WHITE PAPER

Lookout®

Securing Data and Collaboration in Office 365 for the Remote Workforce

This paper focuses on the emerging cloud and data security challenges facing today's organizations as they further adopt cloud applications - specifically Office 365 - to enable the distributed workforce. From ensuring adaptive access controls to properly identifying and classifying sensitive data, practitioners must address a huge array of related requirements as they advance their security best practices to support the cloud and BYOD.

Common questions regarding Office 365 security

How do I secure access to Office 365 email and applications from unmanaged, personal devices?

How do I secure my organization's Office 365 email, applications, and user accounts against internal and external threats?

How do I gain visibility into the content that is being uploaded, downloaded, and shared in my organization's Microsoft Teams application?

Are the sensitive assets in my organization's instance of Office 365 classified and protected with DLP and encryption?

Microsoft Teams user activity skyrocketed during the COVID-19 lockdown, reaching 75 million active users by April 2020. [1]

Healthcare and Financial services face the highest financial risk from the leakage of compliance-related data. [2]

Over 40% of compliance related data in Office 365 is overexposed in file sharing. [2]

Roughly 66% of malware is installed via malicious email attachments. [3]

[1] Source: www.theverge.com
[2] Source: Symantec 1H2017 Shadow Data Report
[3] Source: Verizon Data Breach Investigation Report (DBIR)

Lookout's Continuous Protection Model

Lookout's Continuous Protection Model

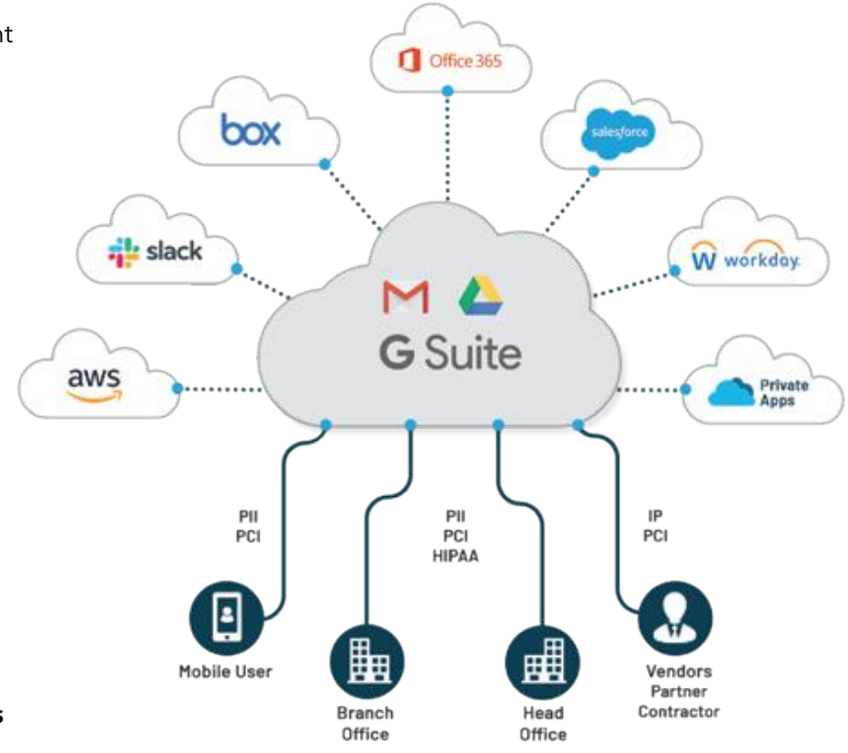
Securing the cloud and remote workforce environment requires continues monitoring of every application, user, device and data set. Ideally, this analysis combines numerous attributes across every application, automatically applying policy controls based on user risk. Meanwhile, machine learning correlates deep contextual data to provide a unique 3D historical view of of normal behaviors and existing cloud security risks.

This model allows security teams 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 Office 365 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 and private applications. CASB delivers deep integration and granular controls for Office 365 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 applications being utilized with **deep application intelligence**
- Real-time management of mobile devices with **EndPoint Security Controls**



- Identify and secure all communication at rest and in motion using **DLP for applications 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, Microsoft AIP, Azure AD, Microsoft ADFS, Thales, Okta, and more.

Information Protection

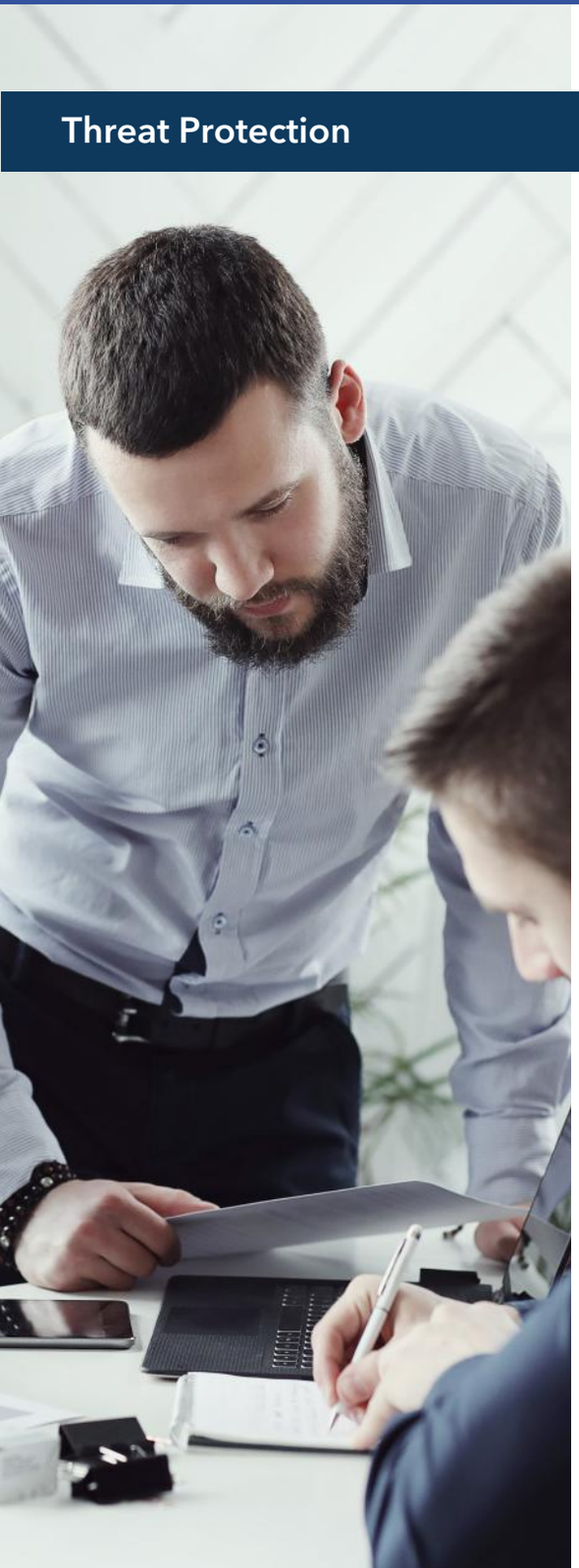
One of the most critical aspects of cloud security is information protection. The ability to achieve compliance, control data access, properly tune firewalls, encrypt data at rest and maintain control as data is shared with partners are just a few of the capabilities delivered by Lookout CASB.

Lookout is unique in providing advanced CASB functionality to Microsoft Outlook and other Office 365 applications including Teams, SharePoint and OneDrive, among others.

- An attribute-based policy engine that inspects data in any mode - API, proxy, and email, providing extensive coverage across all Office 365 collaboration scenarios.
- Enhanced data discovery with comprehensive audit in the cloud to identify and classify sensitive information and enforce remediation to preserve data integrity and compliance.
- Enforce Zero Trust encryption to protect data no matter where it is – "at rest," in-network transit, in the cloud application layers (API, middleware, memory), and in use.

Gartner CASB Magic Quadrant

"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 as evidenced in attacks such as the 2020 SolarWinds incident.

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 Office 365 scans and mitigates potential malware threats including zero-day threats.

- Zero-Trust identity protection integration with IDaaS solutions including Okta, Ping, and Thales.
- Integrated anti-virus anti-malware (AVAM) solution, with URL link protection and on-premise sandbox integration, for detecting and preventing zero-day threats.
- Assessing the standing of users and devices to detect anomalous activities with User and Entity Behavior Analytics (UEBA).
- Automate incident management with centralized management console and integrate with ticketing services and SIEM to operationalize day-to-day activi-ties 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 applications 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 protec-tion, threat prevention).
- Enterprise integrations with on-premises or endpoint DLP, identity services, network edge services, and incident remediation and automation.M to operationalize day-to-day activities and threats.

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 acess do not accidently misconfigure admin setting, overlook open share links, and maintain configuration compliance - automatically

Scenario: Using Office 365 with unmanaged devices

Scenario

- User-owned and unmanaged devices are used to access sensitive data
- Logging through unsecured home networks, lacking the corporate security controls, for remote collaboration
- Employees using personal devices to access both corporate and personal Office 365 accounts and downloading sensitive data

Risks Involved

- An employee using a personal, unmanaged device logs into Office 365 from their home network. This unknowingly introduces the risk of malware introduction into the Office 365 environment that could result in further compromise and the loss of sensitive data. A resulting data breach may lead to compliance fines and reputational damage.

Lookout CASB Strategy

- Enforce identity and context-aware access policies to secure login from any user, device and location
- Apply layered cloud data protection, including integrated DLP, classification and encryption to secure data across clouds and devices
- Apply enterprise digital rights management to protect sensitive cloud data wherever it travels
- Monitor user activity with UEBA and machine learning to identify anomalous behavior and real-time threats
- Leverage deep cloud scanning to discover unprotected data and open shares
- Log cloud security events and report related incidents for end-to-end visibility into user activity
- Automate assessment of your Office 365 configuration with SaaS Security Posture Management to remediate any misconfigurations

Scenario : Confidential emails and Information leaks

Scenario

- Employees sending emails with senstive content to external domains or external teams
- Sharing data to another collaboration applications outside of Office 365 via sending emails

Risks Involved

- Organizations run the risk of intellectual property theft and data leaks through accidental email forwards or collaboration with third-party connected applications. Additionally, lack of visibility over personal devices accessing corporate Office 365 accounts can lead to potential data exposures when an employee downloads a document from a sanctioned cloud and then attempts to upload it to an unmanaged cloud.

Lookout CASB Strategy

- Advanced DLP scanning to identify and protect sensitive information in email subject, body and attachment
- Continuous user behavior monitoring (UEBA) for real-time detection and remediation of anomalous activities
- Encryption of emails and attachments before sending to Microsoft Outlook and Exchange Online servers
- 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

Lookout®

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.