Trustwave®

2020 Data Security Index

Based on a survey commissioned by Trustwave

Table of Contents:

Introduction

Data security is a leading concern for organizations of all kinds – and it will become even more critical in the coming years. Technological trends and developments are changing the way data is stored, along with the way it needs to be protected. Database systems, no matter what their form, continue to grow larger and even more complex. The data itself continues to become not only more valuable, but also more essential for how your organization operates, which makes it an even more tempting target for all manner of malicious actors. To top it all off, high-profile data breaches are making the public more distrustful of organizations who store personal data – and causing governmental entities to create stringent compliance regulations.

As a cybersecurity professional, all of these factors add up to increasing pressures, responsibilities and potential hazards. The total volume of digital data people and businesses have created worldwide is approximately 50 zettabytes in 2020, and is projected to triple by 2025, *per research from IDC*. According to the *2020 Trustwave Global Security Report*, attacks on cloud services have more than doubled, while ransomware demands are now the leading form of incidents during data breaches. And the global annual cost of cybercrime, when factoring in regulatory fines, is projected to run into the trillions in the near future.

Yet, while the threats and exposure to risk are growing, your budgets and staff are not. That's why this report was created: to help you gain a critical edge in the fight to secure your data. We hope that it helps you to gain a better understanding of the data security landscape and the attitudes and actions of your industry peers. Use this report as you see fit – through either a complete read through or a scanning of the key data points. The headlines of each page summarize the findings contained within, to help you gain a quicker understanding. For further reading, visit the *Trustwave blog* to learn more about our continuing research into data and database security.

Key Findings

Critical Concerns

Almost all respondents listed their data security as important or very important, and most organizations rate securing their data as an important cybersecurity concern during digital transformation projects.

Defend Against Malware and Ransomware

When asked to name the threats they most worry about, malware and ransomware were ranked first by 38% of respondents.

Patching Practices

This could be one area where organizations have room to improve. Almost all have a policy in place, but the split between manual vs. automatic patching could be cause for concern, depending on what kind of data you're protecting.

How's Your Hygiene?

While most organizations have implemented continuous database scanning, they might not be scanning as deeply as they think.

Compliance Catch Up

Most organizations believe they are in compliance with key regulations like General Data Protection Regulation (GDPR), but their database strategies reveal potential gaps.

Cloud Cover

Most organizations are moving their data into the cloud, with a hybrid cloud/on-premises model becoming the norm. Most organizations use multiple cloud providers.

Small Teams. Big Responsibilities.

The average size of a cybersecurity team is between 6-15 people, with Asia Pacific companies averaging the smallest teams.

Methodology

Trustwave commissioned a third-party research firm to survey 966 full-time IT professionals who are cybersecurity decision makers or security influencers within their organization. The objective of the survey was to assess the current and expected future states of data security across all data spheres, including on-premises, cloud and hybrid, and to examine some of the key challenges that cybersecurity teams face. Respondents worked at either businesses or government agencies, with 310 respondents in the United States, 254 in the United Kingdom, 200 in Australia and 198 in Singapore. Over 75% of the respondents worked in organizations with over 500 employees, with over 40% part of organizations with over 1,000 employees. The survey was conducted via email in August 2020. Survey results have a margin of error of +/- 5.069% in the United States, +/- 5.67% in the United Kingdom and +/- 6.576% in Singapore and Australia.

Cybersecurity Teams

Cybersecurity Teams Are Small – But Their Responsibilities Are Huge

In this survey, over 75% of respondents were part of organizations with over 500 employees and 40% were part of organizations with over 1,000 employees. Yet, of those polled, most (24%) had a security team size between 16-20. Just 20% had a team of 21 or greater. On average, Singapore had the smallest security team size with 47% reporting having between 1-10 members.

The relatively small size of cybersecurity teams isn't a reflection of the awesome responsibilities they're tasked with. With the average cost of data breaches rising, the stakes for organizations couldn't be higher. And cybercrime is becoming so prevalent, organizations are now putting as much emphasis on detection and response as they are prevention—meaning that small cybersecurity teams are compelled to use managed security services providers and automation tools and services to supplement efforts.

How many individuals are on your cybersecurity team?

	Global	United States	United Kingdom	Australia	Singapore
1-5	9%	6%	7%	14%	24%
6-10	23%	24%	26%	26%	23%
11-15	24%	27%	23%	23%	17%
16-20	24%	21%	25%	26%	25%
21+	20%	22%	19%	11%	11%

The Growing Skills Gap

Even though security teams are small, difficulties in finding qualified candidates are growing – and won't get better any time soon, according to leading research.

- The skills gap effects over 70% of organizations.
- Ramifications of the gap include greater stress, heavier workloads, and inefficient use of tools.
- Many cybersecurity professionals report job stress creating personal problems.

Source: Jon Oltsik, *The Life and Times of Cybersecurity Professionals 2020*, ESG-ISAA, July 2020

The Cloud

More and More Data Is Moving to the Cloud

When asked where their data currently resides, most respondents (55%) said that they use both public cloud and on-premises databases to store data. 17% use public cloud only. Singapore organizations use the hybrid model much more frequently at 73% which is 18% higher than the total, and U.S .organizations use it least frequently at 45%. U.S. organizations store data on-premises only the most at 35%.

The results here are to be expected: most organizations across all industries are moving their sensitive data into some form of cloud storage. But as organizations increasingly use multi-cloud environments and cloud-based services, including cloud-based applications, the focus needs to be on security. There's a common misconception that cloud service providers (CSPs) are responsible for security of the platform or share liability for breaches. That's almost always not true – meaning your team is still responsible for finding security solutions that can work seamlessly no matter where your data resides, whether it's on-premises, in the cloud(s) or split across a combination of both.

Where does your data currently reside?

	Global	United States	United Kingdom	Australia	Singapore
On-premises	28%	35%	29%	28%	16%
Public Cloud	17%	20%	17%	20%	11%
Hybrid Model	55%	45%	54%	52%	73%

.

Most Organizations Use Multiple Cloud Services

When we asked how many third-party cloud services organization use, most respondents at 70% use between 2-4 public cloud services followed by 18% using 0 or just one. 12% use 5 or more. At 14%, the United States had the most instances of using 5 or more public cloud services followed by the United Kingdom at 13%, Australia at 9% and Singapore at 9%. What's interesting here is the added level of complexity that security teams now face, with cybersecurity teams tasked with managing multiple vendors – as well as needing to account for the previously mentioned additional security risks that cloud services create.

How many third-party cloud services does your organization use?

	Global	United States	United Kingdom	Australia	Singapore
0-1	18%	15%	21%	23%	15%
2-4	70%	71%	66%	68%	76%
5+	12%	14%	13%	9%	9%

Types of Cloud Data

More Sensitive Data Moves into the Cloud

Adding to the pressure that security teams face, the types of data that organizations are moving into the cloud have become increasingly sensitive. 96% of total respondents stated they plan to move sensitive data to the cloud over the next two years. More than half (52%) plan to move highly sensitive data to the cloud. Australia respondents, at 57%, lead in plans to move the most highly sensitive data to cloud followed by the United Kingdom 52%, Singapore 51% and the United States 50%.

These findings echo some of the larger trends that have been unfolding. In 2020, the COVID-19 pandemic has pushed organizations towards cloud adoption faster – and with many organizations contemplating permanent increases in remote-working postures, these trends are expected to continue and accelerate. For security teams, the challenges are having a continuous understanding of risks and being able to respond quickly, given their limited resources.

What type of data are you planning to move to the cloud in the next two years?

	Global	United States	United Kingdom	Australia	Singapore
Highly Sensitive	52%	50%	52%	57%	51%
Moderately Sensitive	44%	46%	43%	39%	43%
Not Sensitive	4%	4%	5%	4%	6%

Digital Transformation

Data Is Helping Drive Organizational Change

Digital transformation projects can help organizations rethink how they use everything from the technology they own to the people that they employ to the processes that they perform. IDC research estimates that worldwide spending on digital transformation will reach $2.3 trillion in 2023 – with Forbes reporting that 70% of all companies either have a digital transformation strategy in place, or are working on one. The factors that drive these transformations are often new opportunities – to grow a business, gain efficiencies, serve customers in new ways, and beyond. But digital transformation is also often driven by necessities – to keep up with the competition, comply with new regulations or to update legacy systems.

It's no wonder then that data – and how data is stored and managed – is a big part of most organization's digital transformation projects. When we asked our respondents how they were storing their data during these projects, nearly half of respondents (48%) stored their data in a hybrid model. Second was on-premises at 29%, and third was in a public cloud as a hosted database associated with a SaaS application at 19%. Singapore led in using the hybrid model approach at 12% higher than the global average. What's interesting in these results is that it seems that most organizations feel that a hybrid approach best fits their needs – speaking once again to the increased need for a robust security strategy that adequately protects data stored off-site.

Mission Critical: Securing Organizational Data

Rate the importance of securing data in regard to your organization's digital transformation.
(rate 1 star to 5 stars)

TOTAL:

4.6 Mean (Average)

BY COUNTRY:

- United States: 4.6 Mean
- United Kingdom: 4.5 Mean
- Australia: 4.5 Mean
- Singapore: 4.6 Mean

ANALYSIS

4.6 average out of five stars in terms of how important securing data in regard to digital transformation projects
(5 stars is most important)

Where did you store your data from a recent IT digital transformation project?

	Global	United States	United Kingdom	Australia	Singapore
On-Premises	29%	36%	30%	30%	15%
In a hybrid model (on-premises and in a public cloud)	48%	42%	50%	41%	60%
In a public cloud as a hosted database associated with a SaaS application	19%	15%	17%	24%	23%
In a public cloud as a hosted database	4%	6%	3%	4%	2%
Other	0%	1%	0%	1%	0%

Threats

Anticipated Attacks Don't Always Match Actual Attacks

Organizations all over the world are worried about cyber threats – for good reason. Not only has the COVID-19 pandemic contributed to a startling rise in incidents of all types of cybercrime, but the long-term trends are also alarming. Trying to figure out the methods of how these crimes will be committed is of paramount concern to data security professionals, which is why we asked our respondents which types of threats concerned them the most.

Globally, organizations are most concerned with malware/ransomware at 38%. The second leading cause for concern was phishing/social engineering at 18%. Threat of application attack came in third at 14%. Insider threats, which also include misuse, misconfigurations and human error, came in fourth at 9%. Privilege escalation fifth at 7%. Threats to data coming from new data regulations came in at 6%.

Breaking the data down by country, the United Kingdom placed misconfiguration attacks and privilege escalation as the least cause for concern – even lower than data regulations. Singapore was concerned about attacks due to misconfiguration at 9%. Singapore was also most concerned about phishing/social engineering at 21% – or 4% higher than the global average.

What's interesting here is that, according to the 2020 Trustwave Global Security Report, phishing and social engineering attacks were the most frequent attacks on corporate networks and cloud environments in 2019, which is more accurately reflected in the responses to the question about actual attacks that our respondents have experienced. Because phishing and social engineering can be used as delivery methods for malware and ransomware, there is a connection between the two. And while misconfiguration attacks rank low, in the real world there have been numerous high-profile data breaches causes by database misconfiguration and human errors.

Based on this data, there could be an opportunity for security leaders to reassess the threats they are preparing for, while preparing their company leadership for attacks that might not exactly match those that were expected.

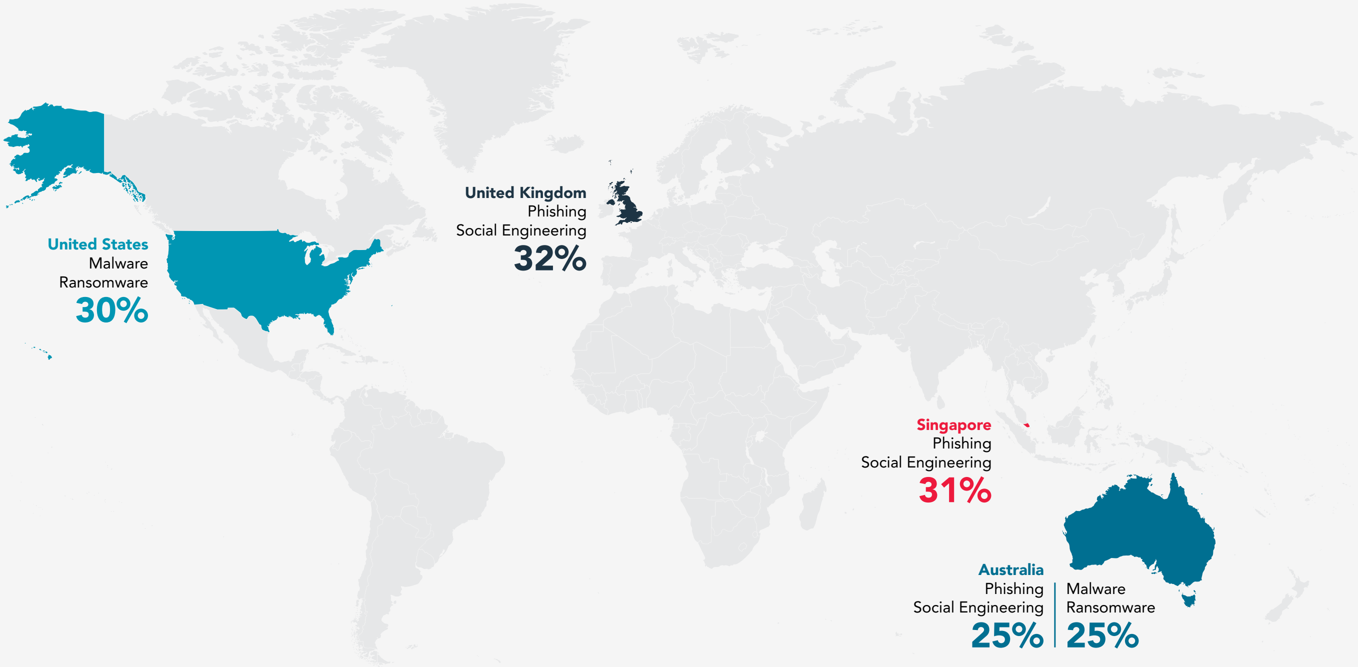
Beware Ransomware

Ransomware, which can be delivered via phishing attacks, are increasingly targeting database programs such as MySQL and MongoDB. Ransomware was the largest share of security incidents Trustwave investigated in 2019, which quadrupled over the previous year to encompass 18% of the incidents. Find the full story in the *2020 Trustwave Global Security Report.*

What type of threat to data are you most concerned about?

	Global	United States	United Kingdom	Australia	Singapore
Malware/Ransomware	38%	38%	42%	37%	36%
Privilege Escalation	7%	9%	4%	9%	4%
Phishing/Social engineering	18%	13%	18%	19%	21%
Insider Threats	9%	10%	10%	9%	8%
Application (Web or Mobile) Attack	14%	12%	14%	15%	15%
Misconfiguration Attack	6%	10%	3%	4%	9%
Data Regulations	6%	6%	7%	5%	5%
Some Other Security-Related Problem	2%	2%	2%	2%	2%

Most Frequent Threats Reported By Country



What types of threats to data has your organization experienced most frequently?

Although all countries viewed malware/ransomware as the top threat to data, actual threats experienced came most frequently from phishing/ social engineering at 27% followed by malware/ransomware at 25% and application (web or mobile) attack at 13%. Privilege escalation came in fourth at 9% followed by insider threats at 8%, data regulations 7% and attacks stemming from misconfigurations coming in last at 6%.

Looking at the data by countries, the U.S. experienced the most malware/ ransomware attacks 30%, followed by Australia at 25%. The United Kingdom and Singapore both experienced the most phishing/social engineering threats at 32% and 31%. Australia had the most threats via application attack at 16% or nearly 4% higher than the next closest country (United Kingdom).

	Global	United States	United Kingdom	Australia	Singapore
Malware/Ransomware	25%	30%	22%	25%	24%
Privilege Escalation	9%	10%	8%	11%	4%
Phishing/Social engineering	27%	24%	32%	25%	31%
Insider Threats	8%	10%	8%	4%	6%
Application (Web or Mobile) Attack	13%	11%	12%	16%	11%
Misconfiguration Attack	6%	6%	5%	6%	8%
Data Regulations	7%	5%	9%	8%	7%
Some Other Security-Related Problem	5%	4%	5%	5%	9%

Cybersecurity Priorities

Database Security Is A Critical Concern

When we asked respondents to rate the importance of their database security strategy in relation to other cybersecurity priorities, it's not surprising that 96% of total respondents felt their database security strategy was either important or very important. This can be seen, of course, as a positive development – as organizational data which tends to house the most sensitive content is and will continue to be a top target for cyber criminals – and the negative consequences of data breaches, including financial, legal and reputational losses, will continue to grow more dire.

Compared to other cybersecurity priorities, how critical is your database security strategy?

	Global	United States	United Kingdom	Australia	Singapore
Very Important	70%	69%	74%	72%	68%
Important	26%	26%	24%	26%	30%
Somewhat Important	4%	5%	2%	1%	2%
Not Important	0%	0%	0%	1%	0%

Patching Practices

Patching Practices Show Room for Improvement

When we asked respondents whether or not they had patching policies in place, 96% answered yes, which of course can be read as a positive. Digging deeper, however, we find that around 71 percent of respondents across the globe are using automatic patching, which is not necessarily the most secure practice. While many workplace computers can be patched automatically, more sophisticated systems, like databases, might benefit from manual patching, which gives IT teams a chance to apply testing and crucial human oversight.

Do you have database patching policies in place?

	Global	United States	United Kingdom	Australia	Singapore
Yes	96%	96%	97%	95%	98%
No	4%	4%	3%	5%	2%

Does patching take place automatically, or is it a manual process?

	Global	United States	United Kingdom	Australia	Singapore
Automatically	71%	72%	69%	78%	67%
Manual	29%	28%	31%	22%	33%

Most Patches Are Applied Within Two Days

When we asked respondents how quickly they were applying patches, 61% of organizations patched within 24 hours with 16% patching within one hour. 28% patched between 24-48 hours. Unfortunately, there were still 4% that said it takes one week to greater than one month. Australia patched the fastest with 66% reporting they patched within 24 hours followed by the United Kingdom at 61%.

Rapid patching is good news, as security drift can be one of the most common causes of breaches. It's estimated that 80% of data breaches could be prevented with basic actions, like patching – however the time between when patches are applied frequently turns out to be a window of opportunity for malicious actors. In addition, it's essential that organizations ensure they regularly assessing their databases to understand what needs to be patched – and that they are aware of all the databases they need to protect. Too often it's the hidden vulnerability that can prove to be the deadliest.

How long does it typically take to fully implement a database patch once it has been issued?

	Global	United States	United Kingdom	Australia	Singapore
Within an hour	16%	19%	12%	18%	15%
Less than 24 hours	45%	41%	49%	48%	42%
24-48 hours	28%	27%	26%	29%	29%
48 hours to one week	7%	8%	10%	4%	8%
One week to one month	3%	4%	3%	1%	5%
Greater than one month	1%	1%	0%	0%	1%

Misconfigurations

Misconfigured databases have been a major problem across all sectors and makes them vulnerable to attacks. For example, criminals target publicly facing cloud databases using the default settings to compromise its databases and then demand a ransom to release them

Source: *2020 Trustwave Global Security Report.*

Data Security Practices

Are Your Security Practices as Hygienic As You Think?

When asked whether they had incorporated continuous database scanning in their environments, 86% of total respondents said that they had. Australia and Singapore were both slightly higher than the total average at 88%. The U.S. and United Kingdom were slightly higher than the total average of those who do not have continuous database scanning in place at 16% and 14%.

While a high percentage of organizations using continuous database scanning sounds like a good result, there still could be cause for concern. Some security teams might not be using scanning tools that are purpose built for their databases, resulting in scans that don't go as deep as they should – or as deep as the people running them think. Additional areas to examine are whether or not scanning tools are looking at potential weaknesses like user rights and patch configurations. These areas of vulnerabilities can often be overlooked—and exploited.

Have you incorporated continuous database scanning in your environment?

	Global	United States	United Kingdom	Australia	Singapore
Yes	86%	84%	86%	88%	88%
No	14%	16%	14%	12%	12%

Automation Might Not Be Automagical

Over-reliance on automation is one of the most common cybersecurity pitfalls, and we were curious as to where organizations stood on this in regard to their database security practices. When we asked our respondents if they had policies in place to automatically check for overprivileged users or that automatically lock down access credentials once an individual has left the organization or changed roles, 89% said that they do.

We believe that this large percent corresponds to our ***previous findings*** that shows a low amount of concern around privilege escalation and insider threats to data. If security teams believe that user privileges are being automatically managed, they rightly feel there's less need to worry. But within that assumption could lie a hidden trap, as security teams could be failing to check user privileges and access against changing company policies, external regulations, and more. As one example: an organization might assume that when a user's access to a certain application is removed, access to the database is also removed, which is not always the case. It always comes back to good security hygiene – which inevitably requires an element of human oversight.

Do you have policies in place to automatically check for overprivileged users or that automatically lock down access credentials once an individual has left the organization or changed roles?

	Global	United States	United Kingdom	Australia	Singapore
Yes	89%	88%	88%	89%	90%
No	11%	12%	12%	11%	10%

VPNs and MFA are Almost Universal

At the time of writing (2020), the COVID-19 pandemic is still taking place – forcing an unprecedented global shift to remote work postures. Therefore, it was gratifying to see that 91% of those polled have VPNs and MFA set up for remote workers. The numbers were even across all countries, with Singapore having a slight edge at 96%.

Do you have VPNs and multifactor authentication (MFA) set up for all employees who work remotely from home (either occasionally or full-time)?

	Global	United States	United Kingdom	Australia	Singapore
Yes	91%	90%	91%	89%	96%
No	9%	10%	9%	11%	4%

Privilege Abuse

Privilege abuse occurs when the privileges associated with user accounts are operated inappropriately or fraudulently. Privilege escalation involves attackers taking advantage of vulnerabilities in database management software to convert low-level access privileges to high-level access privileges. Privilege escalation requires more effort and knowledge than simple privilege abuse. In the breaches Trustwave investigated in 2019, user credentials accounted for 15% of the cloud data and 18% of the corporate/internal network data compromised.

Source: *2020 Trustwave Global Security Report.*

Compliance Concerns

Organizations Might Be Lagging Behind On Compliance

In 2020, compliance with regulations like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) have become a concern for organizations of all shapes and sizes – and we expected that it would have driven measurable changes in database security strategies. Interestingly though, 60% of total respondents said GDPR and CCPA had no impact on their database security strategy since implementations of these new regulations. These numbers were about even across all regions.

This data may reveal a lack of alignment internally within organizations, since provisions like the GDPR's right to be forgotten force organizations to take actions that they were not taking before. Are your legal teams, database analysts and CISO fully embracing all the measure that need to be taken to keep your databases in compliance? Many organizations have taken a wait and see approach and may not have fully embraced all the appropriate changes – which could lead to fines, lawsuits or lost business opportunities in the very near future. For many organizations, now is the time to assess how databases are being stored and managed – and determine whether you have the right tools in place. The good news is that many database security platforms and services include built-in assessment capabilities, to help you ensure you're in compliance with GDPR and CCPA.

Has your database security strategy changed since the implementation of the General Data Protection Regulation or the California Consumer Privacy Act?

	Global	United States	United Kingdom	Australia	Singapore
Yes	40%	36%	40%	38%	46%
No	60%	64%	60%	62%	54%

Compliance-Driven Changes

What Has Changed Due To Regulations?

For respondents who answered yes when asked if their database strategy had changed due to regulations, we asked them to describe how. Some of the common themes in their answers included adding third-party solutions, hiring more staff or purchasing more software, adding layers of encryption and implementing more web applications and firewalls. Interestingly, many respondents indicated that the regulation prompted them to become more vigilant about routine hygiene measures, like patching and backing up data more frequently.

Responses:

- "We deal with a third-party to apply some solutions to manage data patching and management."
- "We needed to implement more software solutions and hire more staff due to the new practices."
- "We have adopted a strategy that is more proactive in securing contact information, government IDs and other relevant information against security breaches."
- "Constant changes are required to meet the regulations."
- "We added additional layers of encryption to sensitive personal data that are on premise and on clouds."
- "More regular updates."
- "We've implemented more security measures."
- "There is better collaboration between all technology platforms."
- "We perform daily backups."
- "We now use web application and database firewalls."
- "We changed our strategy by using web application & database firewalls, encrypting data, auditing and monitoring database activity, etc."
- "We have built in continuous monitoring."
- "Increased regular updates and patches."
- "We were more or less in line with these regulations, all we had to do was make some minor adjustments to ensure compliance."
- "Data was encrypted so only authorized users could access it."
- "We have implemented database security processes such as: protect, audit, manage, update, and encrypt."
- "The housing of data now has to be in Europe."

Trustwave is a leading cybersecurity and managed security services provider focused on threat detection and response. Offering a comprehensive portfolio of managed security services, consulting and professional services, and data protection technology, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries.
For more information about Trustwave,
visit *www.trustwave.com.*

Trustwave®