Lookout

Modernizing Data Security for Federal Agencies

A Platform to Address Today's OMB Cybersecurity Directives	M-21-30	M-21-31	M-22-01	M-22-09
Secure critical software by controlling access to any data and applications	✓			
Secure essential software with remote access capabilities from any location	✓			
Implement user behavior analytics for event logging to identify malicious activity		✓		
Event forwarding capabilities from email+phishing, cloud, DLP and mobile		✓		
Identify suspicious data access behavior with audit logs combined with timing and user-initiated events		✓		
Endpoint detection and response (EDR) for mobile endpoints			✓	
Continuous monitoring and collection of mobile data with rules-based automated response and analysis capabilities			✓	
Proactive threat hunting with visibility into advanced persistent threats			✓	
Accommodate encrypted DNS for both cloud infrastructure and mobile endpoints				✓
Ensure email contents are encrypted in transit, especially externally				✓
Make applications internet accessible, secure without VPN				✓
Implement cloud security services to discover, classify and protect sensitive data				✓
Encrypt data at rest and log decryption attempts by a separate cloud-based third party system				✓

Recent **Office of Management and Budget | The White House (OMB)** directives require agencies to implement enhanced security for cloud services and critical software, comply with event logging requirements for incident response, expand Endpoint Detection and Response (EDR) coverage capabilities to mobile devices, and lastly, implement a Zero Trust Architecture (ZTA) strategy.

The Lookout Security Platform enables government agencies to meet the requirements of each OMB directive and mitigate risk while allowing critical initiatives such as remote work.

M-21-30

Implementation of Critical software

Lookout Security Platform includes CASB to ensure malicious files cannot be uploaded or downloaded and mitigate software, user, or device compromise.

In addition, sensitive data such as Personal Identifiable Information (PII) or other company-specific identifier data is protected in real-time against data loss or data exfiltration.

M-21-31

Maturity model to guide the implementation of requirements across four Event Logging (EL) tiers

Lookout has built-in User and Entity Behavior Analytics (UEBA) capabilities across our platform that associate risk levels to suspicious behavior observed on mobile devices. Combined with our CASB, Lookout can provide detailed insights into privileged user activity and use unique algorithms for determining anonymous activity when accessing cloud resources.

M-22-01

Guidance to implement Endpoint Detection and Response (EDR) including mobile EDR

"EDR combines real-time continuous monitoring and collection of data (for example, networked computing devices such as workstations, mobile phones, servers) with rule-based automated response and analysis capabilities." Lookout is the only mobile solution that provides EDR capabilities supporting advanced investigation and policy development.

M-22-09

Zero Trust Architecture (ZTA) strategy

Lookout ensures organizations can implement a Zero Trust architecture strategy. Our platform enables organizations to enforce unified policies across private, cloud, and internet access. We provide IT security teams the controls to take precise actions with varying degrees of granularity based on the fluctuating risk level of their users, endpoints and the data across the organization.