Organisations in India and across Asia Pacific implement access management solutions to protect themselves from cloud threats in remote working era

- Security concerns around password vulnerability (81%) and the threat of large-scale breaches (78%) are driving organisations to implement access management solutions across APAC region.
- Over half of organisations (58%) report that increased use of cloud applications puts them at greater risk of cyber attacks.
- An overwhelming 67% of Indian organisations report that secure access management is now a priority for the board to help them address their concerns over the lack of solutions.

New insights from the 2020 Thales Access Management Index – Asia Pacific and Japan Edition¹ reveal that concerns around the threats of cyberattacks are prompting businesses in the region to take action. Surveying 500 IT professionals across India, Australia, Hong Kong, Japan and Singapore with responsibility for, or influence over, IT and data security, the threat of large-scale breaches (78%) and security concerns around password vulnerability (81%) are driving organisations towards increasing their implementation of access management solutions.

Thales will host a webinar, “Access Management and Authentication Trends in the Asia-Pacific Region” on 18 November 2020 to discuss the report in more detail. To join, please visit the registration page.

Whilst organisations across the region increase cloud adoption in the remote working era, many (58%) are still concerned that their increased use may make cloud applications a target for cyber-attacks. The reasoning for this varies greatly when comparing the countries within the APAC region. Those from Japan are concerned about the lack of in-house skills to secure cloud applications (65% compared with the APAC total of 53%). In contrast, those from India are most likely (71%) to consider the lack of strong cyber security solutions to implement appropriate protection. Regardless of the reasoning, cloud applications are growing not only in number but also in importance, meaning that securing them properly is essential for organisations in the region.

The report also mentions about security policies around access management. Around two thirds (67%) of respondents from India report that secure access management is now a priority for the board, which should help them to address their concerns over a lack of solutions.

¹ Note: The report mentioned here is an example. The actual reference should be included in the final document.
In order to mitigate these potential threats and simplify cloud access management, APAC organisations are taking action with nearly all (92%) planning to expand their use of smart Single Sign-On (SSO). Most respondents from India view smart SSO as being extremely secure, trusting it to protect sensitive data (56%) and applications (53%).

Organisations also understand the benefits of smart SSO adoption, particularly when it comes to preventing breaches of data (47%), and ensuring customers feel their data is secure (44%). Comparatively in India, 53% see adoption of smart SSO beneficial in preventing breaches of data and 59% believe that smart SSO will boost customer confidence with regard to security of their data. However, fears in the region are likely to still remain with IT leaders citing concerns over inconsistent security protections across cloud (57%), a lack of strong cyber-security solutions to implement appropriate protection (56%), and a lack of in-house skills to secure cloud applications (53%). What’s more, organisations have flagged that ineffective cloud access management can lead to cloud applications becoming a security issue (50%).

Rana Gupta, APAC Regional Vice President for Data Protection solutions at Thales said: “The need for Access Management has never been greater as organisations adapt to support their employees, customers and partners during these unprecedented times. Secure remote access for employees working outside the office is paramount for enterprises operating amid increasing complexity and scale. Cybersecurity must be a boardroom discussion and the current landscape provides IT leaders with an opportunity to rapidly progress their digital transformation plans and robust cloud adoption with the necessary protections in place.”

Cyber breaches are now a board level issue

As businesses react to the changing situation and increasingly see the need for a security-first approach, IT leaders across the APAC region are finding it easier to sell the need for IT security to their boards of directors, with over half (55%) reporting that it is now easy (up from 34% looking at 12 months ago). As businesses continue to work out how to give remote employees the tools to work efficiently wherever they are, while keeping the company safe, access management looks set to form an increasingly integral role in the future. Nearly all respondents (99%) stated that controlling who has access to specific types of data can contribute towards compliance.

Positively, more organisations in the region have revealed their staff are also now trained in security and access management (53%) than two years ago (49%). What’s more, businesses have also revealed an increase in spending (47% from 45%) on access management and nearly half now have a dedicated CISO (47%), up from 41%. However, three quarters of respondent businesses (75%) plan to increase their use of usernames and passwords, despite inherent weaknesses caused by issues like Shadow IT, showing there’s still work to be done.

Rana continued: “As businesses figure out a way to keep themselves running in this pandemic world, the circumstances forcing many to work from home are inherently increasing the security risks at the same time due to the threats related to hijacking of credentials as the cyber-attacks continue to expand. These security concerns are justified as users get to access their systems in huge numbers from their respective remote locations, as well as the increasing adoption of various cloud platforms. Investing in smart access management tools that allow for stepped up secured authentication through a choice of multi-factor authenticators besides enforcing access policies, is the need for the hour. Expanding the use of flawed systems, such as passwords, is only going to lead to much bigger problems.”

1 The 2020 Access Management Index, is a survey of 500 executives in 5 countries in APAC with responsibility for, or influence over, IT and data security. The survey, reporting and analysis was conducted by Vanson Bourne, commissioned by Thales.
About Thales

Thales (Euronext Paris: HO) is a global high technology leader investing in digital and “deep tech” innovations – connectivity, big data, artificial intelligence, cybersecurity and quantum technology – to build a future we can all trust, which is vital to the development of our societies. The company provides solutions, services and products that help its customers – businesses, organisations and states – in the defence, aeronautics, space, transportation and digital identity and security markets to fulfil their critical missions, by placing humans at the heart of the decision-making process.

With 83,000 employees in 68 countries, Thales generated sales of €19 billion in 2019 (on a basis including Gemalto over 12 months).

About Thales in India

Present in India since 1953, Thales is headquartered in New Delhi and has other operational offices and sites spread across Noida, Gurgaon, Hyderabad, Bengaluru and Mumbai, among others. Over 1,600 employees are working with Thales and its joint ventures in India. Since the beginning, Thales has been playing an essential role in India’s growth story by sharing its technologies and expertise in Defence, Transport, Aerospace and Digital Identity and Security markets. Thales has two engineering competence centres in India - one in Delhi NCR focused on digital identity and security business, while the one in Bengaluru focuses on hardware, software and systems engineering capabilities for both the civil and defence sectors, serving global needs.