Lookout®

SOLUTION BRIEF

Lookout CASB for Microsoft Office 365

Overcoming SaaS security challenges
to protect data and minimize business risk

Microsoft Office 365 is one of the most popular SaaS productivity tools to get your enterprise organization up and running in the cloud. However, it can create unforeseen security challenges that must be managed. Firewalls, IDS, IPS, host DLP, and other perimeter security controls don't work in the cloud. The protective borders that encircled data centers and networks no longer exist because your remote workforce and apps have left the building.

Managed endpoints have transitioned to unmanaged personal devices. Data now goes everywhere it's needed. And workers expect instant access to the Office 365 productivity suite from anywhere and on any device. As enterprise organizations scramble to adapt to this new business reality, they are weighing the challenges of keeping corporate data secure and minimizing risk during this massive shift to the cloud.

Lookout has the answer. We pioneered the zero-trust model, founded on the idea that every use of corporate data – from mobile endpoints to the cloud – must be analyzed and controlled based on the operational awareness of identity and context. We have applied these tenets to Lookout CASB to help you cope with the collapse of the perimeter and focus on the two inseparable things that matter most: Data protection and reduced business risk.

Office 365: Welcome to the cloud

Your journey to Office 365 will expose you to some universal SaaS security challenges. Most of those challenges won't be unique to Office 365. But they can serve as powerful practical use-cases to help you design security strategies you can apply to your entire SaaS portfolio.

Let's examine how simple file sharing and email change dramatically with Office 365.

File sharing

Traditional office

- Data stored in managed data centers
- Access controlled at the network edge
- File-sharing decisions centralized and controlled
- Remote access via VPNs

Office 365

- Data stored in Microsoft infrastructure
- Access controls are based on identity, not network factors
- OneDrive and SharePoint simplify user-driven file sharing
- Multimode remote access (mobile, web, API)

Security implications

- The network edge is no longer a control point
- Policy enforcement evolves from "control access to trusted network" to "control access to sensitive data"
- Good-faith users can make devastating security mistakes
- Unmanaged mobile endpoints are more vulnerable to malware

Email

Traditional office

- On-premise Microsoft Exchange servers
- Controlled and managed endpoints
- Tightly controlled remote access

Office 365

- Public cloud-hosted Microsoft Exchange servers
- Any endpoint, any device, multimode access
- Remote access is seamless and transparent

Security implications

- Network-based control points are no longer available
- Unmanaged mobile endpoints expose sensitive data
- Integrated solution makes sharing via email easier and more prone to errors with major consequences

It's a real conundrum: Office 365 reduces user friction while jeopardizing security. To make matters worse, it is difficult to know where Microsoft's security responsibilities end and yours begin.

The shared-security model

In an Office 365 SaaS deployment, you and Microsoft have different responsibilities. The division of labor – called the shared-security model – is a widely applied cloud security concept coined by Amazon Web Services (AWS). Understanding shared security is essential if you want to build a solid cloud security infrastructure. In simple terms, Microsoft is accountable for the security of the cloud itself while you are responsible for security in the cloud. Here are a few examples that illustrate the difference. In the context of a zero-trust security model, your Office 365 responsibilities can appear daunting. With zero trust, every interaction with your data demands a tailored security response. Signals about user context, behaviors, devices and roles must be evaluated alongside information about the data, its sensitivity, format, and destination. Critical policy decisions must be made in real time. And Office 365 likely isn't the only cloud service in use. Salesforce, Box, ServiceNow, and other cloud services need the same protection.

Microsoft

- Physical security of servers and networks
- Compliance with regulatory demands related to the infrastructure itself
- App security, such as ensuring that Microsoft Excel is secure
- Protection of administrative interfaces
- Identity and access management tools

Office 365 subscriber

- Security of data and proprietary information
- Compliance with regulatory demands related to data protection
- Security of business processes and IT practices
- Protection of data access interfaces
- User account policies and privileges
- Policy creation and deployment
- Breach forensics and remediation
- Device configuration and ongoing management

The answer: Lookout CASB

According to Gartner, a cloud access security broker (CASB) is the No. 1 priority for security and risk management leaders. Drawing on our pioneering work in data security for cloud apps, Lookout CASB protects and manages every aspect of your use of Office 365. We also protect other cloud services, making Lookout CASB simple and efficient for all your SaaS rollouts.

CASB protects Office 365 data in transit (as it flows to its destination) and at rest (stored in the Microsoft data center). In-transit protection uses a clientless, reverse-proxy architecture while our at-rest services take advantage of interfaces provided by the Microsoft API architecture.

To protect data in transit, Lookout CASB intercepts cloud traffic before it leaves your organization's control. We perform real-time analysis to determine if the interaction (and the data it contains) complies with your policies. For example, CASB can spot files that contain PII, social security numbers and credit card numbers. We augment that analysis with users' roles, their current location and time zone, and other signals to determine the appropriate policy response. The response can include blocking the transaction, encrypting sensitive data on the fly, and redirecting users so they can work without storing a file locally.

Lookout CASB also reviews files and information stored on Microsoft servers to keep sensitive information out of the cloud. Files are scanned for watermarks, keywords, character patterns, header content, and other indicators so you can quickly fix violations and stay on the right side of data residency compliance rules.

Office 365 email data protection

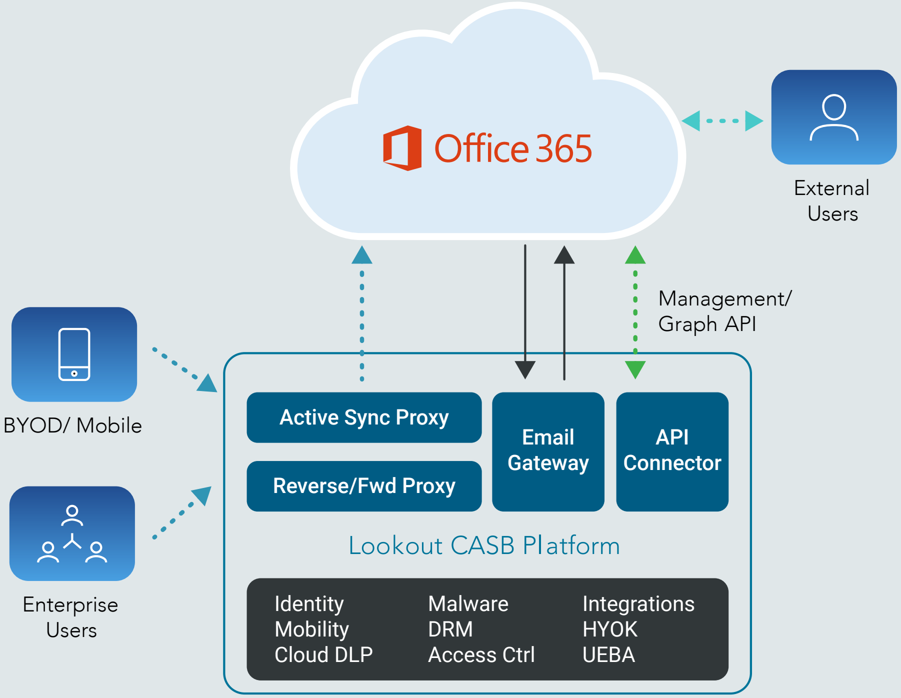
To protect Office 365 emails in motion, Lookout integrates the industry's fastest secure email gateway with CASB. This routes emails from any desktop, mobile device or browser through a secure dedicated gateway for protection. This gateway expands CASB coverage for Office 365, enabling deep visibility into corporate email usage and unprecedented audit capabilities with inline email DLP policies, including:

- Identifying and masking sensitive information in email subject and body.
- Scanning email content and protection by classifying, watermarking, quarantining, or deleting.
- Encrypting email attachments.
- Detecting zero-day threats and malware in email content.

Lookout CASB makes it possible to implement true zero-trust data protection without the overhead of client software. We integrate the widest range of policy enforcement tools, the broadest set of signals to assess risk, and the most flexible deployment models available today.

Email protection

- **Secure email gateway:** All emails are routed through a secure email gateway for DLP actions and malware threat prevention. Policies are enforced on emails before they are delivered to recipients.
- **Email ActiveSync proxy:** The Microsoft ActiveSync protocol lets you apply controls to real-time sync and send activities for Office 365 emails. This feature also enables device discovery and remote wiping of mobile data (email and calendar events).
- **Outlook-on-the-web access (OWA) security:** Adaptive access controls are applied to browser-based OWA. Policies are enforced using the configured access context.



Microsoft Office 365 security scenarios

Using Office 365 with unmanaged devices

Challenges

- User-owned and unmanaged devices access sensitive data
- Travelers use unsecure, shared kiosk computers to access Office 365

Consequences

- Files left behind on public computers spill data
- Device loss or compromise creates a compliance event
- Reputational damage, fines and lawsuits

Lookout CASB

- Intercept all data before it reaches any device – managed or not
- Evaluate a wide range of security signals, including location, device posture, data sensitivity, and more
- Offer a broad menu of control policies for every situation, including:
    - Block, quarantine or mask all Office 365 traffic
    - Encrypt attachments with revocable keys before sending
    - Redirect users to an online Office 365 app to avoid file download
    - Remotely wipe devices

Advantages

Best coverage

- Effective on unmanaged devices and kiosk computers
- Works across all Office 365 products
- Same platform also supports other cloud services like Box, Salesforce and ServiceNow
- Available Microsoft Azure Information Protection for file classification and labeling

Richest set of security signals

- Track users across multiple cloud services beyond Office 365
- Rich device posture information via integrated third-party device management (EMM/EDM) solutions

More options for user-friendly policy enforcement

- Revocable file access with integrated Digital Rights Management (DRM)
- Context-aware redirection sends users to online Office 365 alternatives that don't require file downloads
- Block, warn or simply log violations

OneDrive misuse

Challenges

- OneDrive users are empowered to make file-sharing decisions
- Enables good-faith users to make bad decisions
- Complex detection environment allows sharing to occur via Outlook, clickable links and public permissions
- Policies and regulations preclude storing certain files on OneDrive

Consequences

- Compliance violations and mandatory disclosure
- Fines and expensive remediation
- Loss of reputation and customer trust
- Spills of proprietary information such as customer lists or product secrets

Lookout CASB

- Uses Microsoft-sanctioned Office 365 APIs to scan files for sensitive data
- Assesses policy compliance based on multiple signals like file type and sensitivity, file content, user role, and sharing intent
- Enforcement options balance security with the user experience

Advantages

Fast detection of violations

- Real-time event awareness and analysis
- Fully automated for nonstop protection

Richest set of detection tools

- Powerful DLP engine detects keywords, file types, structured data, watermarks, text patterns, and more
- Powerful rules engine for customized protection
- Off-the-shelf rule templates focused on regulatory regimes or business processes for fast adoption

Flexible enforcement

- Block, quarantine, delete, coach, and notify
- Reduce user frustration by guiding them to policy-compliant options

Insider attacks and compromised accounts

Challenges

- Well-resourced cybercriminals are increasingly adept at cracking account credentials
- Disgruntled employees steal or misuse data for profit or revenge

Consequences

- Catastrophic data loss
- Crippling operational damage that negatively affects business operations and responsiveness

Lookout CASB

- Implements user and entity behavior analytics to identify and |respond to anomalies
- Correlates anomalous behaviors across all cloud services, not just Office 365
- Correlates anomalous behaviors across every entry point, not just managed devices
- Instantly protects data before it reaches the endpoint

Advantages

- Low administrative investment with configuration-free machine learnin
- Comprehensive security across all cloud services and access controls for managed and unmanaged devices

Confidential emails and information leaks

Challenges

- Employees send emails with sensitive content to external domains or external teams
- Sharing data with another collaboration app outside of Office 365, such as emails to Box or Slack

Consequences

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

Lookout CASB

- Monitors and processes every email coming into and going out of a cloud app via secure email gateway
- Advanced email DLP policies:
  - Encrypts emails and attachments before sending to Office 365 server
  - Dynamically removes unknown and unauthorized recipients from mailing lists before sending out emails

Advantages

- Only CASB that provides inline email DLP support
- Single pane of glass for email security, collaboration apps and infrastructure
- Adaptive app intelligence for collaboration apps in Office365 and all trusted apps like Slack and Box
  - Ethical firewalling
  - Granular file-sharing controls
  - Stateful inspection of data with app intelligence and semantics

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.**

For more information visit
lookout.com

To learn more about Lookout CASB, visit
lookout.com/products/cloud-access-security-broker