4 Steps to Address the App Security Gaps of BYOD

Quokka

Contents

BYOD is a Fact of Life —So Are the Risks

We use our mobile devices. A lot. That doesn't stop when we go to work. For IT and security teams in pretty much any type or size of business, bring your own device (BYOD) is now the norm.

While this use of mobile devices and apps offers benefits to businesses and their employees, it also creates increased risks to the organization. Addressing security and privacy threats is extremely challenging, particularly for organizations with smaller IT and security teams and budgets. This guide offers practical advice on how to cost-effectively address those security and privacy risks, without diminishing the benefits and convenience of BYOD.

Key Steps to Success

1. Apply robust security mechanisms
2. Ensure privacy
3. Maximize ease of use
4. Minimize cost and administrative overhead

Requirements to Secure BYOD

- Maximize ease of user enrollment and administration
- Employ identity and access management
- Deploy managed apps via enterprise app store
- Enforce security policies based on device configurations, system settings, installed apps, and target locations of data submissions
- Gain the ability to revoke access to corporate systems and data
- Identify and block phishing attempts
- Filter network traffic to block access to risky nations and ad networks
- Prevent IT from accessing personal information or data
- Adhere to NIST BYOD guidelines

The Benefits & Risks of BYOD

2

The Benefits of BYOD

The use of mobile devices has seen explosive growth in recent years. As in our personal lives, we've come to grow increasingly reliant upon mobile apps to get our jobs done. This acceptance of bring your own device approaches has become very widespread. In fact, more than 95% of businesses allow BYOD.[1]

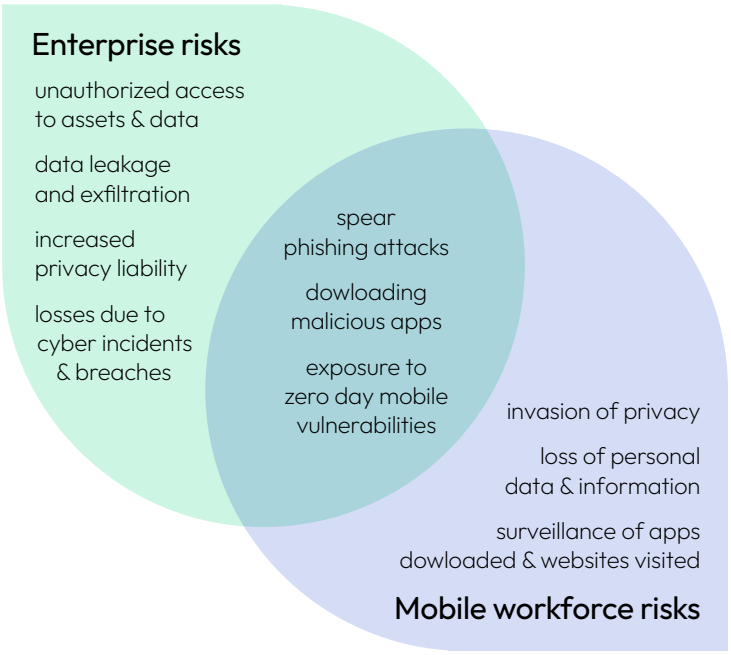
This growth in employee mobile device usage is happening for good reason. For businesses, the benefits include:

- **Productivity.** Through personal mobile device usage, an increasingly mobile workforce can stay connected and get work done from anywhere. Businesses can enable remote and hybrid workers, and any other employees, to stay productive, whether they're at home, on a train, at a café, or in the company's headquarters.
- **Cost and administrative savings.** By enabling BYOD, businesses don't have to purchase or support company-issued devices.

Plus, the workforce benefits too. By leveraging their own mobile devices, they gain greater flexibility to work when and where desired. Further, this offers the convenience that comes with having fewer devices to carry, learn, use, maintain, and keep track of.

The Risks of BYOD

As the ubiquity of mobile devices has emerged, so have mobile device threats. These threats pose a hazard for us as mobile device users, and they pose significant risks to businesses. Further this risk is growing more significant every day. According to a Forrester study, employee-owned mobile devices and corporate-owned mobile devices were the second most commonly reported targets of external attacks, both at 28% with only IoT devices targeted more frequently at 33%.[2]



1 NIST, "Spotlight: The Cybersecurity and Privacy of BYOD (Bring Your Own Device)," December 1, 2022, URL: https://www.nist.gov/news-events/news/2022/12/spotlight-cybersecurity-and-privacy-byod-bring-your-own-device

2 Forrester, "The State Of IoT Security, 2023," May 18th, 2023, URL: https://www.forrester.com/report/the-state-of-iot-security-2023/RES179300

BYOD Presents Uniquely Difficult Obstacles for IT and Security Teams 3

It only takes a glance at headlines from any given week to understand that cybersecurity is difficult. Some of the largest enterprises with the most expansive IT and security teams continue to fall victim to cyber attacks. Headlines tend to focus on the organizations with household names that experience a breach, but that doesn't mean smaller businesses aren't also being targeted and victimized.

Well-funded cyber criminal enterprises and nation states continue to wage attacks with greater frequency. The toolkits and services available to would-be attackers continue to lower the barrier to entry, and make it easier for criminals to scale and adapt their tactics.

For all these reasons, the goal of preventing breaches is inherently difficult to achieve. Further, employee-owned devices present a number of distinct obstacles that other systems and services don't.

Limited Control and Visibility for IT

Over the years, IT and security teams could employ governance controls around traditional, corporate-issued laptops, enforcing policies and controls in terms of usage, updates, security mechanisms, and so on. In contrast, in BYOD scenarios, it is the user that has sole administrative control. They choose when or whether to update their device's apps and operating system and they choose which apps to download.

User Autonomy and Privacy Demands

The fact that employees use their mobile devices for both personal and professional purposes makes enforcing policies difficult. When employees are using their own devices, they tend to be extremely reluctant to have anything about their usage constrained, whether in terms of which sites they visit or which apps they download. Further, they expect that they can keep their digital data and history private.

Legal Exposure

The use of mobile devices for work can expose a business to legal issues in two key ways. First, if a business does do any kind of surveillance on an employee's device, they may run afoul of relevant privacy rules, and, depending on the user's location, those penalties can be severe. Second, if an organization does detect evidence of an employee's criminal activity or malfeasance and doesn't report the matter in a timely fashion, they may be exposed to criminal prosecution.

Vulnerabilities

Mobile devices and applications are exposed to a number of distinct vulnerabilities:

- **Technology.** Mobile devices, OSs, and applications continue to be exposed by unpatched vulnerabilities, so-called "zero-day threats."
- **User behavior.** Even the most well-secured device may be a problem if a user takes risky actions. Employees may get fooled by spear phishing attacks, they may use an unsecured Wi-Fi, or they may elect to download malicious apps.

User Demands for Ease, Simplicity

Fundamentally, mobile users expect ease and convenience, whether doing online banking or checking email for work. This makes it very difficult to enforce security policies and mechanisms. If any security control adds too much complexity, too many steps, or undue inconvenience, employees won't use the control or they will try to circumvent it. In many ways, these issues of avoidance and bypassing controls will typically erode or completely eliminate any potential benefits that a security mechanism can provide. In other words, if users don't consistently and correctly employ the security mechanisms established, it may be worse than having no security at all.

Limitations, Drawbacks of Mobile Security Solutions

Over the years, a range of solutions have been introduced in the mobile device and application market, including mobile device management (MDM), mobile threat defense (MTD), and mobile asset management (MAM) solutions. However, while the specifics can vary, overall, these offerings present significant limitations and problems:

- **Costly and labor intensive.** Many of these offerings are simply too costly and labor-intensive for businesses with small IT teams and budgets.
- **Intrusive, lacking privacy.** These offerings often require IT teams to have full device control and they risk access to private user data and activities.
- **Limited security.** These offerings provide limited control in BYOD scenarios, which diminishes the security they can provide.

The Costly Consequences if Security isn't Addressed

4

Given the fundamental advantages and market forces in play, it is safe to say that BYOD is here to stay.

Those businesses that continue to allow BYOD without implementing effective security will be exposed to a range of significant risks. In fact, 70% of successful data breaches now originate at endpoint devices.[3] Following is more on how your business and your workforce can be affected.

Your Business

In the event of a cyber security incident, corporate assets can be exposed, whether to criminals, nation-states, or ruthless competitors. As a consequence, the business may be hit with a number of significant penalties:

- **Upfront costs.** In the immediate aftermath of a breach, an organization incurs the administrative cost and distraction associated with forensics and remediation. Further, businesses also must often take on the costs of hiring legal, security, and forensics experts.
- **Fines.** Across regions and industries, organizations can be subject to potential fines due to compliance breaches or privacy law violations.
- **Competitive threats.** Breaches can introduce competitive threats from intellectual property exposure and brand damage. In short order, an organization's trajectory and fortunes in the marketplace can be significantly and permanently altered.
- **Reduced sales.** Negative publicity and breach notifications may lead existing customers to move to competitors. Potential new customers may be wary of the organization, and either delay their purchase or go to an alternative.

Your Workforce

Fundamentally, a compromised mobile device can leave personal information and assets exposed. Individuals can be victims of identity theft, financial fraud, surveillance, and other dangers. If an employee is responsible for a breach at work, they can be susceptible to a number of penalties, including diminished job prospects and even termination.

3 | IBM, "What is endpoint security?" URL: https://www.ibm.com/topics/endpoint-security

Key Steps to Establishing Security and Privacy in BYOD Environments 5

As outlined above, there are plenty of unique challenges that make securing mobile apps and devices difficult—but it's not impossible. To meet these challenges, teams need to be able to take the following steps.

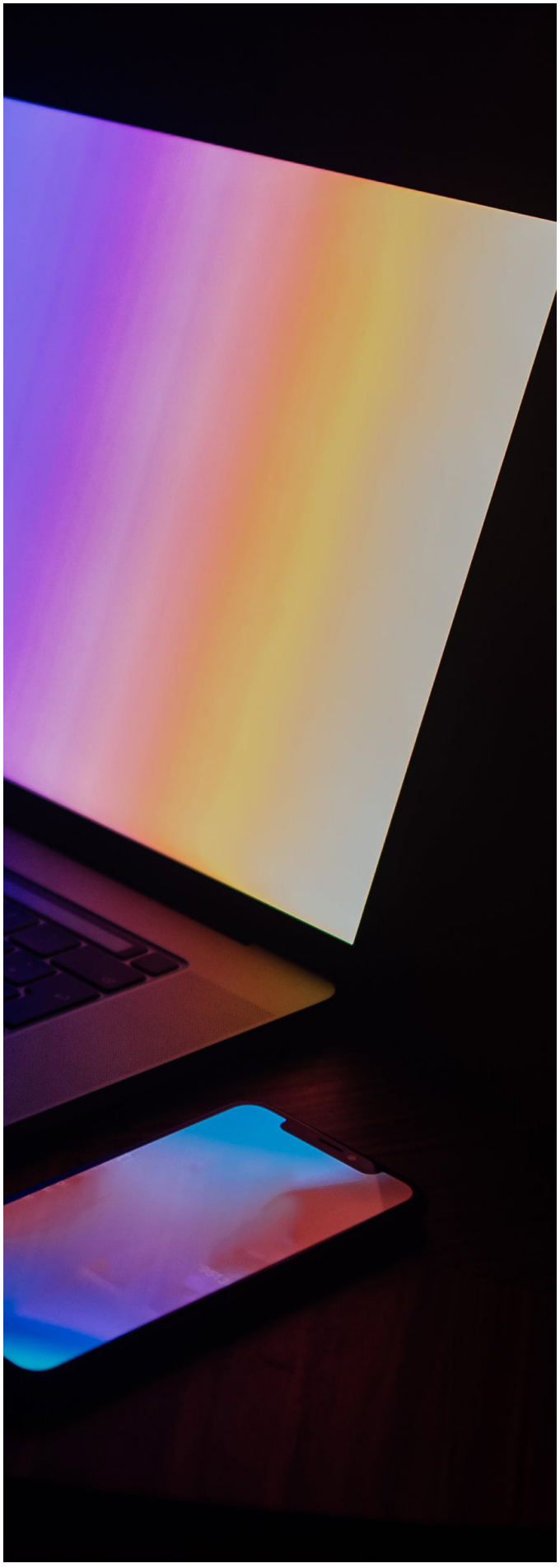
Step 1. Apply Robust Security Mechanisms

IT and security teams need to establish enforceable security policies based on a range of factors, including device configurations, system settings, applications, and the target locations of data submissions. These mechanisms should be aligned with industry best practices and standards, such as the National Institute of Standards and Technology (NIST) Mobile Device Security guidelines (NIST SP 1800-22)[4].

Here are some of the key capabilities required:

- **Test and vet applications.** Teams need to be able to apply security controls based on the security of apps installed on a device, whether those are personal or business applications. Security mechanisms must be able to detect applications that exhibit malicious behavior or zero-day exploits.
- **Validate user identities.** It is vital to leverage identity and access control mechanisms in ensuring only authorized users gain access to corporate systems and services. When risks are detected, mechanisms must be in place to block a users' access to corporate systems and data.
- **Verify that releases and patches are current.** Controls must be able to verify whether devices, OSs, and applications are running the latest patches and releases.
- **Employ traffic filtering.** Teams must be able to filter and block traffic, so they can guard against risky connections, such as access to suspicious ad networks or file transfers to an adversarial country.
- **Prevent phishing attempts.** Teams must have security mechanisms that can identify and thwart phishing tactics, such as text messages with malicious URLs.

4 | Quokka (then Kryptowire) participated in creating the NIST Special Publication 1800-22 and its insights and technologies were part of the example solutions used in the guide under the Cooperative Research and Development Agreement



Step 2. Ensure Privacy

IT and security teams must be able to establish mechanisms that deliver the above security capabilities, without enabling IT or anyone else to gain access to users' personal information or data. Given this, security mechanisms need to be applied without requiring full device control. These security mechanisms also shouldn't track user behavior, such as applications downloaded or browsing history.

Step 3. Maximize Ease of Use for the Workforce

To ensure security mechanisms are employed correctly and consistently, they need to be easy for the workforce to use. Any security mechanisms need to be easy to get started with and require minimal effort thereafter. Users should be able to easily download any security application to their device, enroll, and start using immediately. It is especially vital to ensure identity and access management (IAM) mechanisms are coordinated and streamlined, ensuring users don't have to go through cumbersome controls to verify their identity every time they want to log in to any given service or application.

Step 4. Minimize Cost and Administrative Overhead

To be viable for lean IT and security teams, security approaches must offer maximum efficiency from both a cost and administrative standpoint. Tools employed must be easy to integrate with existing infrastructure. In particular, it's vital to establish effective integrations with the organization's mechanisms for managing identities and permissions, such as IAM tools.

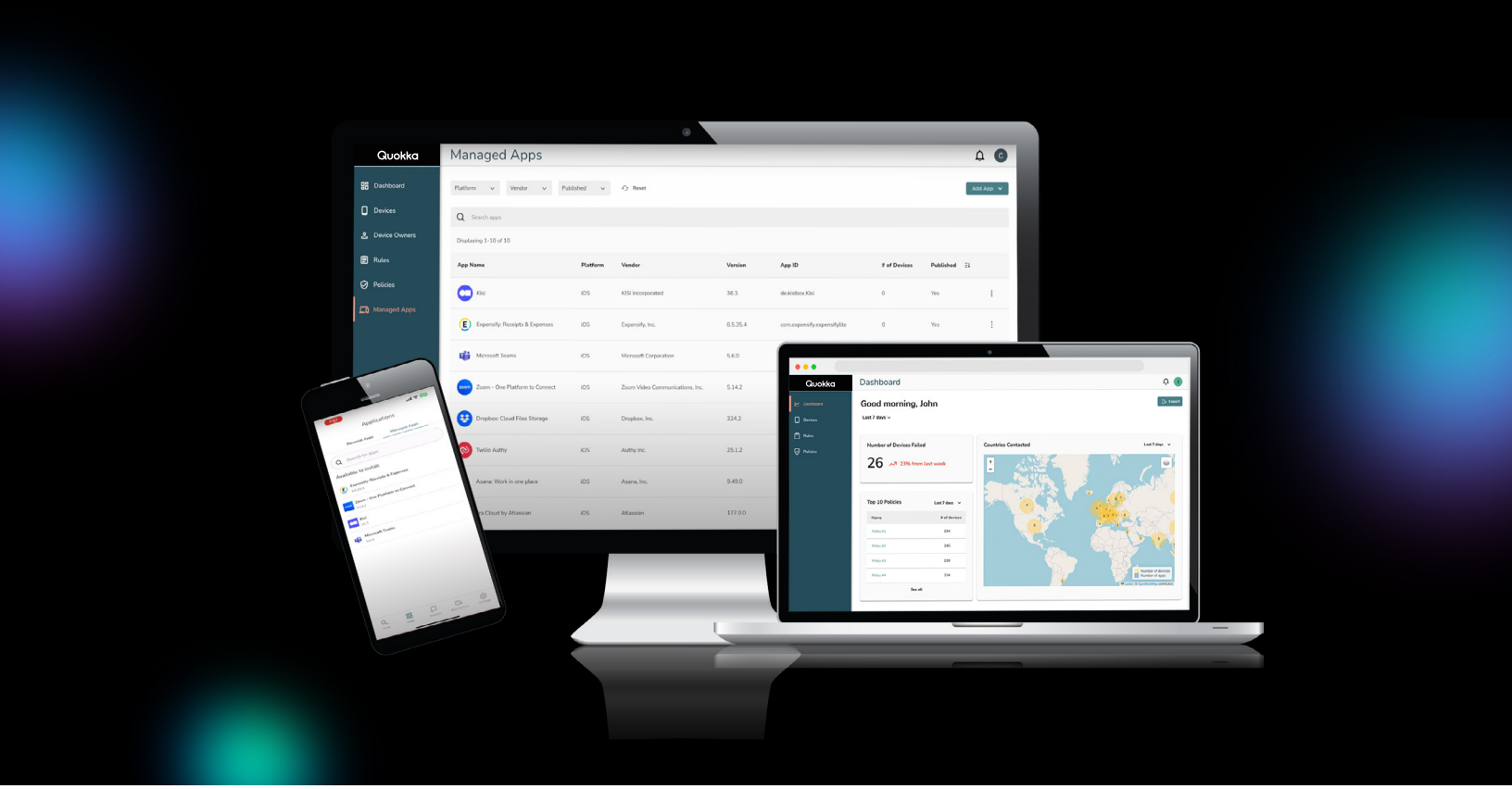
How Q-scout Delivers

6

To address the risks posed by BYOD, your IT and security teams need a privacy-first solution that provides robust mobile endpoint protection. Your teams need Quokka Q-scout.

Qscout

Q-scout is a mobile endpoint management solution that enables your organization to secure employee access to corporate networks, while safeguarding personal privacy. The solution features defense-grade application scanning engines, which are backed by expert research. The solution has been proven to uncover hundreds of zero-day vulnerabilities and threats. It is the only solution that can scan apps, network traffic, and system configurations in the context of each user's mobile device to enable threat detection and remediation. The solution features integration with Okta Verify, providing robust security, while maximizing ease and efficiency.



Key Capabilities

Q-scout offers these differentiated capabilities:

- **Robust security control.** Q-scout offers the controls needed to defend your business and workforce from the devastating effects of data breaches. The product ensures adherence to industry privacy standards, such as those from NIST. Q-scout features integration with Okta Verify. Through this integration, the solution supports a zero-trust approach, ensuring that, at every login, mobile devices and apps are in compliance with policies. The solution can identify and guard against a range of threats, such as submissions to risky locations, clicks on phishing links, and connections to suspicious ad networks.
- **Privacy.** Q-scout can determine if there is a risky device or malicious personal mobile app, without tracking or exposing any personal data of users. Consequently, the solution eliminates the legal liabilities associated with organizational access to employees' private data.
- **Ease of use.** Users can continue to work with their existing mobile devices, while maintaining privacy. The solution is easy to download and start using.
- **Minimizes cost and operational overhead.** Q-scout provides simplified security management, enabling IT teams to manage the security of an entire fleet of mobile devices from a single dashboard. Through Q-scout, administrators can manage access, enterprise apps, and security policies. The solution aggregates contextual mobile security intelligence from each worker's device, and delivers this intelligence to IT and security operators in a unified dashboard. Plus, through its integration with Okta Verify, Q-scout further streamlines upfront deployment and ongoing administration.

Quokka

Find Out More

Request a demo and see Q-scout for yourself. Discover how Q-scout helps you establish effective, efficient BYOD security.

About Quokka

Quokka protects mobile apps and devices used by millions globally. Formerly known as Kryptowire, the company was founded in 2011 with grants from DARPA and NIST, making Quokka the first and now longest-standing mobile app security solution for the US Federal Government. In over a decade since, defense-grade technology has enabled organizations from all sectors to deliver secure mobile apps to their customers and employees, while respecting privacy. With investment from USVP and Crosslink Capital, Quokka is bringing trusted mobile privacy and security to millions more.

www.quokka.io

Quokka