



APAC EDITION

THALES
Building a future we can all trust

EXECUTIVE SUMMARY

2021 Thales Data Threat Report

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



#2021DataThreat

cpl.thalesgroup.com

Contents

03 About This Study

04 Key Findings

05 COVID has Changed Security Strategies

06 Era of Remote Working

07 Breaches and Other Failures

08 Security Threats

09 Quantum Computing

10 Zero Trust Journey

13 Moving Forward





About this study

Alongside the rest of the technology community and the world, security teams were buffeted by the challenges of the last year. The longer-term effects are still evolving, and this APAC edition of the 2021 Thales Data Threat Report explores perspectives on this year and expectations for the year ahead. The wholesale shift to remote working and greater adoption of cloud driven by the pandemic has put greater pressure on security strategy, and because the APAC region makes up a third of the respondents, their views offer valuable insights. Greater use of cloud is raising risk levels as complexity grows and protections like encryption have yet to achieve broad use. While there are lower levels of reported breaches compared to global averages – possibly due to slightly better reported progress in implementing Zero Trust policies – they're still a matter of concern.

The 2021 Thales Data Threat Report is based on a survey of more than 2,600 security professionals and executive leaders, including more than 850 in the Asia-Pacific region.

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:

SENETAS 

 **versasec**

KEYFACTOR

Canon
Canon Marketing Japan Inc.

NTT DATA
NTTデータ 先端技術株式会社

Key Findings

“When questioned about the preparedness of security infrastructure to handle risks (caused by the pandemic), only 20% of respondents said the security infrastructure was very prepared to handle these changes.”



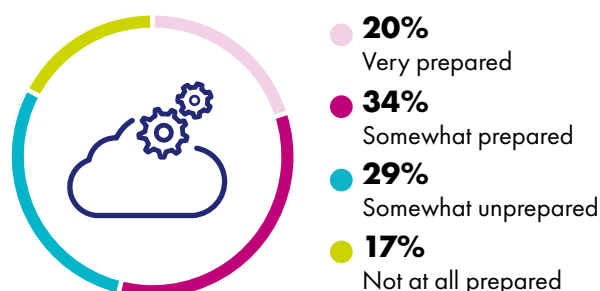
COVID Has Changed Security Strategies

Security strategies and investments have been altered by the changes that the pandemic created. Security teams have had to adapt to a workforce that was suddenly beyond traditional perimeters, working with new tools in new environments. When questioned about the preparedness of security infrastructure to handle risks (caused by the pandemic), only 20% of respondents said the security infrastructure was very prepared to handle these changes. Just over a third (34%) said it was somewhat prepared. Comparatively, 29% said security infrastructure was somewhat unprepared (17% not at all prepared). That's an indication that existing security capabilities weren't well-suited to pandemic-driven changes.

FIGURE 1

Infrastructure Readiness

Q: How prepared was security infrastructure to handle the range of risks associated with the new business operating environment caused by the pandemic?



Source: 451 Research's 2021 Data Threat custom survey

When the survey looked at investments driven by the pandemic, a little under half (44%) of respondents indicated that privacy and security were most important. New working models and corresponding risks could be behind this preference. Existing security infrastructure had to pivot dramatically to address the challenges of remote work – the change from remote being the exception to the norm upended many security approaches. There was also pressure to make infrastructure more accessible, and 32% of respondents said that investment in infrastructure/cloud was most important. Remote work required applications and tools to be available and performant for the masses of newly remote employees. That meant that external, cloud-based infrastructure was coupled with on-premises resources in distributed or hybrid arrangements, an investment option selected by 24% of participants.

The pandemic is affecting future investments as well. The largest percentage of respondents (46%) selected Zero Trust network access or software-defined perimeter technologies as their leading technology to deploy due to the pandemic. Cloud-based access management (access management services that offer policy-based access, authentication and single sign-on delivered from the cloud) was the second most important access technology, selected by 41% of respondents. This aligns with increases in remote work and the challenges in securing a remote workforce.

Era of Remote Working

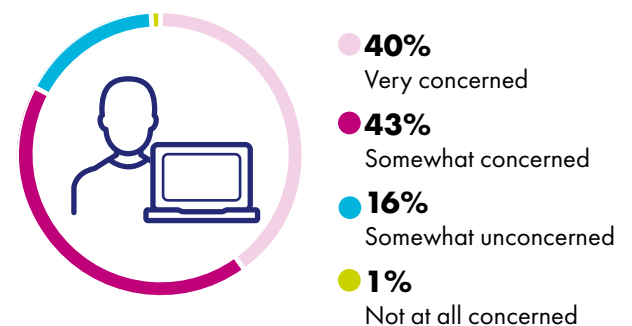
One of the largest changes imposed by the pandemic was the shift to remote working, which raised concerns for security teams; 43% said they are somewhat concerned about the security risks and threats of employees working remotely. A slight majority had some level of confidence in their current access environment: 53% said it could allow employees to work remotely in a secure and easy manner (25% very confident, 28% somewhat confident). However, that leaves a large number (47%) with concerns (and 17% were not at all confident). This is a situation that will need to change as remote working persists.

“53% said it could allow employees to work remotely in a secure and easy manner (25% very confident, 28% somewhat confident).”

FIGURE 2

Concern about Remote Working Security

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



Source: 451 Research's 2021 Data Threat custom survey

Cloud Has Arrived

Increased use of cloud-based infrastructure is here today for most organizations, and it has become the home of more enterprise data. In APAC, 31% of respondents stated that 41-50% of their data is stored in an external cloud, and 25% said that more than half is stored there. When asked about the protections that they had in place, 30% of APAC respondents said that 41-50% of the sensitive data stored in cloud is encrypted. Only 17% of respondents stated that over 50% is encrypted.

Despite a greater adoption of cloud, 46% of respondents agreed that it is more complex to manage privacy and data protection regulations in a cloud environment than in on-premises networks within their organization (23% agreed, 23% strongly agreed). With a chronic skills shortage in cloud security, that's a problem that will require investment in better management technology to address.

A large, stylized number '75%' in a dark purple color, with the percentage sign in a lighter purple shade.

of APAC responders said that they do not have complete knowledge of where their data is stored

A large, stylized number '30%' in a dark purple color, with the percentage sign in a lighter purple shade.

said they experienced a breach in the last 12 months

Breaches and Other Failures

A data breach can be thought of as the ultimate measure of the effectiveness of an organization's security operations. Globally, breaches were reported at a relatively high rate. More than half (56%) of APAC respondents claimed to have experienced a security breach at some point, which was in line with the global average. Out of these, 30% said they experienced a breach in the last 12 months. Interestingly, the indication of audit failures was notably lower than the global average, with 43% reporting a failure versus 48% globally.

One of the challenges with securing data is understanding where data is located and its level of sensitivity. The survey looked at both of these areas, and the results should raise concerns. Only 25% of APAC respondents said that they have complete knowledge of where their data is stored, and about a third (33%) claimed to be able to fully classify their data. While this is in line with global averages, the results show that organizations will have to expend more effort not only to identify where their data is located, but also to understand how to build sufficient protections to prevent breaches.

There is progress in some areas – for example, in the number of respondents indicating that they had avoided a breach notification because the stolen or leaked data was encrypted or tokenized. Slightly less than half (46%) of respondents said that they had been able to avoid notification. With increased use of data protection technologies, that's a number that we would hope to see increase.

Security Threats

The threat landscape is ever changing, and almost half (45%) of respondents reported seeing an increase in the volume, severity and/or scope of cyberattacks in the past 12 months. In APAC, 57% ranked malware as the leading source of security attacks. Ransomware came in second at 48%.

FIGURE 3

Threats Increasing

Q: What types of attacks/threats have you seen increase?

Malware



Ransomware



Credential Stuffing / other password attacks



Phishing / Whaling



SQL Injection



Denial of Service



Man-in-the-middle / Eavesdropping



Brand Impersonation



Source: 451 Research's 2021 Data Threat custom survey

50%

were very concerned about the security threats posed by quantum computing

only

34%

claimed to have a formal strategy and have actively embraced a Zero Trust policy

Quantum Computing

Threats that are more forward-looking were of more concern to APAC survey respondents. About half (50%) were very concerned about the security threats posed by quantum computing. This level of awareness should be generating interest in post-quantum cryptographic techniques and efforts to improve crypto agility.

Zero Trust Journey

Threat models are changing, and organizations are working to adapt their security strategies to address the changes they face. The study looked at aspects of Zero Trust and the ways in which it is being incorporated into operational security plans. When asked about their Zero Trust strategies, 34% claimed to have a formal strategy and have actively embraced a Zero Trust policy. That was ahead of the global average of 30%. Interestingly, those with a formal Zero Trust strategy are less likely to have been breached. When asked to what extent Zero Trust security shapes cloud security strategy, 35% of respondents said 'to a great extent'; 42% rely on some concepts of Zero Trust.

“The lack of higher levels of encryption use may be due to the complexity of managing it across the full infrastructure of an organization.”

only

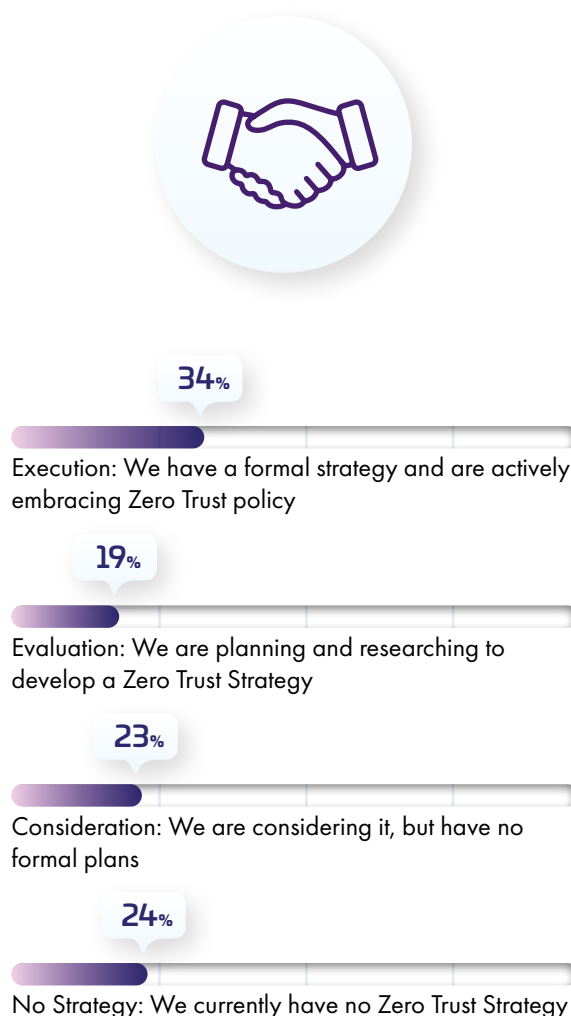
30%

of respondents said that a large portion of their sensitive data in cloud is encrypted

FIGURE 4

Zero Trust Journey

Where are you on your Zero Trust journey?



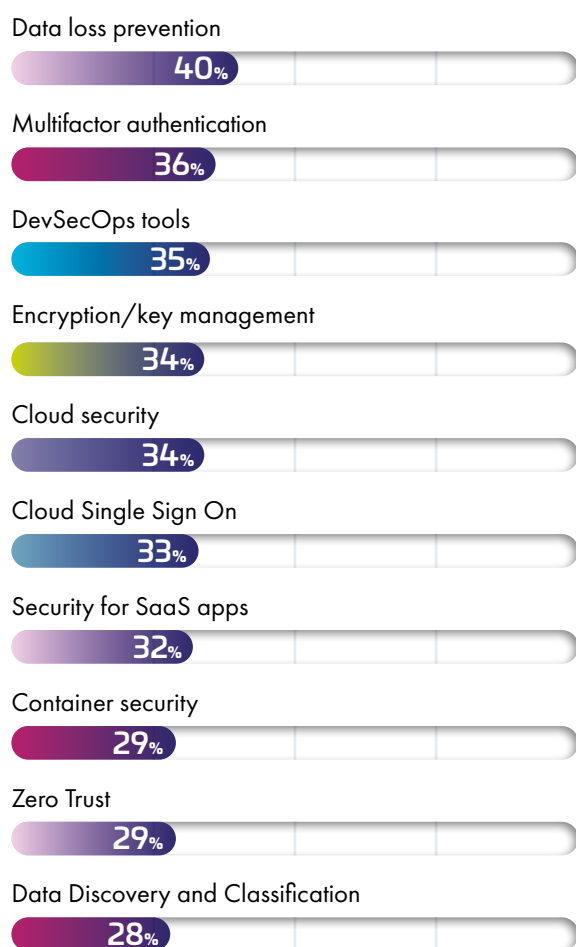
Source: 451 Research's 2021 Data Threat custom survey

Security Spending

Decisions about security spending are always complex. Balancing priorities with budgets requires trade-offs, and the survey looked at how those are expressed. Data loss prevention was ranked first most often, with 40% saying so. Multifactor authentication was second (36%) and was also highly rated as a technology to protect sensitive data in cloud (second at 58% after encryption at 67%).

FIGURE 5

Balancing security spending priorities over budget



Source: 451 Research's 2021 Data Threat custom survey

Data Protection Strategies

The foundation of data protection is a combination of encryption effectiveness and key management strategies. As we've noted earlier, there is room to expand the use of encryption among the study respondents, but without better key management, increases won't improve the overall data security posture. The study looked at the current state of respondents' environments and how they're managing this important area of security operations. Encryption was selected by 67% of respondents as their preferred tool to secure sensitive data in cloud. Key management ranked second, selected by 58%. Tokenization of data was chosen by 52%. There is a significant difference between the level of interest and action – only 30% of respondents said that a large portion of their sensitive data in cloud is encrypted (41-50%).


The lack of higher levels of encryption use may be due to the complexity of managing it across the full infrastructure of an organization. Respondents indicated that this was already complex, with 38% saying that they have five to seven key management solutions in place. Another 14% indicated they have 8-10. That can make it difficult to extend to cloud in an efficient or effective manner, which could explain why a strong majority (61%) of respondents stated that their cloud provider controls all or most of their keys. Only 12% said they fully control their own keys in cloud. For those that had some level of control, different tactics were employed in parallel. APAC respondents were less likely than the global average to use provider consoles, with 47% doing so. They were more likely to use 'bring your own key' (BYOK) strategies, with 40% doing full BYOK and 33% managing brought keys in the provider environment.

Encryption was selected by 67% of respondents as their preferred tool to secure sensitive data in cloud"

only

12%

said they fully control their own keys in cloud

A close-up photograph of a server rack. A hand with pink nail polish is pointing at a server unit. Blue cables are visible at the top of the rack. The background is dark and out of focus.

“The demands of compliance with regulations such as GDPR and the implications created by the Schrems II ruling are showing that native cloud controls alone may be insufficient to protect sensitive data.”

Moving Ahead

The survey offers views of useful paths for organizations to follow as they plan their security strategies. A main lesson of the pandemic is that security strategists need to increase the agility of their security controls and the depth of their understanding of their data protection strategies. The future offers an increase in the hybrid nature of infrastructure, and security teams must have the capabilities to address this more complex environment efficiently. It means that controls and security management will have to extend to cloud in ways that keep each cloud environment from being an isolated operational realm.

The demands of compliance with regulations such as GDPR and the implications created by the Schrems II ruling are showing that native cloud controls alone may be insufficient to protect sensitive data. Organizations need to increase their depth of encryption use and step up to fully delivering on encryption's benefits by controlling the secrets that protect their data through BYOK, hold your own key (HYOK) and bring your own encryption (BYOE) approaches.

Organizational changes are required to ensure that security challenges are understood throughout organizations and that investment priorities are properly aligned. Effective strategy and security investment decisions will be more complicated when perspectives across the organization aren't aligned. This is especially true as regulatory changes and the potential for nation-state collateral damage are forcing them to move ever faster.



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

