Lookout

WHITEPAPER

4 mobile security insights for CISOs

Recommendations from Gartner to prepare for strategic conversations with the CEO and board

Executive summary: where the mobile security market is now

Mobile devices have rapidly become ground zero for a wide spectrum of risk that includes malicious targeted attacks on devices and network connections, a range of malware families, non-compliant apps that leak data, and vulnerabilities in device operating systems or apps.

Read the four mobile security insights CISOs must know to prepare for a strategic conversation with the CEO and board about reducing mobile risks and the business value associated with fast remediation of mobile security incidents.

INSIGHT 1

Secure your mobile ecosystem now

Just as the PC radically changed the way we operate as a society, now it's mobile that's transformed our lives and work. This change from PC to mobile has created a perfect storm – mobile devices with increasing amounts of sensitive data operating in an ecosystem where malicious code, malicious networks, and compromised operating systems are proliferating wildly.

Enterprise security leaders must be able to prevent, detect, and respond to the full range of risks they face from the mobile ecosystem, however; most enterprises currently have zero visibility into the mobile risks they face.

> "Security and Risk managers responsible for endpoint and mobile security must start now to evaluate Mobile Threat Defense (MTD) tools, and gradually implement these solutions in complement to EMM.[1]"
>
> **Gartner Predicts 2017: Endpoint and Mobile Security**

INSIGHT 2

Enterprises are facing a range of mobile risks rapidly increasing in sophistication

As employees access more and more data while on-the-go, the range of mobile risks has expanded from malware to include targeted attacks such as Pegasus and man-in-the-middle, vulnerabilities such as DirtyCow and Drammer, and data leaking apps.

Enterprise security leaders now need to be able to map the likelihood and impact of each different mobile risk for their organization in order to get an accurate picture of their mobile risk profile.

> "Mobile attacks (Pegasus, XcodeGhost) and vulnerabilities (Stagefright, Heartbleed) are increasing in terms of both number and pragmatism.[2]"
>
> **Gartner Predicts 2017: Endpoint and Mobile Security**

INSIGHT 3

Integrate enterprise mobility management and mobile threat defense to achieve security and enable productivity

For security organizations that have already deployed an enterprise mobility management (EMM) solution, Gartner offers initial recommendations for the next steps in securing mobility.

This key insight suggests enterprises integrate an MTD solution with EMM because, "EMM solutions have limitations in that they are unable to detect platform and app vulnerabilities. They are also limited in their capacity to detect malware threats on their own. Mobile threat defense (MTD) tools help to fill this void by protecting enterprises from threats on mobile platforms.[4]"

Only a comprehensive solution like Lookout Mobile Endpoint Security can deliver visibility into and protection from the full spectrum of mobile risks.

To learn more, read the full blog post: www.lookout.com/GoBeyond

> "Integration with EMM leverages the individual strengths of both MTD and EMM tools by using real-time risk assessment information from MTD and taking actions such as restricting access to the secure container, selectively wiping corporate apps or, in the extreme case, unenrolling the device so the device has no access to sensitive data.[3]"
>
> **Gartner, When and How to Go Beyond EMM to Ensure Secure Enterprise Mobility**

INSIGHT 4

Comprehensive mobile security requires the capabilities of two Gartner categories, mobile threat defense and mobile app reputation solutions

Over the last year Gartner has increasingly provided guidance on the mobile security solutions market, specifically the mobile threat defense (MTD) and mobile app reputation solutions (MARS) categories. The Lookout perspective is that on their own, neither MTD nor MARS deliver the holistic security that enterprises need.

> "It is becoming increasingly important that security leaders look at the anti-malware, mobile threat defense solutions market, the products available and how they should be used.[5]"
>
> **Gartner Market Guide for Mobile Threat Defense Solutions**

Enterprise security teams need a mobile security solution to protect their unique intellectual property from mobile attacks, prevent data leakage on a global scale, and deliver the visibility needed to make the right decisions during an incident. This is why enterprises should look for a comprehensive single mobile security solution that delivers capabilities of both mobile threat defense (MTD) and mobile app reputation solutions (MARS) products.

Gartner defines the mobile threat defense category as: "The MTD solutions market is made up of products that protect organizations from threats on mobile platforms, including iOS, Android and Windows 10 Mobile. MTD solutions provide security at one or more of these four levels:

- **Device behavioral anomalies** – MTD tools provide behavioral anomaly detection by tracking expected and acceptable use patterns.
- **Vulnerability assessments** – MTD tools inspect devices for configuration weaknesses that will lead to malware execution.
- **Network security** – MTD tools monitor network traffic and disable suspicious connections to and from mobile devices.
- **App scans** – MTD tools identify "leaky" apps (meaning apps that can put enterprise data at risk) and malicious apps, through reputation scanning and code analysis.[6]

While MARS solutions also detect malware, that is not their focus. Gartner explains, "Different from MTD, MARS products focus on identifying leaky apps – i.e., apps that can put enterprise data at risk.[7]" Organizations should look for a mobile security product that delivers a single MTD + MARS solution for protecting against both malicious and non-malicious behaviors.

Non-malicious apps can present a data leakage risk through:

- Accessing corporate information through calendar and notes applications
- Sending employee or customer data that includes PII externally
- Communicating with cloud services for data storage or retrieval

While such apps may not be explicitly malicious, these app behaviors present a significant risk because of their potential to cause an enterprise to fall out of compliance with regulatory and/or internal policies.

Read more about why the convergence of the mobile threat defense and mobile app reputation market is good news for CISOs.

[1, 2] Predicts 2017: Endpoint and Mobile Security, 16 Nove 2016, John Girard et al.

[3, 4] When and How to Go Beyond EMM to Ensure Secure Enterprise Mobility, 10 June 2016, Manjunath Bhat, Dionisio Zumerle

[5, 6, 7] Market Guide for Mobile Threat Defense Solutions, 28 July 2016, John Girard, Dionisio Zumerle