92%

of organizations are experiencing the effects of shadow IT.

Original survey question:

Which of the following best represents the existence of "shadow IT" at your organization?

Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.

Survey respondents:

302 IT and security decision makers responsible for their organization's cloud security strategies

ESG Insight

The consumerization of IT, fueled by knowledge worker mobility and the prevalence of cloud applications, has created the conditions for substantial employee use of applications not sanctioned by corporate IT groups (i.e., shadow IT). IT and security professionals substantiate this dynamic, with 34% stating they are aware of a significant number of non-IT-sanctioned cloud applications in their organization, with an additional 31% citing awareness of a moderate amount of unapproved cloud application usage. At the forefront of cloud security challenges is the security adage "you can't secure what you can't see" with respect to the multiple blind spots created by the prevalent use of shadow IT applications —these blind spots make answering questions around what applications are in use, who is using those applications, what sensitive data is being stored in those cloud applications, and what else, including malware, is residing in cloud applications impossible to answer.