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 **35%** 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

83% IT vs. **81%** Non-IT Employees

Restrictive policies aren't helping anyone

39% of IT users say: SaaS applications allow "me to bypass IT processes."

18% of IT users say: IT restrictions on applications make it difficult to do my job.

24% of all users say: 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)	SOCIAL MEDIA (led by LinkedIn and Facebook)	FILE-SHARING, STORAGE, AND BACKUP (including Dropbox and Microsoft Skydrive)
15%	12%	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	SECURITY EVENTS, SUCH AS MALWARE INFECTION, DATA LOSS, OR UNAUTHORIZED ACCESS	TOP SECURITY EVENTS
45% Use Facebook	35% have experienced a security event	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

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.

Stratecast | FROST & SULLIVAN

McAfee® An Intel Company