451 Research | Business Impact Brief

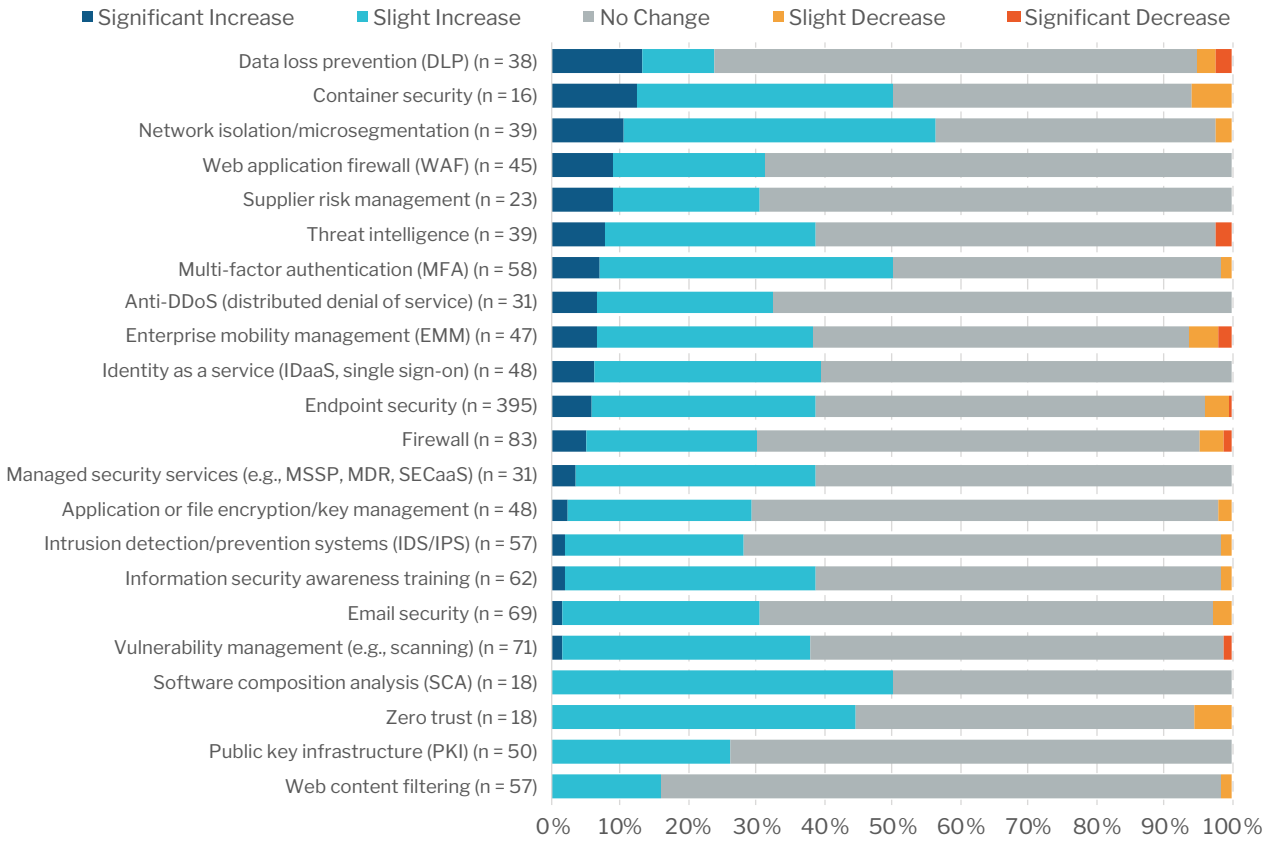
The Need for Cloud-Native DLP

The 451 Take

Data loss prevention (DLP) technology has been around for nearly 20 years. Though still a staple of most firms' overall security strategies, the DLP market has a bit of a tarnished reputation, mainly due to inaccuracy, false positives and poor performance. However, DLP still is a primary consideration for most firms' security strategies for a variety of reasons: massive volumes of new data being created, growing use of collaboration and third-party apps, the seemingly endless string of data breaches, new privacy regulations like GDPR, and recent high-profile fines (Equifax, British Airways). In fact, according to 451 Research's Voice of the Enterprise (VoTE) survey, DLP was ranked at the top of the list of over 20 security categories that are expected to see a 'significant' increase in spending in the next 12 months – by 13% of respondents – followed closely by network isolation/microsegmentation and third-party supplier risk management.

Security Categories Expected to See Significant Spending Increases over Next 12 Months

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2019



However, more workloads are migrating to the cloud, and many existing DLP tools are simply not optimized for cloud environments, whether cloud-based email like Office 365 and the G Suite, or cloud collaboration services such as Box, Dropbox and Google Drive.

451 Research | Business Impact Brief

Business Impact

MOST WORKLOADS WILL RUN AS SAAS APPS IN TWO YEARS. Today, roughly 40% of workloads are run in 'traditional' on-premises environments. However, in two years, that percentage is expected to be more than cut in half, to just 19%, according to 451 Research VotE data. Conversely, SaaS applications are expected to increase from 20% of workloads currently to 28% in 2021, and they will represent the most common architectural option for deploying applications, followed by public cloud (IaaS and PaaS) at 19%.

SECURITY IS STILL THE MAIN CLOUD ADOPTION BARRIER. Despite all of the potential benefits of cloud, security concerns remain a primary obstacle. Survey data from 451 Research shows that 42% of organizations still view security as the main impediment to moving more workloads to the cloud.

CLOUD COLLABORATION PRESENTS UNIQUE CLOUD SECURITY CHALLENGES. As more workloads and sensitive data migrate to collaboration services like Box, Dropbox, Google Drive, One Drive and Office 365, employees are increasingly able to share and collaborate both inside and outside the company walls, which essentially fully delegates access control to end users. However, cloud collaboration can lead to intellectual property or other sensitive information being shared in unintended ways, such as earnings releases made available too early, salary data being shared with the wrong internal groups, or departing employees taking files with them. Aside from the access controls natively built in to each of those services, there is no centralized way to understand how company data is being shared across them, and more importantly, how employees can take actions – either maliciously or mistakenly – that can lead to sensitive data being leaked or stolen.

USERS ARE STILL THE WEAKEST LINK. While many discussions focus on the technological risks of the cloud, users are arguably the biggest vulnerability that most enterprises face. The importance of user-awareness training has been highlighted in recent years, but end-user training can take valuable time away from busy users and only provides security at a point in time rather than continuously validating user actions. Perhaps most importantly, no matter how well they are trained, users are not perfect, and it only takes one mistake to cause a massive breach – or at best, corporate embarrassment – and expose critical information to the entire world.

Looking Ahead

While it's encouraging to see organizations prepared to increase their spending on DLP to address breaches and new compliance requirements, it's important to spend wisely. Budgets should be optimized toward DLP offerings that are capable of supporting both legacy and emerging technologies, including a variety of cloud platforms. In addition, out-of-the-box security from cloud providers is not enough. Microsoft, AWS, Google and other cloud providers are constantly adding new security features and functionality, but it may not be enough to provide optimal security for all firms. 451 Research VotE data shows that nearly half of all firms (~48%) are taking advantage of independent, third-party security offerings to fully optimize the security of their cloud data instead of relying solely on what cloud providers offer, and also to offer a centralized location for managing and applying security policies.

DLP needs to do more than discover personally identifiable information (PII). Historically, DLP has placed a heavy emphasis on discovering and classifying data – typically, PII such as credit card and social security numbers – and writing policies that govern their use. To go beyond just checking off compliance boxes, DLP should also be able to detect more subtle, yet critical threats such as theft of intellectual property and the inadvertent leaking of a quarterly earnings release. False positives have long been the bane of DLP tools, but enterprises can improve accuracy with AI and machine learning – rich context and deep analysis can be used to identify false positives and discover attacks that existing tools might miss.