Lookout + VMware Workspace ONE UEM

With Continuous Conditional Access for VMware Workspace ONE productivity apps

As corporate data goes mobile, integrating a unified endpoint management solution with a cloud-based, mobile threat detection solution provides protection and control of devices and apps outside the reach of traditional perimeter security:

VMware Workspace ONE UEM

- Containerized apps and enterprise data
- Separation of personal and enterprise data
- Access to enterprise email
- Seamless access to enterprise apps with SSO
- Unified policy management
- Secure mobile content distribution
- Advanced DLP for email, content, and apps

Lookout Mobile Endpoint Security

- Continuous assessment of risk for containerized apps
- Protection against phishing attacks
- Detection of advanced jailbreak/root
- Detection of man-in-the-middle attacks
- Control of app data leakage to ensure compliance
- Visibility into sideloaded applications
- Custom remediation policy across threats types

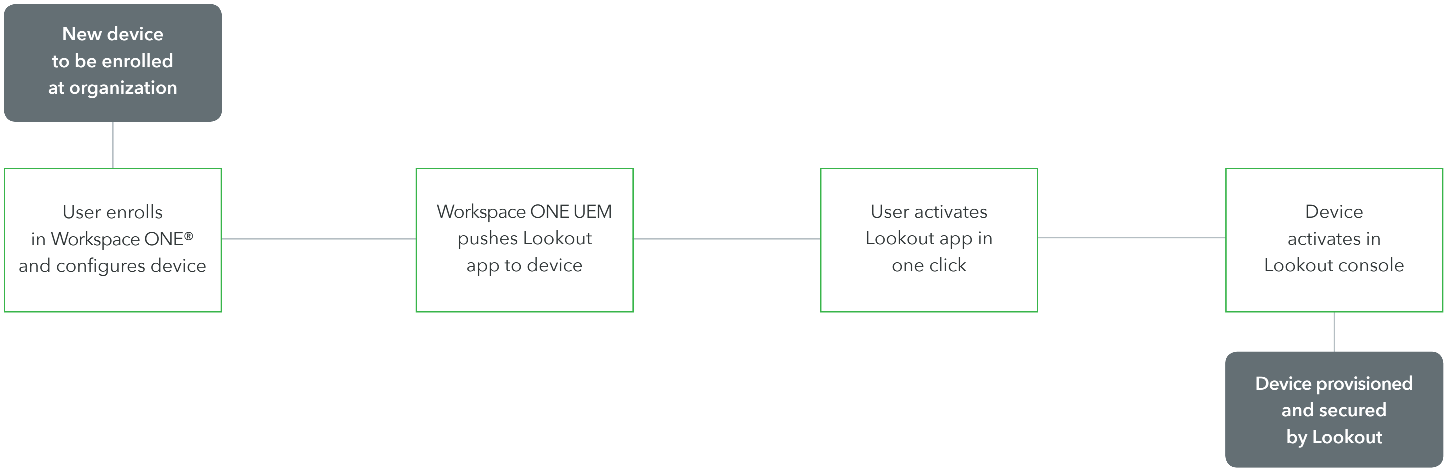
Seamless integration to provide secure mobility

Risks	VMware Workspace ONE UEM	Workspace ONE UEM + Lookout
App distribution	Secure distribution of enterprise apps, to employees	Easily distribute the Lookout endpoint application to employee devices
Policy violations	If a non-compliant device is detected, automated actions are to bring the device back into compliance	Compliance decisions can now take into account presence of threats or risky applications detected by Lookout
App-based risks	Containerizes apps and enterprise data such as emails or content	Provides visibility into apps that leak data as well as malware such as trojans and spyware
Unprotected networks	Through traffic tunneling, network access from devices is isolated to only managed corporate applications on the device	Protection against man-in-the-middle attacks on encrypted enterprise data in transit
Continuous Conditional Access	Access to corporate resources can be revoked automatically if compliance policies are violated	Access to VMware® Workspace ONE productivity apps can be revoked following Lookout's detection of app, network, or OS-based threats
Jailbreaking and rooting	Basic detection of jailbroken and rooted devices	Analyzes hundreds of OS signals to identify attempts to bypass basic jailbreak/root detection
Phishing attacks	None	Prevents connections via malicious URLs in email, SMS, messaging apps and those embedded into apps
Lost/stolen devices	Detect lost or stolen devices or remotely wipe business data and apps	Detect lost or stolen devices or remotely wipe business data and apps
Insecure authentication	One-touch mobile single sign-on across web, cloud and mobile apps	One-touch mobile single sign-on across web, cloud and mobile apps

How the Integration Works

Device provisioning

Integrated with Workspace ONE® Unified Endpoint Management powered by AirWatch®, the Lookout endpoint app can be easily distributed across managed mobile devices, allowing for rapid and scalable device provisioning. The device provisioning process follows these basic flows:



New device to be enrolled at organization

User enrolls in Workspace ONE® and configures device

Workspace ONE UEM pushes Lookout app to device

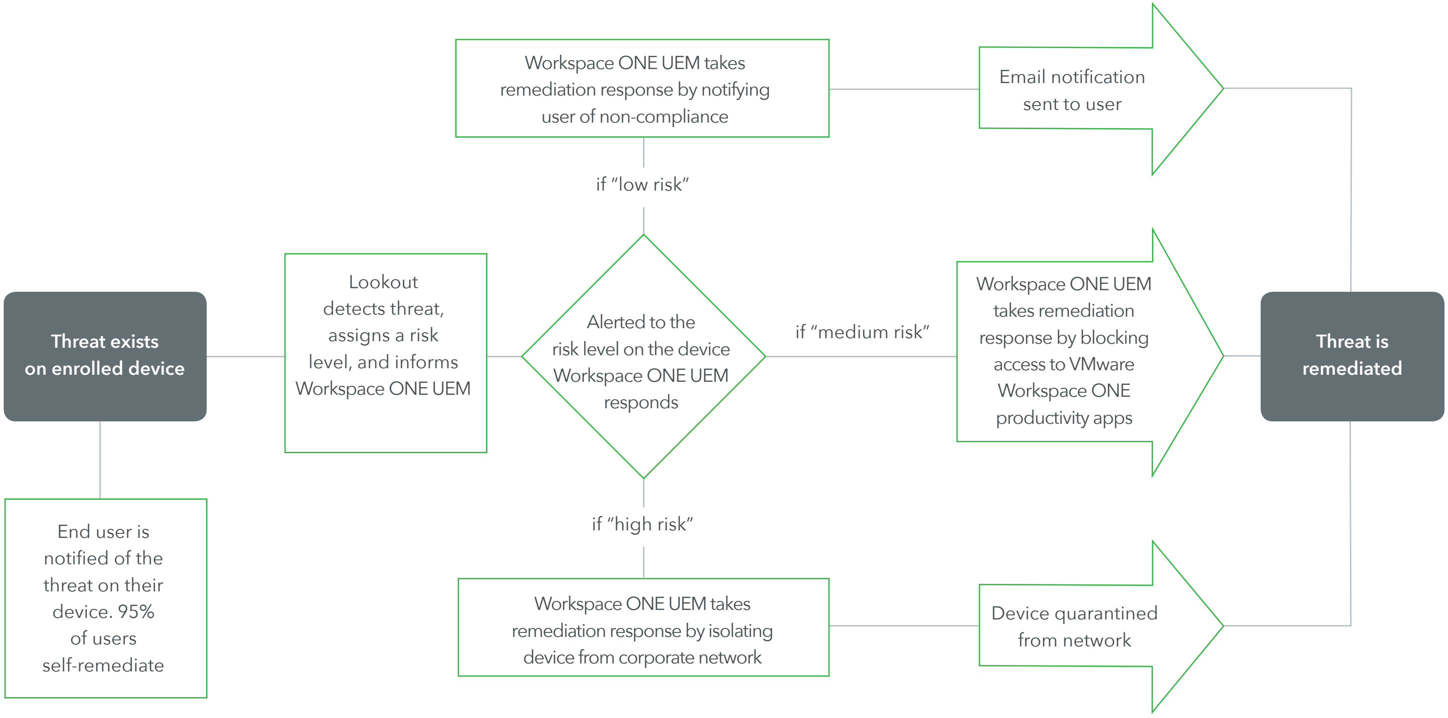
User activates Lookout app in one click

Device activates in Lookout console

Device provisioned and secured by Lookout

Continuous Conditional Access for VMware Workspace ONE productivity apps

With our Workspace ONE UEM integration, at risk devices can be quarantined in real-time using custom remediation policies. This includes the ability to block access to VMware Boxer containerized apps on unmanaged devices based on Lookout risk status. When Lookout detects a threat, the device will be categorized as either “high risk”, “moderate risk”, or “low risk” depending on your security policy settings. The threat remediation process follows these basic flows:



Threat exists on enrolled device

End user is notified of the threat on their device. 95% of users self-remediate

Lookout detects threat, assigns a risk level, and informs Workspace ONE UEM

Alerted to the risk level on the device Workspace ONE UEM responds

if “low risk”

Workspace ONE UEM takes remediation response by notifying user of non-compliance

Email notification sent to user

if “medium risk”

Workspace ONE UEM takes remediation response by blocking access to VMware Workspace ONE productivity apps

if “high risk”

Workspace ONE UEM takes remediation response by isolating device from corporate network

Device quarantined from network

Threat is remediated

Lookout