LevelBlue

PRODUCT BRIEF

Strengthen Your Mobile Defenses with Mobile Security Risk Assessment Services

Mobile devices are crucial tools to stay competitive and build stronger connections with customers.

Gain More Visibility and Control of Your Mobile Devices, Apps, and Data Risks

The dependence on mobile devices/computing helps companies meet business objectives such as driving up revenue while driving down cost. However, these same mobile devices also bring new complexities—every new app adds even more data, with it new potential security gaps that need to be continually assessed and acted upon, to protect your mobile device users.

Just as businesses closely monitor and manage risks for traditional laptops and desktops within their IT networks and endpoint infrastructure, mobile devices and the vast amount of new use cases they enable should also be thoroughly managed and secured.

So how do you find and close the security gaps in your mobile environment? How can you promote greater productivity via mobile and today's "work from anywhere" model, while at the same time providing the necessary security controls for the applications and data that are being accessed?

Potential Benefits:

- Protect work from home users
- Combat phishing
- Control data leakage
- Review and block unauthorized apps
- Mitigate human error with machine learning in near real-time
- Support compliance with NIST, CMMC, ISO, CCPA, etc.
- Improve overall vulnerability management

Scope

- 100 to 500 mobile devices, including BYOD
- Review of information security, strategic and tactical plans
- Review of mobility strategy, policies and standards
- Mobile asset inventory
- Mobile device management solutions and their use
- Incident response planning
- Compliance requirements support

Consider:

- What security threats exist, how do they affect your mobile users, and how often are they occurring?
- What visibility do you have to vulnerabilities at the OS level and on the various versions of the mobile devices and applications in use?
- Do you really know who has access to company data on mobile devices, and what permissions exist for sharing that data?
- Is your security policy for BYOD current, when personal privacy and data sovereignty are becoming so important?

Unique Threats:

LevelBlue Consulting can help you review your current mobile environment and find ways to strengthen your mobile defenses and security ecosystem. Our Mobile Risk Security Assessment is uniquely designed to identify and combat the biggest threats that bypass traditional security controls and take advantage of mobile device users, including:

- **Mobile phishing**—Many phishing attempts occur outside of email, via SMS, social media apps, and QR codes.
- **Malicious applications**—Sideloaded apps can include malware or code used for credential harvesting or the exfiltration of sensitive data.
- **Unsecured networks**—Hotspots or spoofed cellular networks enable attacks capable of decrypting traffic and routing it to third-party servers.
- **Roots or jailbreaks**—These attacks compromise the mobile OS allowing attackers to escalate privileges, steal credentials, and move throughout an organization to do more harm.

Vulnerability Management:

A largely overlooked element of your security posture is the ability to update and enforce vulnerability management policies for iOS and Android devices. This is further complicated by the fragmented nature of OS patches and updates that come at different intervals from the device manufacturers and carriers. Then you need to keep the mobile applications on your devices properly updated as they can become susceptible to threats until the app developer pushes out a new version. If your users are utilizing older versions of mobile apps, they expose your organization to increased risk.

Compliance Considerations:

There are other aspects of mobile device use creating challenges in data leakage and compliance that are more passive in nature. Mobile applications often come with permissions granted by the user to access data typically required for the app to function. For the majority of apps the access granted is not malicious in nature but that doesn't mean it aligns to your business or compliance requirements. For example, some apps request access to your contacts, calendar, SMS archives, microphone or camera, or store and route data across international borders. Although this may not be a direct attack on your mobile security, it nevertheless allows access to sensitive data in unintended and possibly non-compliant ways.

Privacy and BYOD:

Many organizations are still toiling with a complex problem of their mobile device community. Is it possible to maintain the security posture necessary for access to sensitive data with the privacy and productivity benefits of users on unmanaged devices (BYOD)? While there are tools available to secure mobile devices, if not carefully considered the consequences can be costly and reduce the value of mobility to your organization.

- How do you enforce the use of security tools on unmanaged devices?
- Does it make sense for your users to keep separate business and personal devices?
- Do users feel comfortable allowing inspection of personal data such as web browsing history, photos, and SMS?
- If a compromise occurs, will the device be wiped, thereby erasing personal artifacts that cannot be recovered?

These questions are just the beginning to protect your data, that your users' privacy is uncompromised, and that your mobile productivity goals are met.

Thorough Analysis and of Your Mobile Environment

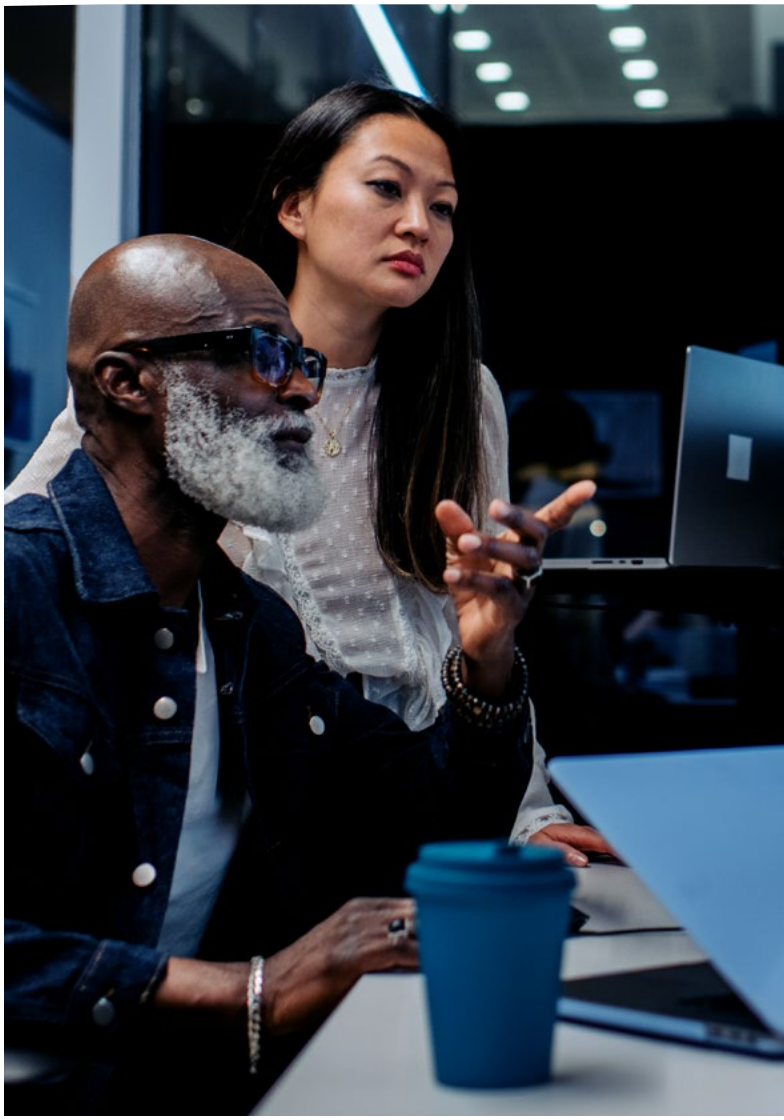
LevelBlue Consulting can help you answer these questions and achieve your business objectives by providing the visibility needed to understand the problems that are unique to your organization. By engaging directly with the stakeholders responsible for both security and mobility within your business, our security consultants will assist you with defining the scope of the assessment and delivering an output that can be used to redefine your mobile security posture.

For organizations utilizing NIST, ISO27001, CMMC, or the MITRE ATTACK framework, or are subject to regulatory requirements such as HIPAA, GDPR, CCPA, insights gained from the LevelBlue Mobile Security Risk Assessment Services can help you make business decisions about how you handle the data and applications on your mobile devices.

Why LevelBlue

Within its comprehensive portfolio of consulting services, LevelBlue offers a unique perspective regarding mobile security while using market leading analysis tools and certified cybersecurity consultants.

Security and compliance policies can be customized and tuned in real-time so that your most sensitive data is protected, and your compliance requirements are extended to include mobile. With LevelBlue Mobile Security Risk Assessment Services, your entire team can gain the visibility needed to understand how your business can optimize the productivity of its mobile workforce.



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.