prdeadlines

Bitglass study finds security gaps remain pervasive across BYOD initiatives

2021 BYOD Security Report reveals security teams continue to lack visibility and technology needed to secure unmanaged personal devices modern threats

SYDNEY, June 16. Bitglass, the total cloud security company, today announced findings from its 2021 BYOD Security Report that show the rapid adoption of unmanaged personal devices connecting to work-related resources (aka BYOD) and why organisations are ill-equipped to deal with growing security threats such as malware and data theft.

The study, a joint venture with Cybersecurity Insiders, surveyed hundreds of cybersecurity professionals across industries to better understand how COVID-19's resulting surge of remote work has affected security and privacy risks introduced by the use of personal mobile devices. The insights in this report are especially relevant as more enterprises shift to permanent remote work or hybrid work models, connecting more devices to corporate networks and, as a result, expanding the attack surface.

"As mobility and remote work environments keep growing, so do challenges ranging from managing device access to handling urgent mobile security concerns," said Holger Schulze, founder, Cybersecurity Insiders. "Our research uncovered a plethora of evidence that shows organisations are not paying enough attention securing unmanaged personal devices and why the time is now for them to think differently when it comes to securing BYOD."

Key Findings from the Bitglass 2021 BYOD Security Report:

BYOD is here to stay

The shift to remote work amid the pandemic resulted in 47 percent of organisations reporting an increase of personal devices being used for work. As a result, a total of 82 percent of organisations said they now actively enable BYOD to some extent. While the use of personal devices has helped businesses improve employee productivity and, while also reducing costs, challenges associated with managing device access and mobile security remain.

Securing BYOD to prevent data loss/theft is a top concern

The most critical concern respondents expressed was data leakage or loss (62 percent). Other apprehensions included users downloading unsafe apps or content (54 percent), lost or stolen devices (53 percent), and unauthorised access to company data and systems (51 percent).

Enterprises are running blind when it comes to securing BYOD devices against modern security threats.

For example, 22 percent of organisations indicated they can confirm that unmanaged devices have downloaded malware in the past 12 months. However, nearly half (49 percent) indicated they are not sure or could not disclose whether the same could be said for them. This lack of visibility can be detrimental to the overall business.

Many organisations are securing BYOD with old tools vs modern threats

A total of 41 percent of organisations reported relying on endpoint malware protection for BYOD—an approach that is not ideal for personal devices which are hard to control and manage. Over a quarter (30 percent) of firms said they don't protect against malware for BYOD at all. While cloud-based malware protection tools are often a far better fit, only 11 percent of organisations surveyed are currently using these measures.

"As enterprises begin to shift to hybrid work environments, personal devices will provide the flexibility and remote access that employees require. This new way of working, however, will undoubtedly stretch the resources of security teams," said Anurag Kahol, CTO, Bitglass. "This is why there has never been a more important time for enterprises to seriously rethink their approach to secure all forms of communication amongst users, devices, apps, or web destinations."

Methodology

Cybersecurity Insiders surveyed 271 cybersecurity professionals, conducted in April 2021, to gain deep insight into mobile BYOD security threats faced by organisations and the solutions to prevent and remediate them. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organisations of varying sizes across multiple industries.

About Bitglass

Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction.Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivalled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company 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.

ANZ media contact

David Frost

Touchdown for Bitglass
+61 (0) 408 408 210
dfrost@touchdownpr.com

Contacts

David Frost
(02) 7903 9567
mailto: david.frost@prdeadlines.com