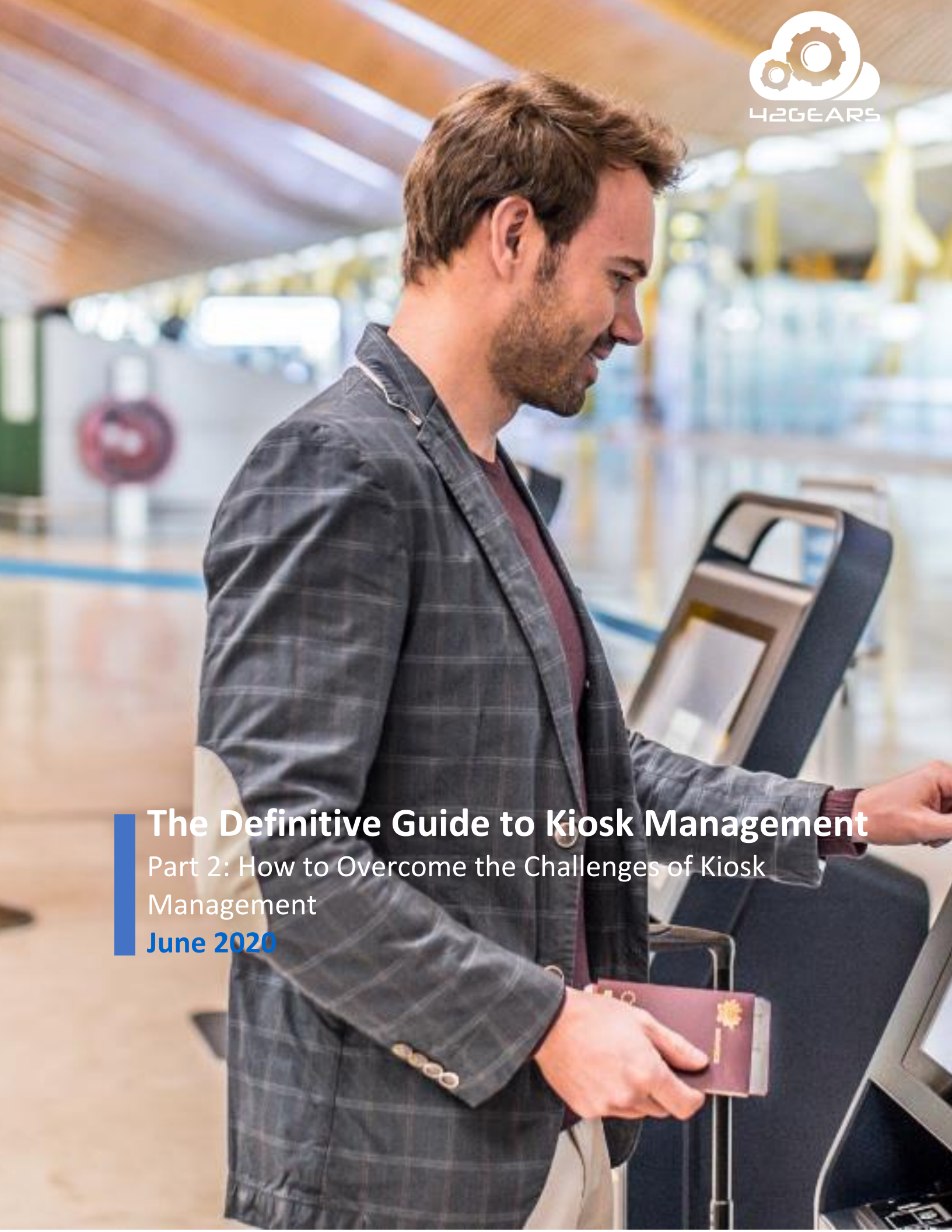

The Definitive Guide to Kiosk Management

Part 2: How to Overcome the Challenges of Kiosk Management

June 2020

Table of Content

Introduction

The Definitive Guide to Kiosks by 42Gears is a two-part series surveying the world of kiosks in the early 2020s. The first white paper of this series explored the ways that kiosks (and kiosk management) can elevate businesses through good interface design and connectivity with Internet of Things (IoT) devices. *Part 2: How to Overcome the Challenges of Kiosk Management*, covers a range of technical challenges and security threats that can make kiosk management difficult, and concludes by reviewing some important tools that make a substantial difference to kiosk owners and managers.

This white paper contains three sections:

Section 1. The Challenges Facing Kiosk Owners: Security

Section 2. The Tools Kiosk Owners Can Use to Overcome Challenges

Section 3. Moving Forward with SureMDM by 42Gears

Section 1. The Challenges Facing Kiosk Owners: Security and Logistics

No matter how well-designed a kiosk's interface might be, security breaches and technical issues will undermine the intended kiosk experience.

Given that kiosks are often placed in well-trafficked areas far from IT admins, they are an alluring target for malicious actors. The consequences of malicious kiosk tampering can range from public humiliation to severe financial hardship, so safeguarding these devices is essential.

Simple Oversights

Many kiosk owners likely focus on thwarting advanced threats, but great harm can be caused by simple oversights that go unnoticed while setting up a kiosk interface. Manipulating kiosks doesn't require hacking skills if kiosks have obvious exploits in their user interfaces.

As an example, *McDonald's kiosks experienced an embarrassing compromise in the late 2010's when Australian teenagers exploited an oversight in the ordering process[1]. If someone ordered a certain item and then removed a certain component from the item, the kiosk would deduct more from the overall order cost than the item was worth. Although quickly patched, the exploit briefly allowed users to get unlimited free food with patience.*

This goes to show that complex and well-thought-out plans to keep devices safe cannot lose sight of the most basic security features.

Complex Security Threats

Kiosk threats come in many forms- and resolving simple oversights isn't nearly enough to protect your business from them.

Bernard Parsons, CEO of the security firm Becrypt, divides kiosk security threats into three kinds: Threats to system integrity, threats to system availability, and threats to system confidentiality[2]. Let's look at each of Parsons' categories in sequence.

Threats to System Integrity

Threats to system integrity are those that involve changing whatever the kiosk displays or does. Juvenile though it may seem, some individuals want to display humiliating or off-topic content (most stereotypically, pornography) on kiosks as a creative exercise- just to see what they can accomplish[3].

Kiosks worldwide have fallen victim to this sort of compromise often, forcing companies to do damage control when the content displayed is intensely off-brand. Although any type of device hacking could pose this kind of threat, a common target is a kiosk's internet browser.

Organizations that set up Internet-enabled kiosks must operate on the assumption that users will access explicit content unless restricted from doing so, regardless of where the kiosk is installed. New York's LinkNYC Wi-Fi kiosks in the mid-2010's exemplify this challenge. These giant kiosks were intended to help New Yorkers of all socioeconomic backgrounds use the Internet, but some

1 https://www.delish.com/food-news/a27091162/mcdonalds-kiosks-free-burger-hack/

2 https://securityboulevard.com/2020/01/securing-interactive-kiosks-iots-with-the-paradox-os/

3 https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-tottenkoph-rev-philosopher.pdf

users quickly commandeered the devices to stream pornography on the giant kiosk screens in the middle of the street.

In order to allow browsing without the risk of showing indecent content, kiosks can employ keyword filtering measures- but even this may not be sufficient, as LinkNYC discovered when it later implemented keyword filtering into its kiosks' browser[4]. A truly secure and safe web kiosk needs to be able to restrict access to just one or a few specific websites.

Many operating systems and services purport to offer "kiosk mode," which restricts devices to specific applications, but kiosk mode needs to withstand common forms of tampering. Writing for the website *IoTforAll*[5], Yiteak Hwang notes that some of these forms of tampering include abusing external links (users will try to access restricted apps by finding links to them in approved apps), touch fuzzing (erratically tapping the screen to exploit the kiosk's way of handling invalid inputs), and data fuzzing (entering invalid data into forms, and exploiting the resulting error message to gain access to other parts of the device).

Threats to System Availability

While threats to system integrity force kiosks to display unwanted content, threats to system availability result in kiosks displaying no content at all. This includes anything that would cause a device to crash, either intentionally or unintentionally. Kiosks that shut down at inopportune times can bring business to a halt- and the more important a kiosk is to the flow of customers, the more damaging the crash.

If kiosks display error messages and their owners need hours to repair them, it reflects poorly on the company. Threats to system availability can come in many forms, but having a way to quickly resolve them after-the-fact is useful no matter the nature of the threat.

Threats to System Confidentiality

When kiosk owners think of security threats, they likely think of threats to system confidentiality- those threats that do not outwardly impair kiosk functionality, but instead relay sensitive data to

4 https://www.vice.com/en_us/article/aek4xb/linknyc-free-public-wifi-removes-browser

5 https://www.iotforall.com/smart-city-security/

a third party. This kind of threat can result in companies losing the trust of their customers, impacting their financial bottom line for years to come.

Threats to system confidentiality can begin as oversights in the way that different system components work together, or they can begin as outright hacking.

In 2019, security experts working for IBM's X-Force Red team discovered vulnerabilities in tablets that ran visitor manager software at major companies. Specifically, some applications had admin privileges over devices, so malicious actors could exploit those privileges to obtain visitor records and other confidential information[6]. This could even potentially be used to print out ID passes with false credentials.

Another victim of this kind of threat is the kiosk company Uniguest[7]. Uniguest had inadvertently made a web page with development tools for its software available publicly. This allowed researchers to manipulate the system in ways that could expose all private information (including passwords, data, and much more) from every customer of Uniguest.

Even if all liabilities of this nature are resolved, malware can invade and devastate kiosks- and the companies that own and run them. For example, a malware attack on kiosks of the food self-service provider Avanti Markets exposed an unspecified number of customers' names, email addresses, and fingerprint data at risk[8].

In order to combat threats to system confidentiality, kiosk owners need to have a coherent approach to managing the kiosks and the apps and content on those kiosks. By using comprehensive software to manage each of these elements, oversights become less likely. Additionally, kiosks need to have some form of mobile threat defense (MTD)- as otherwise, they could be sitting ducks for malware.

6 https://securityintelligence.com/stranger-danger-x-force-red-finds-19-vulnerabilities-in-visitor-management-systems/

7 https://www.securityweek.com/widely-used-kiosks-compromised-hardcoded-credentials

8 https://threatpost.com/micro-market-vendor-warns-of-bankcard-and-biometric-data-breach/126742/

Section 2. The Tools Kiosk Owners Can Use to Overcome Challenges

If you are in the market for kiosks, you should be aware of the various benefits and concerns inherent to your potential purchase options. In this section, we will briefly consider the differences between kiosk choices and what features all kiosks share.

Common Kiosk Choices

Apple (iPadOS) device

Many business owners turn to Apple (specifically, Apple's iPad tablets) when implementing kiosks. In both consumer and enterprise contexts[9], Apple devices enjoy a reputation for strong quality and aesthetic design. Apple offers Apple Business Manager (ABM) for its devices, which allows businesses to quickly enroll devices and distribute application licenses to each device.

In regards to kiosk lockdown, iPad owners can use iPad guided access[10] to keep iPads safe- but this requires continual monitoring by the device owner and is not feasible in a setting with a large crowd flow and a large number of devices. Apple Business Manager enables businesses to run Single App Mode on iPads remotely, which makes using iPads as kiosks much more feasible in commercial contexts.

Businesses can gain further kiosk functionality on iPads if they use a mobile device management solution in conjunction with ABM.

Android devices

Android devices may not enjoy the same brand recognition as the iPad, but these devices come with a range of upsides. They typically cost much less than comparable iPads, and can include an array of custom hardware extensions (such as barcode scanners) and form factors (such as rugged casings) for a variety of needs. Android also offers Android Enterprise, which serves a similar purpose to ABM.

9 https://www.linkedin.com/pulse/choosing-right-device-your-mobility-deployment-prakash-gupta/

10 https://www.42gears.com/blog/how-to-use-guided-access-on-iphone-and-ipad/

The Android analogue to iPad's guided access is Android screen pinning[11], but like guided access, this requires continual physical interaction with the device and is not reasonable for multi-device deployments. Kiosk owners will need to use an MDM solution to remotely lock down devices into kiosk mode.

Windows devices

Windows tablets are a good choice for organizations that would like to provide professional functionality on kiosks (such as full keyboard functionality for kiosks deployed in human resources departments). Additionally, given that many organizations already use an array of Windows devices, IT teams may be familiar with Windows and find it easy to integrate Windows tablets. Kiosk owners may also already have licenses for Windows applications that they can carry over to Windows kiosks.

Windows kiosks offer built-in lockdown solutions if kiosk owners are willing to manually regulate every device, but this is not oriented towards enterprise deployments. As with Android, Windows kiosks rely on the help of mobile device management solutions to deploy kiosk lockdown solutions on many devices at once[12].

Different kiosk attributes

Apps

For users without the technical know-how or persistence necessary to hijack devices, a kiosk's functionality depends solely on what applications are available. For kiosks that constrain users to a single app, optimizing the in-app experience is all that matters. For kiosks that allow users to switch between multiple apps, owners must optimize both the available apps and the interface used to navigate between them.

If you choose to employ an off-the-shelf device, preparing an appealing kiosk interface requires more than just disabling access to off-topic apps. If you need an interface to navigate between apps, that interface needs to be restricted in the same way you restrict the available apps. Additional modifications may also be necessary; for example, if you would like to disable the

11 https://www.42gears.com/blog/android-screen-pinning-turning-consumer-devices-into-single-purpose-tools/

12 https://docs.microsoft.com/en-us/windows/configuration/kiosk-single-app

ability to press a “back” button, you should remove any interface elements indicating the user can go “back” to begin with. If the menu interface doesn’t work properly, or it’s obvious that elements are missing, then the user won’t see the experience as natural.

Because the user’s experience is determined strongly by what apps are available. It should go without saying that you need to be able to restrict users to certain apps- but all of the design challenges mentioned above still apply. If the menu interface doesn’t work properly, or it’s obvious that elements are missing, then the user won’t see the experience as natural.

Browsers

Kiosks that serve limited purposes can likely restrict functionality to a single app, or a couple of apps. But for kiosks that need to answer open-ended questions, including an Internet browser is probably necessary.

Still, as with the LinkNYC example mentioned in Section 1, the open-ended nature of the Internet is as much a hindrance as it is a tool. A few strategies can help to restrict user activity to safe websites and topics, without restricting them from accessing what they need.

One such tool is the ability to lock browsers down to a single web page. Although at odds with open-ended inquiry, locking down a browser is a way to guarantee that users cannot visit inappropriate websites.

Another common strategy is permitting access only to certain websites (i.e. whitelisting). Whitelisting can provide a more open experience than single-page lockdown, while still making off-topic browsing difficult.

Alternately, browser admins can block access to specific websites (i.e. blacklisting). While it is difficult to anticipate and blacklist every undesirable website, kiosk owners can use blacklisting to block some of the most common problematic websites that kiosk users may try to visit.

For kiosk owners who like to have the kiosk experience be as open-ended as possible, keyword filtering may be a good option. Keyword filtering dynamically screens websites based on their content, so even if users find ways to undesirable websites you have never blacklisted, access will be denied.

Keys and keyboards (both physical and digital)

Kiosk owners need to put thought into how they structure the on-screen experience, but they cannot forget about the buttons of the devices they use as kiosks.

Without proper protection, a user could use the physical keys of some devices to navigate away from the kiosk's intended functionality. Whatever mobile device solution you choose needs to have a way to deactivate hardware keys.

Whether virtual or physical, keyboards can also pose a challenge for kiosks and kiosk owners. If kiosk users fill out forms using non-standard characters (such as emojis), this could result in text that the device cannot parse. For this reason, it's necessary to have a way to restrict keyboard inputs to only alphanumeric (i.e. a-z, 0-9) characters.

Section 3. The Next Step: SureMDM by 42Gears

In this final section, we'll look at how to overcome the challenges mentioned thus far, and how to put yourself in the best position for whatever comes next in the kiosk industry.

The best way to get started with kiosk ownership (or improve your ability to manage kiosks you already own) is to use SureMDM, 42Gears' flagship software. In designing SureMDM, 42Gears has taken into account all of the needs, challenges, trends, and liabilities explored throughout both white papers in this series. Using SureMDM, you can easily deploy and manage professional-looking kiosks using off-the-shelf Windows, Android, and Apple devices. You can optimize the tools discussed in Section 2 of this white paper to optimally address the challenges explored in Section 1.

What is SureMDM?

As introduced in the first white paper of this series, SureMDM is a unified endpoint management solution. It can secure a wide range of devices, including kiosks, from a central console. This means that enterprises can set up and troubleshoot kiosks with the same framework they employ for other devices, streamlining the device management process.

Managing kiosks with SureMDM requires downloading an app (also known as an "agent") on a kiosk; from there, admins can remotely monitor, manage, and secure the kiosk. Kiosk managers

can quickly find an array of information on the central console, including battery level and other key indices of device health. SureMDM's Remote Control lets admins repair kiosks remotely, reducing the need for travel to the actual kiosk.

SureMDM's Sister Software: SureLock, SureFox, and SureVideo

SureMDM licenses also provide enterprises with three additional products that extend SureMDM's functionality.

SureLock is a world-class lockdown solution that allows you to lock devices down to just one app, or a few apps. You can go further to fully customize what interface elements appear on screen, and include company logos in the interface.

SureFox is a secure stand-alone browser that lets you offer Internet-connected kiosks without compromising security. You can restrict access to specific websites, block access to specific websites, filter by keyword, or restrict devices to a single Internet page.

SureVideo is 42Gears' tool for non-interactive digital signage, allowing you to play videos in a loop on digital signs without the risk of bystanders interrupting the video playback.

How SureMDM Addresses Common Kiosk Challenges and Threats

Avoiding Simple Logistical Oversights

As discussed in Section 1, small oversights in the way you provide users with features can result in costly or embarrassing exploits. This is especially concerning when it allows users without any technical knowledge to exploit kiosks for enjoyment or profit.

Knowing your kiosks thoroughly is essential, but asking any one person to comb over everything to catch small errors is a daunting task. 42Gears provides extensive customer support from Day 1 with a dedicated Welcome Team. The Welcome team sends each new customer a list of questions tailored to their specific needs, which makes it easy for new kiosk owners to identify the chain of actions that will let them set up devices and avoid oversights.

42Gears offers continual assistance through its managed mobility services partners[13], third-party tech experts who have been trained by 42Gears to be experts at using 42Gears' software. These

13 https://www.42gears.com/blog/how-managed-services-make-device-management-easy/

partners can perform extensive testing, help your troubleshoot devices, and ensure you best practices during set-up, with the same degree of knowledge and professionalism you would expect from 42Gears itself. Depending on the industry, this may involve services like ensuring that data from HR kiosks is securely relayed to the appropriate administrator, or interacting with kiosk interfaces in every possible way to see how the kiosk handles error notifications,

Threats to System Integrity

Threats to system integrity are those that result in kiosks providing functionality you do not wish for them to provide. SureMDM and its sister products are well-equipped to keep devices working as you intend them to be used, even when kiosks feature Internet connectivity.

SureLock keeps users from accessing apps that you do not want them to access on Android and Windows devices. SureLock also safeguards against strange touchscreen behavior designed to trigger error messages, including data fuzzing, touch fuzzing, and exploiting external links. You can also analyze SureLock's usage data to see how users interact with kiosks, and identify any suspicious kiosk activity.

When users use kiosks to head online, you can require users to browse using SureFox for maximum security. In addition to being a secure and encrypted browser, SureFox features essential whitelisting and blacklisting tools, as well as keyword filtering. As with SureLock, you can analyze SureFox's usage data to make sure that your restrictions are effective.

SureVideo lets you keep digital signs safe by playing a looping video playlist of your choice, and making interruption impossible without the proper password. In this way, SureVideo protects signage from strange touchscreen activity, just like SureLock does with interactive kiosks.

If a kiosk were to display unwanted content, admins could shut down or restart the kiosk to begin displaying their content once again.

Threats to System Functionality

Threats to system functionality are those that result in kiosks ceasing function- whether this means freezing, generating error messages (including Windows' dreaded "blue screen of death"), or simply going dark entirely.

Using the SureMDM central console, admins can identify potential indicators of poor device health (such as short battery life) and perform maintenance on devices before they stop working. If devices do malfunction, admins can resolve issues quickly with Remote Control, viewing kiosk screens and controlling kiosks remotely.

SureMDM helps facilitate troubleshooting by ensuring that every kiosk you own has the same operating system version, apps, and app versions installed. If IT admins do need to troubleshoot kiosks, they already know what they are working with, as each kiosk is consistent. On Windows kiosks that have Intel vPro™ AMT technology, SureMDM can remotely power devices on or off at any time, and even maintain control of devices on the BIOS level.

Threats to System Confidentiality

Threats to system confidentiality are those that relay kiosk data to a third party for malicious purposes. SureMDM provides you with an array of safeguards to prevent these threats from emerging and, if they do emerge, neutralizing them right away.

In order to provide the most secure experience possible, 42Gears has partnered with the firm Pradeo. SureMDM provides customers with the option to harness Pradeo's mobile threat defense (MTD) technology. With Pradeo's help, SureMDM can analyze code, identify suspicious network connections, and even track usage patterns to find abnormalities.

Internally, 42Gears is dedicated to keeping kiosk data safe; the organization recently received the international ISO/IEC 27001:2013 designation, reflecting a combination of best practices in data protection, personnel training, and risk management.

Conclusion

Kiosks can make ordinary transactions and processes faster, more engaging, and more likely to result in larger purchases. The range of technologies with which kiosks can interact means that clever kiosk managers can get more out of kiosks than ever before.

Kiosks also face a wider range of potential threats than ever before. Kiosks can display undesirable content, stop working, or maintain the appearance of normalcy while exposing data. If users cannot trust kiosks to be secure, kiosks become an impediment to success, rather than a catalyst.

The suite of software that 42Gears offers puts kiosk managers in the best possible position to succeed. IT admins can manage, secure, and troubleshoot kiosks remotely with SureMDM, restrict kiosk functionality with SureLock, and provide a controlled Internet-browsing experience with SureFox. Plus, admins can secure non-interactive digital signage with SureVideo.

Beginning the process of using SureMDM with kiosks is simple and risk-free. You can try the software free-of-charge before committing to the license. For more information, please visit this link.