prdeadlines

Bitglass reports 84% of organisations will go on supporting work from home, but most aren’t secure

SYDNEY, May 28. Bitglass, the next-gen cloud security company, has released its 2020 Remote Work Report, which analyses how organisations have adjusted to support remote workers amidst the COVID-19 pandemic. Bitglass partnered with a leading cyber security community and surveyed IT professionals to understand how prepared their businesses are for the sudden shift, what actions they are taking in cyber security, and what their top security concerns are now. Currently organisations are struggling to adjust to the new normal. 41% have not taken any steps to expand secure access for the remote workforce, while 50% are citing proper equipment as the biggest impediment to doing so. Consequently, 65% of organisations now enable personal devices to access managed applications. Asked what their organisations are primarily concerned with securing while employees work remotely, 65% of respondents said securing network access. This was followed by securing access to SaaS apps like Slack (55%) and bring your own device/personal devices (55%). For the most concerning threat vectors for remote work, respondents cited malware (72%) and unauthorised user access (59%). “This research indicates that many organisations are not implementing the security measures necessary to protect their data in the current business environment,” said Anurag Kahol, CTO of Bitglass. “For example, while respondents said the pandemic has accelerated the migration of user workflows and applications to the cloud, most are not employing cloud security solutions like single sign-on (SSO), data loss prevention, zero trust network access, or cloud access security brokers. “On top of that, 84% of organisations reported that they are likely to continue to support remote work capabilities even after stay at home orders are lifted. To do this safely, they must prioritise securing data in any app, any device, anywhere in the world.” Key findings include: Malware is the most concerning threat vector, with 72% of respondents citing it as their top concern. From a remote work perspective, the application types that organisations are most concerned about securing include file sharing (68%), web applications (47%), and video conferencing (45%). At 77%, anti-malware is the most-used tool to secure remote work. However, this and other tools like single sign-on (45%), data loss prevention (18%), and user and entity behaviour analytics (11%) are still not deployed widely enough. 63% of respondents said that remote work was likely to impact their compliance with regulatory mandates; 50% named GDPR, specifically. To see all of the findings, download the full report here: https://pages.bitglass.com/CD-FY20Q2-RemoteWorkforceReport_LP.html?&utm_source=pr About Bitglass Bitglass, the Next-Gen Cloud Security company, is based in Silicon Valley with offices worldwide. The company's cloud security solutions deliver zero-day, agentless, data and threat protection for any app, any device, anywhere. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution. Contact David Shephard Bitglass ANZ dshephard@bitglass.com

Contacts

David Frost
(02) 7903 9567
mailto: davidf@prdeadlines.com.au