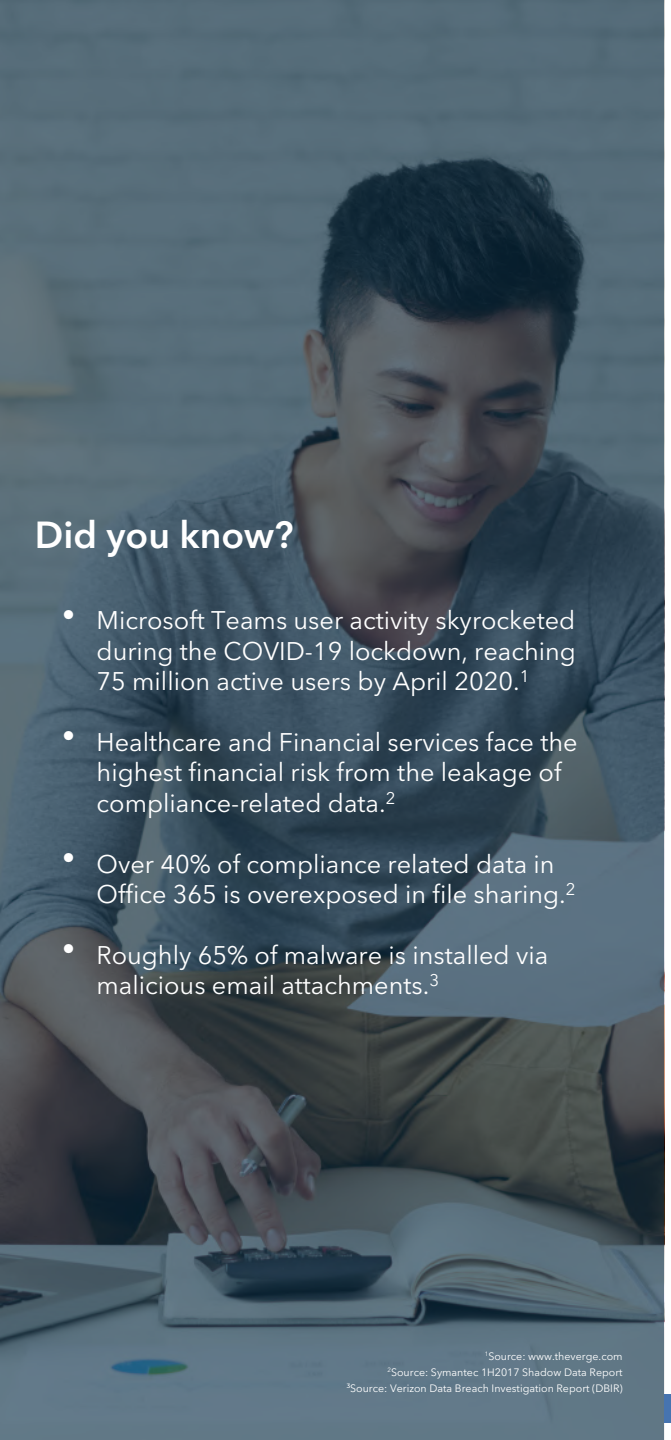
Lookout®

Whitepaper

Securing Office 365 and the Cloud for Financial Services Practitioners

Office 365



Did you know?

- 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 65% 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)

Expanded Remote Workforce Impacts Office 365 and Cybersecurity

Only months into 2020, the COVID-19 pandemic forced many businesses worldwide to pivot quickly, expanding their use of the remote workforce model. To support this change, numerous organizations immediately increased their dependence on the popular Microsoft Office 365 platform to enable business continuity and collaboration.

With every such evolution of computing practices, added security considerations abound. Related challenges of 'working from home' have proven profound among heavily regulated industries such as financial services and healthcare, among others, owing to the critical nature of their work and intensive data security requirements.

Faced with the mandate to enable highly complex workflows spanning a nearly endless array of roles and responsibilities, all while maintaining data protection and regulatory compliance, security practitioners have been forced to tackle challenges of massive scale. If the notion of employees connecting to cloud apps from less secure home networks and unmanaged devices were not enough of a concern, the confidential data has proven consistently demanding.

Addressing Microsoft Office 365 Security

Microsoft® Office 365 has emerged as a leading enabler of financial services based on its wide range of productivity and communications capabilities, from Outlook to Teams, to OneDrive and Sharepoint, Office 365 allows organizations to closely collaborative via email, shared documents, and chat channels, ultimately ensuring cohesive business operations.

Yet, while Office 365 is a powerful productivity enhancer and offers a range of native security controls, it also generates a wider set of cloud security and data protection implications. The platform's highly varied and dynamic collaboration capabilities present an almost endless array of data security and compliance requirements.

The expanded remote workforce has also increased organizations' threat surface in the cloud. According to a report issued by McAfee in May 2020, there has been a 630% increase in remote attacks on cloud services by cybercriminals between January and April 2020, with greater concentration of Office 365 collaboration services.

Intensified by a lack of visibility into and control over remote worker's unmanaged devices accessing cloud services including Office 365, along with other technical challenges, this combination of accessing cloud services including Office 365, along with other technical challenges, this combination of factors has created a massive potential for potential data leaks and malware attacks in the financial industry. This is further underlined by questions of related compliance with data protection laws such as GDPR, CCPA, HIPAA, PCI, and SOX.

Given this reality in today's ultra-collaborative and increasingly distributed corporate climate, security practitioners required a new playbook as they shift their focus to the application of more identity-centric, context-centric, and data-centric strategies, including as it relates to the protection of data traversing the entire Office 365 portfolio.

Key questions every security practitioner must ask they seek to better support Office 365 for remote collaboration include:

- Are my organization's Office 365 email, applications, and user accounts secured against both internal and external threats?
- Do we have visibility into the content that is being uploaded, downloaded, and shared in my organization's Office 365 email and applications?
- Are the sensitive assets in my organization's instance of Office 365 classified and protected with DLP and encryption?

7 Critical Steps for Securing Financial Data in Office 365

Automate assessment of your cloud security posture to remediate any misconfigurations.

Enlist centralize policies across all applications and email services.

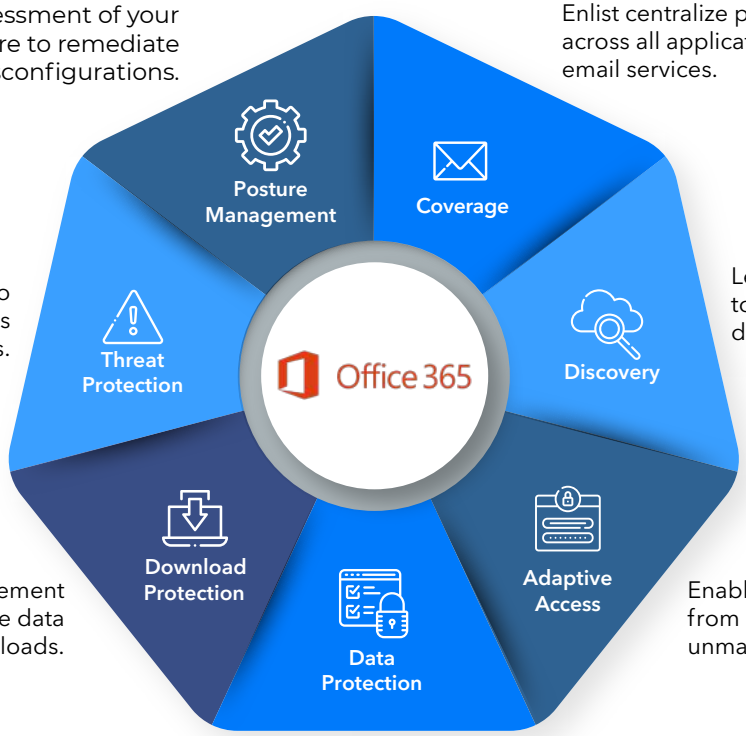
Monitor user activity to identify anomalous behavior and threats.

Leverage deep cloud scanning to discover unprotected data and open shares.

Apply rights management to secure data during downloads.

Enable Zero Trust access from managed and unmanaged devices.

Enforce policies to classify and protect sensitive data uploaded to the cloud.



Centralized Visibility and Policy Enforcement across Apps and Email Services

With increasing adoption of Office 365, in particular, to enable the remote workforce, today's security teams need centralized security controls to maintain 360-degree visibility into the current standing of their users, applications, and data. In addition, they require deep intelligence into their sanctioned cloud environments to respond to potential threats.

Lookout CASB provides an integrated platform approach to financial organization's Office 365 email, collaboration, and infrastructure security requirements, delivering full CASB functionality including applications usage, data discovery, data protection, compliance, and threat prevention - offering the full breadth of capabilities needed to actively secure use of the Office 365 suite.

- **Key elements of CASB include:**
- An attribute-based policy engine that inspects data in any mode - API, proxy, and email, providing extensive coverage across all Office 365 collaboration scenarios.
- The industry's first Secure Email Gateway delivered in a CASB which integrates directly with Office 365, securing email data in Outlook app, Outlook Web Services, and Exchange Online.
- Integrated DLP such that any existing DLP policies can be extended to cloud-native emails to protect sensitive content that may reside in subject lines, body text, or attachments, as well as prevent email forwards to unintended or unauthorized recipients.
- Detailed visibility into Office 365 collaboration apps for deeper understanding of any data being shared across the cloud and user devices, helping to identify and ultimately protect sensitive data from accidental disclosure or exposure.

Scanning Cloud Apps to Discover Unprotected Data and Open Shares

With remote workers collaborating openly across multi-cloud environments, tracking the use of sensitive data has become even more challenging. Protected data may reside across multiple apps, databases, and personal devices, and without proper visibility, enterprises run the risk of compliance failure, security vulnerabilities, and potential data breaches.

Lookout's enhanced Data Discovery solution allows financial services to scan and discover sensitive information used in Office 365 apps, preventing potential data exposure due to a lack of security controls. Upon detection of exposures related to open file shares and other data handling activities across Office 365 applications, Data Discovery automatically enforces remediation actions including encryption, masking, redaction, and deletion, along with blocking file and folder sharing with external domains, thereby preventing the loss of PII, PCI, PHI, intellectual property, and other sensitive information.

Lookout Data Discovery specifically provides:

- A comprehensive audit of data in the cloud to identify and classify sensitive information and enforce remediation to preserve data integrity and compliance.
- An extensive library of prebuilt DLP templates, along with the option to create custom templates to identify security blind spots, detect open shares, and address many global regulations including PCI, HIPAA, GDPR, GLBA, etc.
- Intuitive drill-down dashboards for analysis and visualization of historical file scans and existing policy violations that enable security practitioners to take immediate corrective actions.
- Multiple scheduling options - periodic and one-time, to ensure sensitive data is always properly identified and safeguarded.

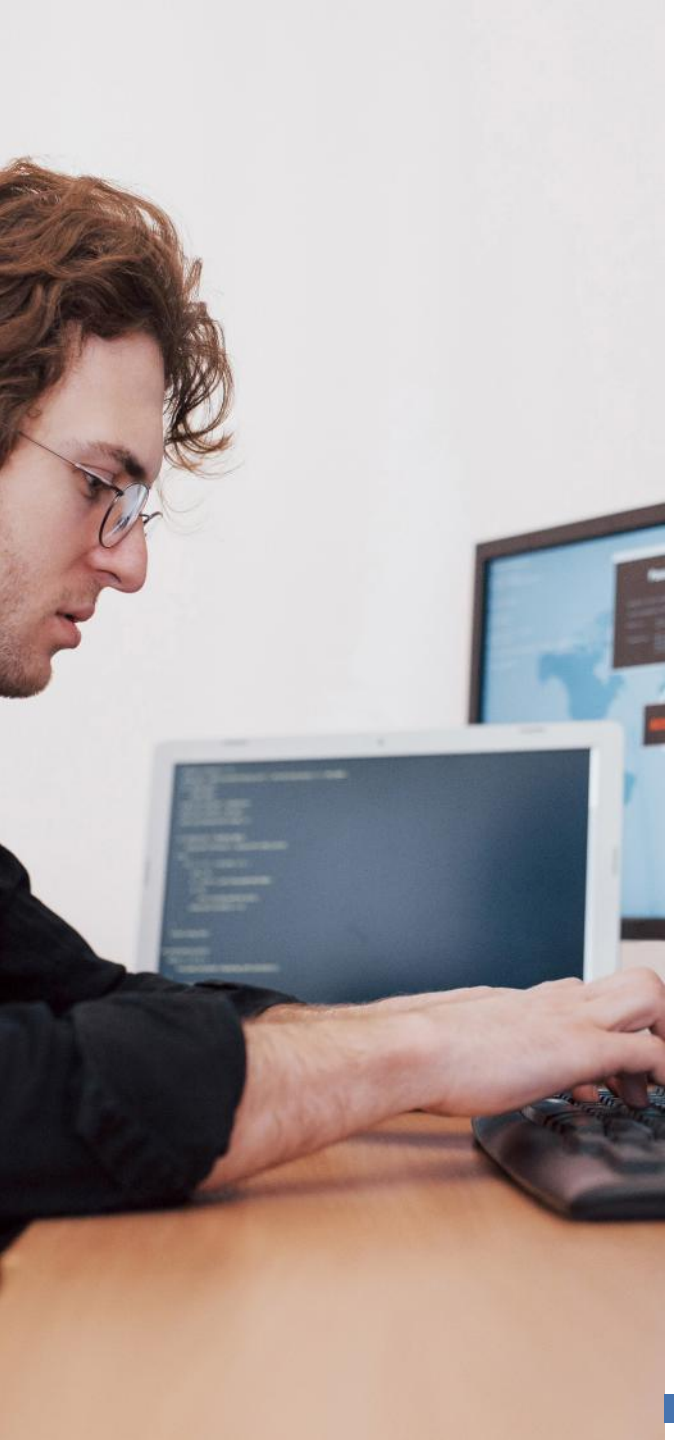
Enabling Zero Trust Access from Managed and Unmanaged Devices

Authenticating the identity of users accessing your most sensitive data and applying strong data protection controls are perhaps the two most critical components of cloud data security for the remote workforce. The continued migration of business-critical workflows and services to the cloud, along wuthg the rapid surge in personal devices used for business collaborations has challenged financial organizations to seek more identity and context-aware access for their SaaS applications.

Lookout's Adaptive Access Controls define context-aware policies to deliver "Zero Trust" access to applications and resources residing in Office 365 environments. This allows organizations to manage access to the cloud from any user, any device, and any location, with automated remediation, such as adaptive user right management upon detection of a policy violation. This extensive context includes location, user, user group, IP address, device/OS type, user behavior, device compliance, and IP risk, among others.

Additional features include the ability to:

- Integrate with MDM/EMM solutions to retrieve the endpoint device type (managed/unmanaged) and enforce device-level access restrictions. For example, blocking thick app access, or allowing read-only access via web browsers used by personal devices.
- Zero-Trust identity protection integration with IDaaS solutions including Okta, Ping, and Thales. This allows for user identity authentication with Single Sign-On (SSO) and Multi-Factor Authentication (MFA), and enables management of access with Adaptive Access Controls.
- Restrict file sharing on unmanaged devices and external domains through SharePoint, OneDrive, or other collaboration applications.
- Detect and block suspicious login times/locations. For example, identifying an attempted log-in from overseas only two hours after the user logged in from North America.



Enforcing Policies to Classify and Protect Sensitive Data in Office 365

As cloud security requirements continue to rapidly mature, financial orgaizations are seeking integrated data protection capabilities that can effectively defend confidential information, including PII or PCI data, shared across multiple collaboration applications. Furthermore, these requirements must extend and adapt to support employees, business partners, and other third-party contractors using both managed and unmanaged devices, from any location.

CipherCloud's industry-leading Data Discovery, Data Loss Prevention (DLP), Rights Management, and end-to-end encryption capabilities extend data security controls to the cloud and enable the use of centralized policies to monitor, classify and protect sensitive data across Office 365 applications and emails.

To help lock down Office 365 data Data Discovery enables organizations to:

- Scan content with DLP policies to protect sensitive information, such as PII, PCI, and PHI data through data classification, rules enforcement, encryption, masking, watermarking, quarantining, or deletion.
- Enable extensive data protection controls for real-time collaboration, including logging, notification, denial, and removal of public links and external collaborators, step-up authentication, application of data classification labels, encryption of files to protect data during downloads, user coaching, document highlighting, redaction, watermarking, permanent deletion, and/or user remediation.
- Classify sensitive data for full visibility into and protection across multiple Office 365 applications, users, and devices - securing intellectual property and other protected information from unintended data exposure.
- Apply 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.
- Utilize CipherCloud Key Management to enable the use of either cloud provider keys or bring your own keys [BYOK] to encrypt data. Data encryption keys are held by customers and never shared with cloud service providers, ensuring control over the protected data.
- Optical Character Recognition (OCR) enables the detection of sensitive information in image files that have been uploaded to the cloud. OCR protection can also be applied to fiules that include imaghes; for example, a PDF or a Microsoft Word file.

Applying Rights Management to Secure Data During Downloads

With the growing use of personal devices for collaboration across Office 365, organizations require end-to-end data protection capabilities as the information travels outside the cloud environment.

CipherCloud's Enterprise Digital Rights Management (EDRM) enforces data protection controls on sensitive data in the cloud by applying automatic encryption. Based on the level of data sensitivity, our EDRM will automatically envelop the data with advanced encryption to enable secure collabora-tion even via email and downloads. Sensitive data downloads are permissible only on managed devices, and only by authorized users who would be given permissions to decrypt the downloaded files using Lookout's lighweight EDRM client.

Lookout's EDRM delivers:

- Full visibility into any data accessed and downloaded by internal and external users, including customers, vendors, and partners.
- Complete ownership and control over data, regardless of where it is being shared. Decryption key revocation and retraction of access in real-time to protect sensitive data on lost or stolen devices.
- Remote control over data with ActiveSync proxy integration. Users can block a connected device or remote wipe the Microsoft Teams content from an endpoint device based on the current device or user risk posture.
- Restriction of file and folder sharing with external group and personal devices on collaboration applications like Microsoft Teams.

Monitoring User Activity to Identify Anomalous Behavior and Threats

Increased use of the cloud poses added malware challenges as threats that are shared between clouds often bypass conventional network anti-virus systems. Viruses, shared by users as attachments or links, can also propagate rapidly through the cloud and cause damage on a massive scale.

Lookout addresses this growing wave of cybersecurity threats by aggregating and correlating related data from the enterprise network, cloud, SaaS, and mobile environments, offering complete visibility into these risks as they occur including:

- Zero-day threat protection for Office 365 applications and email, with industry-leading detection rates. Lookout's integrated anti-virus anti-malware (AVAM) solution scans all inbound and outbound cloud content to defend against viruses, malware, and ransomware and quarantines infected content on the fly, without adding any noticeable latency. Additionally, URL link protection and on-premise sandbox integration allow detection and remediation for even the most challenging Zero-Day threats.

- User and Entity Behavior Analytics (UEBA) that continuously assess the standing of users, devices, and activities within applications to detect real-time anomalous behavior in Office 365 based on variations from anomal cloud usage patterns. Examples of such anomalies might be an abnormally large number of downloads from an individual user, an unusually high volume of login attempts from the same user, or persistant login attempts by an unauthorized account.

- Integration with multiple SIEM solutions including, HP ArcSight, IBM QRadar, Intel Security, LogRhythm, and Splunk, extend user activity log collection from on-prem to the cloud, automating incident management with centralized analysis and reporting of organization's security events.

Automating Assessment of Cloud Security Posture to Remediate Misconfigurations

With the growing cloud popularity and adoption, organizations migrating their business-critical applications to the cloud often overlook a critical cloud security consideration – that being, how to automate security posture across multiple SaaS applications including Office 365, Box, SAP, and Salesforce to reduce the risk of data loss due to configuration error or human oversight.

Lookout's SaaS Security Posture Management (SSPM) offers centralized visibility into all Office 365 security requirements, performing an automated assessment and remediation against industry best practice. SSPM provides both top down and granular view of cloud risk posture in financial organizations through intuitive and drill-down dashboards, real-time alerts, and detailed audit reporting.

Lookout CSB SSPM also includes:

- Extensive templates and rule sets to monitor configurations and remediate misconfigurations automatically.
- Privileged user activity monitoring.
- Scheduling options for continuous compliance with data protection laws including, GDPR, CCPA, HIPAA, PCI, GLBA, SOX, and more.

Integration with Microsoft Services

Lookout CASB integrates with the full gamut of native Microsoft services and controls to provide end-to-end cloud security and data protection, including:

- **Data Classification**
  Integration with Microsoft Information Protection (MIP) to extend data classification and governance to any Office 365 document in any application, including non-Office 365 clouds.

- **Endpoint Security Controls**
  CASB supports Microsoft ActiveSync protocol, allowing enterprises to apply controls for real-time Sync and Send activities for Office 265 apps on any end-user device, including BYOD. ActiveSync also enables device discovery and selective deletion of data from the end-user devices.

- **External Digital Rights Management**
  Integration with Microsoft's Digital Rights Management (DRM) to protect the data downloaded from an Office 365 application to a user device based on predefined policies, including defining what devices are allowed to access the data. For example, users cannot use personal devices to access sensitive data.

Case Study: Leading US Bank uses Office 365 to Securely Collaborate with Millions of Clients

The Challenge:

A large US bank with an extended remote workforce sought to securely collaborate both internally and with externally parties including customers, using Microsoft Teams to simplify file sharing and streamline communications. The bank's loan officers specifically needed to interact directly with consumers, and in some cases share sensitive data related to products including home, auto, and personal loans. This was done using Office 365 services to upload the required documents. While these services anre sanctioned by IT, there was still significant potential for loss of visibility and control over data going to the cloud.

Project Goals:

- Quickly address the expanding work from the home environment for a large number of it's staff.
- Securely standardize on cloud apps for file sharing, virtual meetings, and company-wide collaboration.
- Protect PII, PCI data across all files and endpoints, while unsuring compliance with mandated financial regulations.

Solution:

Lookout CASB provided an integrated cloud security and data protection platform for security services required to protect financial data across multiple Office 365 collaboration applications and email services. Specific capabilities utilized were data loss prevention (DLP) policies with ethical firewalls, secure user access delivered through adaptive access control, protection against malicious behavior by internal or external parties, and advanced malware threat protection.

CipherCloud Differentiation:

A one-stop solution: Lookout is the only CASB vendor enabling data protection and governance across every key element of the Office 365 suite.
Deployment scale: Lookout has the experience (9+ years) in delivering security solutions at scale to service tens of thousands of cloud users constantly engaged in mission-criticalwork.
Business-ready security: Best-in-class cloud security, preserving overall Office 365 user experience and cloud functionality.

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 Top10 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.

