

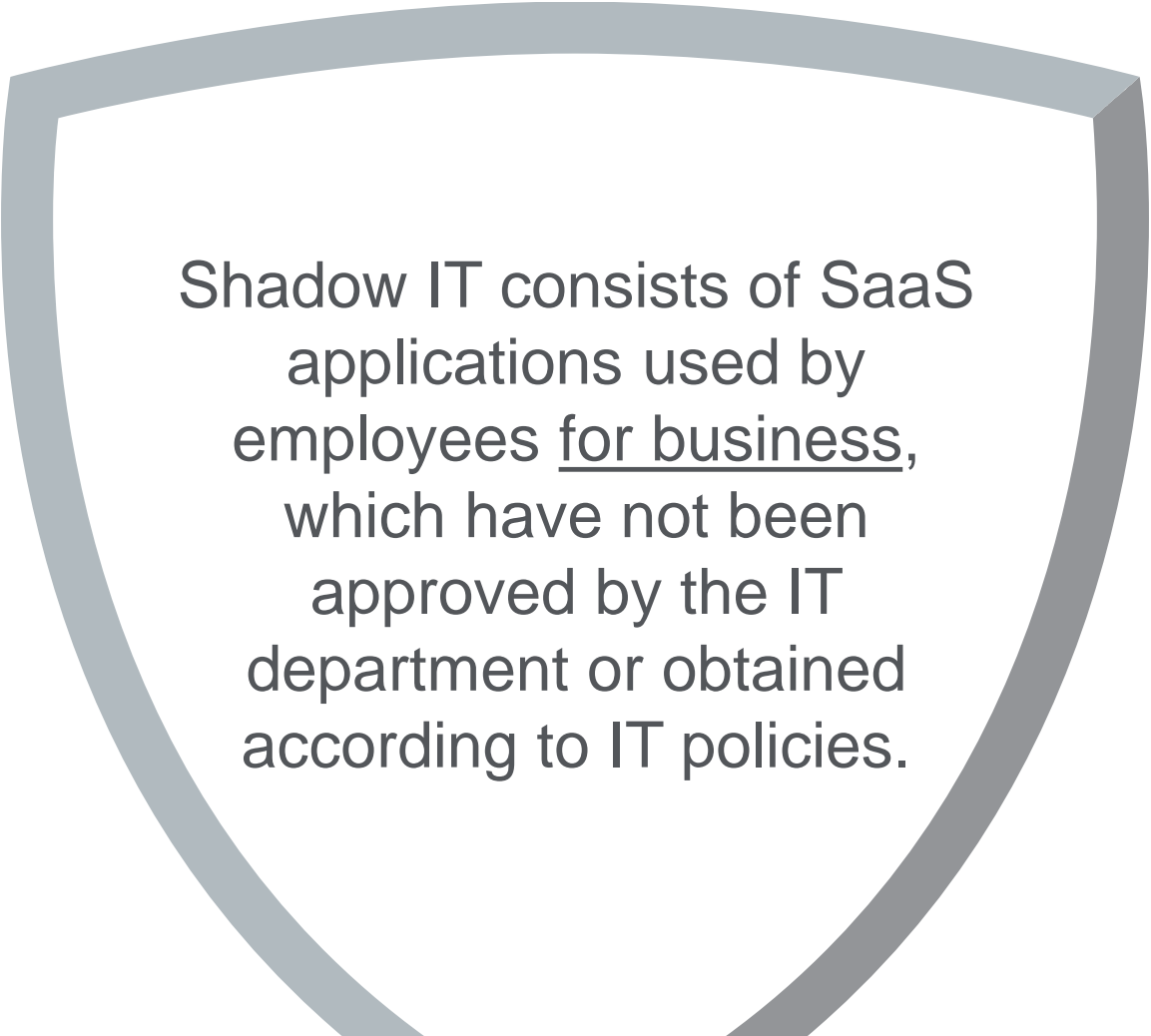


Shadow IT Security Gaps and 7 Resolutions

Ben Cody | Head of Product Management for DLP



TM



Shadow IT consists of SaaS applications used by employees for business, which have not been approved by the IT department or obtained according to IT policies.

Research Undertaken

- Contents based on McAfee / Intel Security Commissioned Report on Shadow IT
- Research conducted by Stratecast | Frost and Sullivan
- Includes 167 respondent companies, and 600 individuals (equal number LOB & IT)

F R O S T  S U L L I V A N

What's driving Shadow IT?

People want to get their job done.

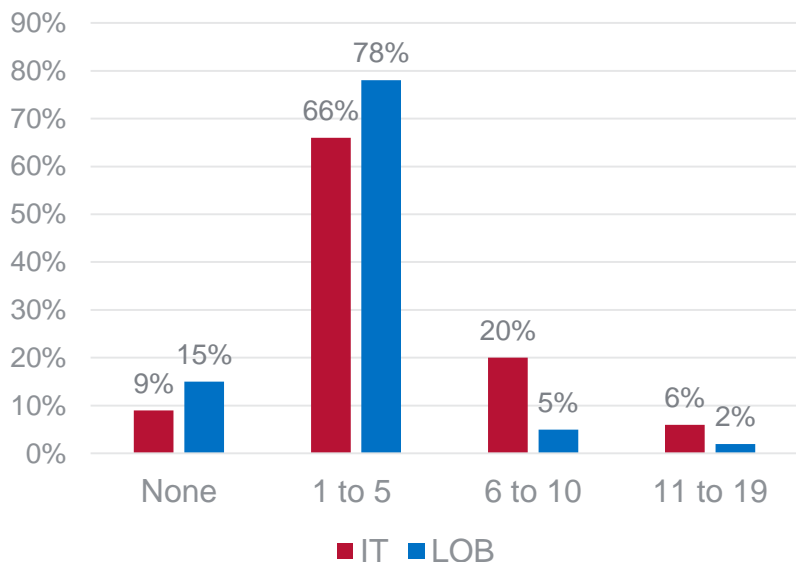
1. Ease of access
2. Ease of maintenance
3. Free or low cost
4. Quick deployment



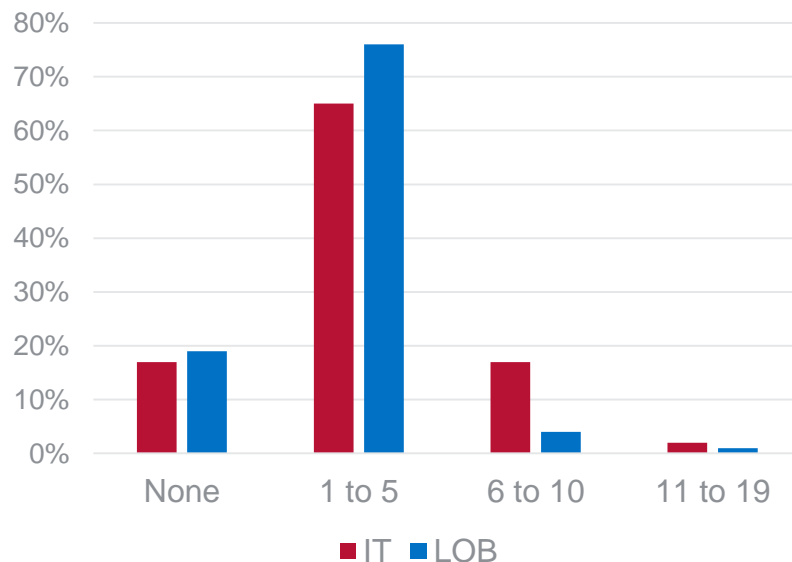
How pervasive is the problem?

Everyone does it, but IT is even more likely to use shadow IT!

Non Approved App Usage by Dept



Number of Apps used by Respondent

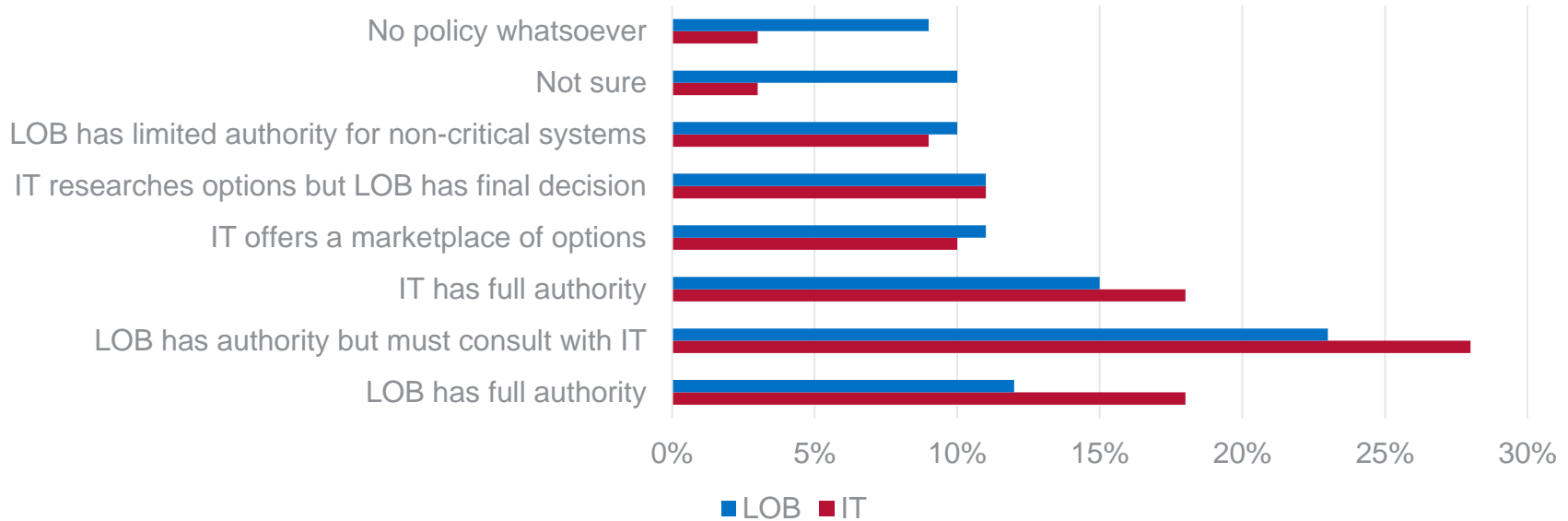


Source: Frost and Sullivan

What exacerbates the problem?

Corporate Policies are not clear or well understood. IT and LOB have different views.

Which statement best describes your organizations SaaS usage policy?



Why do they do it?

Here's the Top Five Reasons

1. They are more familiar with it (the SaaS application).
2. IT process for new application requests is too cumbersome.
3. The non-approved solution meets my needs better than the approved solution.
4. I tried to get approval first, was denied, but am using it anyway.
5. It's free.

What are they using it for?

It's not just Facebook...

Facebook LinkedIn Twitter YouTube Dailymotion Google+ Tumblr
Blogger Wordpress Dropbox Box via Google Drive Microsoft Skydrive Apple iCloud
YouSendIt/Hightail Mozy via Google Apps Microsoft Office 365 Zoho Adobe Creative Cloud CloudOn Open
Xchange Google Docs Microsoft Sharepoint IBM SmartCloud Google Chat AOL Instant Messenger Trillian Jive Webex
Citrix ConferencePlus Adobe Connect Skype InterCall Google Voice Join.me Constant Contact Eloqua Marketo
SurveyMonkey Cvent IBM SPSS Online Indicee Salesforce Netsuite SugarCRM Microsoft Dynamics Oracle On Demand SAP
Business ByDesign ADP Ariba Coupa Intuit Quickbooks Online Paypal DocuSign Gmail Outlook.com Yahoo Mail
AOL Mail Mail.com ISP Zoho Workday SuccessFactors Monster SilkRoad Ceridian Dayforce Oracle/Peoplesoft McAfee Symantec
Trend Micro Proofpoint Websense PingIdentity Booking.com TripAdvisor Expedia Priceline Kayak Travelocity
American Express

Business Productivity is largest category, closely followed by social media.

Fastest growing category of apps are HR, Finance, Legal, and CRM/ERP.

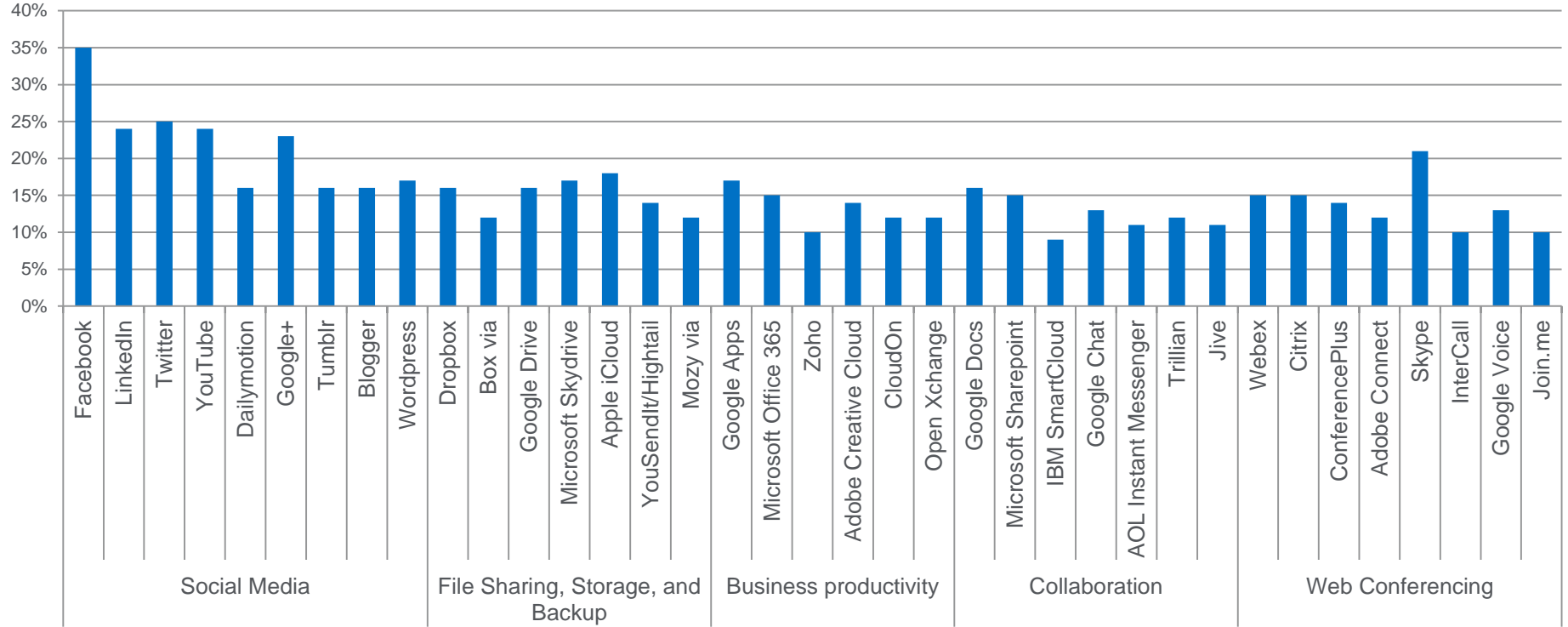
They recognize the risk, but do it anyway!

The Top 5 Security Concerns Users Cited for Shadow IT

1. Sensitive corporate or personal data will be accessed or stolen by unauthorized actors
2. Sensitive corporate or personal data will be accidentally exposed
3. Account information will be compromised
4. Corporate reputation will suffer
5. Data will be lost or deleted

And the risk is real!

Security Incidents by Category / Application



Source: Frost and Sullivan

Seven Steps to Address Shadow IT

Here's what to do

1. Establish a clear policy that aligns with your business objectives and culture
2. Allow users a degree of choice – e.g. 2 or 3 options in each category
3. Consider single sign on tools to reduce password re-use risk
4. Make sure you have an end user awareness and engagement program (no FUD!)
5. Make sure you've got the technology basics in place – email & web gateways, DLP, etc.

Technology Maturity Model – Draft

None

No security controls

Baseline

- + Anti-malware
- + Endpoint device encryption with HW acceleration
- + Mobile device management
- + DLP discovery
- + Device control
- + Email and web gateways
- + Single factor access control
- + Penetration testing / vulnerability scanning

Enhanced

- + Anti-theft: remote locate, lock, wipe
- + Client SSD with encryption
- + Policy based encryption for files and folders
- + Endpoint DLP
- + NDLP monitoring & capture
- + Multi-factor authentication with timeout
- + Secure remote administration, HW enabled
- + Server / database / backup encryption, HW accelerated

Advanced

- + Server SSD with encryption
- + NDLP “prevent”
- + Endpoint detection and response
- + Database activity monitoring
- + Digital forensics capabilities
- + SIEM
- + Threat intelligence exchange / collaboration
- + MFA with walk-away lock

Improved Breach Security, Usability, Cost, Operations

Seven Steps to Address Shadow IT

Here's what to do

1. Establish a clear policy that aligns with your business objectives
2. Allow users a degree of choice – e.g. 2 or 3 options in each category
3. Develop clear metrics for measuring your initiative's success
4. Make sure you have an end user awareness and engagement program (no FUD!)
5. Make sure you've got the technology basics in place – email & web gateways, DLP, etc.
6. Implement rules gradually to reduce risk without undue business impact
7. Develop a comprehensive data protection program

Successful Data Protection

Examples of Key Elements of Program Success

Risk Based
Approach

Clear
Governance
Structure

Defined Policies
and Principles

Centralized IT
Event Triage

Business units
own Data

Business units
own and resolve
incidents

Business units
provide priorities

Senior
Management
Support

Effective end-
user awareness
and training

Technology
shapes end-
user behavior

Step Eight – Bonus

Be more responsive to the business. There's a reason why shadow IT is popular.

- If you are not responsive, you are not relevant. Do you have good processes in place for dealing with demand management? Above and beyond break fix?
- Getting these in place is perhaps the best answer for proactively addressing the problems of shadow IT.



Find Out More

For the full report visit
<http://mcafee.com/shadowit>

Contact Ben at
ben.cody@intel.com

