultimate Guide to BYOD

How to build a secure (and sustainable!) BYOD program for the Everywhere Workplace

Introduction

Spurred on by the pandemic, remote and remote-first work has accelerated the erosion of the traditional network perimeter. Enterprise users now work anywhere, on any network, many times using their own devices to access business apps and data. In fact, Gartner predicts that as much as 48% of the global workforce will remain remote at least part of the time[1]. The majority of these employees, we can reasonably assume, will prefer to use their own devices.

But as the BYOD market grows, so do the security threats, particularly those against enterprise apps and data on unsecured devices, especially those owned by employees. Since the start of the pandemic, phishing attacks have risen 85%, ransomware attacks are up 89%, and four of every five IT professionals believe attacks are getting more sophisticated.

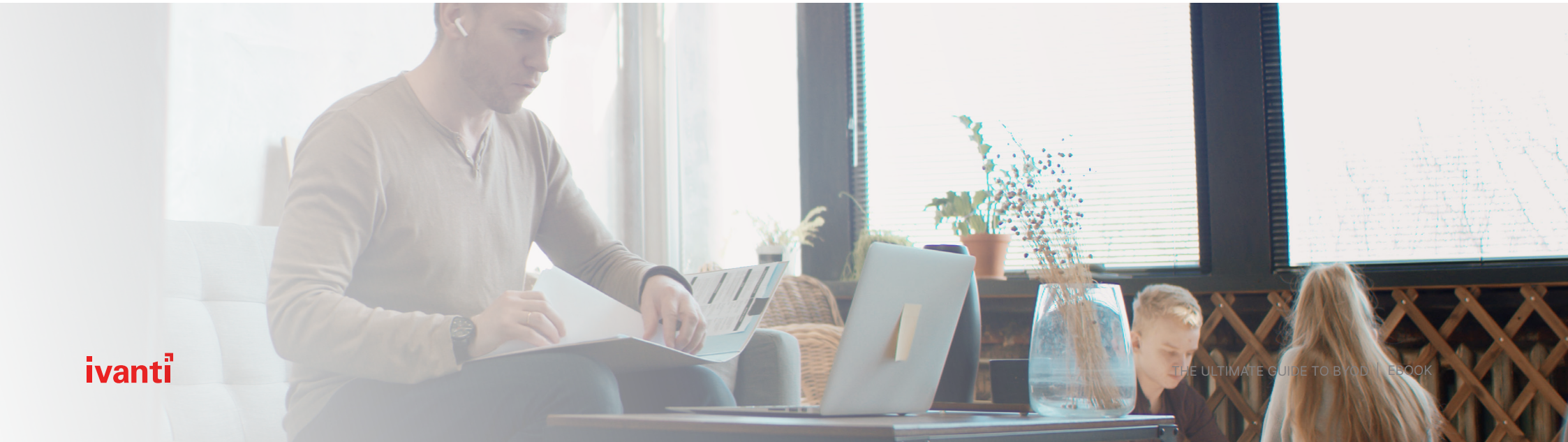
Today, security professionals must reconsider the best practices on which they've previously relied before and during the pandemic, especially when it comes to BYOD. Chances are you've implemented some program to support working-from-home users over the past year. Chances are also strong, your program was built for the short term one in which users were expected to quickly return to the office.

Now, though, as remote and remote-first work becomes the new, permanent reality, it is imperative you implement solutions that provide a secure, contextual connection based on device, app, user, environment, network, and everything else that's involved in accessing data. It's also vital that these solutions empower employees — and do not hinder their ability to work where and how they want.

Building trust in a zero trust world

An enterprise environment based on "zero trust" — a security framework that assumes bad actors are always on your network and treats all endpoints, apps, networks, and clouds to be compromised and hostile — has emerged as a successful model for delivering continuous protection at the user, device, app, network, and data levels in a BYOD world. Zero trust assumes that all access to corporate resources should be restricted until the user has established their identity and access permissions, and until the device has passed a security profile check.

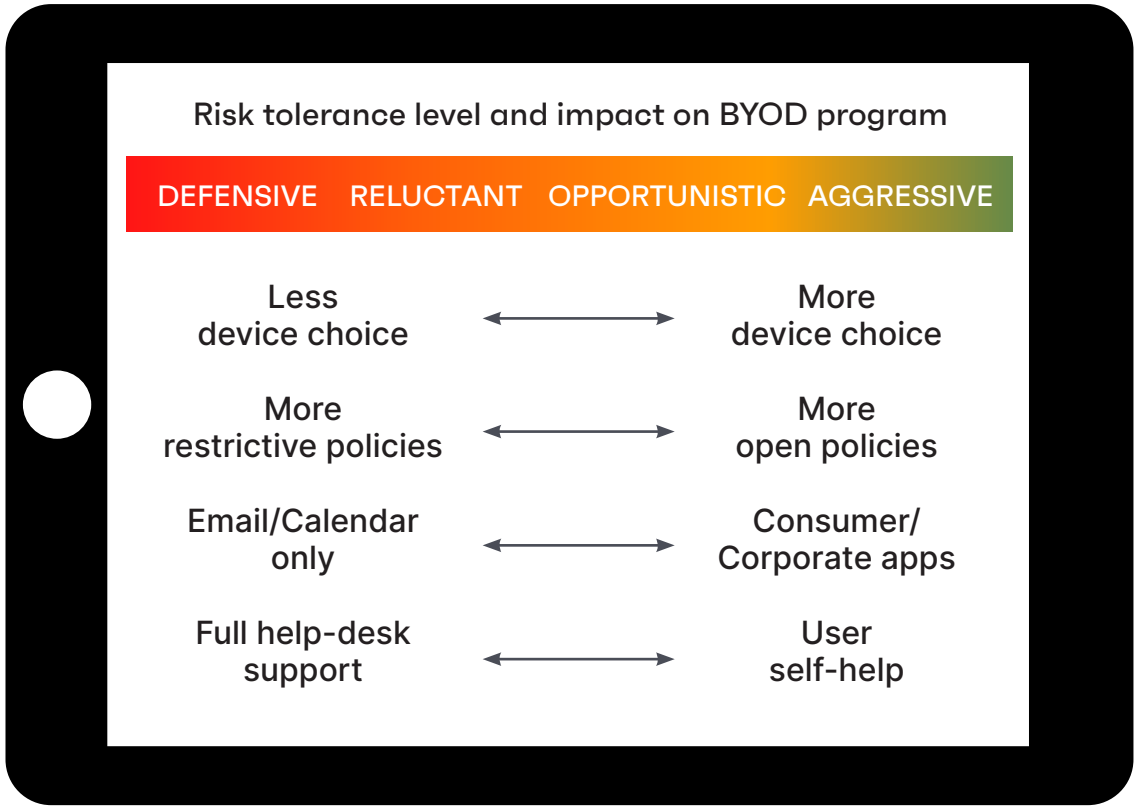
As organizations build and refine their BYOD programs, incorporating zero trust security should be top of mind. In the following sections, we'll look at best practices and recommendations for preparing, building, rolling out, and sustaining a secure and successful BYOD program over the long term.



Part 1:
Prepare Your Organization

Determine your BYOD risk tolerance

Understanding your company's risk tolerance is the first step to understanding how BYOD can work in your organization. Your company's industry may be the main factor determining your risk tolerance. For instance, organizations in healthcare, biotech, financial services, government, or security services will likely adopt a more defensive position toward BYOD than startup tech companies. It's important to keep in mind, though, that every organization, regardless of self-determined risk tolerance, must consider the realities of an increasingly remote or remote-first workplace.



Engage stakeholders early to define program goals

One of the most important steps to developing a long-term BYOD program is getting early buy-in from critical players across the company. While it can be difficult to align the interests of diverse company leaders from executive management, HR, legal, finance, and IT, their support is critical for building a successful program.

While the approval of executive-level stakeholders is essential, you also need to ensure the program will meet the needs and expectations of end users. In general, mobile users expect access to the data they need for both work and personal business, on their device of choice, wherever they are. Any BYOD program that fails to meet these requirements will likely be rejected by the majority of users.

To avoid this outcome, adding one or two employee representatives to the team can help you gain valuable input and feedback on end-user preferences, device requirements, support and communication needs, and more. Anticipating these and other common objections to BYOD can also help you facilitate the planning phase.

To help resolve these and other concerns from the start, you should form a BYOD steering committee comprised of representatives from all stakeholder departments. A steering committee can help groups with different priorities build consensus and define program goals that all stakeholders agree upon. Documenting these goals will serve as a valuable resource to help all stakeholders stay focused on the overall objectives as the BYOD program evolves.

Executive Sponsorship	Human Resources	Finance	IT Operations
We can't get executive support, but let's move the BYOD plan forward anyway.	The company cannot be held responsible for compromised personal data on employee-owned devices.	We can't fund a program that doesn't offer demonstrated cost savings.	We cannot support the huge variety of apps that the business wants on personal devices.
A BYOD project can easily derail without executive sponsorship. Because BYOD programs require participation from diverse stakeholders, executive leadership is often necessary to ensure deadlines and responsibilities are met.	Working together, HR and IT should design clear boundaries between corporate and personal data. Also, your end-user agreement should specify that the company may access personal data if the device is subject to forensic analysis. Also, upon separation from the company, all attempts will be made to preserve personal data on the employee's device, but a full data wipe may be issued if deemed necessary.	Many enterprise workers are already using their devices to access and share company data, email attachments,and other content. When the organization enables secure-choice computing, IT gains a high level of control over corporate apps and data. Secure BYOD also improves user productivity by preserving the native device experience employees already know and love — which directly translates to the bottom line. Specific cost savings can be realized by reducing support costs through an end-user, self-service model that leverages self-help tools, user support communities, social networks, and user forums.	Having the ability to dynamically modify or update security policies, user access, and server configurations on already deployed mobile apps will reduce the operational overhead of managing mobile apps.

Survey and communicate with employees

After you have determined your company's BYOD risk tolerance and stakeholder goals, the next step is to issue a short but specific employee survey across the company. The greater your risk tolerance, the more important it is to tailor the survey to capture user preferences for devices, apps, communication tools, and tech support. To ensure you gather the information needed to design a successful BYOD program, your survey should include questions that identify:

- Which OS/devices do employees currently own and plan to purchase in the future?
- Which factors would encourage BYOD participation?
- Which factors would discourage BYOD participation?
- Which corporate apps are most valuable to users?
- How comfortable are users with self-service support?
- What is the impact of BYOD on company perception, productivity, and work/life balance?

ivanti

Identify your mobile IT capabilities

Now that you know your BYOD risk tolerance, program goals, and user preferences, do you know if you have the right people and resources to build the program your company needs and users want? A capability assessment can help you determine if you have the right people, processes, and technology to enable employees to use their preferred devices, apps, and cloud services.

A capability assessment is actually a simple checklist of requirements, the status of completion or availability, and where the capability or task is in the procurement process. For example, an IT staffing checklist would include all of the resources needed to implement the program, whether those resources are currently available or not, and who is responsible for bringing those people on board. Here's a snapshot of just a few of the staffing requirements you would need to include in the BYOD capability assessment:

	Please place an 'X' in the appropriate column				
Sufficient staffing	Ready	Planned	None	N/A	Comments
IT resources					
Device experts					
Android: <list name(s)>					
iOS: <list name(s)>					
Windows 10: <list name(s)>					
Device testing					
Design process: <list name(s)>					

Part II: Build the Program

Ensure your resources can support BYOD

The technology skills needed to manage a mobile IT infrastructure differ dramatically from those needed to run a traditional desktop enterprise. Procuring the right expertise is critical to executing a successful BYOD program. Here are the recommended roles needed to build and sustain BYOD (keep in mind that one individual can wear many hats; you don't necessarily need one person for each role).

Mobile systems engineer

A mobile systems engineer is a subject matter expert for all aspects of mobile technology. This role encompasses all hardware, software, and networking technologies required to implement a BYOD program. The mobile systems engineer also provides expertise in integrating mobile technologies with enterprise components such as identity, messaging, security, networking, and database services. Their domain of expertise includes:

- Mobile operating systems, such as iOS, Android, and Windows 10
- Carrier networking technologies, such as GSM/CDMA/LTE and underlying protocols
- Mobile hardware, software, applications, application programming interfaces (APIs), and development toolkits

Mobile device expert

A mobile device expert is a "gadget hound" who stays on top of both existing and future devices and software releases that can impact the mobile infrastructure. By staying on top of mobile technology trends, the device expert can prepare the environment to either support or restrict the use of new devices. The device expert is fully versed in popular platforms and manufacturers, including:

- **Android:** Samsung, Motorola, HTC, LG, Sony, Huawei, Lenovo, Acer, ASUS
- **iOS and macOS:** All Apple devices
- **Windows 10:** Lumia, HP, Alcatel 7

Mobile security expert

A mobile security expert is responsible for establishing and updating mobile security policies and controls. The mobile security expert also educates users on social and behavioral security risks, sets appropriate use policy, and helps develop strategies for:

- Mobile security and risk mitigation
- Mobile data protection
- Mobile OS platform review and positioning
- Mobile application threat management

Ensure your resources can support BYOD, continued...

Mobile applications developer

Regardless of whether your enterprise develops its own applications or outsources mobile app development, you may need onsite app developers with the following skills:

- Experience with application development lifecycles and methodologies
- Ability to design and develop iOS, macOS, Android, and Windows 10 apps
- Hands-on experience in Objective-C, Cocoa Touch, iOS SDK, XCode, Developer programs, Java, Google Play, Android SDK and device manufacturer APIs, .NET, Web Services, XML, and HTML5
- Strong object-oriented programming and design skills

Mobile service and support resources

The accelerated lifecycle of mobile devices and services requires an infrastructure that can quickly adapt to constantly evolving conditions. To respond effectively, your enterprise must customize the way services and support are delivered to mobile users because these mobile users have much different needs and expectations than PC users. To be effective, mobile service and support resources must be able to:

- Provide self-service tools to help improve user satisfaction and reduce costs
- Establish a core mobile support group that manages all mobile escalations
- Develop and distribute knowledge base articles, support scripts, and procedures to all users
- Share knowledge through social networking and mobile communities
- Establish clear and regular communication across multiple channels to keep users up to date on service status and changes

The eight components of a successful BYOD strategy

SUSTAINABILITY

Maintain a positive user experience.
While cost and security concerns are important issues to manage, BYOD program sustainability depends on delivering a consistently positive user experience over the long haul.

DEVICE SELECTION

It's a popularity contest.
Survey employees to determine which devices and platforms they currently use and are intending to purchase. Include as many of these devices as possible when the program launches to maximize employee participation.

INTERNAL MARKETING

Build your IT "brand."
Promote your BYOD program as a corporate effort to support work/life balance through increased mobility and flexibility, and position IT as an ally to the modern, mobile workforce.

LIABILITY

Protect your company from legal action.
Define and implement clear policies and procedures that protect your company from threats ranging from the loss of intellectual property and confidential customer data, to legal action, fines, and damage to reputation resulting from data leaks.

APP DESIGN AND GOVERNANCE

Enforce security without compromising the user experience.
In a BYOD environment, apps involve sensitive enterprise data, which can easily be compromised if the device is accidentally lost or targeted by a mobile attack. Your organization will therefore want enough visibility and control to protect corporate apps and data without monitoring a user's personal activity on their own devices.

USER EXPERIENCE AND PRIVACY

Establish employee trust.
Clear communication regarding privacy, and the establishment of a social contract between the company and its employees that clearly defines the BYOD relationship, are critical for establishing employee trust.

Zero Trust Security

Mitigate security risks.
Building a trust model that identifies how and when a device falls out of compliance, steps for remediation, and the extent to which these actions are acceptable to users is absolutely essential.

ECONOMICS

Control the costs of doing BYOD.
Determine how best to structure financial aspects of your BYOD program so that your company realizes maximum return on investment.

1 - Sustainability:

Maintain a positive user experience

In the wake of the pandemic, many companies rushed to create BYOD policies and processes that are not sustainable over the long term. Understandably, enterprises were mainly concerned about implementation costs and security, and tended to focus on those issues over the past year. But without respect for the user experience as remote and remote-first work remains status quo for the foreseeable future, the BYOD program will eventually prove ineffective.

Why? If BYOD policies are overly restrictive, lack adequate support for employees' preferred devices, or are simply too complex and confusing, employees will find a way to either circumvent the policies or end their participation altogether. In both instances, the needs of the company are not met — either security is compromised or business value is lost. So, while cost and security concerns are important issues to manage, BYOD program sustainability depends completely on delivering a consistently positive user experience over the long haul.

2 - Zero Trust Framework:

Establish zero trust security

Today, the average employee, remote or in-office, uses several devices for work, including desktops, laptops, tablets, smartphones, and wearables. Managing the sheer number and range of these devices — whether owned by the employee or company — has introduced extremely dynamic and complex security issues. A zero trust approach to security is the best way to protect company data in an era where IT's traditional static perimeter has given way to the perimeter-less remote enterprise. A zero trust framework enables you to:

- Provision any device (including BYOD) for a user with the appropriate apps, profiles, and policies
- Grant access based on full context (user, device, app, network, threat, time, location, and OS)
- Protect data at rest and in motion by containerizing and eliminating threats on the device
- Enforce security policies (user, device, app, network, threat, time, location, and OS)

3 - Device Selection:

It's a popularity contest

Based on feedback from your initial employee survey, you should have a good idea about which devices and platforms employees currently use and are intending to purchase. You should include as many of these devices as possible when the program launches to maximize employee participation. In addition, your device-selection process should include all of the desired mobile platforms in the program as long as they meet your security and support requirements, such as asset management, encryption, password policy, remote lock/wipe, and email/Wi-Fi/VPN configuration. Without these basics, the mobile platform is not viable for the enterprise.

- Develop a certification plan to ensure that future devices can be evaluated quickly and efficiently for possible inclusion in your program
- Clearly identify which devices are allowed (or not) and why, otherwise employees may purchase devices your program doesn't support
- Ensure your IT team maintains expertise and knowledge about constantly evolving mobile devices and operating systems, otherwise your BYOD program can quickly become obsolete

4 - Liability:

Protect your company from legal action

An introduction or reconfiguring of your BYOD program may also introduce new liability concerns to your business. As part of your BYOD program, you need clear policies and procedures that protect your company from threats ranging from the loss of intellectual property and confidential customer data to legal action, fines, and reputation damage resulting from data leaks. While every business needs to seek specific legal counsel on BYOD liability, your mobile device policy or end user agreement should include:

- Security policies for enterprise data on personal devices (especially since different types of security may be required on different devices; for example, more protection against over-privileged consumer apps might be required on Android vs. iOS)
- Policies for personal web and app usage (during and after business hours, onsite, and offsite)
- Clear limitations for company liability due to the device owner's personal data loss
- Understanding of how BYOD reimbursement (partial stipend vs. full payment of service costs) affects company liability

5 - User Experience and Privacy:

Establish employee trust

Optimizing the user experience should be a top priority for your BYOD program. Clear communication over sensitive topics such as privacy is critical for establishing employee trust. Therefore, a social contract that clearly defines the BYOD relationship must be established between the company and your employees. The contract is a well-defined agreement that helps:

- Identify the activities and data that IT will monitor on the device, such as app inventory, to protect against rogue apps that could compromise enterprise data
- Clarify which security actions IT will take in response to certain circumstances
- Define granular controls such as activity monitoring, location tracking, and application visibility
- Critically assess security policies and restrictions to ensure they are not overly restrictive
- • Identify core services, such as email and mission-critical apps, that the company can deploy to the employee's device
- Preserve the native experience so employees can continue to use their preferred apps for everyday functions
- Communicate when employee devices are out of compliance, the possible consequences, and proactive notifications to help users remediate issues quickly

6 - Economics:

The cost of BYOD

It's never too early to determine how to structure the financial aspects of your BYOD program for the long term. Key issues to consider include how to:

- Pay for devices and service. Determine if the employee will be 100 percent responsible for device and service costs, or if the company will pay a full or partial stipend
- Leverage agreements with mobile operators to provide business, concierge, and self-service options to users
- Explore existing telecom services and processes and, where possible, offer corporate discounts to users, including waivers of termination fees and early upgrade allowances
- Research new carrier services and plans that can improve and enhance the BYOD program
- Save money on help-desk resources by implementing self-help services

7 - App Design and Governance:

Enforce security without compromising the user experience

In a BYOD environment, apps involve sensitive enterprise data, which can easily be compromised if the device is accidentally lost or targeted by a mobile attack. Your organization will therefore want enough visibility and control to protect corporate apps and data without monitoring a user's personal activity on their own devices. To gain employee trust and protect critical data, your BYOD program must implement app design and governance procedures that:

- Provide conditional access to corporate apps and data
- Communicate and justify the extent to which IT supports or restricts personal apps
- Configure app availability based on device ownership because certain internal applications may not be appropriate on personal devices for security reasons
- Define remediation actions, such as notification, restricted access, quarantine, or selective wipe, for app-usage violations

8 - Internal Marketing:

Build your IT "brand"

The process of implementing a BYOD program offers a great opportunity to nurture employee-company relations. You can promote your program as a corporate effort to support remote and remote-first work. The company can also foster the internal perception of IT as a champion of end users and supporter of technologies that employees want to use. In addition, a BYOD program can be used as an effective recruiting tool as more candidates have indicated they'd prefer to work remotely at least part of time rather than fully returning to the office.

Part III: Role Out the Program

“Soft launch” your new BYOD program

After your program goals, policies, processes, and technical infrastructure have been established, you can begin the phased rollout or “soft launch.” By rolling out in phases, you allow a small subset of users to test the program and provide feedback about performance, support, and other issues that you might not have discovered during the initial phases. The BYOD program rollout typically follows three phases: Pilot, Deploy, and Sustain. In some cases, these phases may be combined or skipped altogether, but we’ll describe them in detail for this guide.

Initiate pilot tests

Pilot tests help you troubleshoot and resolve problems before rolling out the BYOD program to the entire company. They provide an opportunity to safely test functionality from end to end and collect user feedback to identify what is working well and what needs fixing.

STEP 1:

Select the sample user group for the pilot

Choose a sample group of users to complete the device registration and configuration process. Your sample group should be a microcosm of the entire company and include a wide range of roles, business units, and job functions so you can test the process of qualifying users by role and manager approval. You should also distribute the BYOD mobile device policy or end user agreement at this stage to ensure users understand the terms of the program.

By including a large percentage of business and non-technical users in your sample group, you can get a better understanding of the average BYOD user experience. However, IT operations staff should also participate in the pilot to ensure any technical issues are discovered during the pilot phase.

STEP 2:

Survey employees to continually improve the user experience

It can't be emphasized enough: You need to survey users during every phase of the BYOD implementation to make sure the program is meeting employee needs and expectations. The three types of surveys include:

- Pre-deployment survey: Captures employee preferences for devices, operating systems, applications, data plans, and support models
- Registration survey: Captures the user's first experience with the BYOD program and can identify any gaps in the device registration process. Because registration is essential to employee participation in the BYOD program, you want to make sure that the process is as fast, efficient, and easy to understand as possible
- Follow-up or closing survey: Provides both specific and open-ended questions to gather feedback about the overall user experience during the pilot test. It can capture metrics on performance and determine if the process has met employee expectations and program goals

Deploy the BYOD program and training service

Once you've ensured that all the registration and configuration processes are in working order, the next step is to fully deploy the program. However, instead of rolling out the program to the entire company, it's best to stage the deployment in phases to minimize potential impacts on performance and availability. By staging the rollout based on geography, department, job function, or other criteria, you can ensure the right resources are available to mitigate any issues.

You will also need to set up effective training and self-service capabilities when you deploy the program. Comprehensive and easy-to-use instructions on device registration and troubleshooting can help streamline the process of bringing employees on board. You might consider conducting your training program in a variety of formats — online, in person, and through written documentation — to support the different ways users access information.

The ultimate goal of user training is to minimize help-desk calls and maintain uptime by anticipating and resolving problems before they lead to lost productivity, compromised data, or more serious issues. And, by providing comprehensive training through self-service guides, online tools, and a broad user community, you can increase employee satisfaction by giving them greater autonomy over how they work.

You've reached a comfortable cruising altitude. Now what?

Once your BYOD program has been fully deployed across your company, the work of sustaining the program begins. The first step is to transition BYOD services from the "Build" team to the "Sustain" team; that is, from engineering to operations staff. This transition includes knowledge transfer, documentation reviews, help-desk services, support, and escalation process design. The handoff process can be labor-intensive and challenging, especially when transitioning to outsourced or third-party support centers. To ensure the transition doesn't impact mobile service levels or security, you need to establish clear processes for escalation, incident, problem, configuration, and availability management.

PART IV: SUSTAIN BYOD SECURITY AND PERFORMANCE

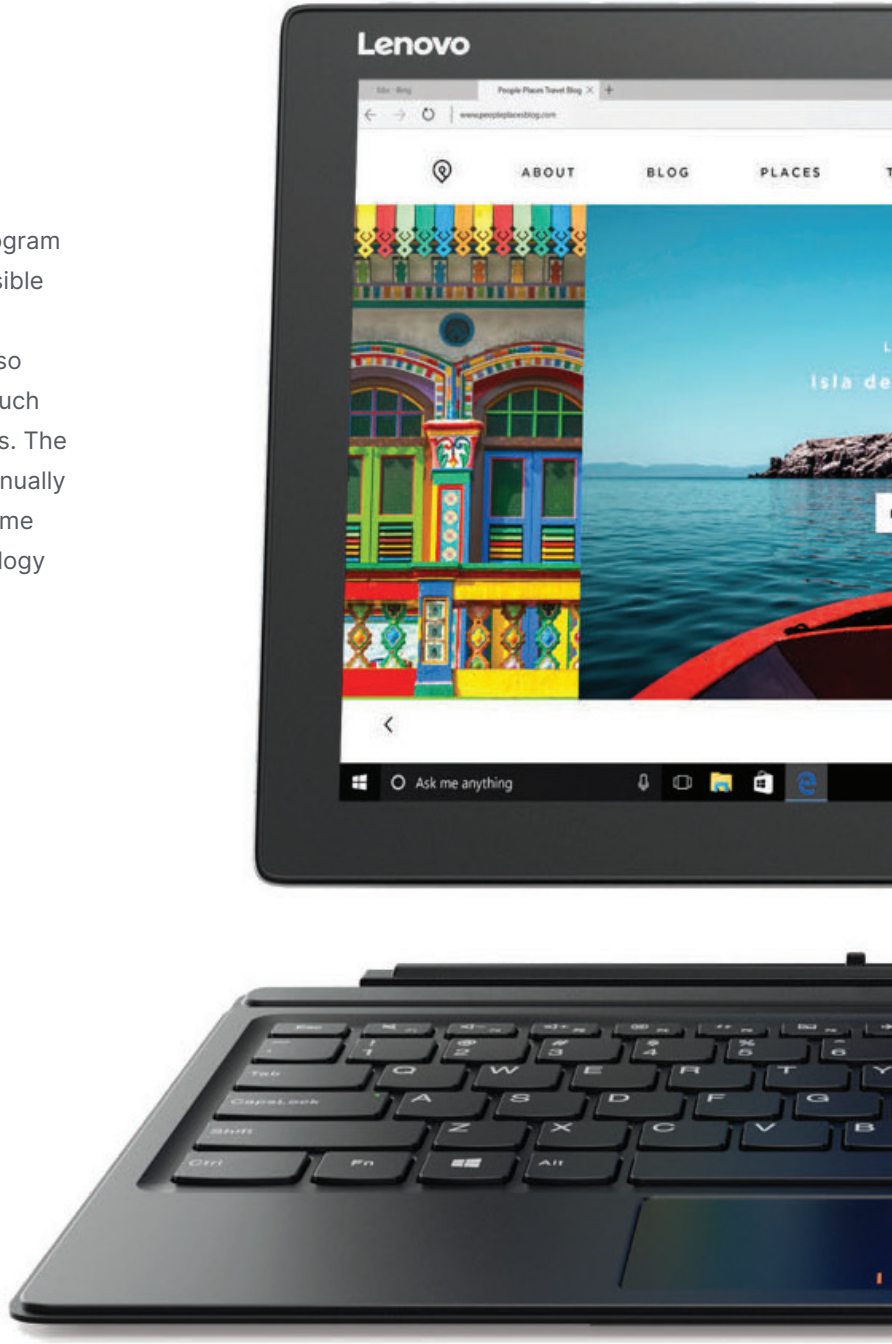
Enable self-reliance, self-service, and self-resolution

In an optimal BYOD program, the old-school model of help-desk calls and tickets gives way to a new era of user-based self-service. Although the need for an IT help desk will never go away, a core component of BYOD is a comprehensive support service that allows users to resolve the majority of incidents without help-desk intervention. The self-service model should allow users to:

- Self-register new devices, monitor and manage current devices, and wipe or retire devices as needed
- Self-remediate hardware, software, application, and compliance issues through clear notifications and resolution instructions
- Stay productive and efficient while maintaining security and compliance

Add more devices, systems, and apps incrementally

As mentioned earlier, the initial rollout of the program should include as many popular devices as possible to encourage employee participation. However, the market constantly introduces new devices, so your company will need a fast, efficient, light-touch certification plan for evaluating all future devices. The certification process must be ongoing and continually evolving. If the process is too heavy, it will become expensive and eventually fall behind the technology curve, so speed and efficiency are essential.



Ensure safe and effective device retirement

The lifecycle for mobile devices is significantly shorter than that for laptops and desktops. Because users upgrade their devices more frequently, you will need to have a secure device-retirement process in place to ensure that corporate data is not compromised if the user upgrades to a new device or leaves the company.

Device upgrade or purchase

In the case of an upgrade or purchase, the user should notify the help desk once the new device has been received. The user should be reminded to back up personal data and apps on the old device and move this content to the new device. The help desk can then complete the security process by removing all network access, configurations, apps, and data that had been granted to the old device.

To support your company's internal marketing efforts, you should already have recommendations for device recycling or donation centers where the employee can send the old device (assuming it won't be passed on to a friend or family member). Encouraging device recycling or donation offers a good public relations opportunity for the company and helps prevent usable devices, with hazardous components, from ending up in landfills.

Separation from the company

The device retirement process for users who are separating from the company is slightly different from the device upgrade process. Instead of being initiated by the user, the separation process should notify the user when access to corporate resources will be revoked and the device retired. The timeline and type of notification may be different depending on whether the separation is due to a resignation, reduction in force, or termination, and should be integrated with existing separation processes in consultation with human resources.

Transform your business with secure BYOD

By following the recommendations in this guide, you can deliver a BYOD program that enables outstanding mobile productivity while keeping corporate apps and data safe through a zero trust security framework.

The success of any BYOD program depends on its long-term sustainability, which means you must ensure the security of your corporate data, encourage user adoption by supporting employees' device preferences, and maintain a flexible technology portfolio that drives business innovation. Using the best practices and recommendations outlined in this guide, you can meet even the toughest IT security and management requirements while giving end users a consistently rewarding remote-working experience.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications, and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security, and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure, and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. Gartner, Designing Security for Remote-Work-First Enterprises, Jeremy D'Hoinne, De'Onn Griffin, Rob Smith, 30 June 2020