Securing Data and Collaboration in G Suite for the Remote Workforce

WHITE PAPER

This paper focuses on addressing the emerging cloud security challenges facing today's organizations as they further adopt cloud applications and BYOD to enable their distributed workforce, specifically Google's Suite of collaboration tools.

Common questions regarding G Suite security

2019 Breach and Information Security Study Findings

Over 60% of data in cloud collaboration apps contains intellectual property or compliance related data

Email and messaging apps are the # 1 vector for cloud data loss

Organizational data created and residing in the cloud apps

Organization size 20 to 500
- over 90% of data
Organization size 501 to 2000
– over 68% of data
Organization size 2001 to 10000
- over 49% of data
Organization size 10001 and up
- over 40% of data

Lookout's Continuous Protection Model

Lookout's Continuous Protection Model

- Securing the cloud and mobile environment requires continuous monitoring and analysis of every device, user, application and data set. Ideally, this analysis combines numerous attributes across every application, automatically applying policy controls based on user risk. Meanwhile, machine learning correlates deep contextual data to provide a unique 3D historical view of the current state of cloud security.

- This model allows security staff to centrally manage and optimize data security controls, eliminating the need to pursue individual incidents spread out across multiple disparate consoles.

Human-Centric Security For Today's Mobile Workforce

Lookout CASB provides advanced security monitoring and control for G Suite applications, BYO devices and data shared across multiple cloud collaboration platforms, including Slack and Box. Delivering continuous protection requires centralized analysis and policy oversight spanning every cloud SaaS application and private app. CASB delivers deep integration and granular controls for G Suite and every relevant business and security application.

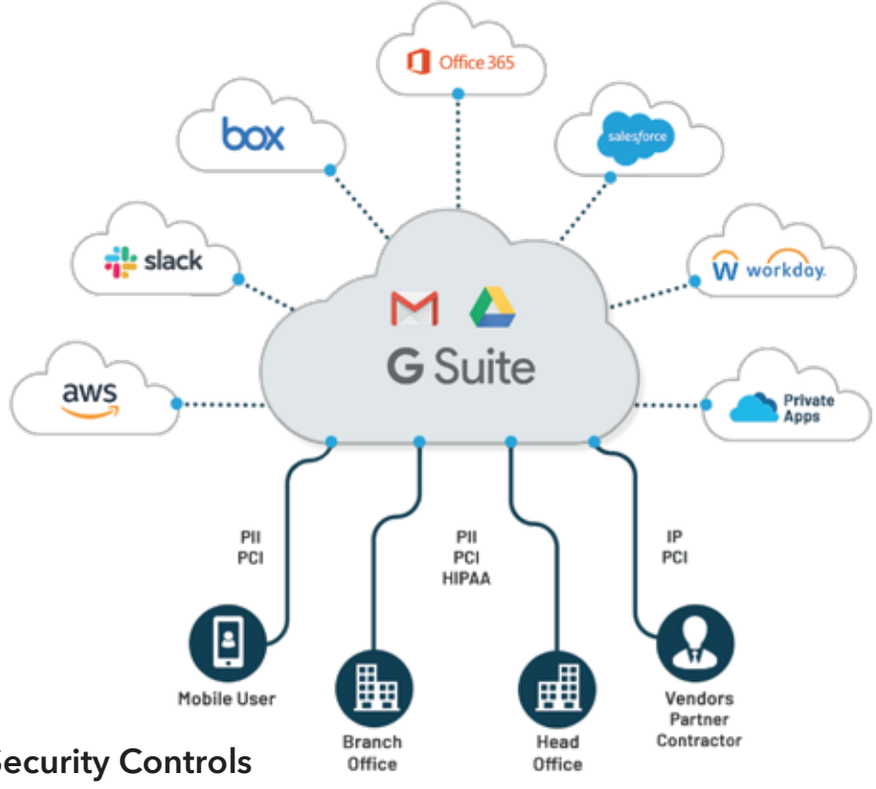
Identify and protect unathorized account access with **Adaptive Access Controls**

Automatically detect and remediate malicious user behavior with **Advanced UEBA**

Point and click incident analysis with **Incident Insights**

Achieve full visibility of cloud apps being utilized with deep **application intelligence**

Real-time management of mobile devices with **EndPoint Security Controls**



Identify and secure allcommunication at rest and in motion using **DLP for apps and emails**

Secure offline collaboration with **Information Rights Management**, built for collaboration

Ensure end-to-end data protection with frictionless **encryption and tokenization**

Gain visibility into years of historical cloud data with **Cloud Data Discovery**

Maintain configuration integrity of cloud apps with **CSPM** for IaaS and SaaS

Integrate with existing enterprise security infrastructure:
Symantec DLP, Juniper AVAM, VMware AirWatch, CloudFlare, Akamai, Okta, and more.

Information Protection

One of the most critical aspects of cloud security is information protection. The ability to achieve compliance, control data access, properly tune firewalls, encrypt data at rest and maintain control as data is shared with partners are just a few of the capabilities delivered by Lookout CASB.

Lookout is unique in providing advanced CASB functionality to Gmail and other Google Suite Apps

- Govern sensitive data across all SaaS and private applications. Run actionable reports for continuous compliance of PII data with latest data privacy laws and regulations - CCPA, GDPR, HIPAA, PCI.
- Continuous Information Protection for Email, messaging, collaboration, data repositories, and private apps using a single policy and management console.
- Intelligent Encryption protecting data in email, messaging, at rest and in motion with information rights management.

Gartner CASB Magic Quadrant, Oct 2019

"Lookout is one of the few vendors that also extends its CASB functionality to Email in Office-365 and G-Suite."

Threat Protection

The cloud introduces new malware challenges – threats that are shared between clouds and often bypass conventional network anti-virus systems. Viruses, shared by users as attachments or links, can propagate rapidly through the cloud and cause widespread damage on a massive scale than previously possible.

Lookout's zero-day threat protection provides integrated malware detection designed for the cloud with industry-leading detection rates. Lookout's anti-virus anti-malware (AVAM) solution scans all inbound and outbound cloud content for malicious code and cleans or quarantines infected content on the fly, without adding any noticeable latency.

Lookout CASB Malware protection for G Suite scans and mitigates potential malware threats including zero-day threats.

- Discover, classify and encrypt sensitive data in existing data repositories and protect against malware and ransomware hidden in cloud apps.
- Threat protection against advanced malware based on behavior analysis, machine learning, and sandboxing.
- Automate incident management with centralized management console and integrate with ticketing services and SIEM to operationalize day to day activities and threats.

Cloud Mobile Security Architecture

Deployment of integrated security controls shouldn't demand significant resources, create unnecessary complexity or overrun expected timeframes. Lookout CASB enables rapid deployment of advanced capabilities to protect data and maintain compliance for all cloud apps within a matter of hours. Lookout CASB architecture offers the full variety of deployment options to address every manner of business requirements and technical infrastructure

Architecture

- Agentless access to enable secure access using BYO or unmanaged devices to employees, contractors, vendors, and partners.
- Zero-trust architecture, combining with IDaaS solutions to deliver end-to-end user and data security from any device, any location, to all trusted cloud applications.
- Multi-mode deployment, working in API, reverse proxy and forward proxy modes, delivering next-gen CASB functionality, addressing all use cases. (visibility, adaptive access controls, compliance, data protection, threat prevention).
- Enterprise integrations with on-premises or endpoint DLP, identity services, network edge services, and incident remediation and automation.

Access Control based on Behavior and Analytics

- Data policy enforcement and sensitive data access control with proper firewalling, cloud to cloud protection, and adaptive control based on user behavior risk scores.
- Configuration management and templates ensure that security staff and those with privileged access do not accidently misconfigure admin setting, overlook open share links, and maintain configuration compliance - automatically.

Scenario: Using G Suite with unmanaged devices

Challenges

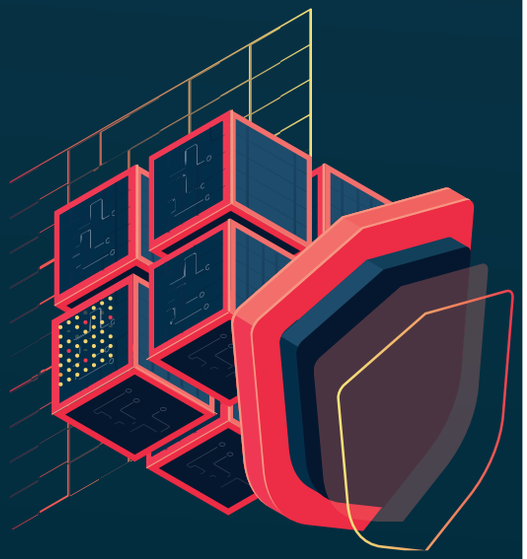
- User-owned and unmanaged devices are used to access sensitive data
- Travelers use insecure shared "kiosk" computers to access G Suite

Consequences

- Files left behind on public computers expose company data
- Device loss or compromise creates a compliance event
- Potential for reputational damage, fines, lawsuits

Lookout CASB Strategy

- Intercept all data before it reaches any device - managed or unmanaged
- Evaluate a wide range of security factors including location, device posture, data sensitivity, and more
- Apply and replace a broad menu of security policies for every situation, including
  - Block, quarantine, or mask all G Suite traffic
  - Redirect user to an online G Suite app to avoid file download
  - Remotely wipe devices



Scenario : Confidential emails and Information leaks

Challenges

- Employees sending emails with senstive content to external domains or
- Sharing data to another collaboration app outside of G Suite via sending emails

Consequences

- Risk of intellectual property theft
- Potential lawsuits by customers for information leakage, leading to loss of reputation and trust

CipherCloud CASB Strategy

- Advanced DLP scanning to identify and protect sensitive information in email subject, body and attachments
- Continuous user behavior monitoring (UEBA) for real-time detection and remediation of anomalous activities
- Encryption of emails and attachments before sending to Gmail server
- On the fly removal of unknown or unauthorized recipients before the email is sent out

The Largest Multinationals in the World Use Lookout CASB

- 5 of the Top 10 U.S. Banks
- 6 of the Top Banks Worldwide
- 3 of the Top 10 Insurance Firms
- 3 of the Top 10 U.S. Health Care Firms
- 3 of the Top 10 Pharmaceutical Firms
- 2 of the Largest Telecommunications
- Firms Government agencies in the United States, United Kingdom, Canada, Australia, and beyond

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit www.lookout.com and follow Lookout on its blog, LinkedIn, and Twitter.

Lookout®