LATAM EDITION

THALES
Building a future we can all trust

EXECUTIVE SUMMARY 2021

2021 Data Threat Report

Data Security in the Era of Accelerated Cloud Transformation and Remote Work

#2021DataThreat

cpl.thalesgroup.com

Contents

05 Security Professionals in LATAM Are Facing Challenges but Have Identified a Path Forward

08 COVID-19 Brings New Challenges for Security

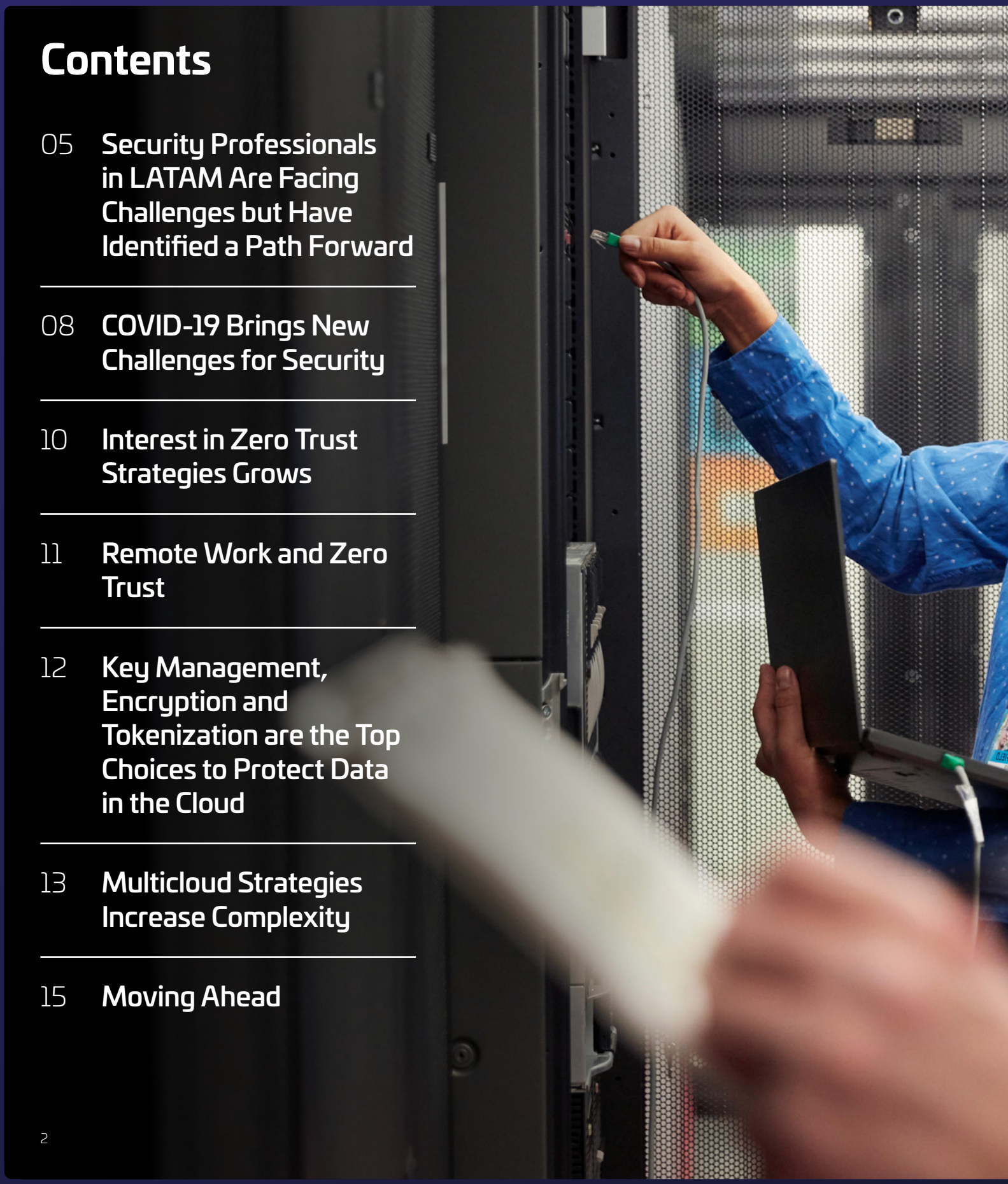
10 Interest in Zero Trust Strategies Grows

11 Remote Work and Zero Trust

12 Key Management, Encryption and Tokenization are the Top Choices to Protect Data in the Cloud

13 Multicloud Strategies Increase Complexity

15 Moving Ahead



About this study

The COVID-19 pandemic has had an immediate and dramatic impact on IT teams around the globe, and its long-term effects are still evolving. The Latin American (LATAM) edition of the 2021 Thales Data Threat Report looks at different aspects of those impacts in a wide-ranging survey of security professionals and executive leadership. Within this executive report, we dive in to understand how LATAM has tackled the threats resulting from the pandemic along with stakeholders' feelings about various aspects of data security.

The 2021 Thales Data Threat Report is based on a survey of more than 2,600 security professionals and executive leaders, including 200 in LATAM.

451 Research

S&P Global
Market Intelligence

Source: 2021 Data Threat custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

Our sponsors are:

ARROW

SENETAS

versasec

KEYFACTOR

SYNNEX WESTCON

F9C Walking Together

FIRST TECH

Adistec

Key Findings

"Companies in LATAM are experiencing breaches at an alarmingly high rate: 49% of LATAM respondents claimed to have experienced a breach."

Security Professionals in LATAM Are Facing Challenges but Have Identified a Path Forward

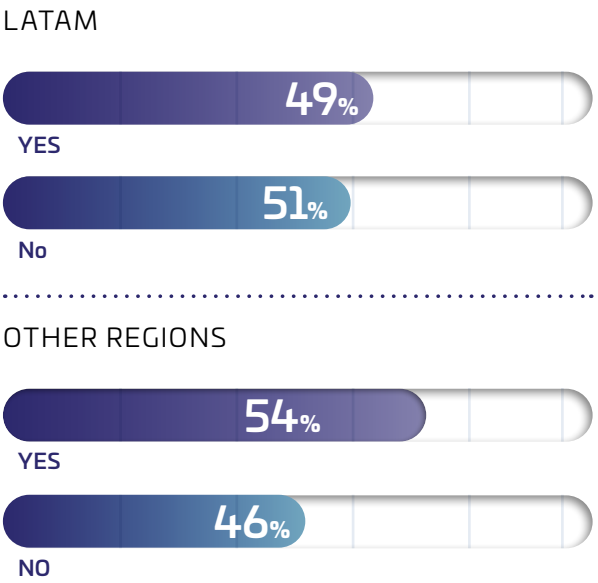
The data gathered from LATAM countries mirrors many of the other geographies we studied. For example, companies in LATAM are experiencing breaches at an alarmingly high rate: 49% of LATAM respondents claimed to have experienced a breach. Moreover, about one-third of these respondents have experienced a breach within the last year. And the problem is not getting any better: 38% of organizations claimed that they have seen an increase in the volume, severity and/or scope of cyberattacks in the past 12 months. Although these percentages fall under the global average, attacks in this region are still increasing, and security professionals are adjusting to prevent them.

FIGURE 1

Comparison of Breaches Between LATAM and Other Regions

Q: Has your organization ever been breached?

Respondents: LATAM and other regions



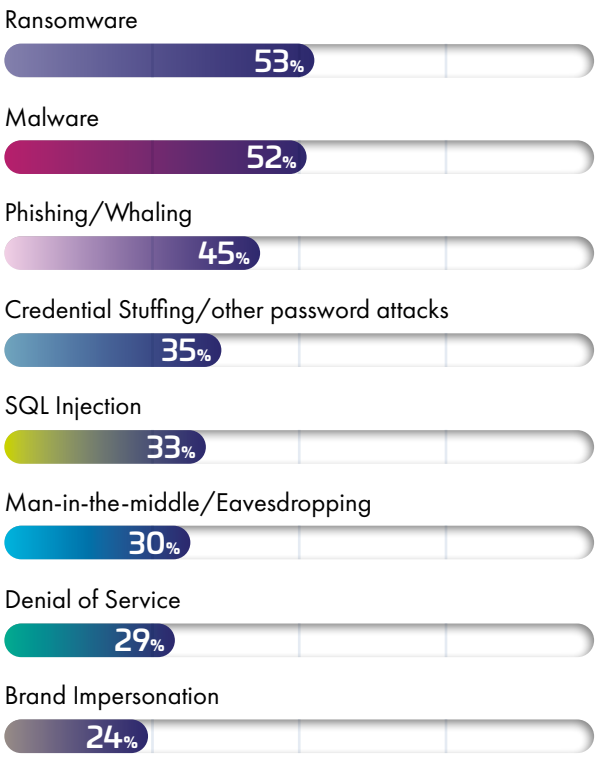
Source: 451 Research's 2021 Data Threat custom survey

FIGURE 2

Largest Increase in Attacks Utilize Ransomware, Malware and Phishing/Whaling

Q: In which types of attacks/threats have you seen an increase?

Respondents: LATAM



Source: 451 Research's 2021 Data Threat custom survey

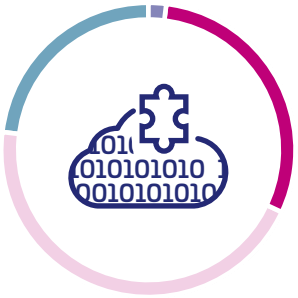
Breaking the data down further shows that LATAM countries have experienced increases in attacks such as ransomware (53%), malware (52%) and phishing/whaling (45%), which is consistent with global results. With the increasing number of attacks, these organizations are employing different technologies to protect their data. They see key management and hardware security modules (42%) as the most effective choice for protecting sensitive data from cyberattacks, followed by encryption (40%). Not surprisingly, encryption/key management was also the number one spending priority for LATAM (46%).

FIGURE 3

Roughly One-Quarter of LATAM Respondents Have Complete Knowledge of Where Their Data is Stored

Q: Do you know where all of your data is stored?

Respondents: LATAM



Source: 451 Research's 2021 Data Threat custom survey

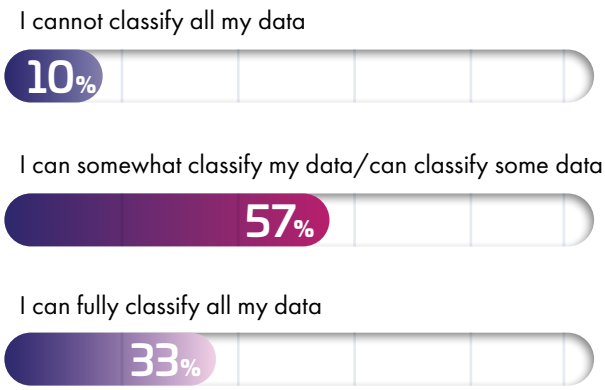
- **2%** I am not at all confident I know where my data is stored
- **30%** I am somewhat confident I know where my data is stored
- **45%** I am very confident I know where my data is stored
- **23%** I have complete knowledge of where my data is stored

FIGURE 4

Only One-Third of LATAM Respondents Can Fully Classify Their Data

Q: Are you able to classify all of your data?

Respondents: LATAM



Source: 451 Research's 2021 Data Threat custom survey

However, there still is work to be done. Unfortunately, only 23% of organizations in LATAM countries have complete knowledge of where their data is stored (vs. other regions at 24%), and just one-third are able to fully classify their data (vs. other regions at 31%).

46%

of Latin American respondents said encryption/key management was their number one spending priority.

COVID-19 Brings New Challenges for Security

COVID-19 has affected organizational processes, changing the ways in which employees interact with their work, with one another and with the outside world. In this case, the job of the security professional has transformed along with the shift from working in offices to widespread remote work. Moreover, a doubling of the emphasis on cloud has increased the pace of cloud adoption already in motion, adding to the complexity of securing the enterprise.

Regarding pandemic preparedness, LATAM was in line with global averages. Only 24% of respondents reported that their security infrastructure was 'very prepared' to handle the range of risks associated with the new business operating environment. Just under half of LATAM respondents (46%) were unprepared to some degree (28% 'somewhat unprepared' and 18% 'not prepared at all').

The shock of the pandemic and subsequent remote work arrangements also shifted mindsets regarding security; 86% of respondents were either 'somewhat' or 'very' concerned about the security risks and threats of employees working remotely (40% 'very concerned' and 46% 'somewhat concerned'). Not surprisingly, the most important investment during COVID-19 was in security and privacy – 46% of organizations followed this route. Other spending plans included investments in infrastructure and cloud (28% of respondents) and investments in distributed cloud (26%).

24%

of respondents reported that their security infrastructure was 'very prepared' to handle the range of risks associated with the new business operating environment.

86%

of respondents were either 'somewhat' or 'very' concerned about the security risks and threats of employees working remotely.

FIGURE 5

Concern About Security Risks/Threats of Employees Working Remotely

Q: How concerned are you about the security risks/threats of employees working remotely?

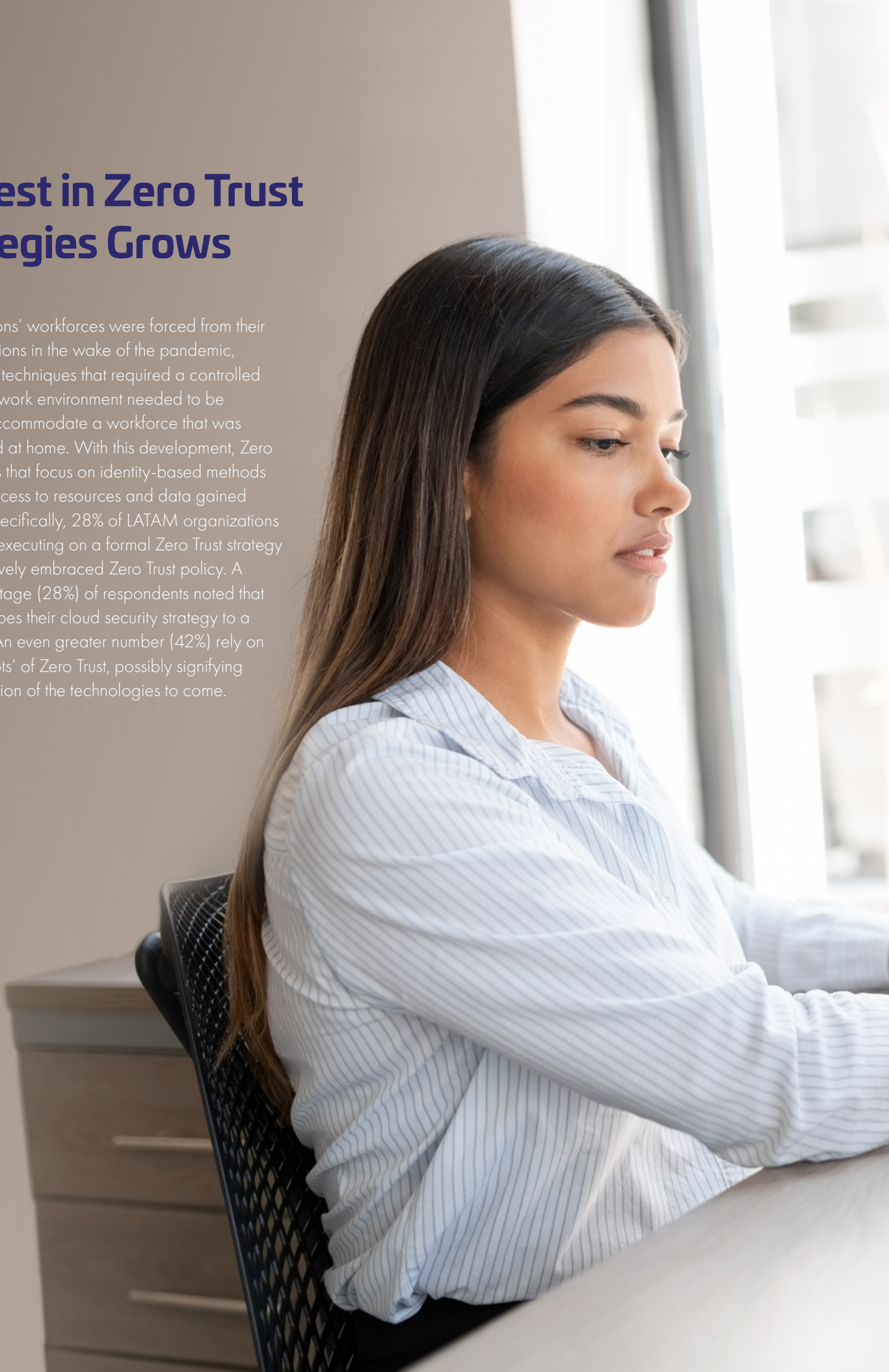
Respondents: LATAM

- **40%** Very concerned
- **46%** Somewhat concerned
- **11%** Somewhat unconcerned
- **2%** Not at all concerned

Source: 451 Research's 2021 Data Threat custom survey

Interest in Zero Trust Strategies Grows

As organizations' workforces were forced from their physical locations in the wake of the pandemic, many security techniques that required a controlled corporate network environment needed to be adjusted to accommodate a workforce that was mostly located at home. With this development, Zero Trust strategies that focus on identity-based methods of granting access to resources and data gained popularity. Specifically, 28% of LATAM organizations said they are executing on a formal Zero Trust strategy and have actively embraced Zero Trust policy. A similar percentage (28%) of respondents noted that Zero Trust shapes their cloud security strategy to a great extent. An even greater number (42%) rely on 'some concepts' of Zero Trust, possibly signifying greater adoption of the technologies to come.



Remote Work and Zero Trust

Organizations displayed mixed confidence with their current access security products, and subsequently, their ability to enable their employees to work remotely in a secure and easy manner. Many issues surrounding the proper provisioning of data and applications were already present in organizations pre-pandemic, so this dramatic shift in the working environment only complicated matters further. An almost even split resulted between those who were confident in their current access technology and those who were not: nearly half (49%) of organizations were 'somewhat' to 'very' confident in their current access security solutions to enable their workers to perform their jobs in a secure and easy manner, while 51% were either 'somewhat' to 'not at all' confident.

FIGURE 6

Organizations' Confidence Level in Enabling Secure Remote Work

Q: How confident are you that your current access security technologies can effectively enable employees to work remotely in a secure and easy manner?

Respondents: LATAM

- **21%** Very confident
- **28%** Somewhat confident
- **30%** Somewhat not confident
- **20%** Not at all confident

In an attempt to bridge this gap, 43% of organizations turned to conditional access. Almost the same percentage deployed Zero Trust network access and software-defined perimeter, while 38% opted to deploy cloud-based access management such as identity as a service or single sign-on, in line with global averages.

Key Management, Encryption and Tokenization are the Top Choices to Protect Data in the Cloud

Organizations continue to shift their strategies to the cloud to capture the many benefits it offers: faster response to business needs, cost reduction, more efficient deployment of resources, and quicker product and service releases. In turn, to accomplish specific goals, they are beginning to utilize the cloud to store sensitive data. In general, the majority (77%) of LATAM respondents said they have placed as much as half of their organization's workloads and data in the cloud.

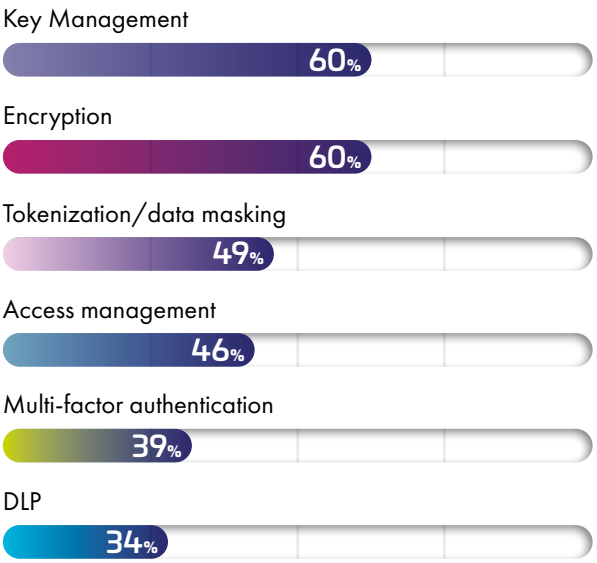
As firms move more of their sensitive data to the cloud, strategies to protect this data become warranted, particularly since one-third of these organizations have experienced a data breach that involved their data and applications in the cloud (slightly below the global average of 41%), while 40% have experienced a breach or failed an audit involving cloud data and applications in the last year alone. To help prevent breaches of sensitive data in the cloud, organizations chose key management (60%), encryption (60%), and tokenization and data masking (49%) as the top choices for securing sensitive data in the cloud. However, when it comes to protecting this data in actual practice, a large part of sensitive data in the cloud remains unencrypted – for sensitive data stored in the cloud, only 20% of organizations encrypt more than half of it.

FIGURE 7

Key Management, Encryption and Tokenization/Data Masking Are Top Technologies to Protect Sensitive Data in the Cloud

Q: Which security technologies is your organization using to protect sensitive data in the cloud?

Respondents: LATAM



Source: 451 Research's 2021 Data Threat custom survey

40%

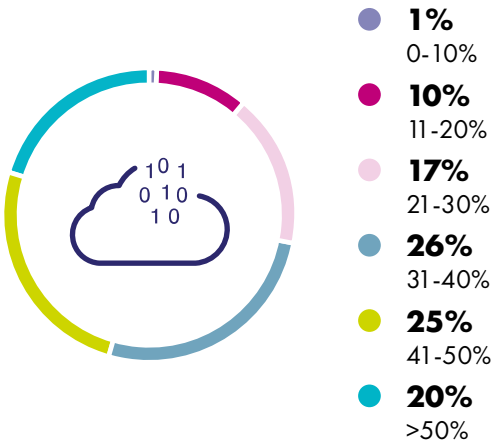
have experienced a breach or failed an audit involving cloud data and applications in the last year alone.

FIGURE 8

One-fifth of Organizations Encrypt More Than 50% of Their Sensitive Data

Q: What percentage of your sensitive data in the cloud is encrypted?

Respondents: LATAM



Source: 451 Research's 2021 Data Threat custom survey

Multicloud Strategies Increase Complexity

Securing the cloud becomes more challenging as different cloud providers are added to the mix. LATAM respondents utilize a wide array of cloud providers, with the most popular being AWS (58%), followed by Azure (40%) and GCP (24%). These organizations also mixed the services of different cloud providers to fit their business needs, with 50% of respondents working with two PaaS providers and 20% with three. For SaaS implementations, 37% of respondents used 26-50 SaaS applications while 22% used more than 50.

> "Respondents rate complexity as their top barrier to implementing data security."

Key management also becomes an issue when using multiple cloud platforms, adding to the complexity of the key management challenge. Just over one-third (34%) of LATAM organizations use five to seven key management products, which can range from enterprise key management vendors to homegrown solutions, spreadsheets, and flat files and HSMs. Moreover, 15% of organizations claimed to use as many as 8-10 key management products.

> “Organizations must also choose how they encrypt and where they manage their keys.”

Multicloud Strategies Increase Complexity Continued

Organizations must also choose how they encrypt and where they manage their keys. One-third of organizations 'mostly' or 'completely' rely on their cloud provider to encrypt data in IaaS and PaaS environments, while 15% solely use the cloud provider's tools and 20% prefer to encrypt it themselves. Regarding key management, 31% of respondents 'all or mostly' use their cloud provider to control encryption keys, and 17% control the keys themselves. Nearly a quarter (23%) of respondents said that their cloud provider controls all of their encryption keys. By managing their own keys, organizations can add an extra layer of security by sheltering this information from breaches resulting from the cloud provider and insider attacks. In other cases, information cannot be stored with the cloud provider for compliance reasons. For some non-critical data, cloud storage may be the best option, but for highly sensitive data, organizations require more protection, which other security options may provide.

Moving Ahead

As the pandemic continues to affect organizations around the world, most continue to face a range of attacks and breaches, such as malware, ransomware and phishing, regardless of their geographic location. Additionally, because of ongoing remote work requirements, security teams must deal with new scenarios on top of the complexity presented by multiple clouds, hybrid environments and a sprawling application estate. In order to fully capture the benefits of the cloud – such as faster responses to business needs, cost reduction, more efficient deployments of resources, and quicker releases of products and services – organizations will need to provide access to data and services in a fast, convenient and, most importantly, secure manner. Based on their awareness of the various challenges they face and the knowledge of the many tools at their disposal, enterprises in LATAM are on the path toward capturing these benefits while reducing the likelihood of successful cyberattacks.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

To download the full report, including 451 Research recommendations visit

cpl.thalesgroup.com/data-threat-report