# Protecting Android Point-of-Sale (PoS) Devices with 42Gears UEM

**September 2019**

www.42gears.com

# Overview

The adoption of Android-based **Point-of-Sale (PoS)** devices across industries is on the rise due to the numerous advantages they have over manual or legacy systems, such as cost-effectiveness, easy software updates, better security, manageability, portability, better integration with third-party software and more. These PoS devices feed data to central systems, which in turn provide a good overview of the business and keep a record of the financial status, inventory, sales and automate multiple tasks, saving businesses a lot of time and effort, while reducing errors.

However, these Android-based PoS devices are also creating a precarious environment for enterprises as they hold so much sensitive information, such as details pertaining to revenue and sales. There is also the question of securing customer information provided at the time of swiping credit or debit cards as PoS machines/devices keep saving those details. The security of PoS terminals should not be overlooked as the financial losses caused by personal data breach can be significant.

*According to the latest IBM data breach report, the global average cost of a data breach is **$3.26 million** in **2019** - Up **6.4 %** from **2017**. The average cost for each lost or stolen record containing sensitive and confidential information is **$144**.*

Additionally, selling credit card information in the black market has become a lucrative business for attackers these days. That is why these PoS devices, terminals, PoS environments, kiosks have become vulnerable and can cause a serious threat for enterprises. To combat these cyberattacks, businesses require to harden the PoS environment.

# PoS threats and its solutions provided by 42Gears

In addition to endpoint PoS devices the PoS infrastructure also includes network servers, desktops, kiosks and more. Since attackers use multiple methodologies for targeting the various levels, 42Gears has protection layers at each level. Let’s explore the various PoS threats and security measures before we move forward to take a look at how 42Gears protects PoS systems:

## Malware Attacks

Malware attacks are mostly used by cyber criminals to gain access to a network. Attackers can do this in different ways, such as by sending a spear-phishing email, or using an SQL injection on a web server, or looking for a peripheral device that uses a default password. Once they get into the network, they try to capture the admin credentials to gain system access. Later, they install RAM scraping malware or network sniffing tools to capture the personal information of customers. After collecting the credit card information in the staging server, they look for some compromised FTP servers or web hosts that have legitimate external access. So that, they can exfiltrate data from the server back to cybercriminals.

### Solutions to malware attacks

As these attacks may happen in three stages - infiltration, data capture and exfiltration, 42Gears follows security measures at all these stages. To prevent threats from entering the environment, admins can set up policies in **42Gears UEM**, such as **block all new applications from installing** and only allow app installation via UEM. This helps prevent installation of malicious apps right at the first level.

The next level is data capture, where attackers somehow manage to install the app and try to run an application to capture data. In 42Gears UEM, admin can set up kiosk policies that prevent anyone from accessing and launching any unauthorized apps on device. If it doesn't run, it can't capture the data. For an additional layer of security, we have **Mobile Threat Defense (MTD)** scanning, which keeps scanning devices to detect threats and send alerts to admins for remedial actions. We have partnered with **Pradeo** to provide enterprises full-fledged data security.

At last, we also have Firewall policy against exfiltration. 42Gears uses application level firewall that ensures only authorized data can go out from the PoS endpoint. The firewall defines which apps on **PoS systems can communicate on the network and what they can communicate with**.

## Physical attack on PoS devices

### Theft

It is difficult for I&O pros to track the numerous PoS devices that are installed and operated everywhere in enterprises. They can be stolen by employees or outsiders. As these devices hold customers' personal information, the physical security of these devices is very important. By stealing these devices, attackers may get the admin credentials or be able to access the data saved in the device.

### Solutions to physical attacks

After stealing the PoS device, attackers may try to get the password or get a hard drive and connect it to some other device to read the data or try to operate the device in safe mode. We prevent all such possibilities by using strong password policies. Also, we encrypt the data at rest, which reduces the risk of data leakage through hard drive. Lastly, we can **disable the Safe Mode** through 42Gears UEM to prevent attackers to run the device in Safe Mode.

## Unauthorized access to PoS

Another way through which PoS devices can get compromised is through the use of USB ports or SD cards. Some disgruntled employee(s) or outsider(s) may plug an external drive into the device through which they can transfer the data to attackers.

### Solutions to prevent unauthorized access

42Gears helps in preventing unauthorized access to PoS via external disks such as USB ports or SD cards. We can **block/disable USB ports or SD cards** through 42Gears UEM.

## Hardening 42Gears UEM backend system

Above mentioned security measures are followed to safeguard PoS terminals against attacks. However, to ensure the security of our customers' data, we harden our backend system as well. Mentioned below are some security measures followed by us:

### Two factor authentication

Customers' data security is our priority. The admin's machine can accidentally or intentionally be used by someone. 42Gears UEM integrates with well-known IdPs like **OneLogin**, **Okta**, **ADFS**, to support 2-factor authentication to log into our console. This is particularly important for companies requiring PCI DSS compliance.

### Data security and encryption

### Device side data security

No card-related data is captured, transmitted or stored in 42Gears servers. Device management related device properties are exchanged with UEM server as per administrator set policies. This data is encrypted both at rest as well as in motion. SSL is used for communication. Data at rest is encrypted using disk encryption and database encryption.

### Server security

42Gears hosts its server on the secure and robust platform provided by **AWS**. Industry standard DLP policies and methods are followed in our infrastructure hosted on AWS.

# Summary

**42Gears** provides comprehensive security for your Android PoS systems and environments through a robust and reliable UEM solution. It helps organizations safeguard PoS terminals and devices by offering application control and system hardening. Further, the solution can block network-based attacks using app level firewall. 42Gears also offers MTD to provide an additional layer of defense. To secure data/device from getting lost or stolen, 42Gears also has Data Loss Prevention (DLP) policies in place.