Lacoon has pioneered a mobile security solution to provide enterprises multi-layered protection against emerging and targeted threats to mobile devices. Going beyond the simple known-attack detection of traditional anti-virus, Lacoon combines sophisticated network and device protection capabilities to deliver a truly comprehensive mobile security solution for your organization.

Lacoon enables safe adoption of bring-your-own-device (BYOD) and corporate mobile initiatives, even in the most sensitive environments. Lacoon protects you against emerging and targeted spyware and malware, including mobile Advanced Persistent Threats (APTs), drive-by and man-in-the-middle (MitM) attacks.

The platform-independent solution can help strengthen the policy management of MDM solutions, giving you the security control and visibility you need to protect your intellectual property and trade secrets from cyber-espionage and cyber-crime.

How Lacoon Mobile Security Works

1. All newly downloaded applications are sent to analysis in the cloud
2. A cloud service emulates the device in the cloud and scans for malicious applications
3. Active Protection is enforced based on the device risk category
4. Network based Active Protection uncovers new, emerging and targeted attacks

Key Features

- Comprehensive mobile security, with network and on-device protection that gives you a mobile defense-in-depth strategy.
- Multiple detection mechanisms, including behavioral detection, complex event analysis and MitM attack mitigation to identify and protect you from known, targeted and yet to be discovered threats.
- Immediate remediation, including virtual vulnerability patching and the removal of infected packages, mitigates the impact of mobile threats.
- Full forensics capabilities.
- Cloud-based, hybrid and on-premise options offer a flexible, seamless deployment.
- Easy integration with leading mobile device management (MDM) providers strengthens their policy enforcement and maximizes your existing investments.
- Support for both Android and iOS devices, without intrusive modifications to the mobile operating system, delivers comprehensive coverage.

Lacoon web-based dashboard
Network Protection

Active Protection
Lacoon delivers network-based Active Protection to protect against:
- **Spyware and malware**, by identifying anomalies in outbound communications to command and control servers and conducting complex event analysis that can uncover new, emerging and targeted attacks.
- **Drive-by attacks**, including exploits of unpatched web browser vulnerabilities.
- **Jail-broken iOS devices**, with network behavior anomaly detection.
- **Wi-Fi MitM attacks**, using secure VPN tunneling between the mobile device and secure mobile gateway.

Application Behavior Analysis
Lacoon uses Application Behavior Analysis in the cloud to detect unknown, polymorphic and zero-day threats by identifying the following malware behavior:
- Utilization of embedded exploits and rootkits.
- Command and control behaviors associated with mobile malware.
- Data leakage behavior associated with mobile spyware.

Device Protection | On-Device Enforcement
Lacoon delivers a mobile application to enforce a secure network channel for Active Protection, to send packages acquired on the device for behavioral analysis in the cloud, and to remediate malicious packages identified on the mobile device. Without Jailbreaking or Rooting, organizations can use Lacoon for:
- Automatic removal of suspicious software downloaded on the device; achieve additional protection by uploading installed applications to Lacoon’s Application Behavior Analysis.
- Enforce a secure channel using VPN.
- Allow maximum privacy for BYOD users, with the ability to toggle Active Protection on and off.

Management
Lacoon provides a web-based management console to simplify mobile device provisioning and ongoing mobile security management, with no disruption to the user experience. System administrators can use Lacoon’s:
- **Alert Investigations and Forensics** – view security alerts and handle incidents with advanced filtering and visualization capabilities that allow you to identify and remove the malicious threat.
- **Mobile Device Risk Assessment** – enables system administrators to enforce security policies according to the known vulnerabilities on each operating system.
- **Granular Controls** – the Active Protection can be toggled on and off by the device owner for maximum privacy, or according to risk information for different device groups.

Competitive Differentiation

<table>
<thead>
<tr>
<th>Capability</th>
<th>Lacoon</th>
<th>Anti-Virus</th>
<th>Secure Web Gateways</th>
<th>MDMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>+</td>
<td>Limited</td>
<td>Limited</td>
<td>–</td>
</tr>
<tr>
<td>Behavioral Zero-Day Detection</td>
<td>+</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Device Agnostic</td>
<td>+</td>
<td>–</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Wi-Fi MitM Protection</td>
<td>+</td>
<td>–</td>
<td>Limited</td>
<td>–</td>
</tr>
<tr>
<td>Enforcement</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>+</td>
</tr>
</tbody>
</table>

© Lacoon Security Ltd. All rights reserved