bizcommunity

A unified threat and data solution is key to POPI compliance

The final sections of the South African Protection of Personal Information Act (POPIA) came int effect on 30 June 2020, informing companies about how they process information for their businesses.

By Carlo Bolzonello 11 Mar 2021

Carlo Bolzonello

There are eight minimum requirements, with perhaps the most important being that businesses and other operators must implement appropriate security safeguards to ensure the integrity and confidentiality of personal information in their possession.

Cloud services are considered 'operators', and are therefore subject to the requirements outlined in the POPIA, bearing in mind that data needs to be considered when data is sent to cloud services, from cloud services, between cloud services, and in cloud services. Simply put, all data flows are subject to the law a need to be monitored and controlled accordingly.

Businesses and operators need to ensure that their data lost prevention (DLP) protocols in a time where 95% of companies have adopted cloud services, and 79% admit to storing sensitive data there. Endpoint DLP – implemented on a business's network – is simply no longer sufficient.

DATA & ANALYTICS

Why POPI compliance is not just an IT issue

Johan Scheepers 7 Dec 2020

This is even more relevant in an increasingly work from home (WF) and bring your own device (BYOD) environment, with these trends expanding the traditional network parameter to the point that business-critic information often lies outside of corporate-managed domains and devices.

Furthermore, as more and more enterprises adopt SaaS and Iaas solutions, it's even more important – wit POPIA in mind – for any activity around personal data to be detected, managed, and controlled, particularl given that companies actively assessing their data exfiltration attempts in IaaS saw an average of 5,314 events each month in 2020.

However, there are few security products that cover all bases when it comes to DLP across endpoint and cloud, and many deploy multiple products. Doing so does close all the gaps – but it does lead to pitfalls, such as differences in DLP policies, data classifications, and content extraction engines.

CYBERSECURITY

Focus on POPIA compliance, data mobility, integrity key in a world with a remote workforce

Ian Engelbrecht 29 Jan 2021

This makes it difficult to ensure consistent DLP detection across products, and in turn, makes businesses vulnerable to data loss, data theft, and in turn, violating the conditions described in the POPIA.

A unified data and threat protection solution will cover all potential data leak vectors, including endpoint, unsanctioned shadow IT apps, sanctioned apps (including email) and cloud to cloud transfers. It's manage via a single console and uses the same DLP technology everywhere.

With the POPIA compliance grace window period nearly closed, businesses that have not yet pivoted to comply with all its requirement – particularly from a security point of view – are likely to attract fines of up tc R10million per breach from the regulator, or a prison fine of up to ten years. Faced with consequences like that, it surely seems foolhardy for businesses to not consult with experts in protecting businesses from cyberattacks

ABOUT THE AUTHOR

Carlo Bolzonello is the South Africa country manager for McAfee.