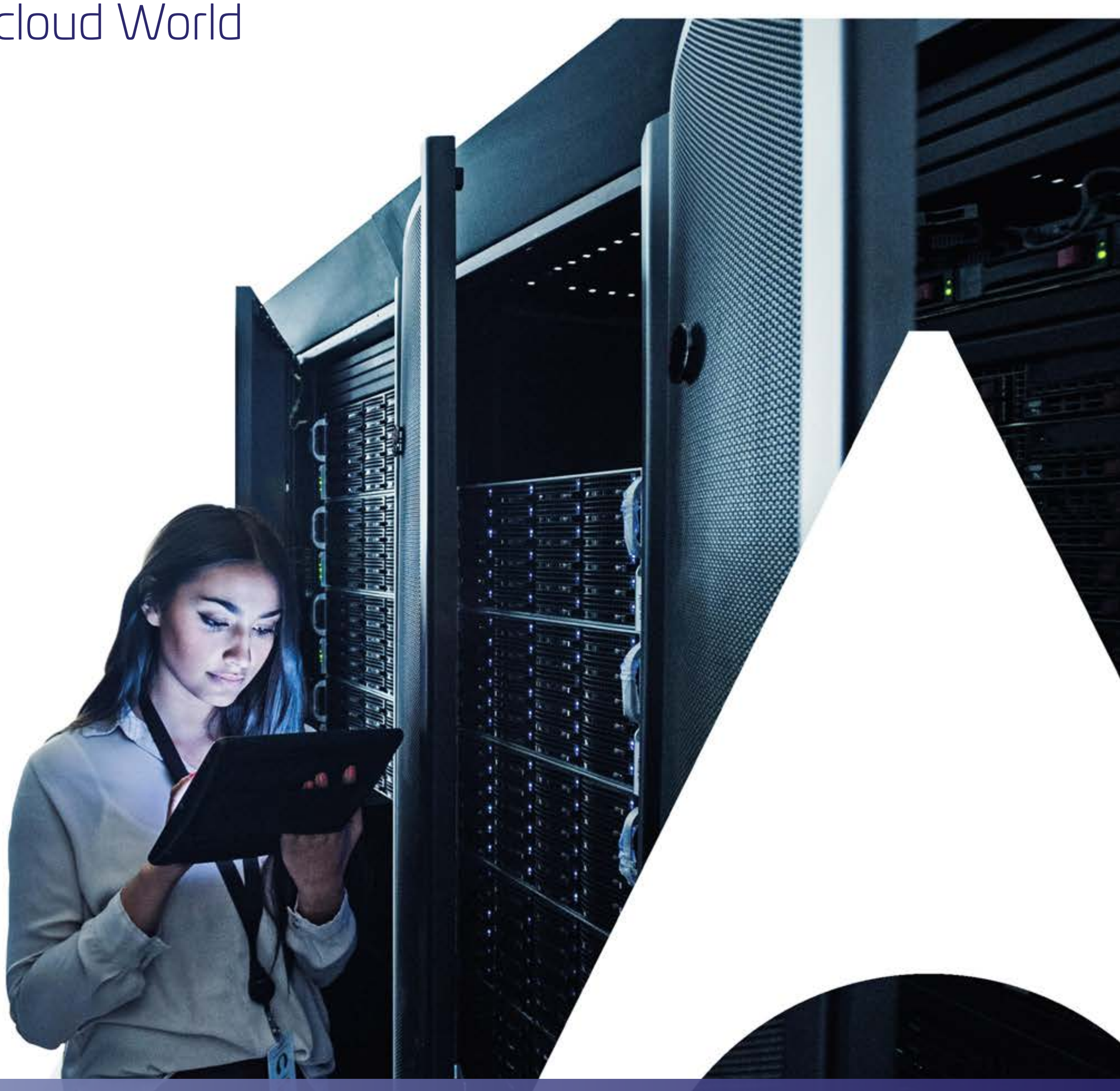
LATAM EDITION

EXECUTIVE SUMMARY

2021 Thales Cloud Security Study

The Challenges of Cloud Data Protection and Access Management in a Hybrid and Multicloud World



#2021AMI

cpl.thalesgroup.com

Contents

4 Introduction

5 Key Findings

5 Multicloud Adoption Is Widespread

6 Cloud Complexity Is a Common Concern

6 Defining Cloud Security Policies Is Squarely for Security Teams

7 Cloud Migrations Are Primarily "Lift & Shift"'

8 Securing Cloud Environments Centers on Key Technologies

9 Encryption Is Not Widespread in the Cloud

10 The Zero Trust Journey

13 Breaches and Audit Issues

13 Moving Ahead

About this study

The pandemic has pushed organizations into many changes in the last year, but the move to greater use of cloud-based infrastructure was already underway. The demands of increased remote work and expanded digital delivery were just some of the imperatives that accelerated cloud use. The 2021 Thales Cloud Security Report, based on data from a survey of more than 2,600 respondents in more than 10 countries across the globe, looks to identify the depth of that change, as well as the current state of and plans for how organizations across a range of industries manage access to enterprise applications, cloud services and networks. This executive summary looks at the Latin American segment of the results and compares and contrasts those results with the global perspective. (The study includes results from Brazil and Mexico as representative of Latin American respondents). The insights in this report were gleaned from the survey data, and it explores the impacts on security strategy and planning.

The results of the survey show that while a strong movement to cloud is in progress, there are limited security controls in place for what is a new infrastructure element for most. Respondents reported significant levels of data breaches – lower in Latin America than the global average, but still concerning. Organizations have an opportunity to accelerate cloud utilization by strengthening cloud security through tactics such as greater use of encryption to enable cloud use by a wider range of workloads.

451 Research

S&P Global
Market Intelligence

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

Our sponsors are:

ARROW

SENETAS

SYNNEX WESTCON

versasec

Adistec

F9C Walking Together

FIRST TECH

Introduction

> “Organizations need to extend and adapt their capabilities to manage security efficiently and effectively in these new, dispersed environments.”

Key Findings

- Cloud usage in Latin America is growing, but some aspects still lag behind other regions. The average number of SaaS applications, for example, is lower in Latin America than elsewhere.
- Respondents also indicated a stronger preference for 'lift & shift' practices for cloud migrations when compared to worldwide numbers.
- In terms of positive practices, Latin Americans reported greater use of encryption in cloud environments, a practice that can contribute to lower residual risk.
- Latin American respondents reported lower levels of cloud-related data breaches and audit issues.

Multicloud Adoption Is Widespread

As organizations addressed the various challenges presented by the pandemic over the last year, they turned to cloud-based infrastructure to give them scale and reach. Cloud capabilities can bring applications closer to employees and customers faster than other options. However, that shift can create its own challenges because this is a new operating mode, and organizations may not understand its characteristics well, and procedures may not directly align with on-premises models. Organizations need to extend and adapt their capabilities to manage security efficiently and effectively in these new, dispersed environments, and survey results show that can be tricky.

Few organizations were working with a single cloud provider for IaaS, PaaS or SaaS capabilities. This mix of providers can create operational complexity because each can have unique capabilities and controls. Latin American averages were close to global numbers both in terms of multicloud and PaaS usage: 58% of Latin American respondents indicated they were multicloud, compared to global at 57%, and the average number of PaaS providers is about two, as is the global number.

There was some variability in the number of SaaS applications in relation to global numbers: while the largest percentage (37%) indicated that they have 26-50 on average, which is similar to the global number, the average number of applications is lower at 49, compared to a global average of 60. The number of SaaS apps grows with organizational complexity as measured by revenue.

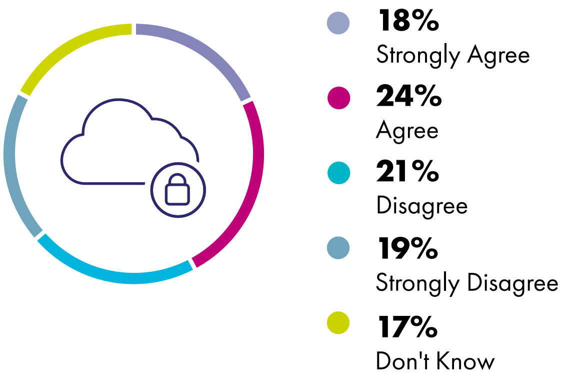
Cloud Complexity Is a Common Concern

The diversity of environments may also be contributing to operational complexity. For example, 42% of Latin American respondents (a little less than the 46% global average) agreed or strongly agreed that it is more complex to manage privacy and data protection regulations in a cloud environment than on-premises networks. This should prompt organizations to look at ways to simplify their operations with security management capabilities that can span the various operating environments and standardize their operational processes across them.

FIGURE 1

Managing Cloud Security is Complex

To what extent do you agree with the following statement: It is more complex to manage privacy and data protection regulations in a cloud environment than on-premises networks within my organization.



Source: 451 Research's 2021 Cloud Security custom survey

Defining Cloud Security Policies Is Squarely for Security Teams

Organizations need to have policies for defining and enforcing security policies that can cut through the complexity of the environments they have to manage. The survey looked at decision-making processes, and 85% of respondents indicated that security teams are involved in cloud security decisions, with roughly an even split between security teams running cloud security independently or in collaboration with cloud engineering teams. However, there is some discrepancy in perception across job roles. Senior leadership views security teams as having greater responsibility, while staff have the perception that there is more collaboration. The same discrepancy exists when looking at roles in the purchase process as another lens into organizational hierarchy.

85%

of respondents indicated that security teams are involved in cloud security decisions.

Cloud Migrations Are Primarily "Lift & Shift"

There are many paths to cloud, and the survey looked at how organizations expect to transition to cloud environments. Latin American respondents stand out here; 62% (well above the 55% global average) indicated that they expect to 'lift & shift' workloads, taking existing workloads and moving them to cloud with a minimum of change. Lift & shift is generally quick for workloads that can easily make the transition, but it can open gaps in protection if not carefully planned, and it may not make the most efficient use of cloud resources. Just 21% said they are expecting to do some level of re-architecting for applications. That's a path that can put native cloud capabilities to work more directly, but it can take more resources to implement. To protect workloads that have been shifted to cloud, organizations need to ensure not only that the controls that existed in on-premises environments can be delivered in their new surroundings, but also that they can be operated effectively and efficiently.

Securing Cloud Environments Centers on Key Technologies

Protecting applications and data in the cloud requires a new set of skills and potentially new technologies. The survey asked respondents to list the technologies they are using to protect data in cloud environments. Latin American respondents came back with encryption and key management virtually tied at 60%, followed by DLP at 49% and access management at 46%. This variability underscores the complexity involved in cloud security management because these three leading technologies should all be in place to effectively secure cloud deployments. Together, they provide a secure foundation for cloud operations.

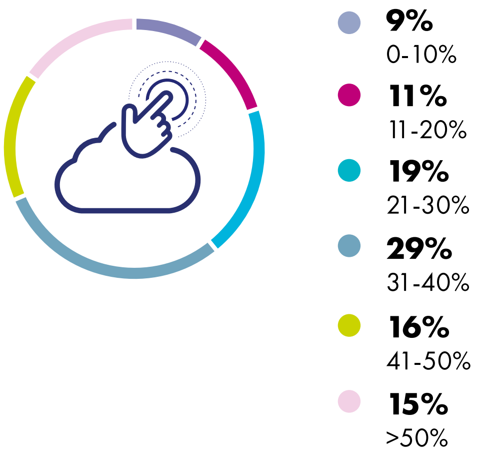
The survey looked at access management for cloud-based applications and found that organizations are using modern authentication technologies like MFA in a selective manner rather than broadly implementing them. Only 15% of Latin American respondents (slightly less than the global average) are protecting more than 50% of their cloud-based applications with a modern authentication technology, which leaves the door open to an attack risk that has been growing considerably. This is clearly an area where additional investment is needed.

Regional considerations on access management appear to align between Latin American and global respondents. Similar to the global numbers of only 16% of respondents indicating they use MFA to secure more than half of their cloud applications, Latin Americans are at 15%. Similar results occur when considering MFA access to more than half of their on-premises applications: 11% globally, 12% for Latin America.

FIGURE 2

Cloud Applications Protected by MFA

What percentage of employees use MFA for cloud applications/SaaS applications?



Source: 451 Research's 2021 Cloud Security custom survey

When considering complexity of securing both on-premises and cloud services with their access management capabilities, 66% of Latin Americans (same as 66% globally) listed the issue as "challenging" or "very challenging".

Only

15%

of Latin American respondents (slightly less than the global average) are protecting more than 50% of their cloud-based applications with a modern authentication technology.

Encryption Is Not Widespread in the Cloud

Data protection is another area that showed considerable underinvestment. Respondents said that encryption is important for data protection, but their responses indicated limited implementation. According to survey results, over 20% of Latin American respondents said they encrypt more than 50% of their sensitive data in cloud environments. This is higher than the global average of 17%. When considering other nuances of cloud usage, just 21% of Latin American survey respondents reported having over 50% of workloads with an external cloud provider (below the global average of 24%). When considering data sensitivity, respondents said that just 20% of the data residing in cloud is sensitive.

The other aspect of data protection effectiveness in cloud is key management. Latin American respondents were above the global average for the control of their keys (39% indicated that they control most or all of their keys versus 34% globally), but they matched the global number (52%) in terms of using cloud provider consoles for that control. Organizations that aren't in control of their own keys not only face the security risk of potential data exposure, but they also can create management complexity in the handling of their key material because they have to coordinate their activities across different environments for the on and off-premises key management systems. Such a situation is not only more resource-intensive but also more prone to operational errors. Investing in a key management system that spans the breadth of an organization's infrastructure can reduce staff workloads and improve the security posture.

Only

20%

of Latin American respondents said they encrypt more than 50% of their sensitive data in cloud environments.

> "Organizations that aren't in control of their own keys not only face the security risk of potential data exposure, but they also can create management complexity in the handling of their key material because they have to coordinate their activities across different environments for the on and off-premises key management systems."

The Zero Trust Journey

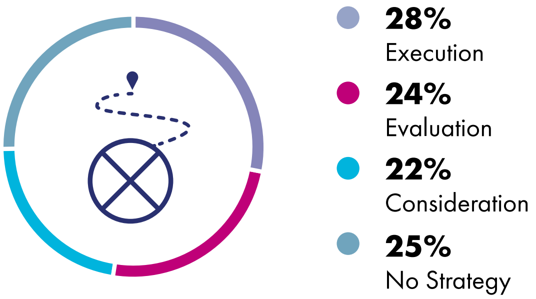
One of the trends that the survey identified was the shift to greater use of Zero Trust operating principles. Organizations are looking to improve their security posture by limiting access and applying more granular, policy-based controls that the Zero Trust operating mindset offers. It's a focus that can be particularly effective in securing the distributed model that cloud offers. Latin American respondents reported that they are early in their journey to Zero Trust; just 28% said they are executing on a Zero Trust plan

Nevertheless, that's an indication that Latin American organizations see the importance of being able to apply more granular controls. It also reiterates the need for investment in the technologies required to achieve Zero Trust capabilities. Zero Trust requires a solid security foundation that includes effectively managed data protection and access management. The survey results show that organizations need to invest in modern authentication, like MFA, and key management systems to deliver the full protection of data encryption.

FIGURE 3

Zero Trust Journey

Where are you on your Zero Trust journey?

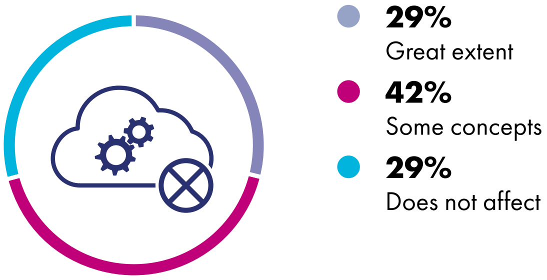


Source: 451 Research's 2021 Cloud Security custom survey

FIGURE 4

Zero Trust in Cloud Strategy

To what extent does Zero Trust security shape your cloud security strategy?



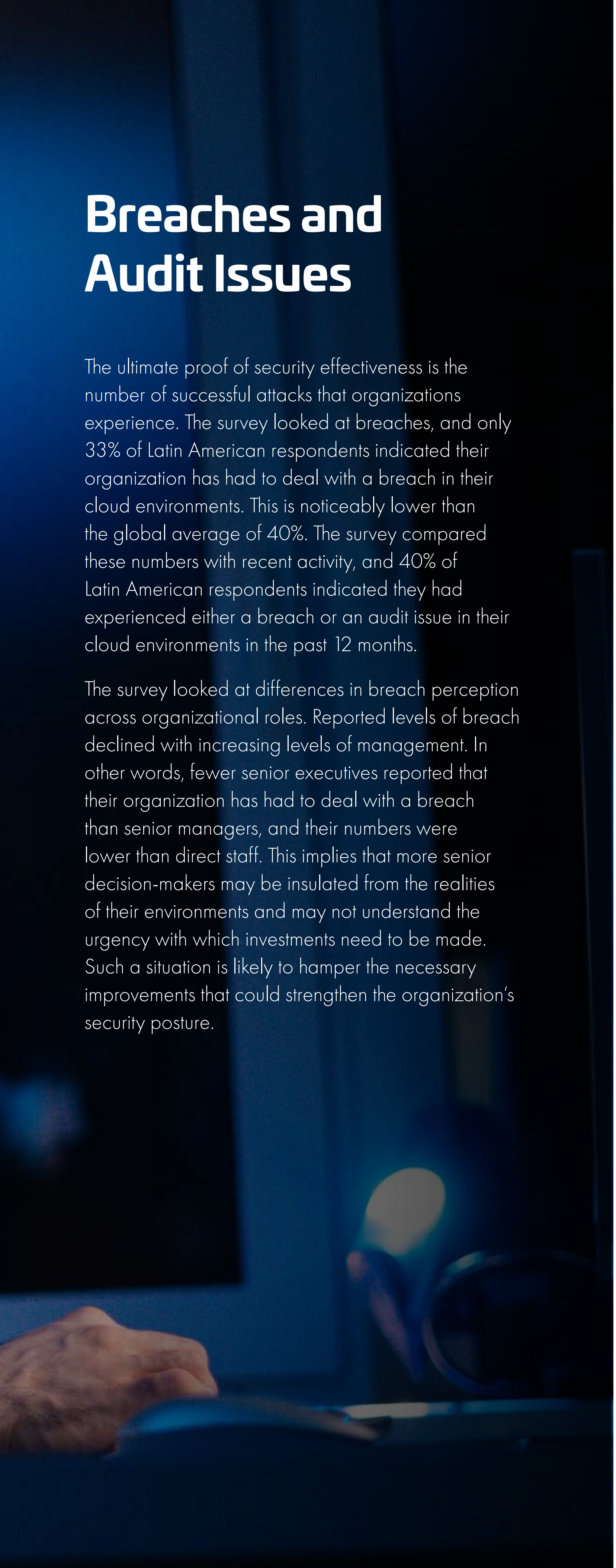
Source: 451 Research's 2021 Cloud Security custom survey

> “Organizations are looking to improve their security posture by limiting access and applying more granular, policy-based controls that the Zero Trust operating mindset offers.”

33%

of Latin American respondents indicated their organization has had to deal with a breach in their cloud environments.

“More senior decision-makers may be insulated from the realities of their environments and may not understand the urgency with which investments need to be made.”



Breaches and Audit Issues

The ultimate proof of security effectiveness is the number of successful attacks that organizations experience. The survey looked at breaches, and only 33% of Latin American respondents indicated their organization has had to deal with a breach in their cloud environments. This is noticeably lower than the global average of 40%. The survey compared these numbers with recent activity, and 40% of Latin American respondents indicated they had experienced either a breach or an audit issue in their cloud environments in the past 12 months.

The survey looked at differences in breach perception across organizational roles. Reported levels of breach declined with increasing levels of management. In other words, fewer senior executives reported that their organization has had to deal with a breach than senior managers, and their numbers were lower than direct staff. This implies that more senior decision-makers may be insulated from the realities of their environments and may not understand the urgency with which investments need to be made. Such a situation is likely to hamper the necessary improvements that could strengthen the organization's security posture.

Moving Ahead

Organizations are working hard to address the forced changes brought on by the pandemic while moving ahead with technology investments that will keep them competitive. Mastering security and operations for cloud-based infrastructure is a required part of this journey. The survey results show that there is considerable use of hybrid and multicloud patterns as businesses expand to get closer to their customers and partners and support a more distributed workforce. The results also show that there is much more work to be done to secure these new infrastructure elements effectively and operate them efficiently. The greater use of hybrid and distributed resources adds operational complexity, and organizations need to invest in capabilities that will allow them to scale up without placing a crippling burden on their security teams.

Methodology

This research was based on a global survey of 2,625 respondents, fielded in January 2021, via web survey with targeted populations for each country, aimed at professionals in security and IT management. In addition to criteria about level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated affiliation with organizations with annual revenue of less than US$100m and with US$100-250m in selected countries.

This research was conducted as an observational study and makes no causal claims.

THALES

Building a future we can all trust

Contact us

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

cpl.thalesgroup.com/cloud-security-research