SHADOW IT
doesn’t have to be SHADY

Bob Justus
CSO & Director GRC Services, Siege Secure
Cloud app revenue explosion

Source: Gartner
Cloud app projects double in 12 months
There are 4,000 enterprise apps today (and growing).
People love their cloud apps, and for good reason

Productivity | Anywhere Access | Collaboration
Business underestimates cloud app usage by 90%.

IT estimate: 40-50

Actual: 461

Source: Netskope Data
Actual: 461

Source: Netskope Data

IT estimate: 40-50

App redundancy
35 HR
26 Storage
18 Finance

This was controlled by IT in the past
61%

Of those surveyed don’t have a or don’t know about their cloud app policy.

- 17% don’t know
- 44% don’t have
People love their cloud apps, and for good reason.

Love doesn’t have to be blind.
STEP 1:
Discover the cloud apps running in your enterprise
STEP 1: Discover the cloud apps running in your enterprise

- 3rd party tools like Netskope can analyze firewall logs (and others) for this information
- Resist the urge to immediately blacklist unsanctioned apps
STEP 2: Understand the context of App usage at a deeper level
STEP 3: Plot a course of action based on risk, usage criticality
STEP 3: Plot a course of action based on risk, usage criticality

- Use an objective criteria for assessing app. The Cloud Controls Matrix from CSA is good start and vendors have taken this to a whole new level.

- After risk, look at usage, including the nature of the content. This will help triage next steps, especially when hundreds of apps are in play.

- Risky usage can be more important than app risk.
STEP 4: Enact a cloud app policy that people can get behind
STEP 4: Enact a cloud app policy that people can get behind

- Consumerization is a strong force — being too heavy-handed with policy is a recipe for revolt
- Consider what other policies need to be modified
- Be transparent about how you’ll treat unsanctioned apps
- Create an amnesty program for cloud app admins that are embedded in business units
STEP 5: Monitor usage, detect anomalies, conduct forensics
• Use machine learning tools to establish baselines and monitor anomalous behavior in real-time
• Use context to reduce false positives and false negatives
• Establish clear rules for forensic analysis to maintain user privacy while protecting data

STEP 5: Monitor usage, detect anomalies, conduct forensics
STEP 6: Identify and prevent the loss of sensitive data
STEP 6: Identify and prevent the loss of sensitive data

- Rely on tools that are built for analysis of content in the cloud (don’t backhaul data on-premises for analysis)
- Leverage rich context around app, user, time, etc. before you look at the data to help reduce unnecessary analysis
STEP 7: Implement security without breaking business process
STEP 7: Implement security without breaking business process

• Understand app usage and dependencies. Talk to users and find out what they’re doing with these apps

• Stop blocking by default. Think about how stopping a specific behavior (i.e., sharing outside of the company) might be enough
STEP 8: Don’t leave users in the dark. Coach them on safe usage.
STEP 8: Don’t leave users in the dark. Coach them on safe usage.

- Users are acutely aware of how an app *should* work. If you’re doing something that changes that experience, let them know.

- A little coaching goes a long ways. You’re buying good will.

- Tell them what you’d *like* them to do instead. Offer alternatives if you’re going to stop something.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Discover the cloud apps running in your enterprise</td>
</tr>
<tr>
<td>2</td>
<td>Understand the context of usage at a deeper level</td>
</tr>
<tr>
<td>3</td>
<td>Plot your course of action based on risk, usage, criticality</td>
</tr>
<tr>
<td>4</td>
<td>Enact a cloud app policy that people can get behind</td>
</tr>
<tr>
<td>5</td>
<td>Monitor usage, detect anomalies, conduct forensics</td>
</tr>
<tr>
<td>6</td>
<td>Identify and prevent the loss of sensitive data</td>
</tr>
<tr>
<td>7</td>
<td>Implement security without breaking business process</td>
</tr>
<tr>
<td>8</td>
<td>Don’t leave users in the dark. Coach them on safe usage.</td>
</tr>
</tbody>
</table>
The real face of shadow IT is you and me.

Ultimately, this is simply unmanaged risk.
ALLOW is the new BLOCK