Briefing Note

Understanding alternative approaches to device security

Introduction

Threats against mobile devices are increasing. The risk to organizations that sensitive information will be stolen is rising. Cyber-attackers are using advanced mobile malware and social engineering to compromise the security of devices.

Today, organizations are looking for cyber-security products to protect their employees against these threats and the market for such products is evolving rapidly. The first generation of suppliers have mostly focused on "Mobile Threat Defense" solutions, which aim to catalogue the vulnerabilities of your mobile devices. For example, they will report devices needing operating system upgrades.

More recently however, a new approach has been gaining traction. Rather than just provide visibility of risks this new approach pro-actively protects against them, acting as a firewall between malicious actors and your mobile device. This short briefing note reviews the two approaches to help you identify which is most suitable for your organization.

Mobile Threat Defense (MTD)

MTD solutions catalogue information about devices across a range of vectors: device configuration, apps, and networks. Information is collected about the operating system version running on the device, the device file system, the permissions which apps use, and the Wi-Fi networks to which the device connects, together with a host of other indicators. IT security analysts can then use this information to make decisions about whether to allow a device access to business applications. Therefore, a device which has significant risks, e.g. jailbroken, can be denied access to organizational information. To do this the MTD relies on integration with the organization's Mobile Device Management system, e.g. Intune, MobileIron, Airwatch, MaaS360.

Challenges

MTD solutions excel at providing visibility of device security risks which were previously invisible to IT security teams. However they have a number of challenges:

- Apple and Google severely restrict the information that MTD solutions can access. This means that their ability to detect security compromises is very limited. For example, MTD solutions were unable to detect the WhatsApp vulnerability which allowed the Pegasus spyware to be installed.
- MTD solutions have been most successful in organizations with large IT security teams who have analysts who are able to 'digest' the information they provide, wade through false positives, and zoom in on the critical risks.
- MTD solutions do not provide effective anti-phishing protection. Phishing is currently the most widespread mobile threat.
- To work effectively MTD solutions require integration with an MDM solution. This makes set-up more complex and time consuming.

A new approach

Recognizing the limitations of traditional MTD solutions, Corrata has pioneered a new approach to mobile device security. Corrata doesn't just collect information about device security risks: it provides protection to prevent these risks from resulting in harm.

Corrata provides protection by acting as an enterprise firewall on each individual device. It examines all incoming and outgoing traffic and blocks connections to malicious internet hosts. This protects against phishing by blocking all access to phishing sites, while the risk of mobile malware infection is combated by blocking access to malware download sites. Malware which has been installed on the device is disabled by blocking communications with its Command and Control servers. Corrata's solution can detect attacks such as the WhatsApp Pegasus infection because it can see the traffic generated by the malware.

Key takeaways:

- Corrata acts to automatically block threats without the need for security analyst involvement. This makes it suitable for organizations of all sizes.
- Corrata works effectively with or without integration with an MDM solution and is simple to deploy and manage.
- Corrata can also provide benefits beyond security: it can be used to control mobile data usage and to enforce acceptable use policies, i.e. by acting as a content filter.