Mobile Application Monitoring

Mobile computing is exploding globally. Internet access via smartphones and tablets is expected to dwarf all other access methods within a few years, potentially putting more than half the world’s population online. Even organizations that have yet to launch a mobile app are at risk, as cyber criminals and unscrupulous individuals are offering thousands of unauthorized applications in a wide range of app stores.

Key Features
- Total Solution allows problems to be resolved quickly and efficiently
- Flexible reporting provides actionable intelligence
- Meaningful alerting delivered via email or customer portal
- Continuously maintained database of monitored online storefronts
- Ability to detect and monitor Android and Apple iOS apps
- Remove rogue apps from storefronts quickly

Key Benefits
- Eliminate need for in-house staff to spend valuable time on manual reviews of online storefronts to find rogue applications
- Avoid negative customer experiences and preserve customer trust by detecting rogue apps earlier
- Minimize fraud and privacy issues
- Protect brand reputation
- Mitigate risk of compliance violations
- Get a better understanding of what apps are associated with your brand name to help internal stakeholders understand need for policies and security oversight
- Help from the experts when you need it

Daily reporting of app landscape to provide situational awareness of application distribution for both Android and Apple.

Response Service will undertake, track, and report on removal of rogue apps from the marketplace.

Cyveillance can help you get all your mobile applications under control to ensure that your customers, revenues and reputation are protected.
Mobile apps can provide criminals an easy means to take advantage of your brand and steal your customers’ personal information or data, deceive them into downloading malware, and compromise their accounts. Spoofing, modifying, or selling mobile apps that brands offer for free are just a few ways that Cyveillance as seen crimes take advantage of the rapid rise of mobile apps.

The threat that a mobile application can present to your customer can change rapidly. Past threats that malicious and unauthorized applications have posed are:

- Unauthorized branded applications
- Unauthorized authentic applications
- Modified authentic applications
- Expired authentic applications
- Malicious aggregator applications
- Mobile device Trojan applications

Our Rogue Mobile Application Detection Solutions provide a capability to monitor the mobile application distribution ecosystem. This capability provides you the confidence for finding those apps that can pose a threat, even if the threat changes tomorrow.

About Cyveillance

Cyveillance is the leading provider of cyber threat intelligence, enabling organizations to protect their information, infrastructure, and employees from physical and online threats found outside the network perimeter. Founded in 1997, Cyveillance delivers an intelligence-led approach to security through continuous, comprehensive monitoring of millions of online data sources, along with sophisticated technical and human analysis. The Cyveillance Cyber Threat Center, a cloud-based platform, combines web search, social media monitoring, underground channel information, and global intelligence with investigative tools and databases of threat actors, domain names and IP data, phishing activity, and malware. Cyveillance serves the Global 2000 and the majority of the Fortune 50 – as well as global leaders in finance, technology, and energy – along with data partners and resellers. For more information, visit www.cyveillance.com. Cyveillance is a wholly-owned subsidiary of QinetiQ, a FTSE250 company which uses its domain knowledge to provide technical support and know-how to customers in the global aerospace, defense and security markets. For more information, visit www.qinetiq.com.

Rouge Mobile App Detection

Cyveillance monitors a wide range of online marketplaces to identify those published applications claiming to be provided by you. Delivery of rogue applications are presented in a client portal as well as timely email alerts. An additional daily email report details all findings and new findings to provide overall situational awareness for your organization.

Response Services

Our Response Service for Rogue Mobile Apps will undertake, track and report on removal of rogue apps from the marketplace or sit on which they are discovered.

Whether you need one element of our service, or a combination of other detection offerings, working in concert, Cyveillance can help you get all your mobile applications under control to ensure that your customers, revenues and reputation are protected.