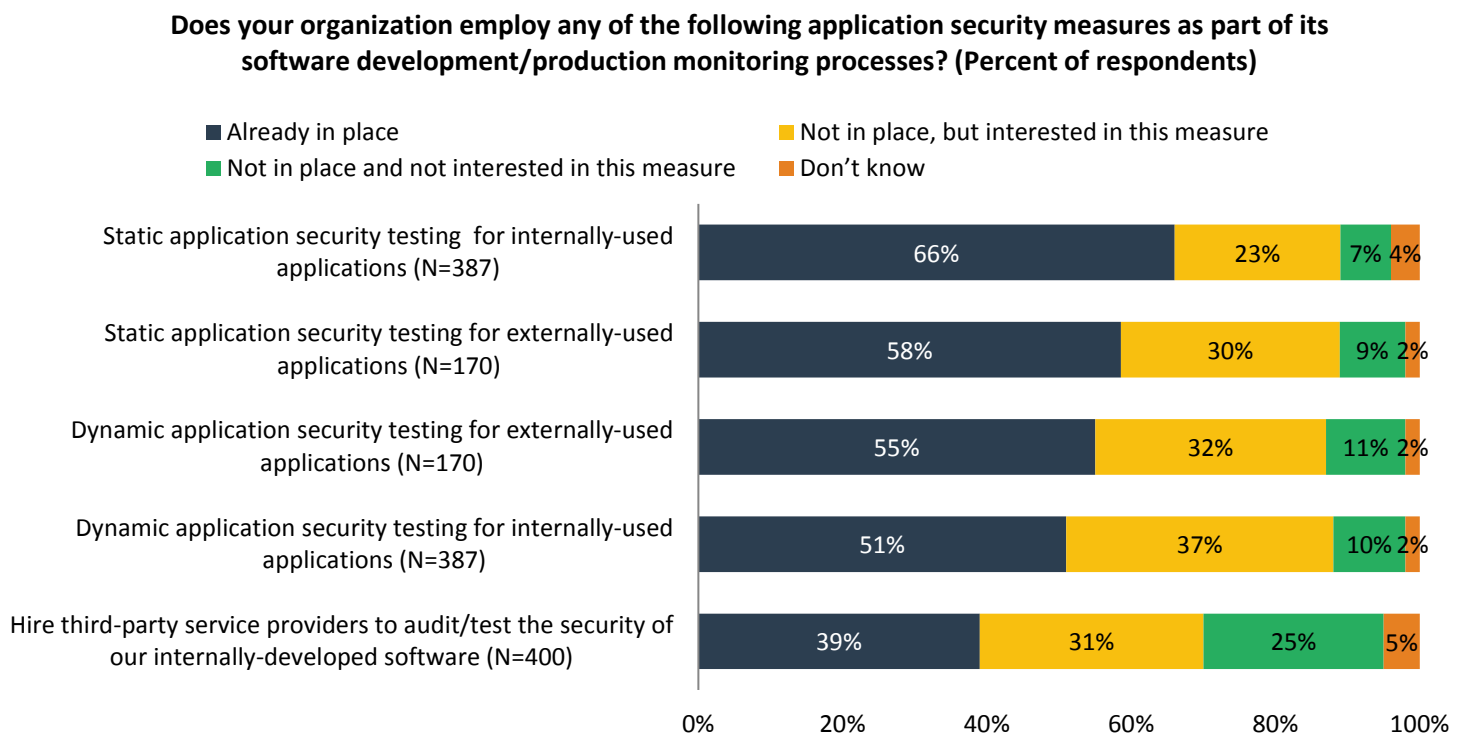that they employ a cloud-first deployment methodology. An additional 44% said that they weigh on-premises technology and public cloud services equally when considering their deployment options. Only 19% of respondents employed an on-premises-first philosophy.[1]

SAST and DAST Obtain Equal Priority

Traditional application development distinguished between internal and external apps. There is a perception that internal apps have limited security risks and possibilities for compromise because they were hidden behind the corporate firewall, and were only used by internal employees. Externally facing apps, or apps with public users, were perceived to have much greater risk. This perception seems to explain the fact that 66% of respondents employ SAST for internal applications while only 51% employ DAST for internal applications.

However, mobile- and cloud-first initiatives may be blurring the lines between what is considered internal or external. Users accessing corporate data through cloud or mobile apps may bypass the corporate firewall to access apps using insecure public and cellular networks. Performing both static and dynamic testing of all apps, and incorporating and automating AppSec into AppDev should become a best practice, regardless of the app deployment or use model. This concept is reflected in the research results: Including respondents that are interested in SAST and DAST respectively, usage for each should normalize over time (see Figure 4).

Figure 4. Use of Application Security Measures as Part of Software Development/Production Monitoring

Does your organization employ any of the following application security measures as part of its software development/production monitoring processes? (Percent of respondents)

■ Already in place   ■ Not in place, but interested in this measure
■ Not in place and not interested in this measure   ■ Don't know

Static application security testing for internally-used applications (N=387)	66%	23%	7% 4%
Static application security testing for externally-used applications (N=170)	58%	30%	9% 2%
Dynamic application security testing for externally-used applications (N=170)	55%	32%	11% 2%
Dynamic application security testing for internally-used applications (N=387)	51%	37%	10% 2%
Hire third-party service providers to audit/test the security of our internally-developed software (N=400)	39%	31%	25% 5%

0%   20%   40%   60%   80%   100%

Source: Enterprise Strategy Group, 2017

AppSec Crossing Organizational Boundaries

In traditional development organizations, the security team was siloed from the development team. Often, security was an afterthought—something to be bolted on to the app at the end of the development processes. This led to vulnerabilities being discovered mostly after the fact, when the app was compromised and the organization was breached. However, ESG

---

[1] Source: ESG Research Report, *2017 IT Spending Intentions Survey,* March 2017.