



SECURING THE WHENEVER, WHEREVER, WORKFORCE

A Cybersecurity Professional's Guide to
Security for the Mobile-Cloud Era

 **FORCEPOINT**
POWERED BY Raytheon



Contents

- 3** KEEPING UP WITH THE INCREASING SECURITY RISK OF THE MOBILE-CLOUD ERA
- 4** SECURITY CHALLENGE: CLOUD APPS AND MOBILE DEVICES
- 5** THE SECURITY BLIND SPOTS INHERENT IN THE BYO WORLD
- 6** WHY SECURITY FROM CLOUD AND CLOUD APPLICATION PROVIDERS ISN'T ENOUGH
- 7** SECURITY STARTS WITH YOUR MOBILE WORKERS
- 8** MUST-HAVE CASB FUNCTIONALITY FOR SECURING MOBILE-CLOUD USE CASES
- 10** THE RIGHT CHOICE FOR MOBILE-CLOUD SECURITY
- 11** FORCEPOINT CASB
- 13** REAL-WORLD EXAMPLES OF SECURING MOBILE-CLOUD ACCESS
- 14** NEXT STEPS

KEEPING UP WITH THE INCREASING SECURITY RISK OF THE MOBILE-CLOUD ERA

The two megatrends of cloud-based applications and mobile devices have been a boon for company productivity, agility, and innovation. The mobile-cloud combo empowers employees to work and be productive literally anywhere.

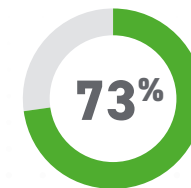
However, the mobile-cloud era has created a conundrum for cybersecurity teams: how to secure mobile devices (particularly unmanaged bring-your-own devices (BYOD)) accessing cloud applications (which may or may not be sanctioned by IT) that store sensitive corporate data outside the control of traditional on-premises security solutions.

It's a challenge that grows more critical—and difficult—to surmount on a daily basis as various parts of the

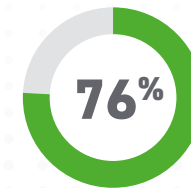
business continue to adopt software-as-a-service (SaaS) at an unprecedented rate. Security teams question how they can secure what their companies don't control or even own. How can they protect against both intentional and unintentional data leakage stemming from users accessing cloud applications from a variety of devices, including their own personal ones?

The short answer is to focus on securing people, protecting them from compromise as they use the cloud from any location, on any device. This guide highlights the security challenges and gaps in visibility that cybersecurity teams face and what they can do to mitigate the risk inherent in the mobile-cloud world.

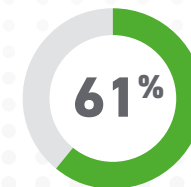
The rise of the remote/ mobile worker



NEED TO WORK REMOTELY



NEED TO ACCESS COMPANY DOCUMENTS AWAY FROM THE OFFICE



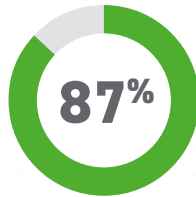
NEED TO ACCESS COMPANY DATA ON THEIR OWN DEVICES

Source: Nexsan, "Security and Speed Top Barriers to a Truly Connected Workforce, Survey Reveals," June 7, 2016.

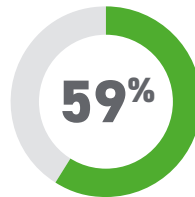
SECURITY CHALLENGE: CLOUD APPS AND MOBILE DEVICES

1.87
BILLION 

MOBILE WORKERS AROUND THE GLOBE BY 2022, REPRESENTING 42.5% OF THE GLOBAL WORKFORCE



COMPANIES THAT RELY ON EMPLOYEES HAVING ACCESS TO MOBILE BUSINESS APPS FROM THEIR PERSONAL SMARTPHONES



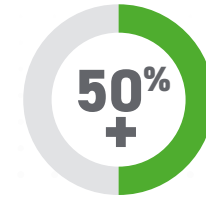
ORGANIZATIONS THAT HAVE A FORMAL BYOD POLICY



600 TO 1,000
SAAS APPS
USED AT A TYPICAL COMPANY



THE PORTION OF SUCCESSFUL ATTACKS EXPERIENCED BY ENTERPRISES THAT WILL TARGET THEIR SHADOW IT RESOURCES BY 2020







IT SPENDING FOR SHADOW IT IN LARGE ENTERPRISES

THE SECURITY BLIND SPOTS INHERENT IN THE BYO WORLD

When the devices being used by employees are owned and managed by your company and the applications employees are using are hosted within your own datacenter, it's easier to provide adequate protection against cyberthreats. But let's face it, this scenario is starting to become an increasingly rare occurrence.

The more likely situation today is trending towards a BYO-everything environment with employees or their business departments providing their own devices, internet access, applications, and more. This rise in mobile devices together with the growing use of cloud-based applications for everything from email to customer relationship management to financial reporting has given rise to a number of blind spots and security problem areas for security teams.

SCENARIO		SECURITY GAP
Authorized users accessing approved cloud applications from unmanaged endpoint devices		Unmanaged endpoints are vulnerable to breaches and other exploits that can steal legitimate credentials.
Authorized users accessing unapproved cloud applications (shadow IT) from unmanaged devices		Organizations can't enforce endpoint protection—even when using enterprise mobile management or mobile device management solutions—on unmanaged personal devices that access unsanctioned cloud applications over public, mobile, and wireless networks.
Authorized users accessing approved cloud applications on managed devices		Managed devices can be vulnerable to insider abuse, attacks, and theft.
Unauthorized users (that is, cybercriminals or insiders with malicious intent) using stolen credentials to access cloud applications (both approved and unapproved)		Approved cloud applications can be targets for account takeovers and malicious insider threats. Security teams have no visibility into company usage and storage of sensitive corporate data in unapproved cloud applications.

By 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.

Source: Gartner, "CASB Platforms Deliver the Best Features and Performance," February 24, 2017.

WHY SECURITY FROM CLOUD AND CLOUD APPLICATION PROVIDERS ISN'T ENOUGH

Given the incredible uptake by companies of all sizes, you'd think that cloud and cloud application providers would be highly focused on providing security capabilities that address mobile/cloud application security blind spots. And to be clear, to some extent, they do provide capabilities that help.

However, security in the cloud is most often a shared responsibility. At the simplest level, the cloud provider is responsible for the security of the infrastructure while its customers are responsible for their data and user activities on top of that infrastructure.

This means that security aspects such as user behavior, access and usage

policies, and compliance are your organization's responsibility. The same holds true for unmanaged devices. Cloud application providers generally don't distinguish between managed and unmanaged devices, nor do they provide compensating endpoint control capabilities.

It's up to your company to secure access to cloud applications by both managed and unmanaged devices, as well as protect users and data, and detect and prevent cyberthreats.



By 2018, 40% of Office 365 deployments will rely on third-party tools to fill in gaps in security and compliance, which is a major increase from fewer than 10% in 2015.

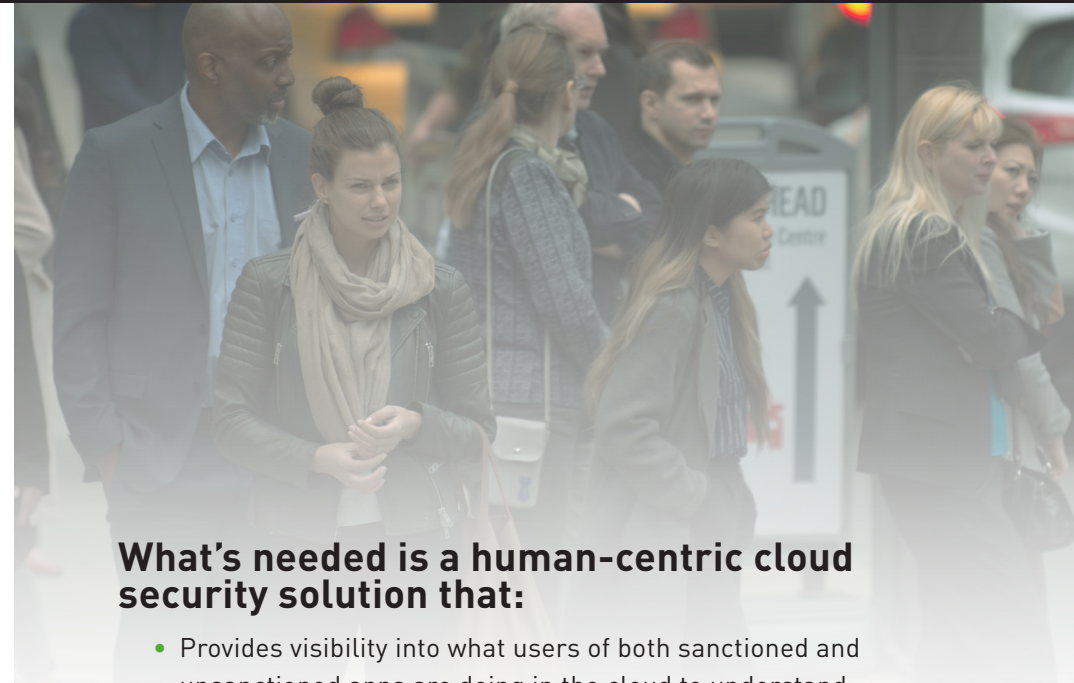
Source: Gartner, "CASB Platforms Deliver the Best Features and Performance," February 24, 2017.

SECURITY STARTS WITH YOUR MOBILE WORKERS

Every security team knows that network perimeter defenses and endpoint protection aren't the answers when it comes to securing mobile workers. After all, employees today rely on a dizzying combination of sanctioned and unsanctioned cloud applications and managed and unmanaged devices.

So what is the answer? It's focusing on the one common denominator across all the scenarios: the human. Visibility into user and entity behavior must become the focal point of your security efforts.

Insight into usage patterns and device profiles enable proactive policy enforcement and account protections across managed and unmanaged endpoints. This insight gives you a way to surface and respond to abnormal user activity to protect both your users and data in the cloud.



What's needed is a human-centric cloud security solution that:

- Provides visibility into what users of both sanctioned and unsanctioned apps are doing in the cloud to understand risks and protect users and data
- Monitors and controls how users interact with any cloud application
- Identifies users at risk and prevents risky usage
- Enables policies and protections that are specific to users accessing cloud apps on BYOD (unmanaged) devices
- Delivers data loss prevention (DLP) to protect data at rest in the cloud and data in transit

Increasingly, this type of solution is a set of functionality called a cloud access security broker (CASB).

“ “ **By 2020, 85% of large enterprises will use a cloud access security broker platform for their cloud services, which is up from less than 5% today.**

Source: Gartner, "Market Guide for Cloud Access Security Brokers," October 24, 2016.

MUST-HAVE CASB FUNCTIONALITY FOR SECURING MOBILE-CLOUD USE CASES

CASB functionality provides enterprises with visibility and control over usage of cloud applications. The right solution can help your organization secure mobile users on both managed and unmanaged devices as they access sanctioned and unsanctioned cloud applications.

Not all CASB offerings deliver the robust set of capabilities and support for all cloud applications that enterprises need to secure all of their use cases. To address the mobile-cloud use cases presented earlier, look for a full-featured CASB solution that includes the following functionality.

SCENARIO 1

Authorized users accessing approved cloud applications from unmanaged endpoint devices



CASB FUNCTIONALITY

- Applies granular policies, including DLP policies, for both managed and unmanaged laptops, tablets, and mobile phones (browser or rich mobile applications) to potentially limit uploads, downloads, and sharing of sensitive data based on destination, user, or application
- Inspects files and content in real time to ensure that sensitive information stays protected

SCENARIO 2

Authorized users accessing approved cloud applications on managed devices



CASB FUNCTIONALITY

- Employs user and entity behavior analysis (UEBA) to observe user behaviors and detect anomalies to identify and minimize risk as users use cloud applications
- Enforces controls that ensure the safe and productive use of any cloud application
- Includes threat and risk detection for account takeover and brute force attacks as well as detecting anomalous data usage from unusual locations and session hijacking
- Leverages existing data protection policies to prevent data loss for data at rest and data in transit
- Detects malicious code embedded into documents stored on cloud-storage solutions that could execute a ransomware attack once downloaded into your network

MUST-HAVE CASB FUNCTIONALITY FOR SECURING MOBILE-CLOUD USE CASES

SCENARIO 3

Authorized users accessing unsanctioned cloud apps (shadow IT) from unmanaged devices



CASB FUNCTIONALITY

- Discovers cloud applications from network log files from your firewall, proxy, router, and other sources
- Helps you manage unsanctioned cloud applications once they've been discovered
- Blocks high-risk applications from being accessed by any device from within the network

SCENARIO 4

Cybercriminals/malicious insiders using stolen credentials to access cloud applications



CASB FUNCTIONALITY

- Employs UEBA to detect anomalies and protect and remediate account takeover threats in real time
- Detects user account behavior that is anomalous relative to automatically-learned usual behavior, according to preconfigured and customizable policies
- Triggers various security actions including automatic account blocking in real time when anomalous behavior is discovered
- Discovers unsanctioned cloud applications so you can bring them under secure management to protect against cyberthreats and malicious insiders accessing the applications and data

“ “ **By 2018, the 60% of enterprises that implement appropriate cloud visibility and control will experience one-third fewer security failures.**

Source: "CASB Platforms Deliver the Best Features and Performance," Gartner, February 24, 2017.

THE RIGHT CHOICE FOR MOBILE-CLOUD SECURITY

As a leader in cloud application visibility and control, Forcepoint understands that human behavior is at the center of the security equation, particularly when it comes to mobile workers. Human-centricity and knowledge of critical data and intellectual property underpin the Forcepoint philosophy for our cloud security solutions.

Understanding user behavior and intent is the determining factor necessary to distinguish an employee making an honest mistake from a malicious insider or a user who's been compromised. This insight enables Forcepoint to stop the bad and free the good—stopping bad cyber activity while allowing people to do good work.

This is the approach we use to address the mobile-cloud world with capabilities such as CASB.

Forcepoint CASB

With Forcepoint CASB, you gain visibility into how users are using cloud applications, which cloud applications they are using, and whether they are engaging in high-risk activities. You can enforce policy and controls for users, devices, and cloud applications to prevent account-centric threats, meet compliance requirements, and protect data. You'll even find often-used CASB capabilities such as application discovery and risk reporting integrated into Forcepoint Web Security solutions, removing the need to add yet another security product to manage.



FORCEPOINT CASB

Here's what makes Forcepoint the right choice for securing today's mobile-cloud world:

- **ADVANCED UEBA:** Forcepoint CASB observes user behaviors and detects anomalies to identify and minimize risk as users use cloud applications. Your organization gains additional insights into what users are doing with data to protect them from compromise as they use the web and email from any location, on any device.
- **DEVICE CONTROL:** Forcepoint distinguishes between managed or corporate-owned devices and unmanaged/ BYOD. It uses granular security policies to give employees the flexibility to use their preferred devices without compromising security.
- **COMPREHENSIVE APPLICATION DISCOVERY:** Forcepoint uncovers cloud application usage, including the use of unsanctioned and high-risk applications.
- **SUPPORT FOR ANY CLOUD APPLICATION:** Forcepoint CASB supports any cloud application—including non-browser-based, rich applications—by inline proxy, with no changes required to the system. Forcepoint offers deep support for Microsoft Office 365, Amazon Web Services (AWS), Salesforce, Google Apps, Box, Dropbox, NetSuite, Workday, Microsoft Azure, and other popular cloud-based applications and services.
- **DATA LOSS PREVENTION:** Forcepoint CASB provides state-of-the-art DLP capabilities for data at rest in the cloud and in motion, as well as integration with market-leading Forcepoint DLP via ICAP.
- **ADVANCED MALWARE DETECTION:** Forcepoint CASB integrates with Forcepoint Advanced Malware Detection, a high-performance malware analysis platform that provides deep content inspection and interacts with malware to entice it into execution to be blocked or alerted on.
- **FLEXIBLE DEPLOYMENT:** Forcepoint delivers full out-of-band (API mode) and inline (proxy mode) capabilities that include real-time blocking and multifactor authentication.

THE RIGHT CHOICE FOR MOBILE-CLOUD SECURITY

Corporate Employees, Mobile
Workers and Hackers



Google G Suite



Forcepoint CASB Solution Components

GOVERNANCE

- Discover shadow IT apps & assess risk
- Discover & manage sensitive data in cloud file-sharing apps
- Identify admins and inactive, external, and former employees
- Centrally assess data and security configuration settings
- SIEM enablement

AUDIT & PROTECTION

- Detect behavioral anomalies & prevent attacks in real time
- Real-time & API-based, comprehensive user activity monitoring
- Control sensitive data with DLP policies
- Enforce risk-based MFA
- Prevent data proliferation to unmanaged devices

SECURITY SUITE

- All capabilities from Governance and Audit & Protection

REAL-WORLD EXAMPLES OF SECURING MOBILE- CLOUD ACCESS



Banking

Metro Bank provides unparalleled levels of service and convenience to its customers. When it comes to IT, Metro Bank is an innovator as well, with an emphasis on enabling its 1,400 colleagues across the UK to communicate and collaborate effectively. The bank deployed Forcepoint CASB to secure off-network access to Microsoft Office 365 and control BYOD access effectively while improving employee productivity.



Pharmaceutical

A top pharmaceutical manufacturer for generics needed to control managed and unmanaged device access by employees. Forcepoint CASB provides the manufacturer with device fingerprinting and behavior-based anomaly detection, as well as detection of user credential account takeover attacks and activity auditing.



Entertainment

The largest music corporation in the world needed to manage Microsoft Office 365 access from BYOD users. Forcepoint CASB provides visibility and control of devices, a complete audit trail of all actions performed on all Office 365 applications, and real-time detection and prevention of account takeovers.



NEXT STEPS

**Learn more about Forcepoint CASB at
www.forcepoint.com/cloud-app-security.**

About Forcepoint

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit www.Forcepoint.com and follow us on Twitter at @ForcepointSec.