



## Cybersecurity in Latin America

SPONSORED BY



# Contents

Introduction .....	03
The business implications of cybersecurity for Latin America .....	04
Latin America is standing up to the cybersecurity challenges facing it .....	05
Latin America's spending on cybersecurity .....	08
Compliance and regulation .....	11
The evolving landscape of cyber threats in Latin America ....	14
Ransomware: one of the key cyber threats targeting Latin America .....	17
The sectors targeted by ransomware .....	18
The CISO view: key takeaways from CISO interviews across Latin America .....	20
TecPar achieves real-time visibility, faster security response, and streamlined IT operations with Tanium .....	23
Recommendations .....	25
Sponsor .....	27

# Introduction

**According to Latin America thinktank Canning House, Latin America stands at a key juncture.** The “diminishing influence” of the West should offer the developing world’s most democratic and diverse region a bigger opportunity to shine on the world stage. The region’s attractions include a strong commitment to peaceful co-existence, respect for territorial integrity, human rights, free elections in most countries, and the environment. It has an abundance of natural resources, many of which are critical to the energy transition, and has ambitions to reorder the world’s security, diplomatic and economic architecture to accommodate new powers. It also enjoys good relationships across Africa, the Middle East and Asia, and enjoys substantial global soft power, including Brazil’s role in 2025 as the president of the BRICS Global South political and economic cooperation forum.

According to a World Bank blog, a recently published Cybersecurity Economics for Emerging Markets report highlights how Latin America’s rapid post-pandemic digitalization has outpaced the region’s cybersecurity capacity. By 2024, Latin America and the Caribbean had become the world’s fastest-growing region for disclosed cyber incidents, with a 25% average annual growth rate in the last decade.

This paper will discuss how Latin America is starting to take greater control of its cybersecurity landscape, including educating its end users, implementing new cybersecurity legislation across the region, playing a key role in international cybersecurity movements. All of these elements will play their part in developing Latin America’s cyber confidence, and ultimately, fostering its cyber resilience.



**HERIBERTO CABRERA**  
DIRECTOR OF TECHNICAL  
SOLUTIONS ENGINEERING,  
LATAM, TANIUM

---

*“The cybersecurity landscape in Latin America is a complex mix of opportunity and risk, where rapid digital transformation collides with persistent threats and risks. Yet, I firmly believe that establishing foundational visibility is key to identifying risks early and preventing attacks. This paper offers valuable insights into key challenges Latin American businesses face and provides real-world examples of how organizations are successfully elevating their cybersecurity posture.”*



# The business implications of cybersecurity for Latin America

**Organizations in Latin America are under constant cybersecurity pressure, with a growing risk landscape and continual new operational challenges.** The frequency and severity of data breaches and cyber incidents is rising. Cyber threat actors are ramping up their efforts and evolving their tactics to take advantage of unprepared or underprepared organizations. And that means most organizations. Attack surfaces are expanding because workforces are more remote, there is increasing Internet of things (IoT) device usage, greater prevalence of artificial intelligence (AI) in cyber technologies, including generative AI, and growing geopolitical risks.

Latin American countries exhibit the highest percentage of ransomware use in attacks on

organizations (79%) compared to the global average (53%). That suggests threat actors view organizations in Latin America as being more susceptible to ransomware attacks compared to the rest of the world, and so target them more widely. In terms of data breaches, Verizon's 2023 Data Breach Investigations Report findings show that 'system intrusion, social engineering and basic web application attacks represent 94% of breaches' in Latin America. According to the Latin America CISO 2023 Cybersecurity Report, 71% of cybersecurity leaders surveyed said that cyberattacks on their organizations increased from the previous year. That challenging cyberattack landscape explains why Latin America needs to increase its spending on security.



# Latin America is standing up to the cybersecurity challenges facing it

**Brazil has become a key player in the global market in the cybersecurity sector.** It has had to, because an increase in digital threats, due to the growth in online services in the country, coupled with a growing digitalization of services, has led to a need for more robust investments in cybersecurity. According to one survey, cyberattacks grew by around 70% in Brazil in one year. The need for greater cybersecurity investment has in turn increased demand for both more qualified cybersecurity professionals, as well as a need to develop more innovative solutions.

Despite the increasing numbers of attacks, Brazil's progress in developing its cybersecurity industry has led to it being named by LinkedIn Economic Graph as occupying the third global position in the growth of the cybersecurity sector. The ranking is based on the significant increase in the number of vacancies and cyber professionals specializing in the sector, as well as the importance of cyber protection for the continuity of services and business security.

The Latin America region has become a magnet for cyberattacks. Latin America currently receives more than 1,600 cyberattacks per second; As well as the growth in cyberattacks in Brazil, Mexico accounted for over half of all cyber threats reported in Latin America in the first half of 2024.

Latin America is one of the world's least-prepared areas for cyberattacks, according to an index compiled by the United Nations. Several reasons have been suggested for the region's cybersecurity challenges. One of the problems comes from what might be regarded as a definitive move towards an online, digital environment as a result of the Covid-19 pandemic, with Latin America witnessing notable innovation in areas like fintech and e-commerce.

The problem was that related and necessary efforts and investments to keep digital systems safe did not follow, and so effective cybersecurity measures have been lacking.

.....  
According to Louise Marie Hurel, founder of the Latin American Cybersecurity Research Network, *"Latin America's entrepreneurial and innovative spirit does not come with a concern for security,"* as reported in Americas Quarterly.  
.....

One of the first warning signs was a large ransomware attack that impacted Costa Rica in April 2022. The attack affected exports and exposed gigabytes of sensitive information online. In hindsight, it was a warning sign, a wake-up call for the entire region Latin America region. Some nations responded to it. Chile, in particular, did. And some countries have commendably started to put guardrails in place. But the red warning light has yet to be heeded by all.

One of the problems is a lack of education on the topic, which is allied to cyber naivete. And Latin America is not unique in having that problem. According to an IBM study, 95% of all cyberbreaches start from a human error. A successful phishing attack is one that gets someone to click on a video or an unbeatable offer they can't resist and then installs malware that invades a company's systems. A breach will then often stay undetected until the ransomware begins, or company data appears for sale on the dark web.

This is what happened to Argentina's entire population in 2021 after an anonymous hacker allegedly leaked the entirety of Argentina's National Registry of Persons, offering select information for sale on a dark web forum.



Similarly, residents of Medellín in Colombia bore the brunt of the consequences after a public services company, Empresas Públicas de Medellín (EPM) suffered a ransomware attack in December 2022 carried out by the BlackCat/ALPHV group, which disrupted the company's operations.

This lack of public awareness, allied to Latin America's still maturing cyber legislation, leaves IT security teams having to pick up the pieces.

On the following page are just a few snapshots from across Latin America in 2024, which demonstrate how Latin American organizations have been suffering from a siege of cyber breaches.

What these attacks show is that across the Latin America region, authorities need to reinforce cybersecurity legislation. Just as in Europe, where a series of cyberattacks led to the EU Cyber Solidarity Act, a data leak in Chile led to immediate action to tackle the situation. Chile enacted a comprehensive Cybersecurity and Critical Information

Infrastructure Framework Law to enhance the country's digital security landscape. The new law established the National Cybersecurity Agency (ANCI), which will have regulatory and enforcement powers over both public and private entities, ensuring a coordinated response to cyber threats.

The challenge now for other Latin America countries is to follow Chile's lead and enact similar laws to reinforce countries' own digital security landscapes. That is especially the case for Brazil, Mexico, and Colombia.

Another positive note in the face of escalating ransomware risks and the need for greater data security, is that government officials acknowledge the importance of strengthening cybersecurity across public and private sectors. One way of closing gaps in cyber readiness and response is to push ahead towards creating a cyber-resilient culture from the ground-up. A useful tool here is the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, which can be adapted to meet local needs.



## 2024: A Year of Cyberattacks

### JANUARY

Paraguay's largest internet provider, **Tigo**, was the victim of a ransomware attack that compromised its data center and impacted over 300 companies. The Black Hunt ransomware group encrypted over 330 servers and compromised backups, web pages, emails, and cloud storage.

### APRIL

Mexican food group **Grupo Bimbo** suffered a cyberattack that disrupted supply chain operations and exposed sensitive company data, requiring emergency protocols to restore operations.

### JUNE

Mexican telecom company **Claro** suffered unauthorized access which compromised millions of customer records, highlighting considerable vulnerabilities in telecom security records.

### JULY

An attack on several **Mexican government websites** led to temporary outages and website defacement by hacktivist groups.

A **massive data breach in Chile** came to light. The data leak affected over 10 million individuals, exposing sensitive personal information and raising concerns about the country's data protection infrastructure. The breach was traced back to a poorly secured database, which allowed unauthorized access to millions of personal records.

### AUGUST

The portal of the state government of **Alagoas** in Brazil was targeted by a cyberattack, disrupting access to essential services and data for several days. The attack was attributed to a group focused on government institutions.

The **Prefeitura de Ponta Grossa** in Brazil was hit by a ransomware attack on the city's administrative systems, which led to a suspension of various public services. The attackers demanded a ransom in cryptocurrency.

The Mexican social security institute, the **Instituto Mexicano del Seguro Social (IMSS)**, was hit by a ransomware attack that disrupted services and threatened the release of sensitive patient data unless a ransom was paid.

### SEPTEMBER

**Empresas Públicas de Medellín (EPM)** in Colombia fell victim to a cyber intrusion that hit operational systems, causing interruptions in electricity and water supply across Medellín.

The **Hospital das Clínicas**, São Paulo, Brazil, suffered a ransomware attack which encrypted patient records, disrupting services and raising concerns about healthcare data security.

### DECEMBER

Costa Rica's state-owned energy provider, **Refinadora Costarricense de Petróleo**, known as RECOPE, suffered a ransomware attack that required a shift to manual operations and a call to US experts for help.

# Latin America's spending on cybersecurity

## Brazil has comfortably the greatest level of spending on cybersecurity in Latin America.

The country will spend around \$9 billion on cybersecurity in 2028. Mexico will spend \$3.6 billion, Colombia \$1.3 billion, and Chile around \$1 billion. The rest of South and Central America together almost matches Mexico's spending.

The biggest growth in cybersecurity spending for Latin American countries, in particular Brazil, Mexico, Colombia, and Chile is in network security, which has a compound annual growth rate between 2023 and 2028 of 21.3%. The next most important cybersecurity

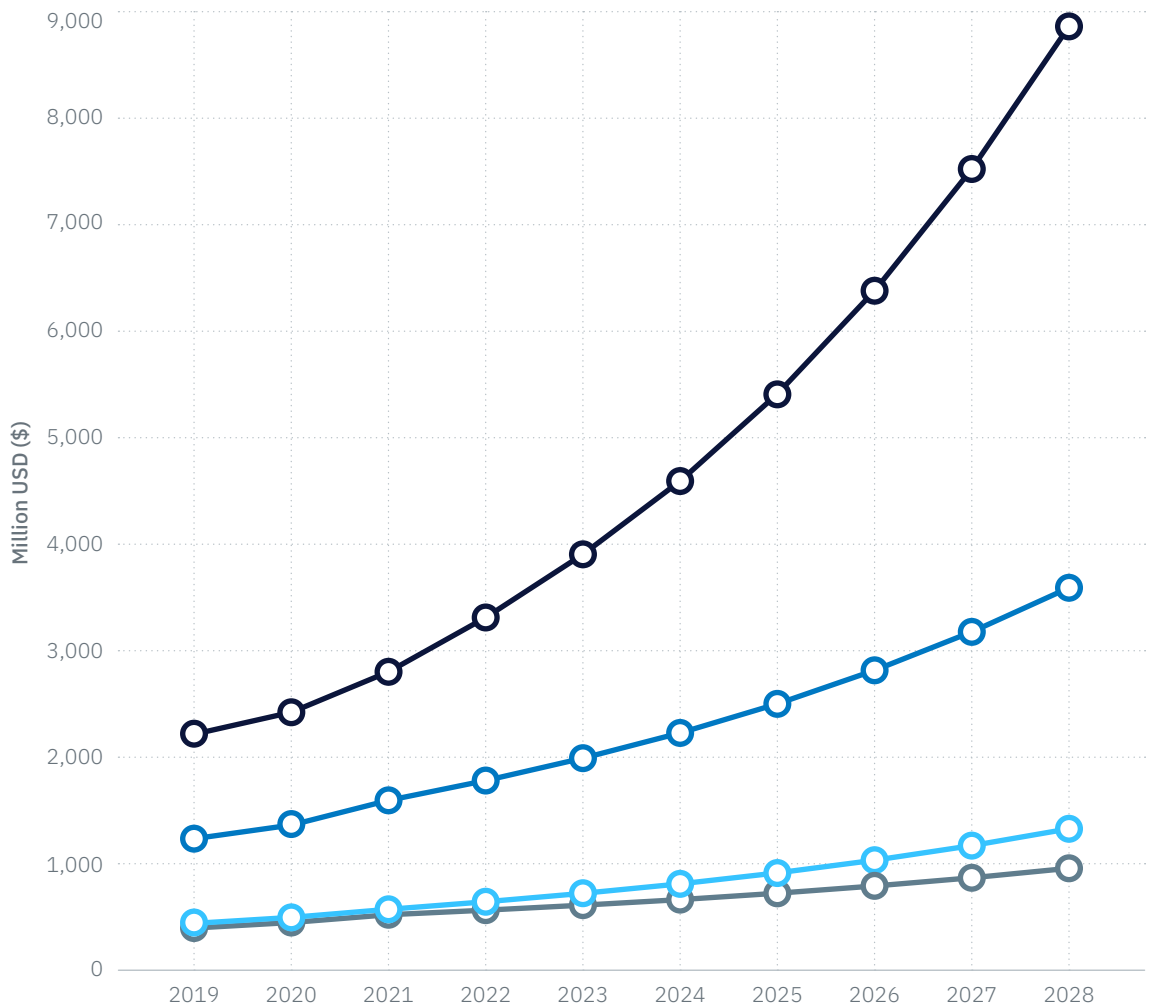
product or service is web security, with a 19.8% CAGR over the same time period. Other notable growth rates are for fraud prevention and transactional security (19.3%) and application security (19.2%).

The greatest spending is in managed security services, which has a CAGR of 15%. Other notable CAGR rates are content filtering and anti-spam appliances (15.9%), network monitoring and access control (15.5%), multi-factor authentication (12.3%), and endpoint security (12.1%).

### Brazil dominates Latin America's spending on cybersecurity, outstripping Mexico, Colombia, and Chile

Brazil's CAGR from 2023 to 2028 is 17.8%, ahead of Colombia (12.9%), Mexico (12.6%), and Chile (9.38%)

Key:  
● Brazil  
● Mexico  
● Colombia  
● Chile



Source:  
GlobalData



The chart below shows the breakdown on security spending by vertical. The vertical featured are energy, healthcare, manufacturing, financial markets, government, information

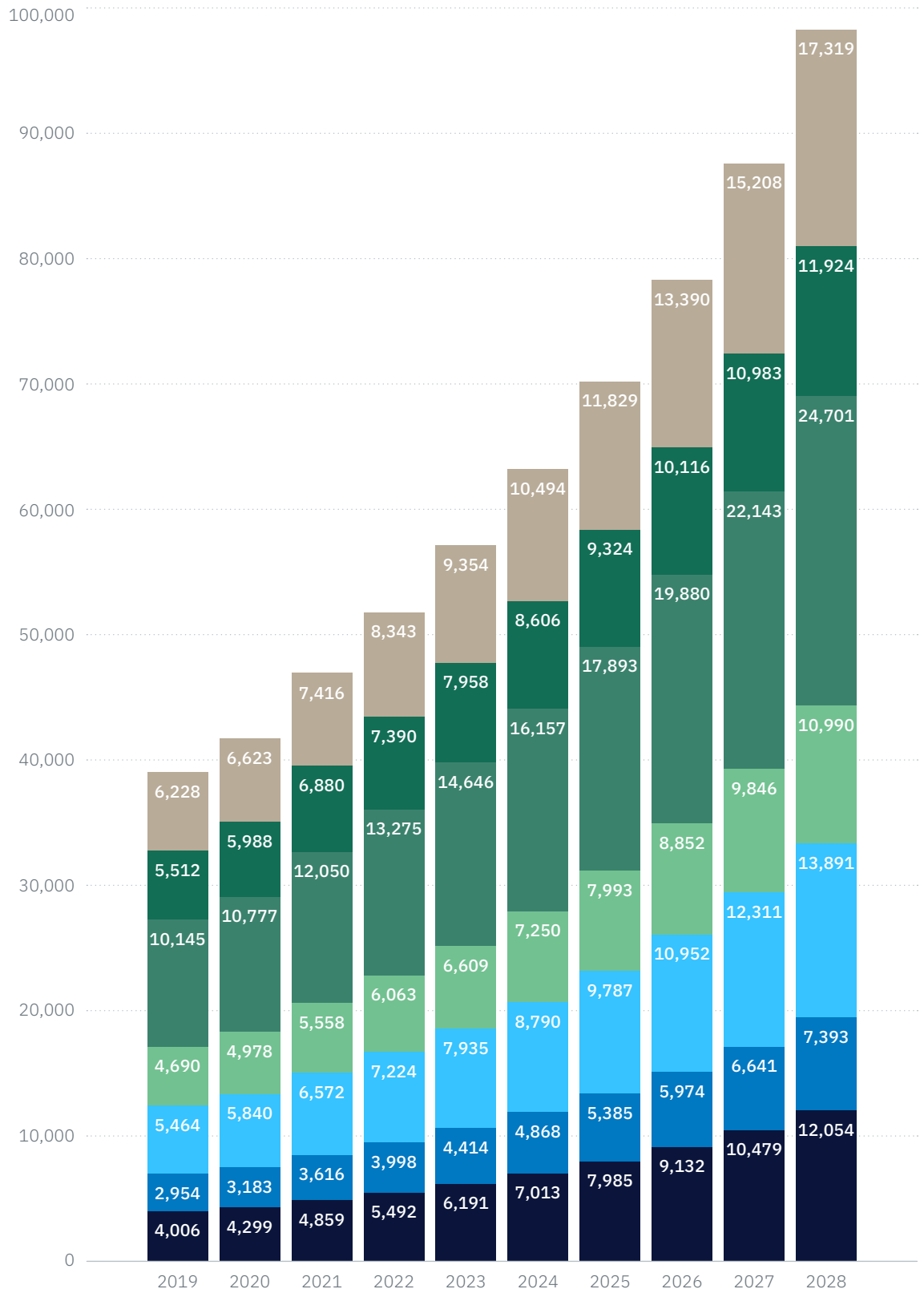
technology, insurance, and retail banking. Retail banking accounts for the greatest spending on security, followed by information technology, manufacturing, and energy.

**Retail banking, information technology, energy, and manufacturing are the biggest vertical market spenders on security in Latin America**

Energy, at 14.3%, has the highest compound annual growth rate (CAGR)

Key:

- Retail banking
- Insurance
- Information technology
- Healthcare
- Government
- Financial markets
- Energy



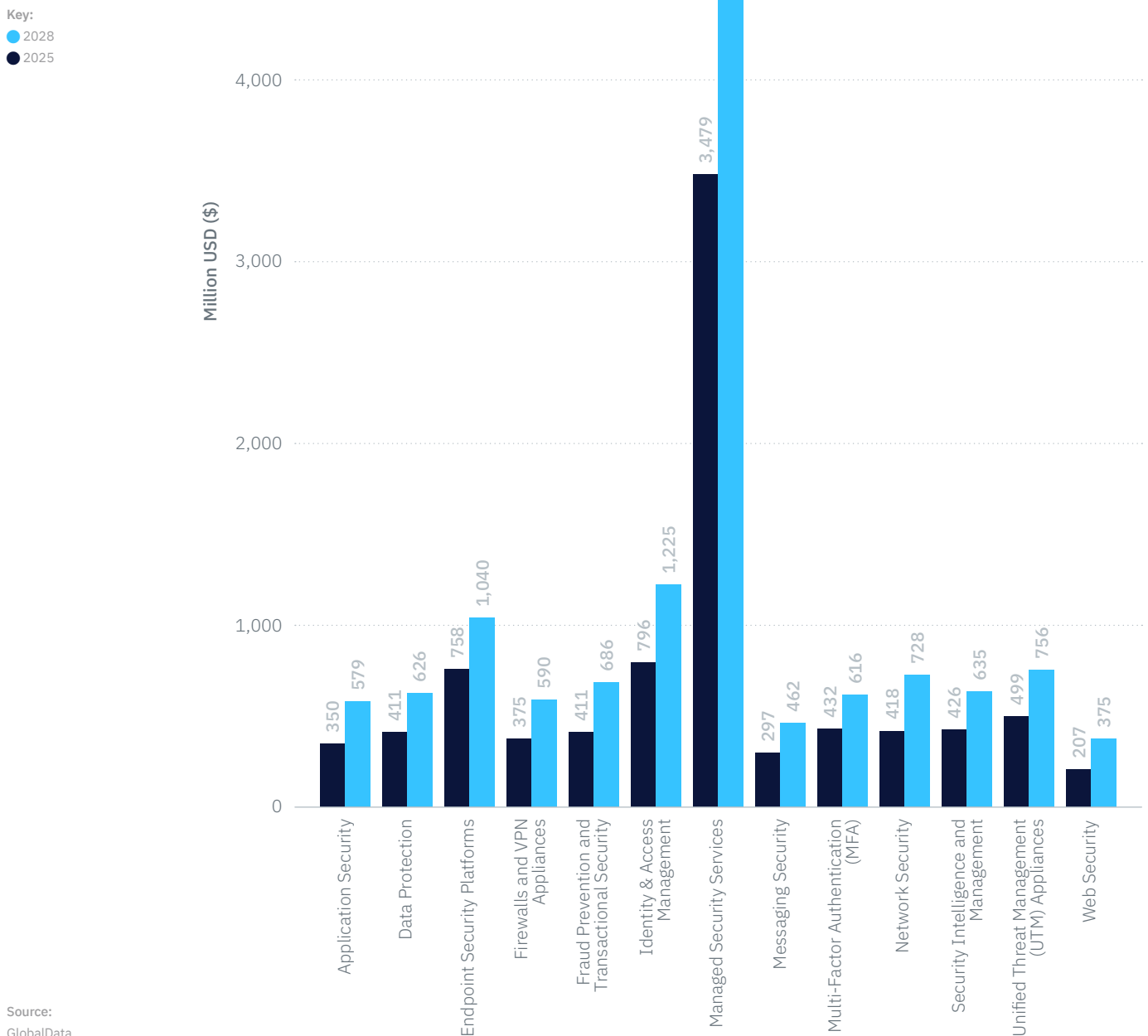
Source:  
GlobalData

The chart below details Latin America cybersecurity spending for 2025 and 2028 by product. The product areas with the strongest compound annual growth rate (from 2023

to 2028) are application security (20.43%), fraud prevention and transactional security (20.45%), web security (21.04%) and network security (22.68%).

**Managed security services will dominate the Latin American cybersecurity product mix, both in 2025 and 2028**

Identity and access management and endpoint security will also play a major role



# Compliance and regulation

**In its Global Cybersecurity Outlook 2024, the World Economic Forum (WEF) referenced the ‘cyber inequity’ among certain geographies as a concerning issue, describing the lower number of self-reported cyber-resilient organizations in Latin America and Africa (in comparison to higher numbers in North America and Europe) as a gap that ‘unsurprisingly ... tends to mirror other global development indicators.’**

At the heart of these issues in Latin America is a lack of effective cybersecurity compliance and regulation. But things are starting to change. Chile enacted a comprehensive Cybersecurity and Critical Information Infrastructure Framework Law to enhance the country’s digital security landscape. And now other countries are also following suit.

## BRAZIL

**Cybersecurity in Brazil saw a significant regulatory milestone with the creation of the National Cybersecurity Policy at the end of 2023.**

The National Cybersecurity Policy, known as PNCiber, is intended to improve national cybersecurity and to align it with international best practices. The launch of PNCiber was accompanied by the creation of the National Cybersecurity Committee (CNCiber) an important monitoring development to designed to oversee the implementation and evolution of the policy, as well as evaluating and proposing updates to it.

The PNCiber was created to guide cybersecurity activities in the country. The principles of PNCiber include national sovereignty, guaranteeing fundamental rights, prevention of cyber attacks, resilience to cyber incidents, education and technological development in cybersecurity, cooperation between public and private entities, and international technical cooperation. PNCiber’s launch demonstrates the government’s growing attention to cybersecurity and paves the way for the development of a digital security culture in the country.

Similarly, the National Cybersecurity Policy is an important milestone in the protection of Brazil’s digital infrastructure and will require continuous collaboration and adaptation to changes in the cyber threat landscape to achieve its full security and data privacy potential.





## MEXICO

### **According to one estimate, Mexico has the highest rate of cybercrime in Latin America.**

That assessment is based on the size of its economy (the fifteenth-largest in the world) and the degree of internet penetration in the country (which stands at 83.2%). Mexico also accounted for the second-highest percentage (17%) of online advertisements regarding ransomware data theft in Latin America.

Creating a National Cybersecurity Strategy is a positive development to try and prevent cyberattacks. But it is not a guarantee of success. Mexico's National Cybersecurity Strategy (ENCS), published in 2017, has suffered from a lack of effective action. And yet, ENCS still offers a possible starting point for what needs to be done to make Mexico more cyber-resistant.

Mexico took its time adopting a national cybersecurity law. Legal provisions on cybersecurity were instead spread across laws in different sectors, such as finance, telecommunications, labor, consumer protection, and intellectual property. It was not until April 2023 that the Mexican Congress finally introduced a National Cybersecurity Bill.

Its most important provisions include: developing specific legal protections for digital rights (for example, digital inclusion, net neutrality, and online consumer protection); requiring private companies to collaborate with the government to address cybersecurity matters; creating an executive-controlled National Cybersecurity Agency to coordinate cybersecurity efforts, and undertaking countermeasures to combat malicious cyber activity.



## COLOMBIA

### **In 2022, the Colombian government issued legislation, Decree 338, that established general guidelines for digital security governance, with which it sought to combine and boost legal development, technical advances, as well as state and private knowledge to strengthen the country's cybersecurity.**

This decree strengthened the line of work of digital security in Colombia, which is necessary for the protection of critical national and industrial infrastructure that is on the receiving end of malware and ransomware attacks globally.

Decree 338 commits Colombia's Ministry of Information and Communications Technologies to raise the inventory of national cyber public critical infrastructures and essential services in cyberspace, updating them every two years. The legislation also promised the creation of sectoral CSIRTs (Computer Security Incident & Response Teams) as well as a National Platform for the Notification and Monitoring of Digital Security Incidents, a space that will serve for the notification and management of cybersecurity incidents.

In a summary of Colombia's digital economy, published in September 2024, the International Trade Administration, part of the US Department of Commerce, noted that Decree 338 would enhance digital security, but added that compliance can be demanding, particularly for smaller businesses needing more resources and expertise.



## CHILE

**Chile's cybersecurity law is the gold star for Latin America. Chile moved towards a more resilient cyber landscape for its citizens and the Latin American region on March 26, 2024, when it enacted the new Cybersecurity and Critical Information Infrastructure Framework Law.**

The new framework and the regulations it creates enable Chile to strengthen its digital security.

A key part is Chile's new National Cybersecurity Agency (ANCI), which is designed along the lines of cybersecurity agencies in other countries, such as the US Cybersecurity and Infrastructure Security Agency (CISA) and the UK's National Cyber Security Centre (NCSC-UK). ANCI will have advisory, regulatory, supervisory and sanctioning powers, both for public and also for private organizations.

Chile's new law also establishes "essential services," which must follow ANCI's requirements. These essential services include critical infrastructure, banking, transportation, the energy sector, telecommunications, healthcare, the pharmaceutical industry and information technology. Companies in these sectors will be required to have cybersecurity plans, be regularly reviewed and conduct cybersecurity simulation exercises.

The law establishes minimum requirements that covered entities must implement to prevent and mitigate cybersecurity incidents, and also includes incident response requirements to help agencies and companies better respond to cybersecurity incidents. It also mandates required reporting so the government can track incidents and coordinate additional responses if needed.



# The evolving landscape of cyber threats in Latin America

**In 2024, Brazil held the chairmanship of the G20 group of the world's twenty largest economies.** The year culminated in the G20 summit in Rio de Janeiro which discussed the world's most pressing challenges. One might argue that cybersecurity should have been added to the list of topics discussed alongside social inclusion, global governance reform, and energy transitions because Brazil's growing international influence is making it a target for cybercriminals.

The bigger Brazil's growing profile on the world stage becomes, the more it is at risk, both from cyberthreats from abroad, and from a thriving criminal ecosystem from within. Brazil is now the world's fifth-most-populous country and in 2025, it will assume leadership of the now expanded BRICS intergovernmental forum of developing countries, which Brazil originally founded with Russia, India and China, and later South Africa.

There are, however, some rankings that Brazil would perhaps prefer to lose. For example, Brazil is the second-most-targeted country of ransomware-as-a-service group RansomHub, based on listings on its leak site, according to a blog post from Google's Threat Analysis Group.

"As Brazil's influence grows, so does its digital footprint, making it an increasingly attractive

target for cyberthreats originating from both global and domestic actors," the blog post says. "At the same time, the threat landscape in Brazil is shaped by a domestic cybercriminal market." Those cybercriminals include mainly Brazilian Portuguese-speaking hackers, who are carrying out account takeovers, carding fraud, financial data exfiltration using banking malware, and ransomware across Latin America.

It is not just Brazil that is seeing unwanted cyber interest. In Mexico, Fresnillo, the world's largest primary silver producer and Mexico's largest gold producer, admitted in July 2024 that attackers gained access to data stored on its systems during a recent cyberattack. The company mining revealed in a filing with the London Stock Exchange that it was "the subject of a cyber security incident which has resulted in unauthorized access to certain IT systems and data."

Upon discovering the attack, Fresnillo said it had initiated response measures to contain the breach, and its IT experts are investigating and assessing the incident's impact in coordination with external forensic specialists.

The following summarizes the state of cybersecurity trends across Latin America.

## A challenging picture

More than 1,600 cyberattacks are reported in Latin America per second, making cyberattacks one of the fastest-growing security problems in the area. At the same time, the economic damages of cyberattacks exceeds 1% of some countries in the Americas' GDP and rises to 6% if critical infrastructures are attacked. The volume and sophistication of cyberattacks registered in Latin America are on the rise, with organizations in countries like Brazil and Mexico ranked among the top global targets for cybercriminals. Both countries are particularly appealing for hackers due to the region's combination of increasing digitization and generalized cybersecurity immaturity.



## Concerns about geopolitics

A complex and often shifting geopolitical landscape has the same serious implications for cybersecurity within Latin America as around the rest of the world. No region can afford to be complacent about cyber threats from criminals, “hacktivists,” or hostile states, and least of all Latin America. Developing countries, including those in Latin America, are expected to respond effectively to cyber threats, but lack the structural factors to do so. Disparities in development across the region mean that the cybersecurity needs of different countries can vary significantly. Brazil’s cyber defense capabilities are generally well regarded, though still are not as sophisticated as those of Western states or as well organized as Chile’s. Meanwhile, when it comes to global geopolitical issues, Brazil does not fully partner with North American and European states, but has cautiously engaged in cyber cooperation with China and Russia and supported some of their initiatives. Brazil’s role in cyber governance and its stance on international cyber norms will be shaped by its strategic interest in maintaining an independent, influential position in global affairs.

## Skills gap and responsibility gap

A complex and often shifting geopolitical landscape has the same serious implications for cybersecurity within Latin America as around the rest of the world. There is a substantial cybersecurity skills gap worldwide, with demand significantly outweighing supply. According to GlobalData’s Job Analytics, the average number of open cybersecurity jobs per month globally in 2022 was just under 180,000. The average number of closed cybersecurity jobs per month was significantly less at a little over 60,000.

A 2022 survey by the World Economic Forum found that 59% of businesses would struggle to respond to a cyberattack due to the shortage of cybersecurity talent and skills. Cyberattackers exploit skills gaps in organizations to extract information. The general lack of cybersecurity staff everywhere compounds the problem.

In Latin America there is an estimated cybersecurity workforce gap in Mexico and Brazil of nearly 516,000 people. This means that the shortage of cybersecurity personnel in Mexico is second only to the shortage in the United States. However, there is notable growth in cyber jobs. The growth rate for cyber professionals in Mexico in 2024 was 64.6%, against a growth rate of 27.3% for other professions. Chile’s growth rate was 28.7%, against a growth rate for other professions of 2.9%.

## AI drives social engineering fears

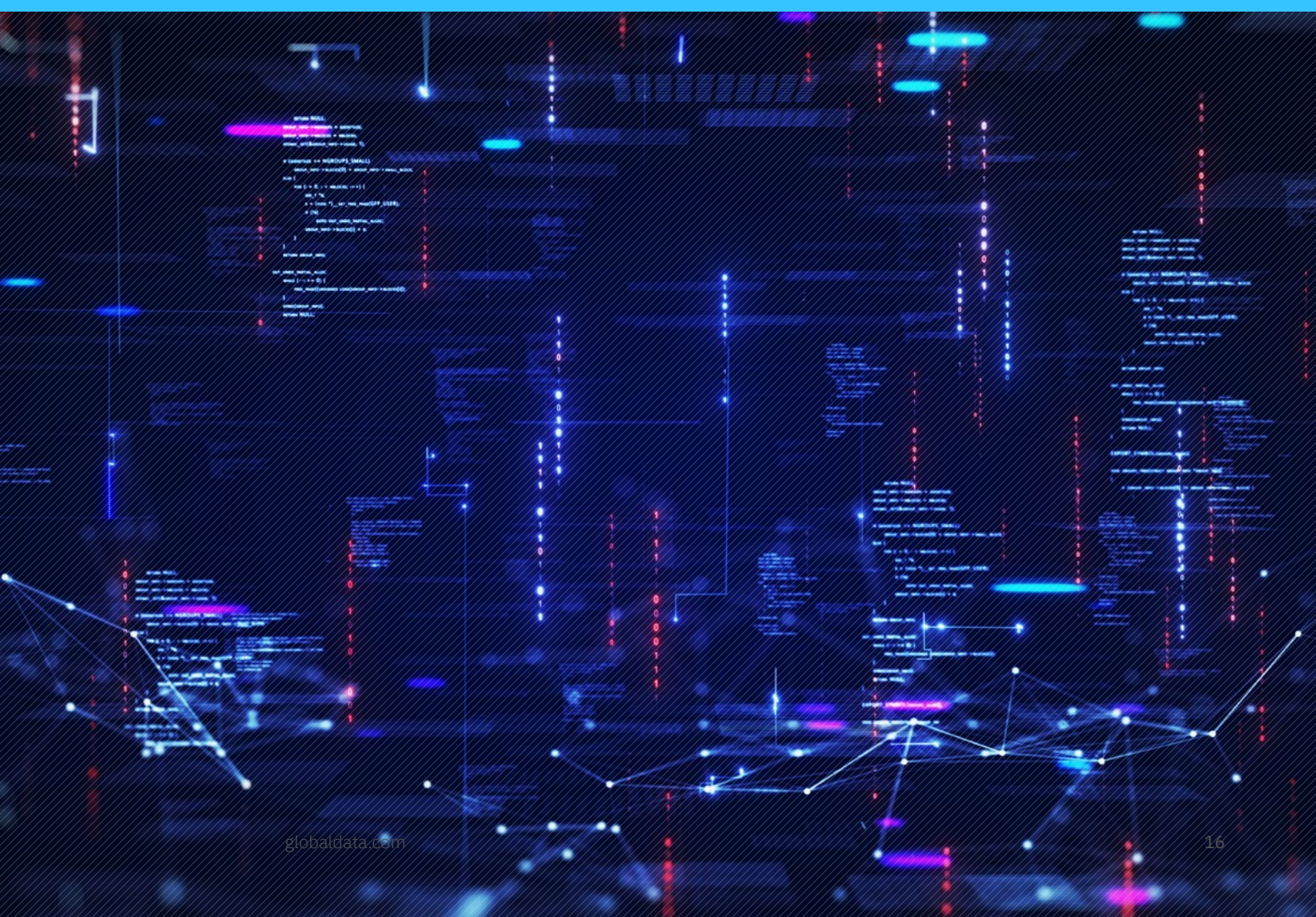
While other technologies such as cloud solutions have become more commonplace in the region over the last few years, with similar issues surrounding people, processes, and technology continuing – for example, up to 41% of organizations in Latin America have been struggling to fill cloud security roles since 2022 – AI has quickly become the new vector of both defense and attack over the last year. Generative AI will provide threat actors with powerful new tools to conduct convincing social engineering at scale. Advanced natural language models like ChatGPT will enable attackers to churn out personalized, targeted phishing emails and text messages that appear remarkably human. Attempts to manipulate staff via social media are set to rise. As this technology advances, we may see threat groups use deepfakes to spread misinformation or compromise high-value targets through tailored social engineering attacks across communication channels.

## Managing the people problem

One of the major challenges in Latin America is in ensuring that employees are adequately aware of the cyber issues they face. That means having to adapt to new standards and regulations, improve collaboration, or increase budgets for training and education on cybersecurity issues. Education is key because 41% of cyberattacks in Brazil have been successful in the last two years. Yet 60% of organizations say they are focused almost entirely on fighting successful attacks rather than trying to prevent them. 72% of businesses believe their organization would be more successful at defending against cyberattacks if it devoted more resources to preventive cybersecurity. That means creating strategies to convince boards for greater budgets by ensuring they fully understand the risks posed by cyberattacks and by failing to overcome the people problem.

## An expanding threat landscape

The threat landscape faced by Latin American companies is continually expanding beyond current cyber defenses. Many of the largest risks from 2023 have been exacerbated going into 2024. An escalation of ransomware attacks, AI-based predictive social engineering opening up new threats, and a lack of necessary Zero Trust architectures means threats remain significant for businesses throughout the region. Hence, strengthening the shield that companies use to protect themselves from these cyber threats is becoming necessary through the training of cybersecurity professionals and adequate legislation. Cybersecurity is now a primary concern for organizations in Latin America.





# Ransomware: one of the key cyber threats targeting Latin America

**Latin America continues to be a major target for ransomware attacks from 2023 to the present.** Over 100 ransomware attacks have been reported, with Lockbit leading with 59 attacks, followed by Alphv, Clop, and others. The manufacturing sector has been the hardest hit, experiencing 18 attacks, followed by financial services and technology, each with 10.

Retail and logistics have also faced significant disruptions. One of the particular concerns is the sale of compromised data, including email accounts and sensitive databases, is prevalent, highlighting regional cybersecurity vulnerabilities. Advanced malware campaigns are increasingly targeting the finance, technology, and government sectors.





# The sectors targeted by ransomware

## Ransomware attacks have predominantly impacted the following sectors:



**Manufacturing:** Approximately 18 attacks, making it the most affected sector. These attacks have disrupted production lines and caused significant financial losses.



**Financial Services:** Around 10 attacks, targeting banks, investment firms, and other financial institutions, often leading to data breaches and financial fraud.



**Technology:** Approximately 10 attacks, impacting IT services, software companies, and technology providers, leading to data breaches and operational disruption.



**Retail:** About 9 attacks, causing disruptions in supply chains and financial losses due to ransom payments and data breaches.



**Logistics:** Approximately 7 attacks, affecting transportation and warehousing services, leading to delays and financial impacts.



**Education:** Around 5 attacks, targeting schools, universities, and educational institutions, often leading to data breaches and operational disruption.



**Legal:** Approximately 5 attacks, impacting law firms and legal services, leading to breaches of sensitive client information.



**Energy:** Approximately 4 attacks, targeting utilities and energy providers, leading to significant operational disruptions.



**Government:** Approximately 4 attacks, impacting government agencies and services, leading to data breaches and operational disruption.

The chart on the following page indicates how many cyber incidents in Latin America have evolved beyond just aiming for financial gains, especially in developing countries, where 59% of cyber incidents are politically driven, according to the Cybersecurity Economics for Emerging Markets report published by the World Bank. Latin America has seen a shift to what are described as “hybrid” incidents. For example, a ransomware attack to government institutions that caused economic losses of about 2.4% of GDP (Costa Rica, 2022); data breaches to public agencies that exposed confidential records of nearly every citizen (Ecuador, 2019; Argentina, 2022); a malware attack that provoked the shutdown of all public bank branches (Chile, 2020); and a cyber incident that prevented citizens abroad from casting their votes during the presidential election (Ecuador, 2023).

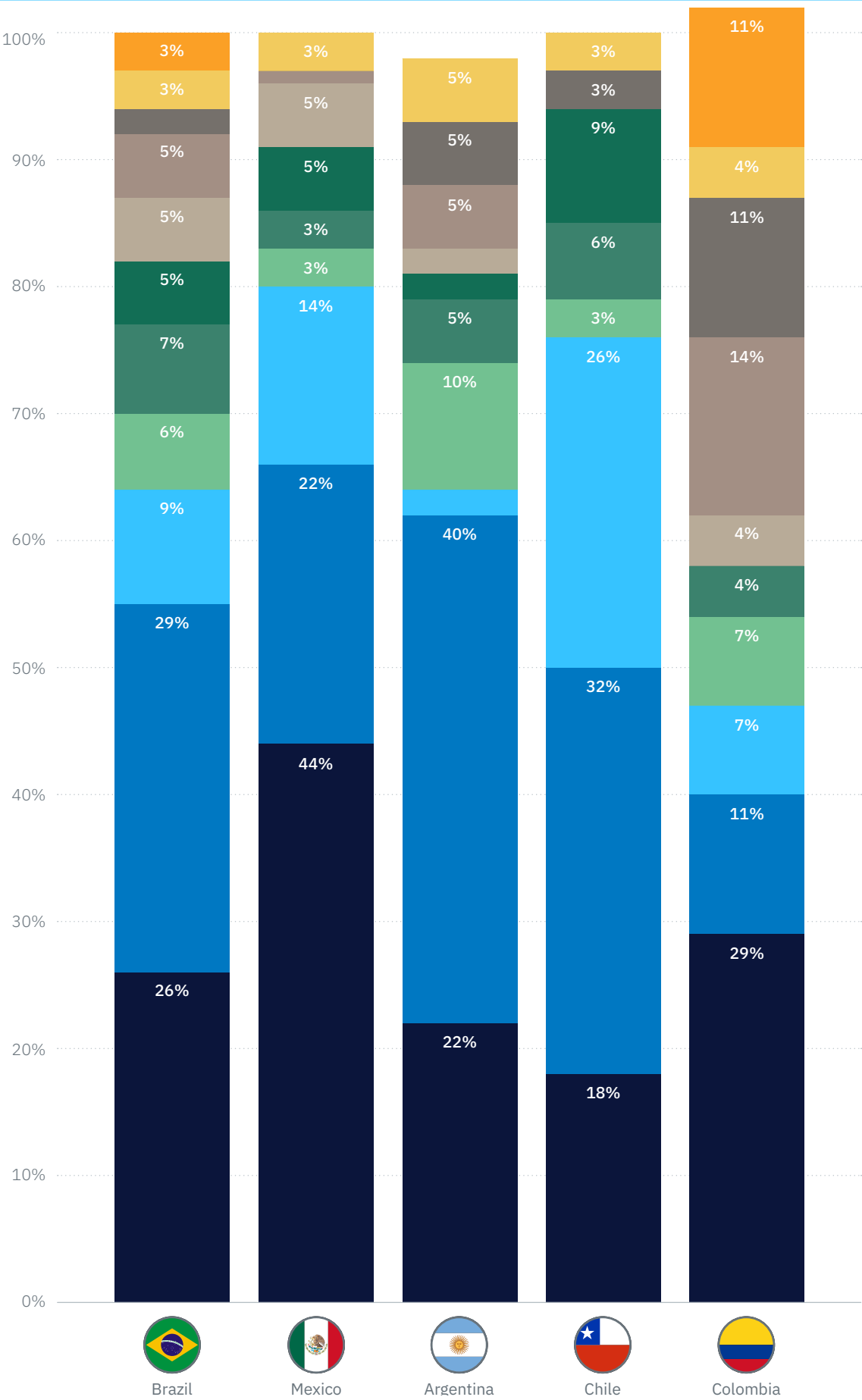
The picture for Brazil, Mexico, Colombia, and Chile follows this trend. In Brazil, 29% of cyber incidents are in public administration; in Mexico, 22%; Colombia, 11%; and Chile, 32%. Finance and insurance are also areas for significant activity. In Brazil, the finance and insurance sector has been targeted in 9% of cases; in Mexico, 14%; Colombia, 7%; and Chile, the largest number, 26%.

Other notable sectors in Brazil are information, 7%; professional and services, 6%; and retail, 5%. In Mexico, retail and manufacturing both account for 5% of cyberattacks. In Colombia, the areas for concern are utilities, 14%, and healthcare, 11%. In Chile, 9% of attacks are in retail and 6% in information.

**Public administration and finance are the two most targeted sectors across Latin America**

Latin America, Distribution of disclosed cyber incidents by sectors, 2013-2024

- Key:
- Educational services
  - Transportation & warehousing
  - Healthcare & assistance
  - Utilities
  - Manufacturing
  - Retail trade
  - Information
  - Professional & sciences
  - Finance & insurance
  - Public administration
  - Other



Source:  
World Bank  
Note:  
Numbers may not add up to 100% due to rounding.

# The CISO view: key takeaways from CISO interviews across Latin America

**The following conclusions can be drawn from a survey of chief information security officers (CISOs) carried out by the Latin America CISO report in 2024.**

To better understand the cybersecurity landscape in Latin America, over 150 CISOs and other high-level professionals in the region were surveyed. The goal of the survey was to attain an overview of what cybersecurity professionals in the region think about topics such as RMFs, the use of public cloud-based cybersecurity infrastructure to mitigate risk, and more.

The policy recommendations included investing in 'human-capacity building' to counter CISO concerns about insufficient training and cyber threat awareness, and the establishment of risk management frameworks. Several Latin American countries have taken steps to develop cybersecurity frameworks as part of their digital agendas. But many government agencies are not obligated to report incidents or follow best practices.

The recommendation of a voluntary risk management framework would combine the establishment of a mixed-governance cybersecurity agency, a national CSIRT, in countries that have yet to implement one, and the creation of sector specific cyber incident databases. The creation of the

agency and response team would combine with legislative and regulatory actions, such as enacting comprehensive cybersecurity laws, implementing mandatory reporting requirements for cybersecurity incidents to a centralized location, and providing incentives for private-sector participation in cybersecurity initiatives.

Further recommendations cover investment in cybersecurity technology and the adoption of public cloud solutions, and better centralized reporting and training systems to enhance collaboration across different sectors and agencies.

When it comes to industries' spending on cybersecurity, according to GlobalData, the most notable sectors for Brazil, Mexico, Colombia, and Chile are banking, retail, IT, manufacturing, and energy. In Brazil, banking cybersecurity revenues will account for \$645m in 2028; IT and retail, \$477m; and manufacturing, \$339m. In Mexico, in 2028, IT spending will account for \$272m; retail, \$221m; manufacturing, \$195m; and energy, \$170m. In Colombia, by 2028, it is retail spending, \$141m, that accounts for the greatest spend, followed closely by banking, \$138m, energy, \$120m, and utilities, \$51m. In Chile, the greatest spending in 2028 will be in retail, \$128m, followed by energy, \$56m, utilities, \$46m; and manufacturing, \$44m.





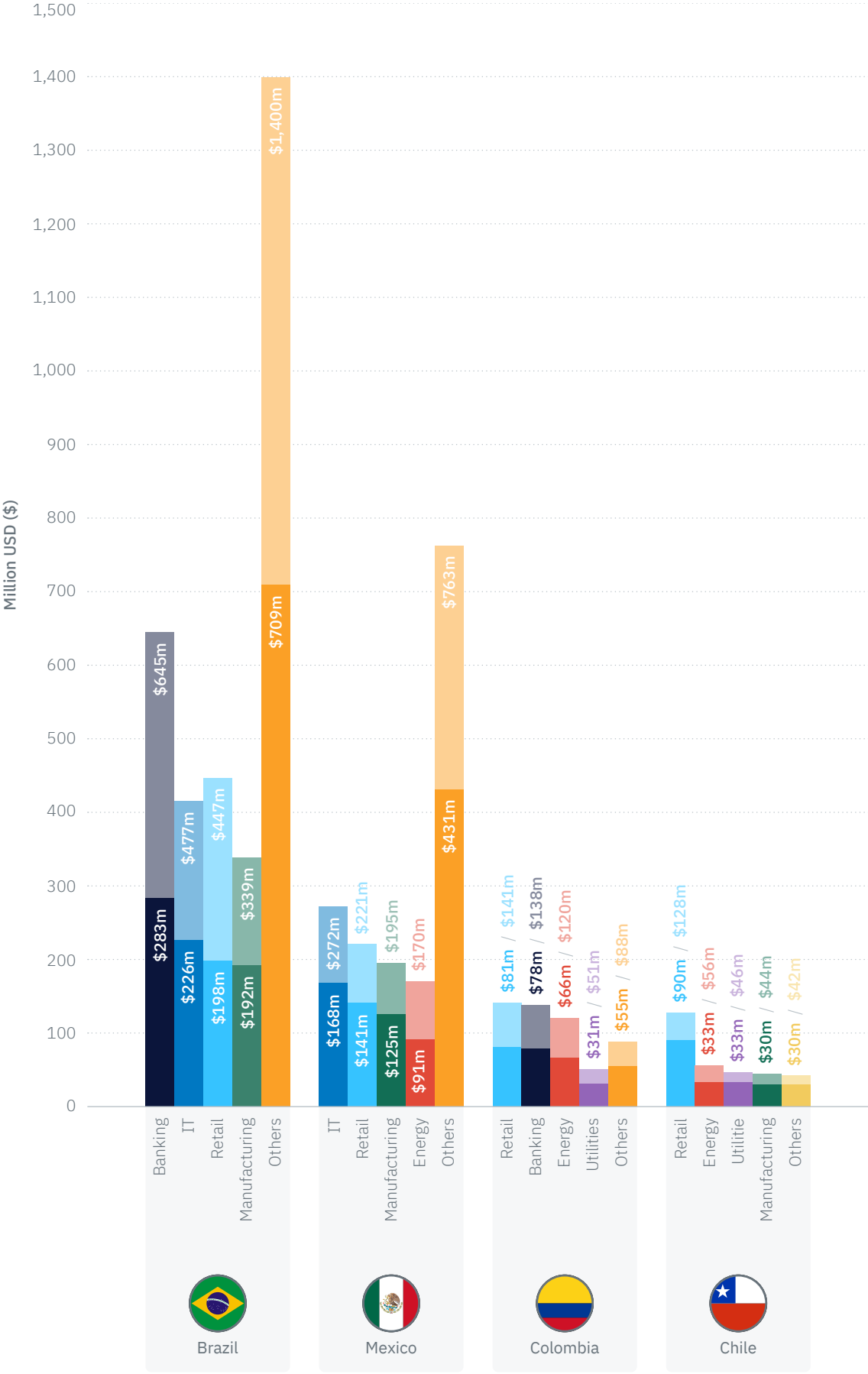
Banking, retail, IT, manufacturing, and energy are the key drivers of cybersecurity spending in Latin America

Cybersecurity market revenue in 2024 and 2028 by top five industries in select Latin American countries

Key

Solid colours = 2024

Tinted colours = 2028



Source: GlobalData

Note: The Others segment includes agriculture, arts, entertainment, recreation, wholesale, business & professional services, construction & engineering, ICT-related services, miscellaneous services, and real estate, rental, & leasing.

GlobalData's exposure map below gives an overall idea of the level of cybersecurity-related activity going on in each of the four Latin American countries, and how they compare to each other. Cybersecurity related news, social media posts, company filings, patent applications and deals are tracked based on which country they occur within.

The map shows that Brazil is the most prone to and proactive in terms of cybersecurity in Latin America, followed by Mexico and then closely together by both Colombia and Chile.

Brazil is by far the most active in terms of cybersecurity-related news and deals. Brazil's news count for cybersecurity is double that of Mexico, and nearly six times that of Colombia and Chile. Brazil's deals and its filings on cybersecurity are three times those of Mexico. Colombia and Chile are very similar in their numbers of deals and filings, but Colombia's cybersecurity jobs count is over two and a half times that of Chile. One surprise is that Mexico's cybersecurity jobs count of 19,069

comfortably outstrips Brazil's own 14,928 count. But in all other areas: news, deals, filings, and social media, Brazil is significantly ahead of Mexico.

Looking more closely at cybersecurity-related jobs posted in Latin American countries over the last two years from 2023 to 2025, both Brazil and Mexico saw over 40% growth in the number of cybersecurity-related jobs posted in 2023 and 2024. Mexico's percentage increase of 47% marginally beat that of Brazil at 45%.

It is still early in 2025, but data for jobs in January 2025 already shows Mexico creating significantly more jobs than Brazil. Mexico posted 1012 cybersecurity-related jobs compared with 691 for Brazil.

Although Colombia and Chile have also seen significant growth in cybersecurity-related jobs of 49% and 47% respectively, the totals of 4460 jobs for Colombia in 2024 and 1810 for Chile in the same year, are well down on the job numbers for Brazil of 9,528 and 12,979 for Mexico.

Cybersecurity exposure map segmented by select Latin American countries and cybersecurity related jobs posted in select Latin American countries between 2023 – January 2025



<b>News</b>	294	142	51	59
<b>Deals</b>	77	21	12	13
<b>Jobs</b>	14,928	19,069	5,471	1,962
<b>Filings</b>	2,162	749	239	283
<b>Social media</b>	1,007	839	218	180

<b>2023</b>	6,569	8,800	2,992	1,233
<b>2024</b>	9,528	12,979	4,460	1,810
<b>January 2025</b>	691	1,012	290	154

Source:

GlobalData

Note:

GlobalData's exposure map enables determine the strategic focus of companies on themes, sectors, locations, etc. based on the level of considering the last 5 completed years and the current year or the relevant period available for different alternative datasets. Darker the shade, higher the activity in that combination and vice versa. Data extracted 06 February 2025.

# TecPar achieves real-time visibility, faster security response, and streamlined IT operations with Tanium

## CASE STUDY



**Brazilian telco Brasil TecPar faced significant challenges in gaining visibility and control over its rapidly expanding IT environment, driven by accelerated mergers and acquisition (M&A) activities and customer growth.** The company, which has over two million connected customers, the company turned to Tanium and its Brazilian partner Secureway to manage its infrastructure.

Brasil TecPar had seen rapid growth through multiple acquisitions that helped expand its customer base to over 2 million. But such rapid expansion and M&A complexities led to a fragmented and dynamic IT environment with numerous endpoints across diverse systems and regions.

Managing this environment became increasingly difficult for TecPar, with visibility gaps, inconsistent patch management, and growing security vulnerabilities. As a result, the IT team struggled to maintain control over the infrastructure, facing challenges in identifying vulnerabilities and managing endpoints efficiently. The diversity of operating systems

(Windows, Linux, macOS, and Solaris) further complicated the situation, making it hard to ensure consistent security updates across the network. What Brasil TecPar needed was a solution to help regain control, integrate new assets, and strengthen its security posture.

To address its IT challenges, Brasil TecPar partnered with Secureway to implement the Tanium platform for its real-time visibility and endpoint management capabilities. Tanium's solution helps Brasil TecPar to manage its complex and growing infrastructure, helping the IT team to monitor and manage all endpoints from a single console, regardless of operating system.

Tanium's platform allows Brasil TecPar to automate patch management across its entire network, drastically improving response times to vulnerabilities and reducing the manual workload on IT teams. The ability to identify, track, and remediate vulnerabilities in real time ensures that Brasil TecPar can maintain the security and stability of its systems as the company continues to grow.





## Outcome

Brasil TecPar achieves enhanced IT control, improved security, and significant operational savings. With Tanium, Brasil TecPar gained total visibility over its complex and expanding IT environment, allowing for precise, real-time control of all endpoints. The platform's real-time insights also improve decision making, enabling the IT team to identify and resolve vulnerabilities faster than ever before.

Tanium's centralized management console automates patching, updating, and security measures, reducing manual effort and ensuring the entire infrastructure is secure and up to date. This leads to significant operational efficiencies, allowing the IT staff to allocate time and resources toward more strategic projects.

As a result, Brasil TecPar can maintain a strong security posture while continuing to expand and serve more customers.

## Summary

- **100%** visibility over all connected devices across diverse operating systems.
- **30%** faster response time to security vulnerabilities after Tanium integration.
- **One** console manages all security patches and updates using Tanium.
- **Operational savings** achieved by automating IT processes and optimizing resources.

## TecPar at a glance

- **Industry:** Telecommunications
- **Size:** 3,200 employees
- **Headquarters:** Sao Paulo, Brazil
- **Revenue:** R\$ 1 billion (2023)

“Maintaining complete visibility of our assets is essential to guaranteeing the security of our information and further boosting the success of our business.”

**IGOR ALVES COSTA**  
INFORMATION SECURITY MANAGER, BRASIL TECPAR

# Recommendations

1

## PREVENTION IS BETTER THAN CURE

No matter where you are in the world, when it comes to increases in cyberattacks, preventing attacks is a better bet than trying to find a cure for them. Investing in preventative cybersecurity measures will reduce costs in the long run, because it is always more costly to recover from a cybersecurity attack than to prevent one. Yet, despite constant warnings over threats to business operations from cyberattacks, organizations consistently only shut the stable gate after the horse has bolted, even though they know that the reactive approach always means increased costs.

2

## YOU CAN'T SECURE WHAT YOU CAN'T SEE

Effective endpoint security requires having a comprehensive view of every device on your network. Organizations manage thousands of endpoints across distributed, hybrid networks, and identifying all devices, servers and cloud connections continues to be the number-one priority for IT executives. The trouble is that modern security breaches are increasingly sophisticated, and, in future, more AI-enabled, making it increasingly difficult to protect your network with traditional security defences alone. Only by adopting an effective real-time platform that delivers fresh critical data to help organizations stay ahead of threats, can security and IT teams reduce risk by discovering and managing endpoints, shrink the attack surface with rapid updates, and deliver the necessary patches to reduce vulnerabilities.

3

## A SINGLE SOURCE OF TRUTH

Legacy infrastructure and tooling fail to provide a complete picture of the corporate network and so offer only a partial solution for individual issues. Security and operations teams often have to manage with incomplete, dated information provided by legacy vulnerability management tools, which results in both teams just coping with data, leaving vulnerabilities that never become fully remediated. Friction follows between two teams that should function seamlessly as one to ensure operational efficiency and sound cybersecurity protection for the organization. Friction discourages collaboration and impacts business outcomes. The teams should be working in tandem, breaking down siloes, and sharing data effectively. Having a real-time view of all endpoints facilitates the rapid identification and remediation of vulnerabilities. A proactive stance also not only bolsters an organization's security but also streamlines operations and reduces costs.

4

## WHEN COMPLIANCE COMMITMENTS GROW, FULL VISIBILITY OF ASSETS IS KING

Latin American organizations are facing the challenge of ever-growing compliance requirements. But compliance demands become much more manageable when you can see and control every endpoint, identify non-compliant systems, pinpoint devices that are not meeting compliance standards, and prioritize critical risks by analyzing compliance gaps and focusing on the most important issues to address. Continuous monitoring also means that organizations can maintain real-time visibility into their compliance status through ongoing scans. Forewarned is forearmed.



#### THE IMPORTANCE OF RESILIENCE

For Latin American organizations, the mark of their ability to cope with cyberthreats is not so much about avoiding attacks – because there are too many to avoid - but how resilient they are to those attacks. The mark of an effective cybersecurity approach is how quickly you can get up and running again. In Latin America, having strong risk management frameworks is a good start. According to a World Economic Forum survey, nearly three-quarters (72%) have integrated a risk management framework into their cybersecurity strategy. And 94% of respondents agree that such frameworks can enhance organizational resilience to cyberthreats.



#### MORE AUTOMATION, MORE EFFICIENT SECURITY TEAMS

With security skills at a premium and cyber teams needing to be more efficient as a result, organizations in Latin America will benefit from automating common IT operations and security tasks in real-time. An automated platform helps IT and security teams increase their efficiency by automating repetitive tasks, a significant benefit given the skills shortages and budget constraints faced by most organizations. When patching servers and remediating vulnerabilities, organizations typically need to stop all services and confirm they are turned off before proceeding. By using an automated platform, businesses can control specific services, verify their status, and deploy patches within that platform.



# Sponsor



Tanium Autonomous Endpoint Management (AEM) offers the most comprehensive solution for intelligently managing endpoints across industries, providing capabilities for asset discovery and inventory, vulnerability management, endpoint management, incident response, risk and compliance, and digital employee experience. The platform supports 34 million endpoints worldwide, including 40% of the Fortune 100, delivering increasingly efficient operations and an improved security posture at scale, with confidence, and in real-time. For more information on The Power of Certainty™, visit [www.tanium.com](https://www.tanium.com) and follow us on [LinkedIn](#) and [X](#).



## We are the trusted, gold standard intelligence provider to the world's largest industries

We have a proven track record in helping thousands of companies, government organizations, and industry professionals profit from faster, more informed decisions.




Our unique data-driven, human-led, and technology-powered approach creates the trusted, actionable, and forward-looking intelligence you need to predict the future and avoid blind-spots.

Leveraging our unique data, expert analysis, and innovative solutions, we give you access to unrivaled capabilities through one platform.

### HEAD OFFICE

John Carpenter House  
7 Carmelite Street  
London  
EC4Y 0AN  
UK

Tel: +44 20 7936 6400

 GlobalDataPlc  
 GlobalDataPlc  
 GlobalData.com

### DISCLAIMER

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, GlobalData. The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that GlobalData delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such, GlobalData can accept no liability whatsoever for actions taken based on any information that may subsequently prove to be incorrect.