IDC ANALYST BRIEF

Sponsored by: Tata Communications

The sudden proliferation of widely distributed workforces and an increased adoption of cloud-native solutions and devices connected to corporate networks call for a resilient, adaptive, secure, and connected network.

Secure Transformation Can Only Be Achieved With a Unified Enterprise Network

May 2022

Written by: Hugh Ujhazy, Vice President, Internet of Things and Telecommunications, IDC Asia/Pacific

Introduction

The COVID years can only be described as a time of prolonged and fundamental change. IDC's Digital Enterprise Pulse Survey revealed that 70% of enterprises have accelerated their digital transformation (DX) plans due to environmental, cultural, and customer-led changes arising from the pandemic.

Many organizations needed to rapidly adopt cloud-based services to streamline operations and meet the needs of a distributed workforce. Yet, many did not consider the implications of the technology and the transition to it.

By implementing completely new technologies almost overnight, many network and security teams found themselves unable to fully secure their massive, fragmented networks and maintain a holistic view of attack surfaces.

There is no doubt that digital acceleration will help companies push innovation, optimize operations, and achieve competitive advantages. Those who have embraced the new market order have thrived, with profits up and demands for services at an all-time high, just as unemployment figures dip to the lowest level in decades.

AT A GLANCE

WHAT'S IMPORTANT

Digital transformation is accelerating, much of it depending on effective collaboration based on agile, secure connectivity. Those who get it right have thrived.

KEY TAKEAWAYS

» Understand the workload and networks making up your digital environment

» Prioritize automation and orchestration to simplify management of the network to meet the needs of all users

» Leverage best practices by engaging with expertise to build a future-proofed road map for the connected enterprise

However, if chief technology officers (CTOs), chief information security officers (CISOs), and their network and security teams don't take a step back and spend time getting their networks in check, there could be unforeseen security issues further down the line. With the attack surface continually expanding and the sophistication of cyberattacks growing, this will only add to the problem. IDC's Enterprise Communications Survey found that only

21% of enterprises in Asia/Pacific felt confident that their networks could adapt to the changing demands of cloud, Internet of Things, edge and distributed working models.

Managing the proliferation of risk

IDC forecasts that global network security spending will grow at a CAGR of 11% from 2021–2025 to exceed US$46 billion by 2025. The sudden proliferation of widely distributed workforces and an increase in cloud-native solutions and devices connected to corporate networks have increased risks across enterprises globally. There are challenges inherent to home networks, which are not as secure as those situated within traditional corporate environments. Previously, employees were the only concern in terms of internal threats. Now, anyone sharing the home network could theoretically be able to create new risks to corporate assets.

A number of current challenges to seamless teleworking are noted as falling into the following buckets:

- Problems related to inconsistent connectivity and bandwidth
- Security related to using ad hoc personal devices as work-from-home (WFH) equipment
- Data caps for internet services that might constrain daily business functions such as access to SaaS programs
- Work-from-home employees lacking technical knowhow or ready access to troubleshooting
- Problems recreating the face-to-face work environment
- Difficulty creating a cohesive culture with a hybrid workforce

According to IDC's Cloud Pulse 2Q20, cybersecurity tops the list of digital transformation investment for large organizations in Asia/Pacific for the next five years. Further, more than 62% of respondents in IDC Asia/Pacific Security Services Sourcing Survey 2020 had stated that they expect security spending to increase due to the COVID-19 pandemic. While a majority of the survey respondents (70%) acknowledged that security is currently underinvested in their organization, 76% of them admitted that security is not their area of expertise, and they would rather engage a trusted provider to help with their security needs.

IDC predicts that by 2023, digital transformation and business volatility will drive 55% of A2000 organizations to deploy remote or hybrid-first work models, redefining work processes and engaging diverse talent pools.

IDC predicts that by 2023, digital transformation and business volatility will drive 55% of A2000 organizations to deploy remote or hybrid-first work models, redefining work processes and engaging diverse talent pools. Hence, the security risks introduced by remote workers will prevail. That is why it is essential for organizations to have a thorough knowledge of their attack surfaces and possible exposure to vulnerabilities.

Businesses must strike a balance between mitigating that risk without negatively impacting business functions. By uniting security policies and analytics, security stakeholders can smartly use data from their complex layers of security, networking, and cloud technologies to secure across the modern enterprise. This will empower them to gain complete control of their networks and systemic risk. Simultaneously, it will help them to establish more holistic security strategies for future digital transformation initiatives.

Keeping pace with change

Whether it is keeping pace with digital acceleration or managing a hybrid remote workforce, the 'new normal' will require more agility and change than ever before. But security policy alterations cannot be rushed. They should be adequately analyzed and properly deployed without introducing new risks.

To get there, security and network teams should utilize context-aware change management that ensures new security policies are adequately analyzed and properly deployed without introducing new risks. At the same time, CISOs must confirm that all regulatory and compliance-related benchmarks are still being met. Good visibility provides the foundation needed to innovate without exposing the organization to undue risk.

Make faster, more informed decisions

As businesses grow, the number of staff and internal applications will increase in complexity. According to IDC research, most enterprises have employed mechanisms to increase the security of hybrid and remote work environments. These include added security patches to home equipment, increased frequency of vulnerability scans, added endpoint security measures, and enhanced remote IT operations. This will make networks even more convoluted, so getting a handle on network topology should be a priority before it gets out of control. Therefore, strategies should be put in place to improve communication between people, technologies, and processes.

With a more unified view of the network and its inherent security policies, businesses can better navigate across organizational silos and disparate technology systems. With improved visibility, security teams can quickly map out and close vulnerabilities while validating rapid configuration changes. These are often stumbling blocks when it comes to digital transformation efforts. In doing so, CISOs and their respective security teams can keep pace with an ever-dynamic network perimeter. They will also be armed with necessary insights to make more informed decisions and drive critical digital transformation efforts.

Conclusion

In an ecosystem where constant change is now the norm, businesses should immediately take stock of their networks. If any mistakes inadvertently slipped through due to frantic attempts to ensure business continuity during the pandemic, now is the time to uncover them. Otherwise, they will only become more entrenched. If enterprises can obtain a holistic view of networks and security, a solid foundation for future growth and stability can be realized.

About the analyst

Hugh Ujhazy, ***Vice President, Internet of Things and Telecommunications, IDC Asia/Pacific***

Hugh is based in Sydney and leads the Internet of Things (IoT) and Telecommunications research practices for IDC Asia/Pacific. Besides leading the research and analysis of fixed and mobile network services across the region, which includes evaluating service provider and equipment vendor strategies, Hugh also drives research and thought leadership on IoT use cases. Hugh's insights help vendors, enterprises, and governments understand and navigate the evolving IoT ecosystem, identify potential solution vendors and partnership opportunities, develop go-to-market strategies and messaging, define and evaluate emerging IoT-enabled business models, and assess the financial and operational impact IoT will have on their organizations.

MESSAGE FROM THE SPONSOR

Tata Communications' point of view

Most enterprises in the digital trailblazer quadrant are in a constant "evaluate and evolve mode", creating a visible divide between have and have nots. Amitabh Sarkar, Vice President, Tata Communications, notes that a digital-first approach has helped enterprises achieve major competitive advantage, and the pandemic has only exacerbated this digital divide.

Our clients are looking to rearchitect their networks and build a digital fabric which is resilient, adaptive, and secure to deliver business outcomes. This digital fabric intuitively connects with an embedded layer of cloud-enabled security to deliver zero-trust network access, and also places the end-user experience at its core.

Two years on, we have helped many enterprises in the Asia/Pacific region to not only mitigate digital inequality but also build relevant and new revenue streams. Your journey starts today.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Asia/Pacific

83 Clemenceau Avenue
#17-01 UE Square West Wing
Singapore 239920
T 65.6226.0330
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.