DATA SHEET

RSA® Mobile Lock

Secure authentication on managed and unmanaged devices

Benefits

- **Universal Trust:** Ensures secure access across all mobile devices, managed and unmanaged.
- **Seamless Integration:** Built directly into RSA Authenticator App for iOS and Android.
- Monitors threats without impact on the user.
- **Proactive Threat Management:** Stops the spread of threats without interrupting user activities. Protects authentication without disrupting any other device functions.
- **Customizable:** Adjusts to your specific security needs with no additional effort on your part.
- **Effortless Compatibility:** Works with existing systems (MDM or MTD); no new installations required.

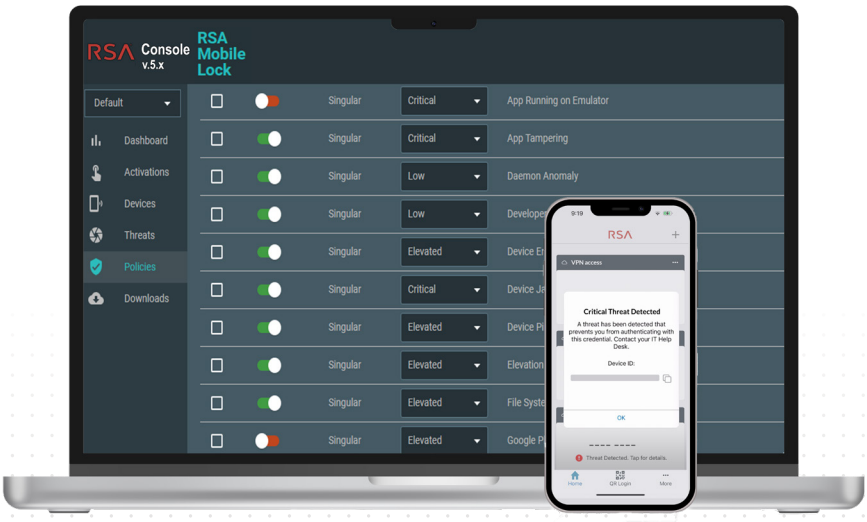
Trust the authentication process

RSA Mobile Lock identifies security threats on mobile devices and can restrict new authentication requests, thereby securing access to protected resources. This capability enables organizations to establish trust by systematically validating mobile authentication throughout their IT estate while actively identifying threats.

Respond to threats

When a user attempts to authenticate, RSA Mobile Lock searches for threats on their mobile device; if a threat is detected, it is reported in the Mobile Lock console, the authentication process can be restricted, and access to secure environments, including company data, enterprise systems, and customer records, is then prevented. This proactive measure effectively contains threats, preventing them from spreading beyond a single compromised device and averting widespread consequences for an organization.

Using the Mobile Lock console, organizations can easily customize the list of threats they wish to detect. They can also define if the detected threat should only be reported in the Mobile Lock console (for compliance monitoring), or the authentication process should also be restricted. Mobile Lock can detect a variety of threats, including jailbroken/rooted devices, malware, suspicious apps, MITM attacks, debug mode enabled. These are just a few examples; for a comprehensive list of all detectable threats, please visit the Mobile Lock FAQ.



Admin view of Mobile Lock console

User view of threat detected on mobile phone

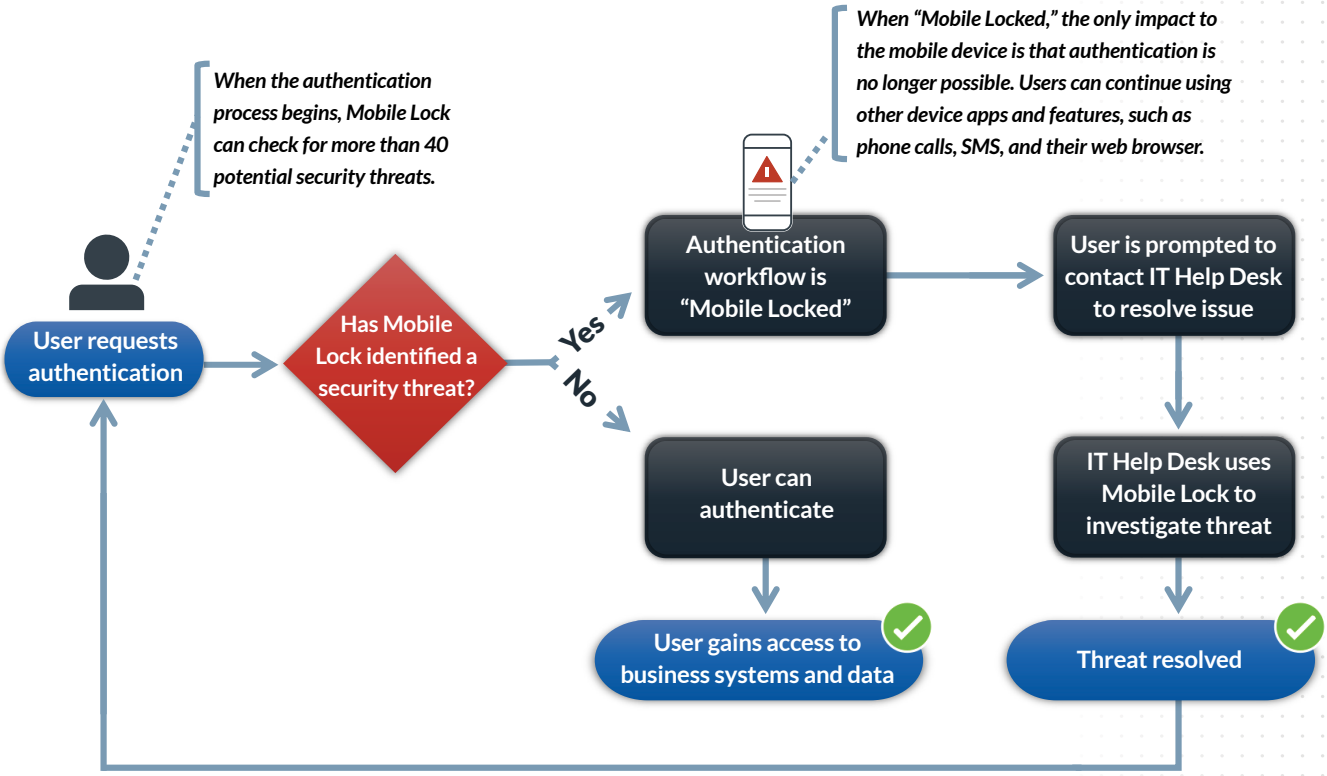
OWN YOUR IDENTITY.

Minimize the impact on users

Given the prevalence of Bring Your Own Device (BYOD) policies today, it's essential to consider how requirements to enforce corporate security on personal devices can potentially disrupt the user experience. RSA Mobile Lock minimizes this risk by seamlessly integrating into RSA Authenticator for iOS and Android, eliminating the need for a separate installation. Additionally, if Mobile Lock detects a threat, the solution only suspends the user's ability to use RSA Authenticator, and maintains their ability to make calls, text, browse the internet, and use other device features.

RSA Mobile Lock: the workflow

RSA Mobile Lock protects the authentication process and stops mobile devices with security concerns from accessing valuable corporate assets. While not visible to users, Mobile Lock scans the device every time an authentication is attempted.



About RSA

The AI-powered RSA Unified Identity Platform protects the world's most secure organizations from today's and tomorrow's highest-risk cyberattacks. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, and enable compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments. For additional information, visit our website to **contact sales**, **find a partner**, or **learn more** about RSA.