

# The Hidden

# Truth Behind Shadow IT

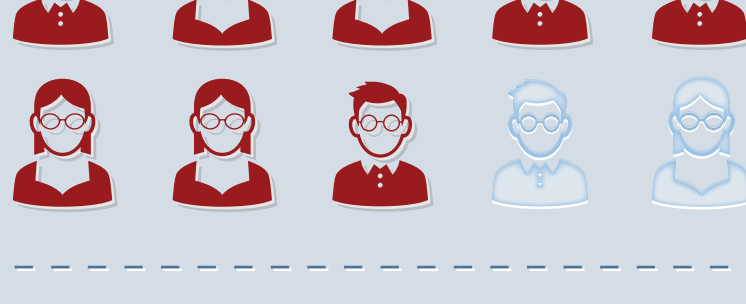
Employees are increasingly circumventing corporate IT policies to choose their own applications, thanks to the low cost and easy accessibility of cloud-based Software as a Service (SaaS). But without IT oversight and security policies applied, sensitive corporate data can be left at risk. Businesses must find a way to balance employee choice with asset protection.



## FIRST, ADMIT IT

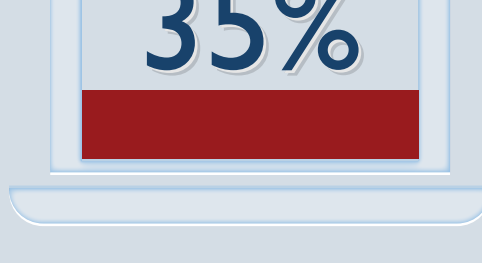
More than

# 80%



of employees admit to using SaaS applications in their jobs without IT approval

Nearly

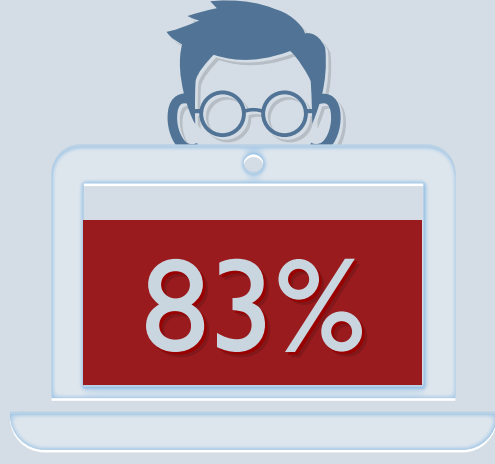


of all SaaS applications used in business are not approved, contributing to Shadow IT



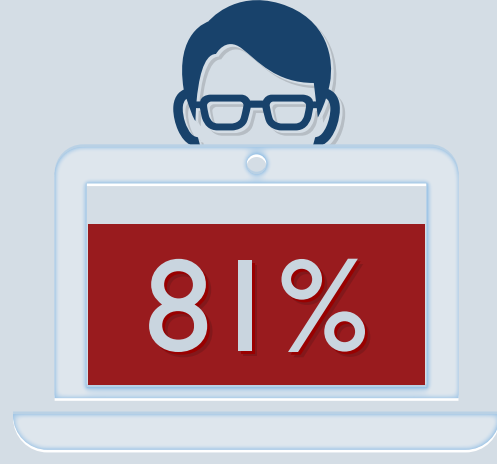
## IT PROFESSIONALS ARE THE WORST OFFENDERS

IT is more likely to use non-approved SaaS



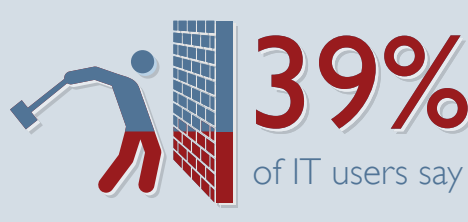
IT

vs.



Non-IT Employees

Restrictive policies aren't helping anyone



SaaS applications allow "me to bypass IT processes."



IT restrictions on applications make it difficult to do my job.



Non-approved software meets their needs better than the IT-approved equivalent.



## POPULAR APPS ARE RISKY BUSINESS

Shadow IT encompasses the most popular SaaS categories

### BUSINESS PRODUCTIVITY

(including Microsoft Office 365 and Google Apps)

# 15%

### SOCIAL MEDIA

(led by LinkedIn and Facebook)

# 12%

### FILE-SHARING, STORAGE, AND BACKUP

(including Dropbox and Microsoft Skydrive)

# 11%

Used without IT approval or policy applied

The most popular apps, approved or not, should not be left unsecured

APPS USED BY ORGANIZATIONS WITH OVER 1,000 EMPLOYEES



# 45%

Use Facebook

SECURITY EVENTS, SUCH AS MALWARE INFECTION, DATA LOSS, OR UNAUTHORIZED ACCESS



# 35%

have experienced a security event

TOP SECURITY EVENTS



# 19%

Infected by malware



# 40%

Use Google Apps



# 17%

have experienced a security event



# 27%

Leaked sensitive data



# 36%

Use Dropbox



# 16%

have experienced a security event



# 24%

Unauthorized access

On average

# 15%

of employees have experienced a security, access, or liability event while using SaaS



## RECOMMENDATIONS



### Ditch the dictatorship.

Don't block popular SaaS applications outright. Employees are often simply trying to get their jobs done.



### Be inclusive, not exclusive.

Provide access to a broad range of apps, giving employees the freedom to select what best meets their needs.



### Protect employees and corporate data.

Implement a security solution that transparently enables secure access to SaaS applications, protects against malware, and prevents data loss.



## VIEW THE FULL REPORT

at [mcafee.com/webprotection](http://mcafee.com/webprotection)

SOURCE: Stratecast | Frost & Sullivan research.

SPONSOR: McAfee, Inc.

DEFINITIONS

Shadow IT: Employees' use of non-approved SaaS applications to do their jobs.

SaaS: Software as a Service. Cloud-based applications, accessible via the Internet or other network.

© Frost & Sullivan