proofpoint

Containerization and App Reputation

Containerization alone cannot defend against dangerous and malicious apps

While containerization of mobile apps offers a needed layer of protection, the technology itself is not a sufficient defense against the threat of malicious or dangerous Android and iOS apps.

As Gartner reported, "Through 2017, seventy-five percent of all mobile security breaches will be through apps, not through deep technical attacks on the OS."

According to leading enterprise mobile management (EMM) vendors, such as MobileIron and AirWatch, containerization should be used as part of a layered defense that also includes device management, containerization, and app threat prevention.

With the mounting risks of malicious and dangerous apps to enterprise mobile security, less than 10 percent of all government agencies and corporations employ all three of these safeguards.

What is a secure container?

A secure data container is a third-party mobile application that is used to separate and secure a portion of a device's storage from the rest of the device. The goal of containerization is to isolate an application to prevent malware, intruders, system resources or other applications from interacting with the application – and any of its sensitive information — secured by the container. Using a secure container is also sometimes referred to as sandboxing.

Some devices offer native device security, but their effectiveness varies. Container applications are available on Android, iOS, BlackBerry and Windows Phone operating systems from enterprise mobile management solution vendors like MobileIron, AirWatch, Good Technology, and BlackBerry.

The myth about containerization on a BYOD device

There's a mistaken belief that apps outside the container will not pose a threat in an enterprise BYOD environment. This position overlooks the fact that many mobile risks relate to the access devices have to corporate networks and the theft of credentials to internal resources. As a result, containers are only a partial solution.

In other words, if malicious or dangerous apps reside outside the container on a BYOD device and connect to a corporate network, internal WiFi, or VPN, you may have just invited the enemy into your network.

Let's take a closer look at several scenarios.

1. Network profiling apps

A conscientious Android user decides to improve the security of their BYOD device, and downloads a "security app" from a legitimate marketplace that was developed by a Chinese publisher. Once the user brings the device to the office, the new app monitors the device for network connectivity and profiles the network, sending that data to servers in China. This user is unwittingly enabling the mapping of the corporate network, which can be used by attackers. These types of apps must not be allowed inside a corporate network.

Non-containerized apps that profile a corporate network may also send data to sites that do not have an agreement with your company. These sites can sell your data and have no obligation to notify your company.

2. VPN hijacking apps

If a dangerous or malicious, non-containerized app shares the same VPN connection used by containerized apps on the device, it's possible for the bad app to mine data, access internal resources, or scan the corporate network.

In short, the app creates a back door into the network for attackers.

3. Data mining apps

Employees may object to using two different calendaring apps (one containerized, the other built-in to the device), so IT offers connectivity to the corporate calendar from non-containerized apps. An employee brings to work a device with an app that mines their calendar and communicates that data to servers over the Internet. If the employee works at a company targeted by hackers that data may be used to mount spear-phishing attacks, obtain employees' email addresses, stealing corporate conference call numbers and PINs, and when executives travel. This scenario can also include corporate address books.

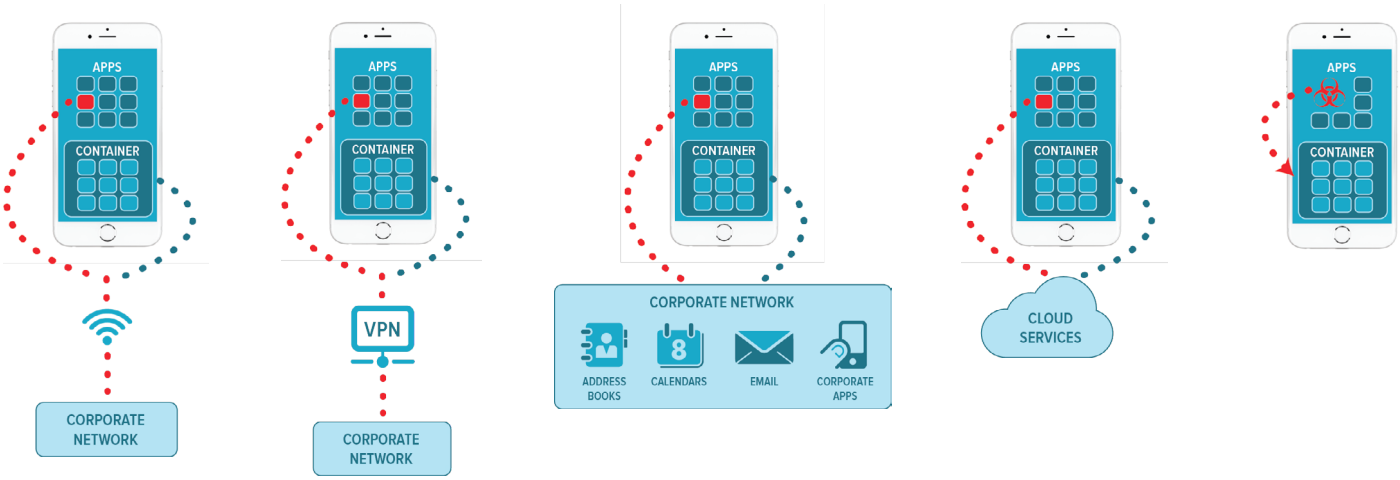
4. Cloud accessing apps

Non-containerized apps may gain access to the same cloud services of containerized apps through credential sharing, key rings or app-phishing on the device.

Containers only protect the flow of data to cloud services from those apps that are containerized. If a malicious or dangerous app outside the container accesses the same cloud service where data from containerized apps is stored, attackers could gain access to corporate data.

5. Container busting apps

A teenaged child jailbreaks or roots Mom's tablet over the weekend to download a free version of a cool game. They then un-jailbreak or un-root the tablet. Later Mom brings her tablet to work and connects to the internal WiFi. While Mom is taking notes on her tablet during a team meeting, the Trojanized game may communicate with a command and control server over the Internet, informing the server which network she is on. The command and control server then instructs the Trojanized game app to serve as a Remote Access Trojan, allowing attackers access into the corporate network. Similarly, containers may be broken by malware that roots or jailbreaks a device.



Mobile app containers are an important defense but not sufficient by themselves

Mobile app containers cannot protect against all app threats. IT may or may not be able to place certain apps in a container. Other types of containers can only house media pushed by IT onto the devices, but not the files users create on their own devices. Other kinds of container software protect email and attachments, but not other files.

Mobile software containers can only be part of a much broader mobile security strategy that includes a dynamic app reputation service that analyzes each app outside the container. TAP Mobile Defense by Proofpoint provides enterprises with comprehensive protection and visibility against malicious and privacy-leaking iOS and Android apps which frequently lead to advanced persistent threats (APTs), spear phishing attacks on employees, and leaked corporate data.

The TAP Mobile Defense service works in conjunction with enterprise mobile management solutions, such as AirWatch and MobileIron, to provide dynamic app threat detection and protection.

Proofpoint's app analysis engine powers TAP Mobile Defense. Proofpoint's team of analysts, cryptographers and cybercrime specialists have analyzed more than 3 million free and paid iOS and Android apps from more than 650,000 publishers. Each app is scored against more than 1,000 potentially malicious and privacy-leaking behaviors to determine whether it is risky or safe.

About Proofpoint

Proofpoint Inc. (NASDAQ:PFPT) is a leading security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving & governance, and secure communications. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against phishing, malware and spam, safeguard privacy, encrypt sensitive information, and archive and govern messages and critical enterprise information.

892 Ross Drive
Sunnyvale, CA 94089

1.408.517.4710
www.proofpoint.com