LevelBlue

SOLUTION BRIEF / JUNE 2024

The Importance of Mobile Security

Protecting Your Connected Devices is Essential to Safeguard Employee and Customer Data

Today's Mobile Transformation Offers Opportunities

Today's businesses continue to gain more productivity and flexibility through mobile devices. Faster mobile speeds, driven by 5G and the adoption of cloud and mobile-first solutions, enable employees to connect and work from almost anywhere. In fact, more than half of all internet traffic worldwide is driven through mobile devices[1] and the expectation for mobile-optimized experiences is growing.

Ripe for Attack

Today's dependence on mobility leads to vast amounts of data being accessed through a web of interconnected business and personal devices. This is a perfect storm for hackers. Organizations, therefore, must assume that every device with access to sensitive information is vulnerable to attack unless proven otherwise.

Users' experience on mobile devices also make them more vulnerable to attack. Mobile phishing through SMS, social media, messaging platforms, and other vectors is one of the largest threats. Cyber criminals are savvy in the many ways they exploit how mobile users interact with messaging and other communication on their devices. As a result, attacks on mobile devices continue to increase.

Benefits of a Mobile Security Solution

- **Security** – Mobile Threat Defense provides cloud-based mobile threat protection that's always on and continuously updated without interrupting users. Combined with Unified Endpoint Management, it allows businesses to take immediate action on a device if it experiences a threat while keeping company data protected.
- **Productivity** - Embrace flexible and diverse mobility programs to support your business, including Bring Your Own Device (BYOD), kiosk, monitoring, and rugged applications. Benefit from centralizing and automating mobile security and management tasks.
- **Privacy by design** – Protect employee privacy and maintain regulatory compliance while safeguarding corporate assets.
- **Phishing** – Protecting mobile endpoints guards against one of the major points of entry for cyberattacks. This helps keep your business out of the headlines and helps maintain your customers' trust.

The Mobile Security Gap

Enterprises strive to have well-structured security measures for PCs to provide protection against app-based, device, network, and web threats. Yet, although mobile devices have just as much access to sensitive data, thanks to cloud-first platforms, most organizations take limited action to protect them. The Mobile Threat Defense (MTD) market is in the early stages of adoption compared with other endpoint security markets such as the Endpoint Protection Platform (EPP) market, but it continues to grow, predominantly in regulated and high-security sectors.

Mobile Device Management or Unified Endpoint Management (MDM/UEM) systems offer management capabilities that can provide some level of protection. However, an MDM/UEM alone may leave the critical data on those devices vulnerable to risks associated with unsecured web content, malicious and/or risky apps, and always-on cellular or insecure Wi-Fi connections. A dedicated mobile security solution can help close these dangerous security gaps that traditional tools do not cover.

LevelBlue

What Can You do to Protect Your Business?

You can incorporate mobile security into your end-to-end cybersecurity strategy by:

1. **Aligning Mobile Security With Your Overall Security Architecture and Platform.**
2. **Including Mobile Threat Detection for Every Smartphone and Tablet.**
3. **Utilizing Tools to Centrally Manage Your Mobile Security.**

An effective mobile security solution can help with three of the top enterprise mobile security concerns:

Action	Protect Against Phishing	Extend Zero Trust to Mobile	Protect Employee-Owned Devices
Mobile Concern	**Beyond Corporate Email** Phishing links can be delivered in virtually any SMS, mobile app, QR code, and personal email with the aim of stealing credentials or downloading malware.	**Device Risk Visibility** Most mobile management platforms monitor mobile status at discrete intervals, with limited ability to address the device's risk profile.	**Productivity and Privacy** Allowing unmanaged devices to access your network presents security concerns and could impact user privacy.
Solution	**Phishing and Web Content Protection** Utilize machine learning from the Lookout Mobile Endpoint Security graph. The platform collects telemetry on almost 200 million devices to offer increased 360-degree protection from known and unknown phishing attacks on all mobile devices, while maintaining end-user privacy.	**Mobile Threat Detection Integrated with MDM/UEM** Continually assesses the risk profile of devices, and dynamically changes Zero Trust access controls to provide conditional access that helps protect your data.	**Mobile Applications Management** Integration with cloud productivity suites (such as Microsoft Office 365 and Google Workspace) allows you to restrict access when the risk profile of the device increases while maintaining protection policies.

Mobile Security Built for Business

How it Works

Lookout Mobile Endpoint Security helps protect organizations from threats on iOS, Android, and Chrome OS devices. Its cloud-based platform and lightweight mobile application helps optimize battery life, processor load, and the user experience. The Lookout security graph combines industry-leading artificial intelligence (AI), driven by the largest mobile threat dataset, to detect emerging threats with high fidelity. By analyzing threat intelligence data both from supported devices and external sources, Lookout recognizes the malicious and suspicious behaviors that indicate breaches, while also protecting user privacy.

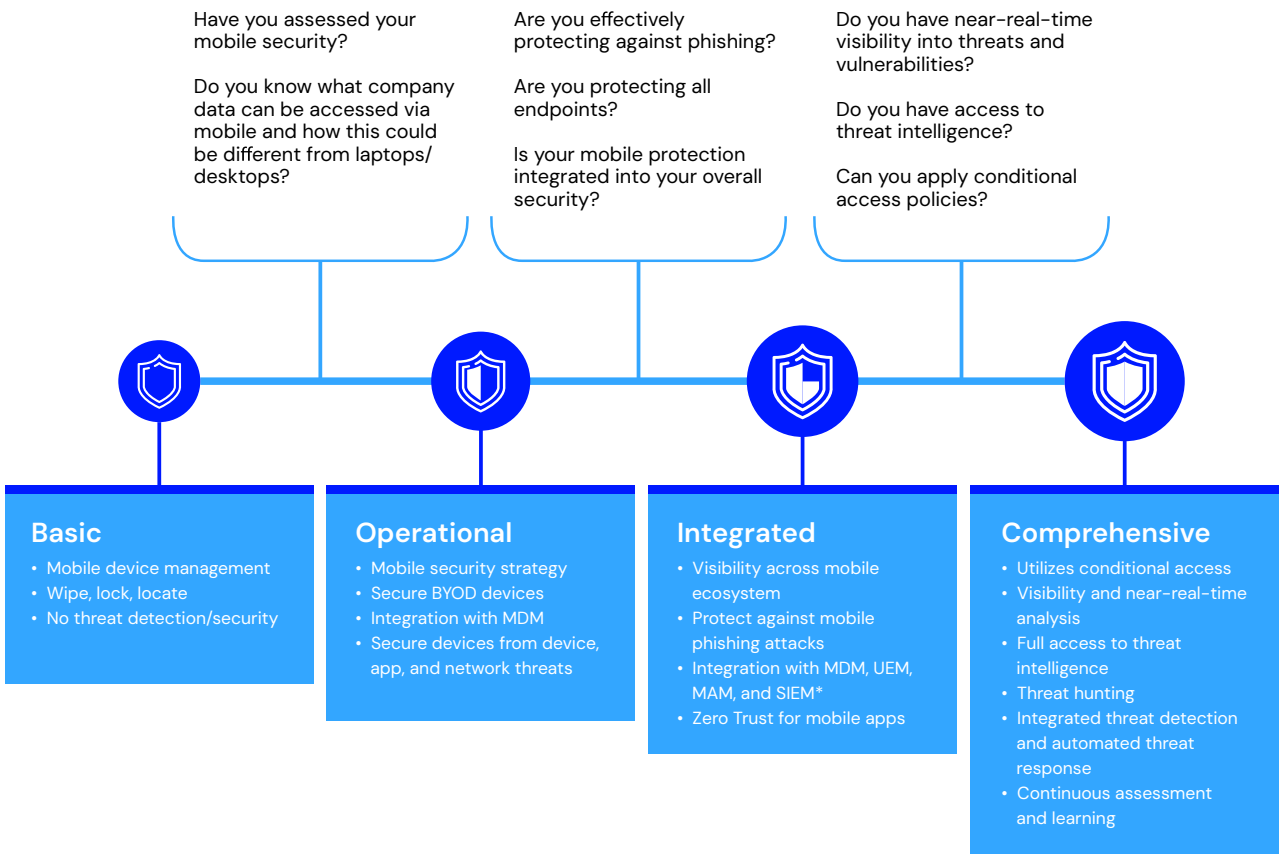
Centralize Device Management and Administration

Mobile security and management should no longer be viewed as separate functions. LevelBlue integrates Lookout Mobile Endpoint Security with MDM/UEM, partnering with the industry's most innovative endpoint management vendors. This integration allows for automated remediation of threats identified on mobile devices before they can impact your business.

Evolve Your Mobile Security Approach

LevelBlue can help elevate your mobile endpoint security posture to deliver the comprehensive protection today's environment demands.

Mobile Endpoint Security Maturity Model



*MAM - Mobile Application Management; SIEM - Security Information and Event Management

We're Here for You

As an expert advisor in your mobile security journey, LevelBlue offers a unique perspective and expertise. Experienced, certified consultants take the time to understand your unique environment and goals to implement policies and solutions that align with your business needs. The LevelBlue Customer Support Desk supports your mobile security solution 24/7. You can quickly establish or scale your mobile security program while minimizing cost and complexity – freeing up your existing resources for other business priorities.

With our industry-leading mobile security solutions, LevelBlue can help you safeguard your mobile assets, act with confidence against threats, and drive efficiency into your security operations.

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

To learn more about LevelBlue Mobile Security, visit us here.