Forcepoint

CW Squared

Ebook

Securing Your Wherever, Whenever Workforce

A Cybersecurity Professional's Guide to Today's Hyper-connected World

Table of Contents

Keeping Up: Security Risks in Today's Hyper-connected World

Mobile devices and cloud-based applications that empower teams to work anywhere have been a boon for business productivity, agility, and innovation. However, this new way of working presents a new challenge for cybersecurity teams: securing mobile devices accessing cloud applications that store sensitive data outside the control of on-premises security solutions.

It's a challenge that grows more critical as businesses continue to adopt software-as-a-service (SaaS) at an unprecedented rate. And it raises big questions for security teams:

- → How do we secure what the company doesn't control or even own?
- → How can we protect against intentional and unintentional data leakage from users accessing cloud applications from a variety of devices, including their own personal ones?

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

Keeping Up: Security Risks in Today's Hyper-connected World

Security Blind Spots in the BYO World

Your security team would probably agree that the ideal state includes employees using devices that are owned and managed by your company and applications that are hosted within your own datacenter.

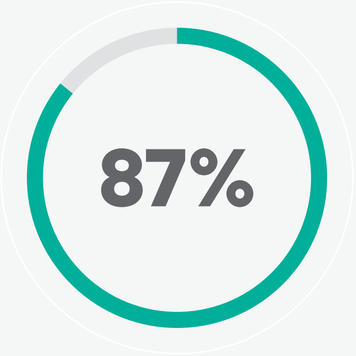
However, such a scenario is growing increasingly rare. The real state is trending toward a BYO-everything environment, with employees or their departments providing their own devices, internet access, applications, and more. This rise in mobile devices combined with the growth of cloud-based applications—for everything from email to customer relationship management to financial reporting—has created new problem areas for security teams.

600 to 1,000

SAAS APPS used at a typical company

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

IT spending for shadow IT in large enterprises

The Truth About Security from Cloud and Cloud Application Providers

You'd think that cloud and cloud application providers would be highly focused on addressing mobile/cloud application security blind spots.

And to some extent, they do provide capabilities that help. However, cloud security is most often a shared responsibility: The cloud provider sees to its own infrastructure security, leaving customers to secure their data and user activities on top of that infrastructure. This means your business is responsible for elements such as user behavior, access and usage policies, and compliance.

The same holds true for unmanaged devices. Cloud application providers generally don't distinguish between managed and unmanaged devices, nor do they provide endpoint control to compensate. It's up to your company to secure access to cloud applications by both managed and unmanaged devices, protect users and data, and detect and prevent cyberthreats.

The Truth About Security from Cloud and Cloud Application Providers

Security Starts with Your Mobile Workers

Employees today rely on a dizzying combination of sanctioned and unsanctioned cloud applications and managed and unmanaged devices. And, as any security team would tell you, network perimeter defenses and endpoint protection aren't enough.

So—what is the answer? It's focusing on the common denominator across all the scenarios: the human. So, to secure your wherever, whenever workforce, visibility into human behavior must take a front seat.

Insight into usage patterns and device profiles makes it possible to enforce policies proactively and exercise account protections across managed and unmanaged endpoints. The result? This is your key to identifying and responding to abnormal activity to protect both your users and data in the cloud.

The Case for Cloud Access Security Brokers

Given the shared responsibility debacle of cloud and cloud application providers, many organizations are taking matters into their own hands (or rather, those of a professional) by adopting a Cloud Access Security Broker (CASB). Acting as a second line of defense between cloud providers and cloud users, CASBs will be used by 66% of enterprise businesses by 2022.

By 2022, 60% of large enterprises will use CASBs, up from 20% at the end of 2018.

GARTNER, "MAGIC QUADRANT FOR CLOUD ACCESS SECURITY BROKERS,"
OCTOBER 29, 2018

Optimizing Mobile-cloud Security with the Right CASB

Understanding human behavior and intent is the only way to distinguish an employee's honest mistake from a malicious insider or compromised user. This insight enables us to stop the bad and free the good—halting detrimental activity while allowing people to do good work. It's an approach that can extend to numerous mobile-cloud capabilities, including CASB.

Optimizing Mobile-cloud Security with the Right CASB

Security Starts with Your Mobile Workers

With the most robust CASB solutions, you can gain visibility into how people are using cloud applications, which 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 the vendor's web security solutions, removing the need to add yet another security product to manage.

Here are seven features critical for security in today's hyper-connected world:

Advanced UEBA:
Observes human behaviors and detects anomalies to identify and minimize risk. 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:
Distinguishes between managed and unmanaged devices, with granular security policies to give employees the flexibility to use their preferred devices without compromising security.

Comprehensive Application Discovery:
Uncovers cloud application usage, including the use of unsanctioned and high-risk applications.

Support for any Cloud Application:
Including non-browser-based, rich applications—by inline proxy, with no changes required to the system.

Data Loss Prevention:
Secures data at rest in the cloud and in motion and integrates with market-leading Forcepoint DLP via ICAP.

Advanced Malware Detection:
Integrates with a high-performance malware analysis platform that inspects content and entices malware into execution so it can trigger an alert or block.

Flexible Deployment:
Full out-of-band (API mode) and inline (proxy mode) capabilities that include real-time blocking and multifactor authentication.

Optimizing Mobile-cloud Security with the Right CASB

Key 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

Enable SIEM

Audit & Protection

Detect behavioral anomalies & prevent attacks in real time

Real-time & API-based, comprehensive user activity monitoring

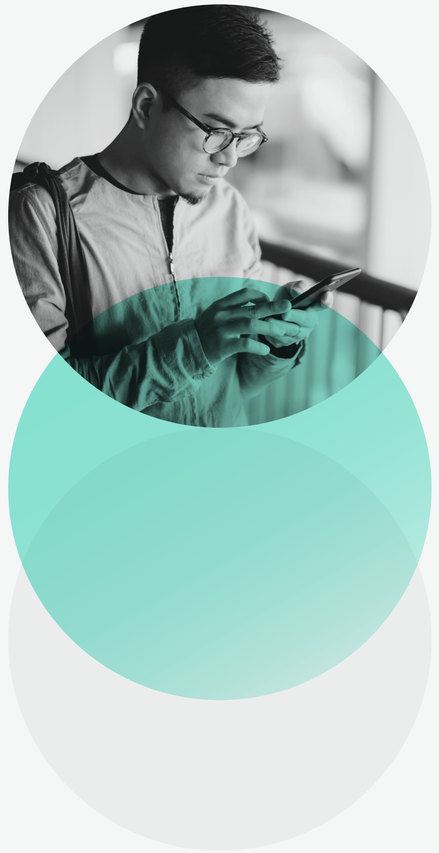
Control sensitive data with DLP policies

Enforce risk-based MFA

Prevent data proliferation to unmanaged devices

Security Suite

All capabilities from Governance and Audit & Protection



Forcepoint

CW Squared

4 Old Park Lane London W1K 1QW

T: 020 3995 4445

E: contact@cw-squared.co.uk

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

© 2020 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
[Securing-Your-Wherever-Whenever-Workforce-Ebook-USEN] 1APR2020