IDC VENDOR SPOTLIGHT

Cybersecurity in Cloud Ecosystems and Challenges in Mobility

June 2018

Carlo Dávila

Sponsored by: Kaspersky Lab

The cloud adoption trends in Latin America have created IT environments in which data and workloads, whether on-premise or in public, private, or hybrid cloud, are accessed from numerous equipments and devices within and outside the organization. So, cybersecurity should be restated from the cloud and for the cloud, and according to the company's risk profile.

In this document, we will describe how the evolution of cloud and its different ecosystems (e.g., EPC, PCS, DHPC, and ODHPC [see the Definitions section]) have increased the complexity and the attack surface in IT areas of Latin American businesses. In the same way, we will analyze the adoption of mobility in organizations in the region and the current state of investment for these environments. Additionally, we will review the offer of Kaspersky Lab solutions to face increasingly sophisticated and automated threats, their relationship with the evolution of cloud and mobility, and, finally, how organizations should change their approach to invest in cybersecurity.

I. INTRODUCTION

According to *IDC FutureScape: Worldwide IT Industry 2018 Predictions, LA Implications*, by 2021, the investment in the cloud — including services, hardware, and software — is expected to reach US$11 million, leveraging heterogeneous environments. 80% of the investments in multicloud environments, even from different suppliers.

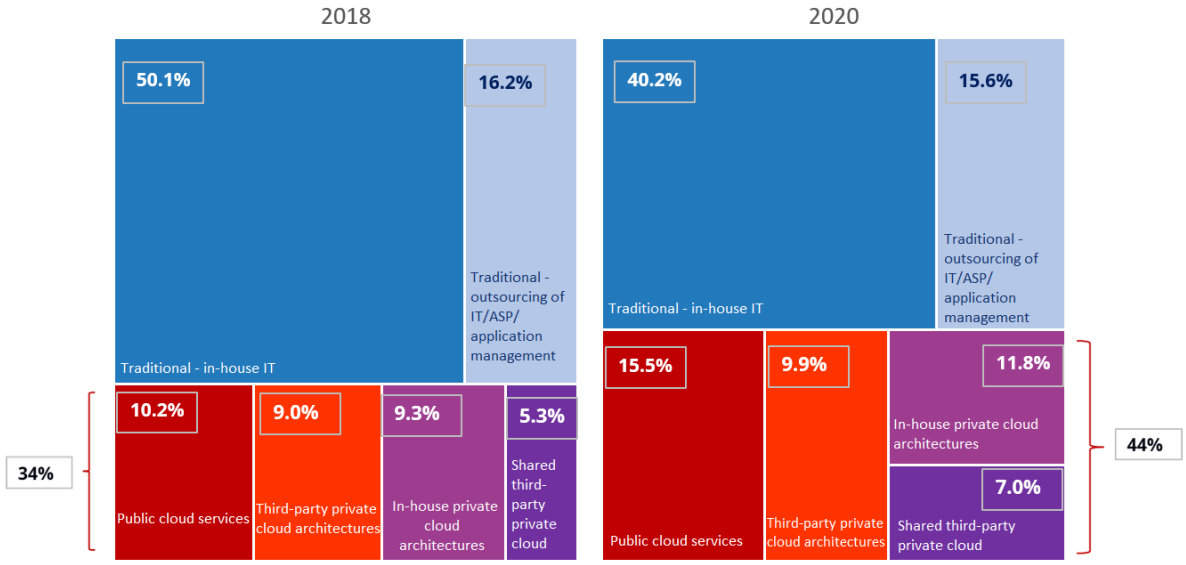
As shown in Figure 1, IDC IT Investment Trends 2017Q4 states that by 2020, 44% of the enterprise IT infrastructure will be managed in the cloud.

Moreover, the cloud infrastructure (IaaS) and applications (SaaS) are within the IT strategic priorities during 2018 for more than 23% of Latin American organizations[1] to improve the efficiency in the business resources and infrastructure and streamline the use of applications. Along with the cloud services, there are mobility initiatives that add more dynamism to the use of applications that have already been migrated to cloud environments to raise the efficiency levels in the business. These initiatives are prioritized by 31% of the organizations in the region, and they are among the elements that have increased the risks in security, considering the boom of devices and computers as access points within and outside the organization.

[1] IDC IT Investment Trends 2017Q4 (based on interviews with organizations with more than 100 employees in services, utilities, government, retail, manufacturing, and finance industries).

FIGURE 1

Multicloud Environments in Latin America



Source: IDC Latin America IT Investment Trends 2017Q4

Although cybersecurity is the main concern for CISOs, since 45% of the organizations in the region consider it the main investment initiative for 2018, the analysis of the IT budget allocation for this concept is not aligned with the growth of cloud and business mobility. Currently, the companies allocate less than 10% of their total IT budgets to security solutions, according to IDC Latin America Cybersecurity Report 2017. The same report reveals that three out of five organizations consider that there will be a 15% budget reduction in cybersecurity.

With this panorama of growth in cloud and mobility, and the restriction on IT resources, IDC considers that cybersecurity strategies should envision the security from these perspectives:

- The main entry points of potential attacks (i.e., end users' computers and mobile devices)
- The workloads in heterogeneous environments
- The datacenter itself or the services provider

To do so, what is needed is an understanding of the corporate risk profile and the company's operational and information models, relying on advanced and automated solutions and tools, along with additional layers of security services.

II. DEFINITIONS

The following definitions of cloud ecosystems are relevant to the development of the present document:

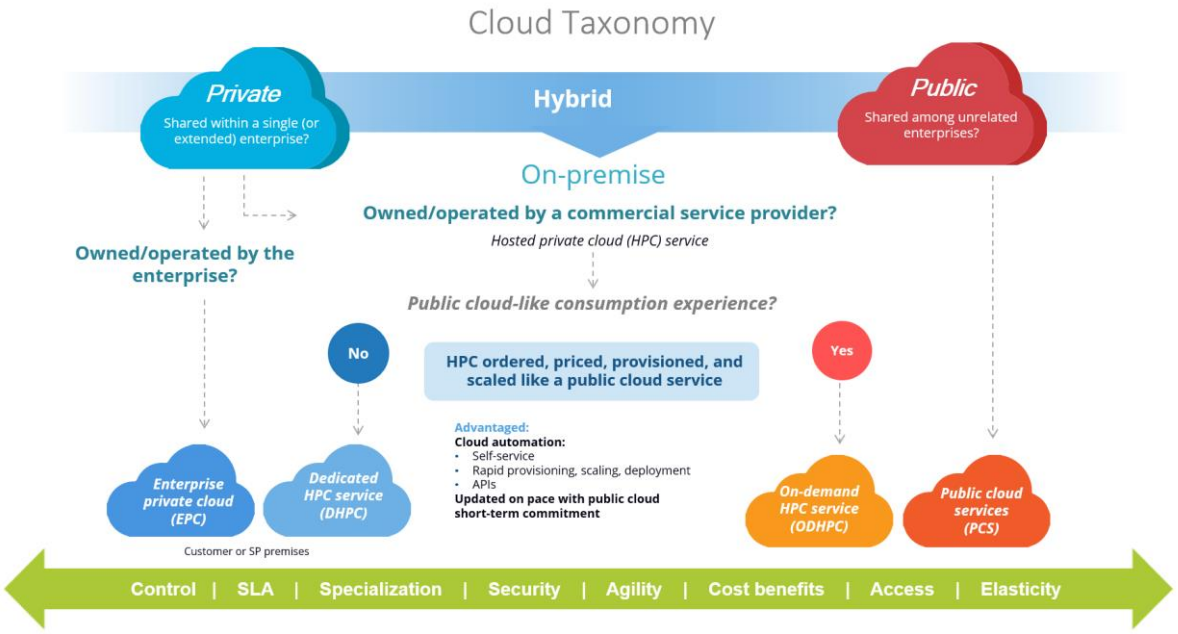
- **Cloud services ecosystems**
  - **Public cloud services (PCS)**. These are services provided and consumed on demand in a subscription model delivered by a provider through the internet to a company, such as:
    - **Infrastructure as a service (IaaS)**. This includes servers or virtual machines and storage from a provider that is paid for the used services.
    - **Platform as a service (PaaS)**. This is an on-demand environment for development, testing, administration, and delivery of applications. It includes databases and integration tools.

- **Software as a service (SaaS)**. This offers applications for users and organizations, such as industry solutions, collaboration tools, and security applications, among others.

- **Private cloud**. The services are provided by the company itself or a third party with a central operation and extended operation facilities, with more restrictions to access and a higher level of commitment of resources with long-term contracts. The private cloud can be classified as follows:
  - **Enterprise private cloud (EPC) services**. The resources are exclusive to the same company. The infrastructure, services, and administration, which reside on-premise, are the property and responsibility of the organizations.
  - **Dedicated hosted private cloud (DHPC) services**. They are hosted in the facilities of a services provider under a contract for a specific period. This model is essentially a cloud version of the traditional offers of managed hosting.
  - **On-demand hosted private cloud (ODHPC) services**. The hosting is in the facilities of a services provider that provisions resources dynamically to the dedicated use of an organization from a shared group.
- **Hybrid cloud**. It is an enterprise IT architecture that combines heterogeneous computing resources; public and private cloud infrastructure (IaaS), middleware (PaaS), and database/application (SaaS) resources; and nonphysical IT assets in an automated self-service configuration based on consumption and use policies.

FIGURE 2

Cloud Taxonomy



Source: IDC Taxonomy, 2015

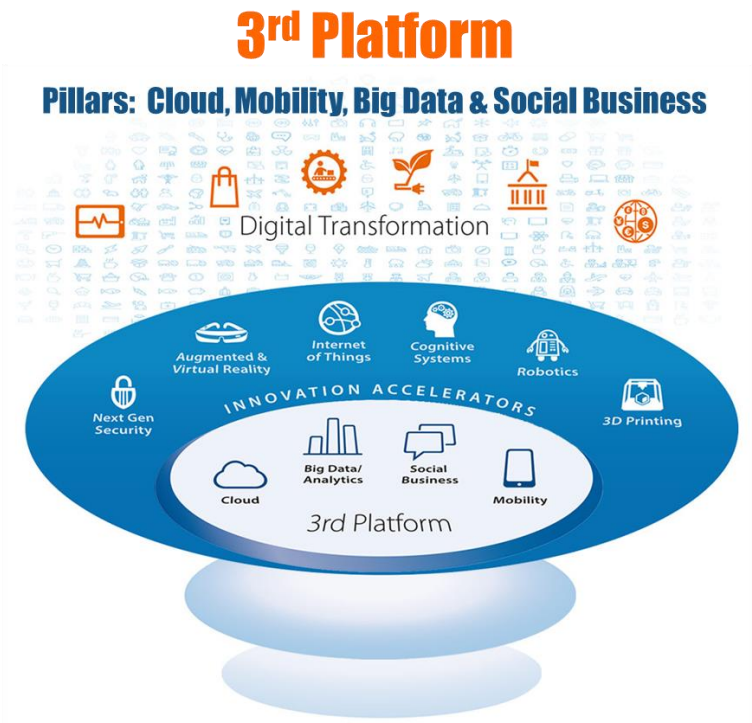
- **3rd Platform and innovation accelerators**. There are four pillars that make up the 3rd Platform of the current technologies in organizations: mobility, cloud, social business, and big data/analytics. They are the basis of the digital transformation of the businesses. The innovation accelerators are

disruptive technologies, such as next-generation security, virtual reality, Internet of Things, cognitive systems, robotics, and 3D printing (see Figure 3).

- **Digital transformation**. It includes transformation processes in five dimensions:
  - Leadership to develop a vision for the digital transformation of the business.
  - Omni-experience that enables the attraction and increase in customer loyalty.
  - Information to gain a competitive advantage.
  - Operating model to implement more efficient and responsive business operations.
  - Workspaces to transform the way to access, connect, or leverage human talent in a digitized economy.

FIGURE 3

The 3rd Platform — Basis of Digital Transformation



Source: IDC, 2018

III. TRENDS WITH IMPACT ON THE CYBERSECURITY OF THE BUSINESS

On the road to designing a cybersecurity platform aligned with the cloud's mobility and implementation strategy, you should consider the main access points, from the users' desktops to mobile devices, endpoints, and smartphones, as well as the risk profile of the industry where the business takes place.

The Need to Protect the Main Access Points Against Cybercrime

According to IDC Latin America Cybersecurity Report 2017, at present, phishing, malware, malvertising, and signature attacks are the most common in America, recording five to six incidents a year. To be specific, 76–84% of the attacks are of external origin in companies of any size or industry. Moreover, threats have become more sophisticated and have some automated processes that require

less action from the infected user to spread throughout the organization. This is because as companies have become digitized, more cybercriminals take advantage of the black markets to obtain automated tools and share privileged information that enables them to filter faster in the environments of an organization through employees, who inadvertently may have received an email on their desktops or mobile devices (endpoints) with malicious files. An action, as simple as clicking on a suspicious file or link, can result in virus propagation or hijacking the technology infrastructure and data of the company. It should be highlighted that 31% of the organizations have not yet implemented internal communication programs on potential security events. Meanwhile, 27% of the companies follow a communication protocol that is restricted to management levels. This approach negatively affects the first line of defense of a company — the employees — since Latin America is not a region that is actively investing in security services oriented to raise awareness on risks and attacks on the business itself.

Security Challenges in Mobile Environments

According to IDC IT Investment Trends 2017Q4, currently, 43% of medium-sized business employees in Latin America are relying on mobile devices to work. 80% of midsize and large corporations enable employees to connect from mobile devices (own or financed by the organization) to platforms and business applications. When we talk about mobility, we refer to the possibility of access to the network and the services of the technology infrastructure in the organization, from laptops, tablets, smartphones, or cell phones, whether for business or personal purposes. This makes clear the challenge of managing the access and security of multiple devices that can be used by employees, business partners, and customers who also interact with the company's data and information. Because of this situation, the majority of employees who oversee the IT security (CISOs) are concerned when mobility is within the top priority initiative for the organizations. Additionally, and according to the IDC Latin America Cybersecurity Report 2017, 85% of the CISOs consider that laptops and desktops with Windows operating systems are the most vulnerable endpoints, followed by smartphones (43%) and tablets (23%) with Android operating systems. Despite being aware of the safety risks of mobility, 55% of the companies in the region are not planning specific security investments for mobile environments (see Figure 4).

FIGURE 4

What Is the Status of the Investment in Mobile Security?

Source: IDC Latin America Cybersecurity Report, 2017

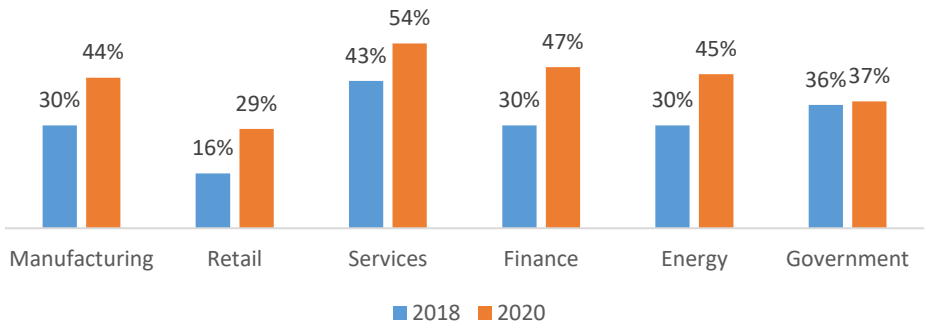
The Adoption of Cloud and Cybersecurity in Latin American Industries

Although 2018 is a year of elections or changes in federal administration, an atmosphere of optimism in IT investment in Latin America persists. More than 36% of the countries in the region consider that the investment will be greater by 2020. Particularly, as seen in Figure 5, the industries that currently invest the most in the cloud are services and government. However, by 2020, the finance, manufacturing, and energy markets will have the greatest dynamism in investment in the cloud, increasing by up to 17 percentage points. The figures shown include multicloud environments, such as:

- Public cloud services
- In-house private cloud architecture
- Third-party private cloud architecture
- Shared third-party private cloud

FIGURE 5

Percentage of Cloud Budget from the Total Annual IT Spending by Industry

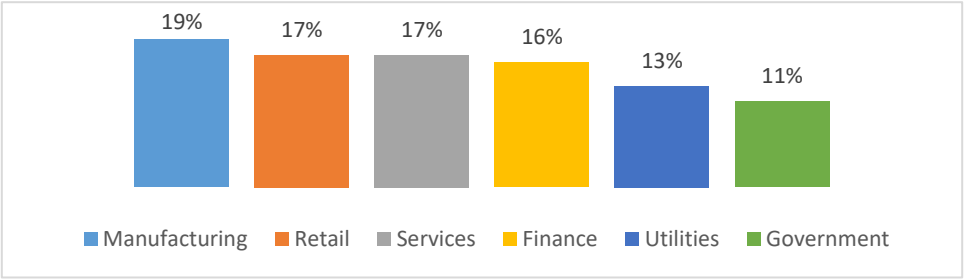


Source: IDC IT Investment Trends 2017Q4

From the security perspective, again referring to the IDC Latin America Cybersecurity Report 2017, the companies that allocate a higher percentage of their total IT budgets to cybersecurity are from the manufacturing (19%), retail (17%), services (17%), and finance (16%) industries (see Figure 6).

FIGURE 6

What Percentage of the IT Budget Is Allocated to Cybersecurity Solutions?



Source: IDC Latin America Cybersecurity Report, 2017

It is important to highlight that finance invests the most in endpoints security and security analytics, more than twice compared with any other industry, being one of the markets with the highest security requirements and regulations. The contrast is in the government sector, with 11% of the total IT budget in security spending. The main concerns on attacks in this industry, as well as finance, are phishing and malware.

For manufacturing, the most frequent attacks are phishing, malware, malvertising, and data hijacking (ransonware) in the corresponding order. One of the challenges for this industry is the adoption of disruptive technologies (e.g., Internet of Things) and, on the other hand, industry-specific risks, such as threats to the SCADA systems.

As explained earlier, each industry will have different paces to adopt cloud and mobility as well as divergent challenges on business security. Therefore, an analysis of the total IT ecosystem should be implemented to define a cybersecurity strategy according to the profile risk and business models of the organization.

IV. ADVANTAGES OF A CYBERSECURITY PLATFORM BUILT FROM THE CLOUD AND FOR THE CLOUD

The trend of multicloud environments in Latin America certainly makes it imperative to create a strategy that considers the use of a cybersecurity platform integrated and managed from the cloud and for the cloud. What we mean is to be able to manage security with a 360-degree vision, relying on security analytics, threat intelligence, process automation, cognitive, and network visibility systems to protect each layer and instance of cloud (public or private), the owned datacenter, and hosted workloads in a services provider, mobile devices, endpoints, and smartphones.

When an organization defines in its security strategy a change in the investment models, moving away from specific products and focusing more on the consumption of platform solutions, it manages to reduce the impact of certain CISO concerns with regard to:

- Fragmented infrastructure
- Budgets with capex profiles
- Need for a significant number of cybersecurity professionals
- Associated costs with training and certifications

If also, to be oriented to cybersecurity platforms, the organization seeks to establish a contract with a service model, and it may find additional benefits related to:

- Budgets with opex profiles
- Pay per use
- Associated costs to platform updates
- Scale capabilities
- Orchestration, consolidation, and centralization of security management
- Automation of processes
- Reduction of costs related to on-premise installations, power, and computing capabilities

V. OFFER AND CHALLENGES OF KASPERSKY LAB IN LATIN AMERICA

Kaspersky Lab is a global cybersecurity company with more than 20 years of experience in the market. The company uses its expertise in threats and security intelligence to develop security solutions and services to protect organizations, critical infrastructure, governments, and consumers around the world.

Kaspersky Lab's approach is to detect and neutralize any form of malware, based on knowledge of threats anywhere in the world and in any language, so it has a team of security researchers in Europe, Middle East, Asia, the United States, and Latin America, known as the Global Research and Analysis

Team (GReAT). Recently, and as part of its global transparency initiative, the company announced the opening of its first Transparency Center in the city of Zurich, Switzerland, by the end of 2019. Data of customers — in a first phase, from Europe, North America, Japan, Singapore, Australia, and South Korea — will be relocated, stored, and processed there. Moreover, Kaspersky Lab will relocate in the same facilities the programing tools to develop software based on its source code and will start to assemble the antivirus databases, signed digitally in Switzerland before the deployment on endpoints of customers worldwide. Kaspersky Lab will look forward to the independent supervision of a nonprofit organization, with the needed qualification to implement technical evaluations and software audits. Customers of Kaspersky Lab are diverse, from home and microenterprise users to medium-sized and large corporate organizations, in virtually any industry. Its installed base is 400 million users and 270,000 corporate clients.

The security portfolio of the company is extensive, including terminals protection and other security solutions as well as specialized services to combat the most advanced and evolving digital threats. In response to the security needs in endpoints and hybrid environments, Kaspersky Lab provides cloud-based security management consoles:

- **Protection of main endpoints**
  - **Kaspersky Security for Microsoft Office 365**. A security console, which similar to Microsoft Office 365, resides in the cloud. It is based on advanced technologies, such as automated detection systems, sandboxing, real-time threat information, and machine learning, to block the entry via email (Exchange Online) of ransomware, malicious files, spam, phishing, and Business Email Commitment (BEC), among others, while preventing the blocking or deletion of legitimate emails.
- **Mobile security**
  - **Kaspersky Endpoint Security Cloud**. This is a security solution for endpoints in Windows, Linux, Mac, and mobile devices, for personal or business purposes, that access to business data and information that reside in applications, shared folders, and cloud or on-premise platform servers, as per the European Union's General Data Protection Regulation. The configuration of security is centralized from the cloud through an online and remote management console.
- **Security for heterogeneous and multicloud environments**
  - **Kaspersky Hybrid Cloud Security**. It is an integrated security solution with Amazon Web Services and Microsoft Azure for software-defined (Linux or Windows) datacenters, protecting data, networks, systems, and workloads in physical, virtual, or cloud environments with orchestration techniques, operational hygiene, and cyber protection through intelligent behavior analysis and automatic learning algorithms, based on machine learning and artificial intelligence.
  - **Vertical solutions for industries**. These are solutions for industries with very specific regulatory and compliance requirements in cybersecurity, such as finance, telecommunications, healthcare, government, and manufacturing.
- **Digital corporate security**
  - **Business continuity strategy**. This includes threat and defense management solutions based on security technologies and cybersecurity services according to the organization's risk profile, from identification of attacks, to incidents investigation, to response and remediation, to functionality risks at every layer of the enterprise infrastructure.
  - **Corporate professional programs**. These are solutions on security awareness, sandboxing as a service, standard and premium support, and qualified security services, from design and implementation, updates, evaluation, and configuration of solutions by risk profile, to the remote or onsite monitoring and evaluation of the administration of security systems.

Kaspersky Lab delivers its solutions through more than 60 certified distributors in 19 Latin American countries. Technical and commercial training for its business partners is free through the partners' portal that includes interactive videos, webinars, and online exams, enabling a continuous education and update.

Challenges in Latin America

Similar to other providers of cybersecurity solutions, Kaspersky Lab faces challenges in Latin America. Firstly, there is insufficient investment and resources of organizations to protect the cybercrime target access points, which are desktops or the organization's end-user devices, permanently under attacks that are more and more intelligent and automated. Enterprise security awareness programs are required to be implemented along with the adoption of more automated and intelligent tools for timely threat detection.

Secondly, mobility initiatives have created the need for managing and protecting, locally and in the cloud, numerous endpoints from which enterprise data and information are accessed. This has also triggered the need for a specialized and constantly updated security staff on the evolution of cyberthreats. The reality in the region is that it is not easy to find security experts with the right certifications and who are able to manage multiple security products, even from different vendors.

Finally, we have different cloud instances, from public cloud services to private cloud architectures managed by a company or a services provider and hybrid environments. The result is a complex and quite heterogeneous environment. CISOs should continue managing the security of traditional IT environments and, at the same time, create a cloud-native security strategy that is in accordance with the organization's risk profile.

VI. CONCLUSIONS AND RECOMMENDATIONS

The losses associated with cybercrime in Latin America reached US$90 million, while the total IT investment in the region represented only 45% of such amount, according to a report by the Inter-American Development Bank and the Organization of American States in 2016. This gives us a dimension of the challenges in Latin America, a region where investment and security resources, risk prevention, and awareness strategies are not yet enough to cope with the growth of cloud and mobility projects.

IDC recommends that organizations should analyze the use of a cybersecurity solutions platform according to their IT ecosystems and risk profiles, based on the changes in the business model and their physical, virtual, and cloud infrastructure.

- Implement security threat awareness programs throughout the organization and design communication policies on cybersecurity incidents.
- Analyze the different layers of the IT infrastructure, workloads, networks, and services as well as the different local and cloud access points.
- Adopt a proactive and comprehensive security model for risk interpretation, determination of timely actions, and implementation of incident response programs, whether in-house or contracted as a service.
- Rely on next-generation security tools that can be cloud-native and based on security analytics and threat intelligence and complemented with cognitive and network visibility systems that expedite the work of the IT staff and enable an immediate, automated, and intelligent response to new threats.
- Evaluate the costs of updates, certifications, and training of staff on cybersecurity solutions with company-owned resources and compare them against the contracted services of security solution providers.
- Count on the services by security professionals for business executives and the IT area to help build use cases and justification of security solutions by the industry requirements and regulations where the business takes place.

It is also important to consider that security attacks are increasingly sophisticated and intelligent. So, it is important to rely on cybersecurity experts' consulting services for the design and evaluation of an appropriate security strategy, the constant monitoring and tracing of threats and risk indicators, and the audit of the corporate security that guarantees the business continuity.

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