IDC EXECUTIVE BRIEF

Cybersecurity Platforms: The Pursuit of Business Efficiency

April 2018

Carlo Dávila

Sponsored by: Kaspersky Lab

The digitization of the companies in Latin America on the 3rd Platform (i.e., cloud, mobility, social business, and Big Data/analytics) and the adoption of the Internet of Things (IoT) have resulted in an information technology ecosystem wherein the administration of security environments has become more complex. The challenges for the IT area are diverse: the insufficient traditional security strategies for digital business applications, the management of multiple security products from different vendors, the lack and high cost of talent in cybersecurity, and the restrictions on budget and number of specialized and certified personnel assigned to the security of the technology infrastructure.

This document analyzes why organizations should develop a less fragmented and complex IT environment, managed through an integrated cybersecurity platform with simplified security tools.

I. IDC OPINION

Traditional security products and conventional investment models make IT security management more complex.

Digital transformation, considered as a process in which organizations leverage changes in their business architecture to offer new products, services, and business models, is based on what IDC defines as the 3rd Platform technologies — cloud, social business, Big Data and analytics, and mobility. These disruptive changes to gain business competitiveness have resulted in more challenges related to cybersecurity to protect workloads in hybrid environments (on-premise and public, private, or hybrid cloud), with more vulnerable access points from smart mobile devices and social networks, including collaborative environments and data analysis within and outside the organization.

In other words, the impact of digital transformation on a company's information and operations further extends the attack surface. It is for this reason that a traditional security strategy is not enough to respond to the threats in new IT ecosystems, which are increasingly distributed, scalable, and mobile.

Another important aspect is that, over time, organizations have been investing in best-of-breed solutions for specific business security needs. The outcome is the presence of multiple security products and tools from disparate IT vendors, each with different use or licensing policies, and certification requirements, making it difficult to manage them. IDC has identified more than 70 cybersecurity manufacturers with presence in Latin America around the seven security product profiles defined by IDC.

According to the IDC Latin America Cybersecurity Report 2017, three out of five companies believe there will be a 15% reduction in cybersecurity investment. Currently, 50% of companies follow an investment model wherein they allocate less than 10% of their IT budget for cybersecurity solutions. It is also important to highlight that, at present, 31% of companies do not implement communication policies on security incidents. This may affect the first line of threat response (i.e., the employees). The former makes it clear that organizations need to develop cyberthreat awareness programs to develop their collaborators' prevention capabilities, hiring specialized services to support them in risk mitigation in a more efficient manner.

In addition to this scenario, increased attacks on networks, workloads, and web applications have made it evident the need to count on certified and specialized IT security staff. If we consider the presence of multiple manufacturers in the IT ecosystems of the organizations, it is understandable that the requirement of staff is greater, which creates additional challenges for CIOs and CISOs in Latin America, where three out of four companies consider it difficult to find personnel sufficiently qualified in cybersecurity.

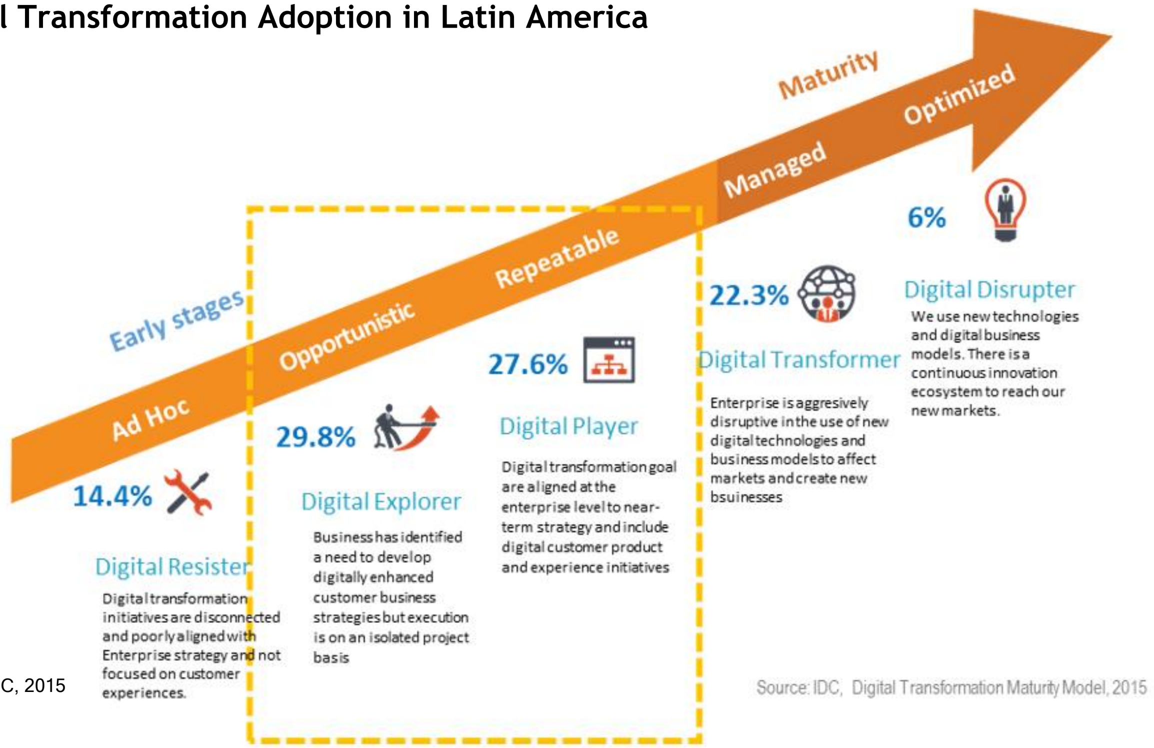
II. The Impact of Digital Transformation, Cloud, and Mobility on the IT Ecosystem

Investment in digital transformation initiatives has had a sustained growth (at a CAGR of 23% since 2015) in Latin America, expected to reach US$58 billion by 2020. Most of the businesses in the region are at an early stage of the digital transformation adoption, as seen in Figure 1. The new ecosystem, based on the 3rd Platform and innovation accelerators, such as the IoT, requires investment in security solutions aligned with the new digital ecosystems. However, only 6% of the organizations consider cybersecurity as a business transformation enabler. This is worrisome, given its impact on the operability of the organizations, the data sensitivity of the company and its business partners and customers, and the fulfillment of legal requirements in the country where the business is run — particularly in industries with greater regulation, such as government, finance, and telecommunications.

According to a report published by the Inter-American Development Bank and the Organization of American States in 2016, losses associated with cybercrime reached US$90 billion in Latin America, a region where the total enterprise IT investment is around 45% of such amount.

FIGURE 1

Digital Transformation Adoption in Latin America

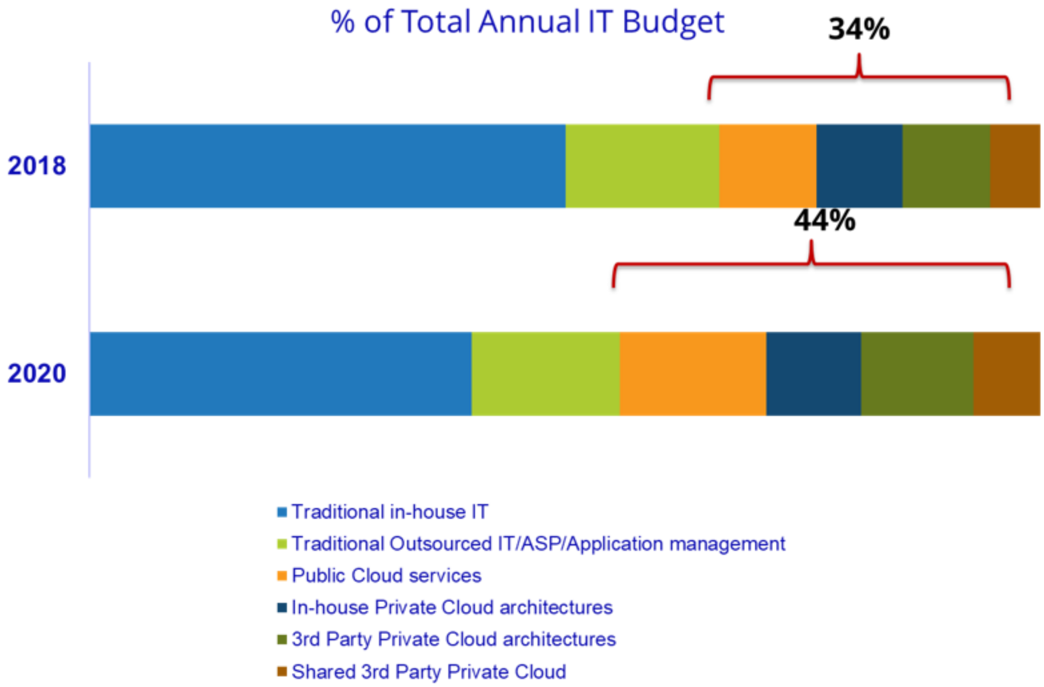

Maturity
Optimized
Managed
Repeatable
Opportunistic
Ad Hoc
Early stages
14.4%
Digital Resister
Digital transformation initiatives are disconnected and poorly aligned with Enterprise strategy and not focused on customer experiences.
29.8%
Digital Explorer
Business has identified a need to develop digitally enhanced customer business strategies but execution is on an isolated project basis
27.6%
Digital Player
Digital transformation goal are aligned at the enterprise level to near-term strategy and include digital customer product and experience initiatives
22.3%
Digital Transformer
Enterprise is aggresively disruptive in the use of new digital technologies and business models to affect markets and create new bsuinesses
6%
Digital Disrupter
We use new technologies and digital business models. There is a continuous innovation ecosystem to reach our new markets.
Source: IDC, Digital Transformation Maturity Model, 2015

Source: IDC, 2015

Cloud and mobility are the most dynamic pillars of the 3rd Platform in business transformation, making resources more efficient and speeding up the use of applications (see Figure 2). Thereby, the cybersecurity platform must be managed by integrating it into the security strategy from/to the cloud management profile, coupled with the management of traditional IT ecosystems (i.e., managing the security at the customer's premises; in the service provider's datacenter; in cloud environments [public, private, or hybrid] considering the access to workloads; and from mobile devices, endpoints, and smartphones). In other words, the cybersecurity strategy must be aligned with a 360-degree approach to the digital transformation's new operations and information models.

FIGURE 2

Multicloud Environments in Latin America



Source: IDC Latin America IT Investment Trends Survey 2017Q4

At present, mobility is among the top 5 priorities for Latin America businesses; 31% of the organizations in the region have pointed it out in the IDC Latin America Investment Trends, 2017Q4. Likewise, mobility is also a source of greater concern for IT areas. 85% of those responsible for cybersecurity (CISOs) believe that Windows-based laptops and desktops are the most vulnerable endpoints, followed by Android smartphones and tablets with the same operating system. Considering that security in a mobility ecosystem includes specific products, such as mobile security and vulnerability management, mobile identity and access management, mobile gateway access and protection, mobile information protection and control, and mobile threat management, it is surprising that only 45% of the CISOs are considering including such solutions within their investment plans in cybersecurity.

CISOs face budget reductions and lack of specialized personnel to manage security environments. On the one hand, 75% of the organizations are investing up to 20% of their IT budget in cybersecurity. However, 69% of them are making cuts of up to 40% in this matter. Also, 14% of the organizations are experiencing a reduction in the ratio of cybersecurity-specialized personnel over the total number of employees in the IT area. This could be due to the fact that 24% of the CISOs believe the recruitment of cybersecurity professionals is expensive, and 45% of the CISOs state that they do not find sufficiently qualified professionals to manage enterprise cybersecurity. The challenges become more evident if we consider that within the same organization, there is a need to administer multiple security products from different manufacturers. Therefore, change is required from a specific product approach into a platform of cybersecurity solutions, according to an organization's digital ecosystem and its new risk profile based on the changes in the business model.

This platform of cybersecurity solutions will reduce the impact of some of the main concerns of CIOs/CISOs, since integrating and automating certain processes of cybersecurity management, with machine learning tools, among others, simplifies the administration and contributes to reducing the need for a greater number of specialists in cybersecurity.

III. FUTURE PERSPECTIVES

In Latin America, the security solutions market is estimated to reach US$3 billion by the end of 2018. By 2020, the value is estimated to hit US$4.2 billion, with a CAGR of 12% in five years. From this last figure, it is estimated that 62% will come from the adoption of security services managed by third parties.

The growth of security services is driven by the pursuit of efficiency by organizations and the use of scarce resources, both economic and human capital. 14% of the CISOs in the region are considering outsourcing their cybersecurity management. The reasons are:

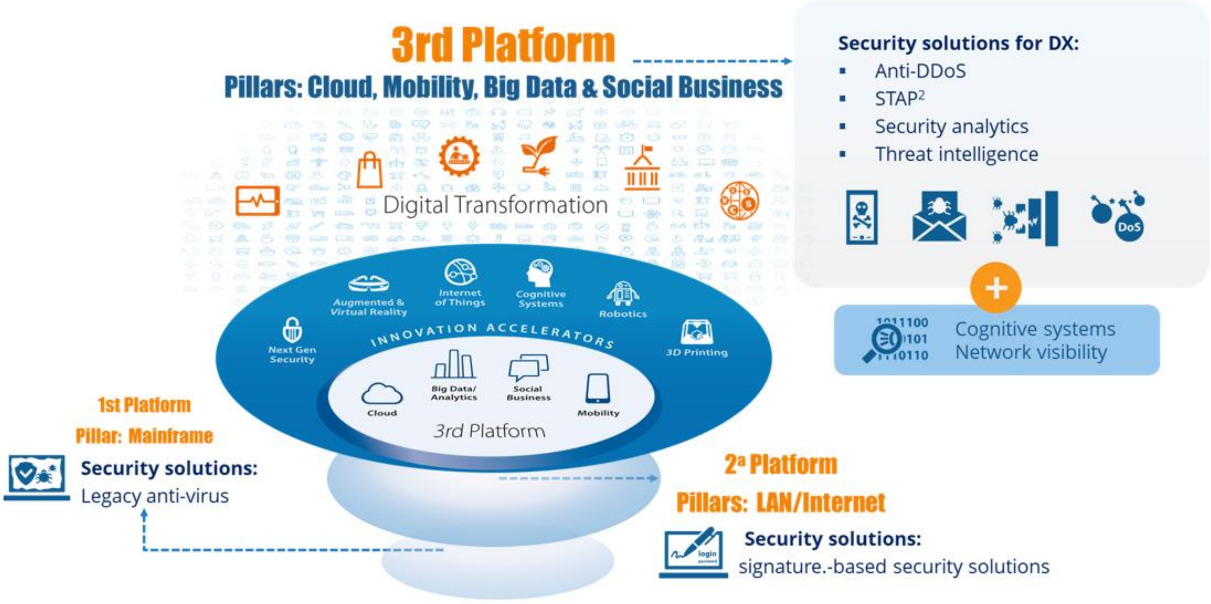
- The complexity of managing multiple security products from different vendors in the same technology infrastructure.
- The cost of certifications and training in security products.
- The lack of qualified professionals to manage the deployed solutions.
- The challenge to keep up to date on new threats that are increasingly sophisticated, complex, distributed, and evolving into automated processes.

IV. ESSENTIAL GUIDANCE

As enterprises adopt digital transformation projects, they must implement an analysis to know their enterprise risk profile and define a security strategy aligned with the 3rd Platform ecosystem and its innovation accelerators, such as automation and the Internet of Things, while looking for the optimization of resources and IT budgets (see Figure 3).

FIGURE 3

Security Solutions for Digital Transformation



More on 3rd- Plaform: http://www.idc.com/promo/thirdplatform

[2] Specialized Threat Analysis & Protection (STAP)

Source: IDC, 2018

IDC lists the following recommendations to implement a more efficient cybersecurity platform:

- Remember that digital transformation is based on the 3rd Platform, so you should not continue investing in traditional solutions, usually designed for the 2nd Platform.
- Include an analysis of cybersecurity according to your business transformation projects by identifying new elements in the IT ecosystem.
- Remember that disruptive technologies, such as robotics, automation, and the Internet of Things, result in a greater number of access points that require cybersecurity solutions with visibility, intelligence, and advanced analytics, and the use of cognitive systems.
- Analyze the consumption of cloud services and the execution of mobility projects, considering the following in the security strategy:
  - The administration of the environments in your premises.
  - The profile of workloads moved to the cloud and/or to hybrid environments.
  - The mobile ecosystems from which the company's business platforms are accessed.
- Evaluate and compare your strategic security plan and the use of a platform in your premises versus hiring an outsourced cybersecurity service, considering the costs of upgrades, certifications, and training in new security solutions.

- Implement a proactive and comprehensive security model for an adequate threats interpretation, the determination of timely actions, and the execution of an incident response program, whether internal or hired as a service.

And finally, change the cybersecurity investment approach with a 360-degree strategy, according to the new operations and information models of the digital business, relying on tools and services to simplify their management.

Sources and References

IDC Latin America Cybersecurity Report 2017

IDC Worldwide Security Products Taxonomy 2018.

IDC Digital Transformation Maturity Model, 2017

IDC Worldwide Semiannual Digital Transformation Spending Guide, 2017

IDC Web Application Firewalls: Critical Component of API Security

IDC Latin America Investment Trends, 2017Q4

2016 Cybersecurity Report Inter-American Development Bank and Organization of American States

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,100 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries.

IDC's analysis and insight help IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a subsidiary of IDG, the world's leading technology media, research, and events company. To learn more about IDC, please visit www.idc.com.

Follow IDC on Twitter at @IDC.

IDC Latinoamérica

4090 NW 97th Avenue Suite 350,
Doral, FL, USA 33178
+1-305-351-3020
Twitter: @IDCLatin
www.idclatin.com
www.idc.com

Copyright Notice