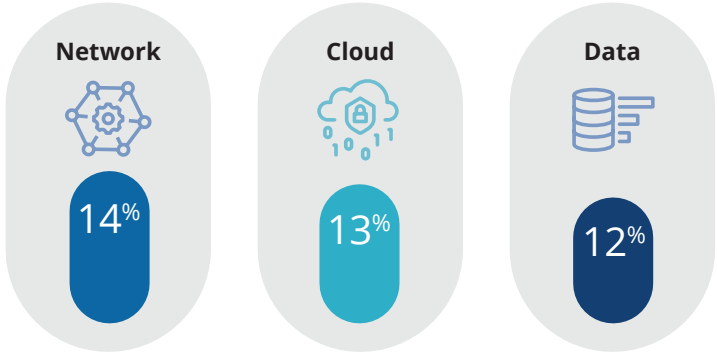
Why is PROACTIVE SECURITY paramount in the digital-first era?

IN THE DIGITAL-FIRST ERA, Asia/Pacific (AP) organisations are adopting newer, more innovative technologies at an accelerated rate. To improve service delivery at an optimised cost, they leverage advanced technologies, such as cloud and edge computing, AI-powered data analytics, and IoT. By doing so, modern IT infrastructure has become more distributed, diverse, and perimeter-less, with the concepts of internal and external boundaries essentially dissolved. However, modern IT architectures' new decentralised nature severely exposes businesses to increased technology risks and cyberattacks.

In a recent survey by IDC, the Worldwide CEO Sentiment Survey, cybersecurity was the top priority for AP organisations' boards in 2022, ahead of digital sovereignty, AI ethics, and sustainability. Additionally, IDC's Security Sourcing Survey 2022 revealed that **most AP organisations believe they are most vulnerable to a severe security breach regarding their network, cloud assets, and data storage, making these three areas of focus for security investment in the region to date**. Thus, it is not surprising that enterprises everywhere prioritise security to mitigate risks and protect sensitive data and assets.

Importance to board priorities

Areas most vulnerable to security breach



Sources: IDC WW CEO Sentiment Survey 2022 (APJ n = 123) and IDC Security Sourcing Survey 2022 (APJ n = 869)

Shifting from a reactive to proactive approach towards cybersecurity

Conventional security controls are often designed to react and respond to a cyber incident after it has occurred. Proactive security, on

the other hand, pre-emptively finds, identifies, and addresses inherent security vulnerabilities within an organisation's IT system before bad actors can exploit it. In the simplest term, it refers to a set of strategies that prevent an attack from happening, with organisations taking an offensive stance to improve their security posture.

More often than not, organisations that adopt proactive security strategies also embrace the Zero Trust approach – a security framework that requires authorisation of every single access to the system, both internal and external.

Some of the methods that are involved in proactive security posture include threat hunting, vulnerability assessment and scanning, network and endpoint monitoring, network segmentation, and sandboxing, among others.

More often than not, organisations that adopt proactive security strategies also embrace the Zero Trust approach – a security framework that requires authorisation of every single access to the system, both internal and external. As part of this approach, an organisation may implement additional measures, such as multi-factor authentication, user behaviour analysis, continuous validation, security awareness training, and more. However, organisations often lack the resources to implement proactive security controls. In such cases, businesses must turn to a security provider to guide and help them achieve the desired security posture.

Turning to experts for integrated security services

Security providers in the region have the excellent technical expertise and vast experience in business risk or direct cyber risk strategy services that can help organisations build effective proactive security strategies that align with their business goals. Security providers have integrated adjacent security technologies, such as advanced threat protection, analytics, intelligent automation, and threat intelligence, to provide a more comprehensive security control for a unified platform approach. They are also able to centralise monitoring and incident response functions via their security operation centre (SOC), often staffed with a team of security analysts to protect clients' digital assets. Perhaps more importantly, by working with a trusted security partner, organisations can always access a security expert and resources to continuously improve their security posture as their IT infrastructure continues to evolve. ■