OCT – DEC 2021

SECURITY SOLUTIONS TODAY

DATA PROTECTION DURING REMOTE WORK

How can organisations secure their data during remote work arrangements?

IN THIS ISSUE

CONTACT

ASSOCIATE PUBLISHER Eric Ooi (eric.ooi@tradelinkmedia.com.sg)

EDITOR Ming En Liew (sst@tradelinkmedia.com.sg)

MARKETING MANAGER Felix Ooi (felix.ooi@tradelinkmedia.com.sg)

HEAD OF GRAPHIC DEPT / ADVERTISEMENT CO-ORDINATOR
Fawzeeah Yamin (fawzeeah@tradelinkmedia.com.sg)

CIRCULATION Yvonne Ooi (yvonne.ooi@tradelinkmedia.com.sg)

OCT - DEC 2021
SECURITY SOLUTIONS TODAY
DATA PROTECTION DURING REMOTE WORK
How can organisations secure their data during remote work arrangements?

Vectors Credit: Freepik.com
Designed by Fawzeeah Yamin

SECURITY SOLUTIONS TODAY
is published quarterly by Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399
Tel: +65 6842 2580
ISSN 2345-7112 (E-periodical)

Disclaimer: The editor reserves the right to omit, amend or alter any press release submitted for publication. The publisher and the editor are unable to accept any liability for errors or omissions that may occur, although every effort had been taken to ensure that the contents are correct at the time of going to press.

The editorial contents contributed by consultant editor, editor, interviewee and other contributors for this publication, do not, in any way, represent the views of or endorsed by the Publisher or the Management of Trade Link Media Pte Ltd. Thus, the Publisher or Management of Trade Link Media will not be accountable for any legal implications to any party or organisation.

Views and opinions expressed or implied in this magazine are contributors' and do not necessarily reflect those of Security Solutions Today and its staff. No portion of this publication may be reproduced in whole or in part without the written permission of the publisher.

For advertising interests, please email us at **info@tradelinkmedia.com.sg.**

HEALTHCARE SECTOR UNDER INCREASED CYBER ATTACKS DURING THE PANDEMIC

Image: www.freepik.com

The healthcare sector cannot seem to catch a break this pandemic. Besides fronting the battle against Covid-19, healthcare has also been fielding attacks of a different kind; the 2021 Global DNS Threat Report by EfficientIP and International Data Corporation (IDC) reveals that the industry has faced devastating DNS attacks throughout the pandemic. The average cost per attack in healthcare has increased to US$862,630, a 12% rise from last year and the sharpest increase seen by any industry.

Of the six industries examined, healthcare is the most likely to suffer application downtime, have the highest rate of compromised websites, and the highest rate of brand damage – all of which are causes for concern in an industry already stretched thin by the pandemic.

With healthcare needs being high during a pandemic, downtime in apps, services, and cloud service can be a matter of life and death. Further, the sensitivity of customer information within the healthcare sector makes them a particularly attractive target for cyber criminals. This is evident from the Threat Report, with rates of stolen customer information increasing by 13% from last year, to 23% this year.

The increasing trend of attacks on the healthcare sector has been observed for many countries in the Asia Pacific region, especially in the Philippines, Thailand and Malaysia. On average, healthcare organisations each suffered 6.71 DNS attacks over a 12-month period, and it took an average 6.28 hours to mitigate each attack.

The most common DNS attack type observed in healthcare is phishing, with 49% of healthcare companies surveyed experiencing a phishing attack. Other popular forms of cyberattacks include DNS-based malware, DNS tunneling, and DNS domain hijacking.

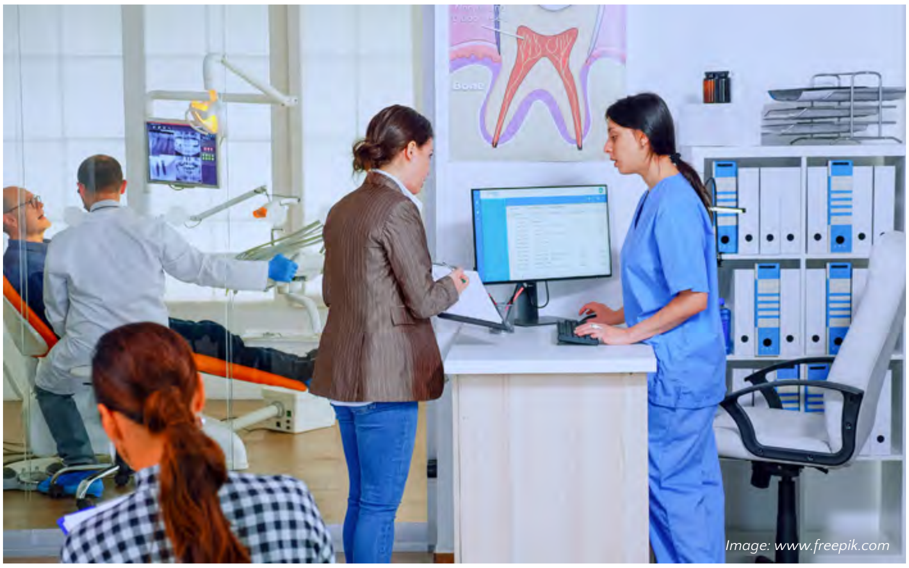


Image: www.freepik.com

The Singapore healthcare sector also found itself to be at risk for government data hacks through malware. The government previously detected millions of internet connected medical equipment including ultrasound machines, patient monitors and medical imaging equipment vulnerable for attacks.

The above data spells out the importance of cyber defense strategies in the healthcare sector. To protect themselves, healthcare companies have turned to Zero Trust and smarter DNS security. The Threat Report shows that the healthcare industry is planning, implementing or running Zero Trust initiatives more than other industries, and is the strongest believer that using DNS domain deny-and-allow lists for improving control over which users can access which apps is valuable for Zero Trust.

More details on the impact of DNS attacks on healthcare and how companies can shore up their defenses can be found in the 2021 Global DNS Threat Report. ■

RUBRIK ANNOUNCES STRATEGIC AGREEMENT WITH MICROSOFT

Rubrik, a cloud data management firm, has announced a strategic agreement with Microsoft that includes a Microsoft equity investment in Rubrik to drive go to market activities and co-engineering projects to deliver integrated Zero Trust data protection solutions. This will address rising customer needs to protect against surging ransomware attacks, which are growing at a rate of 150% annually. Together, Rubrik and Microsoft will provide Microsoft 365 and hybrid cloud data protection and integrated cloud services on Microsoft Azure.

Rubrik is addressing the most pressing data challenges for enterprises: rapid recovery from ransomware, automation of data operations, and the transition of data to the cloud. The Rubrik and Microsoft collaboration brings these offerings to the next level, providing Zero Trust data protection for hybrid cloud environments spanning data center, edge and cloud, including Microsoft 365.

Image: www.freepik.com

As part of this collaboration, customers and partners gain additional data protection, so that critical Microsoft 365 data is secure, easily discoverable, and always accessible in the case of a malicious attack, ransomware attack, accidental deletion, or corruption. Rubrik also offers additional support and protection for Microsoft 365 including instant search and restore and policy-based management at scale. Additionally, Rubrik and Microsoft provide long-term archival of Microsoft 365 data for the purposes of regulatory compliance.

Image: www.freepik.com

Image: www.freepik.com

With Rubrik and Microsoft, mission-critical applications such as SAP, SQL, Oracle, VMware, as well as enterprise NAS workloads can tightly integrate protection and automation with Azure, which is critical as customers accelerate their digital transformation. Working with Microsoft, Rubrik will help customers address these priorities while providing agility to migrate data to the cloud and achieve improved productivity and optimize resources.

Rubrik takes a Zero Trust approach to data management, which follows the NIST principles of Zero Trust for everyone interacting with data. This means operating with the assumption that no person, application, or device is trustworthy. To meet this standard, data must be natively immutable so that it's not modified, encrypted, or deleted by ransomware. Using Zero Trust Data Management architecture, enterprises can recover their data after an attack and avoid paying ransom.

This collaboration builds on Rubrik and Microsoft's long-standing relationship, which supports more than 2,000 mutual customers globally, and hundreds of petabytes of data under Azure management across six continents. ■

HOW THE GAMING INDUSTRY ATTRACTS CYBER CRIMINALS

Gaming is on the rise across the world. According to data from Statista, there are currently more than 3.2 billion video game players worldwide, with its growth only being compounded by the pandemic. Market intelligence firm IDC estimates that the industry raked in US$179.9 billion in revenue in 2020. With its boom, the industry has become fertile ground for hackers.

Cybersecurity software provider Check Point confirms this; their Mid-Year Security Report reveals that gaming organisations have experienced a 29% spike in cyberattacks.

Big names across the gaming world have come under attack, including Capcom, creator of popular games Street Fighter, Mega Man, Resident Evil, Devil May Cry and Monster Hunter franchises, as well as CD PROJEKT RED, the company behind hits like The Witcher and Cyberpunk 2077. Most recently, Electronic Arts, one of the world's largest gaming companies, fell victim to theft of data and source code.

Gamers themselves are not spared. The massive community, which actively uses modern technology, micro-transactions, and online payments, poses an attractive target and are often used as a conduit to attack or blackmail organisations. With most games using a microphone or camera, successful cyberattacks can also grant hackers access to copious amounts of sensitive information by eavesdropping on victims and spying on them.

Most concerning, however, is the prevalence of account theft. Cybercriminals are constantly on the lookout for vulnerabilities they can exploit that allows them control of gaming accounts, giving them access to credit card information and other sensitive data. If small amounts are being stolen, there is a chance that players may not even notice this is happening.

Stealing via phishing is another common threat. This involves attackers luring victims with rewards and bonuses, and subsequently stealing account login details by imitating official sites. Numerous games have been exposed to contain vulnerabilities that hackers can exploit to steal accounts, data, and money, or to eavesdrop and spay. This includes battle royale game Fortnite, and Electronic Arts' Origin game client.

In order to minimise the threat of potential attacks, Check Point recommends using two-factor authentication, whereby a security code will be required when logging in from a new device. Additionally, operating systems and applications should be regularly updated to eliminate any known security weaknesses. ■

Image: www.freepik.com

SAFETY & SECURITY ASIA 2021 SINGAPORE

THE 19TH INTERNATIONAL SAFETY & SECURITY
TECHNOLOGY & EQUIPMENT EXHIBITION

A Hybrid Event

Secured Technologies For A Secured Future

Sands Expo & Convention Centre
Marina Bay Sands Singapore, Halls E & F

24 – 26 November 2021 (Physical Event)
10 November – 9 December 2021 (Virtual Event)

From security robotics and integrators to enterprise security and manpower services, Safety & Security Asia 2021 is the region's most comprehensive showcase for the commercial, industrial and residential security sectors. Given today's ever-evolving technological changes, the strategic deployment of safety and security equipment and solutions is clearly an integrated part of the built environment landscape.

Organised by Conference & Exhibition Management Services (CEMS), the 19th Safety & Security Asia 2021 is one of seven key pillars for the Architecture & Building Services (ABS) Exposition, an annual all-inclusive three-day event that brings together thought-provoking conferences and cutting-edge equipment and solutions for Asia's built environment.

Organised By

CEMS®
Conference & Exhibition
Management Services Pte. Ltd.

A Part Of

Architecture &
Building Services 2021
Design Solutions for the Built Environment

Concurrent Hybrid Events

ArchXpo 2021
The 7TH International Exhibition of
Architecture & The Built Environment

iFaME
INTERNATIONAL FACILITY
MANAGEMENT EXPO 2021
The 8TH International Facility Management Equipment,
Products, Technology & Services Exhibition

DESIGN ASIA 2021

LIGHTING ASIA 2021
The 7TH International LED + Lighting Technology Show

WORK SAFE ASIA 2021 SINGAPORE
THE 7TH INTERNATIONAL WORKPLACE SAFETY
TECHNOLOGY & EQUIPMENT EXHIBITION

FIRE & DISASTER ASIA 2021 SINGAPORE
THE 17TH INTERNATIONAL DISASTER, EMERGENCY MANAGEMENT &
FIRE PREVENTION TECHNOLOGY & EQUIPMENT EXHIBITION

For enquiries, please contact:

Cheah Wai Hong
cheah@cems.com.sg   Tel: (65) 9689 0152

Conference & Exhibition Management Services Private Limited
1 Maritime Square, #09-56, HarbourFront Centre, Singapore 099253
info@cems.com.sg Tel: (65) 6278 8666 Fax: (65) 6278 4077
ssa@cems.com.sg ssa_sponsorship@cems.com.sg

GBG PARTNERS SEON TO ENHANCE FRAUD PREVENTION SOLUTIONS FOR FINTECHS AND DIGITAL BANKS IN APAC

The Covid-19 pandemic has seen a spike in consumer uptake of digital banks. In 2020, a threefold increase in the customer bases of digital banks as compared to traditional banks within Asia Pacific. In mature economies like Singapore and Hong Kong, high fintech adoption rates have been observed. Meanwhile, developing countries like Vietnam, Cambodia and the Philippines are gearing up to achieve financial inclusion.

As the risk and complexity of financial crime increases, fraud prevention firms GBG and SEON have announced a partnership to enhance solutions for fintech organisations, banks, and digital banks in the Asia Pacific.

With this partnership, effectiveness in combating modern-day fraud is increased by validating the most active e-lifestyle based consumer touchpoints (email addresses, IP location, social media, phone, and SIM data) to detect fraudulent anomalies in account application and loan origination, as well as to onboard new-to-bank population.

Financial institutions (FIs) can look forward to reducing fake and malicious email address usage to as low as 0%, and increase detection of suspicious IP-related applications and transactions by up to 80%.

FIs utilising the GBG Intelligence Center, a key module in GBG's flagship end-to-end financial crime management solution - Digital Risk Management and Intelligence platform, benefit from enriched data intelligence to augment fraud detection and prevention accuracy by reducing manual work for FIs, false positive and false negative rates.

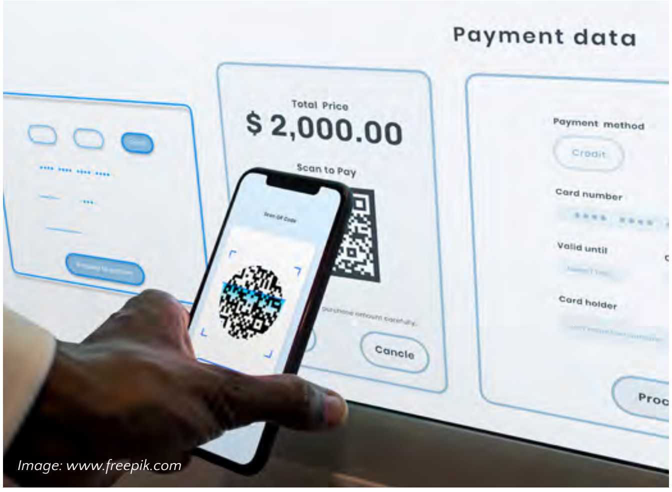


Image: www.freepik.com

SEON adds to the performance of the Intelligence Center with its track record of zero false positives for email, phone and IP. With fraud costs increasingly outweighing fraud management spend, this partnership helps risk management teams increase efficiency by reducing time spent on manual tasks (e.g. checking of email, phone and IP data) by up to 50%. Furthermore, as remote working arrangements continue, the ability to automate fraud detection and prevention with a high degree of accuracy remains crucial.

Image: www.freepik.com

Complementing GBG's artificial intelligence (AI)-driven approach to fraud detection, SEON uses open data and whitebox machine learning, giving businesses complete visibility and total control of how the AI decisions are made.

The integration of SEON's access to data with GBG Intelligence Center will provide enterprises with a more thorough and unified fraud detection process, while maintaining data and privacy standards with 100% GDPR and ISO 27001 compliance.

The GBG Intelligence Center, with SEON incorporated, will be available to FIs across APAC, including Vietnam, Cambodia, the Philippines, Malaysia, and Thailand. ■

tradelinkmedia.biz

SECURITY SOLUTIONS TODAY

OUR LATEST ISSUE

May-Jun 2020

ASSOCIATE PUBLISHER
Eric Ooi
EDITOR
JoAnn Chia

Security Solutions Today (SST), published bi-monthly since 1992, is one of the leading security trade publications in Asia. The magazine features industry news, market / technological updates, case studies / application stories on projects, product showcases for new and current security products / devices in available in the market, and security trade show previews and reviews. We feature latest technologies in Access Control, Video / CCTV Surveillance & Storage Systems, Intrusion/ Alarm Detection, Integrated Security Systems, Security Communication

All · Projects · Case Studies · Products & Technologies · Others · Industry Links · Magazines

LATEST

Office 365 Phishing Campaign Exploits Samsung, Adobe And Oxford Servers
Jun 28 2020

Office 365 Phishing Campaign Exploits…
Jun 28 2020

UK-US Data Deal Puts Brexit Data Adequacy Pa…
Jun 19 2020

Businesses Face Cybersecurity Risk Due …
Jun 14 2020

Identiv Develops NFC-Enabled Body Temperat…
Jun 07 2020

NEWS

COVID-19: How CIOs can prepare for business…
May 22 2020

Government Tells Social Media Companies They Mu…
May 15 2020

NCSC Tackles Unconscious Bias In Security Terminology
May 08 2020

Cyberattacks On Banks Seen Spiking, Says Carbon Black
Apr 30 2020

Application Performance For Remote Workers Becomes…
Apr 24 2020

Zoom User Credentials For sale On Dark Web
Apr 17 2020

SPONSORS

Microengine

P1000i
PoE Controller

UPCOMING EVENTS

IFSEC International 2020
London, United Kingdom
FROM Sep 08.2020 10:00
TO Sep 10.2020 16:00

ASEAN Super 8
Kuala Lumpur, Malaysi
FROM Oct 20.2020 10:
TO Oct 22.2020 16:00

IFSEC Southeast Asia 2
Kuala Lumpur, Malay
FROM Oct 20.2020 10:
TO Oct 22.2020 17:00

OS-H Asia 2020

sst.tradelinkmedia.biz

Visit our website for the latest information

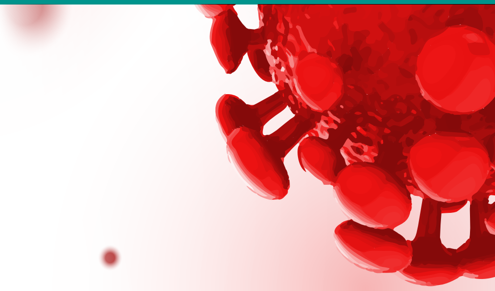
News In The Industry · Upcoming Exhibitions · Download Magazine Issues

SECURITY SOLUTIONS TODAY
SECURING INFRASTRUCTURE FROM RANSOMWARE
How do we defend important infrastructure against dangerous cyber threats?
SAFE CITIES, THE SMART WAY
SECURE
KEEPING EVENTS SAFE
TECHNOLOGY IS RESHAPING MUSEUM & BORDER SECURITY
FUNDAMENTALS SMART BUILDINGS
LAND AND ER SECURITY

Host Data Loss Prevention in an Age of Remote Work

Image: www.freepik.com

When the world faced the brunt of Covid's impact in early-2020, economies worldwide entered an unprecedented age of remote working. Work-from-home (WFH) became the norm as organisations adapted to lockdown and safe distancing measures. Research and advisory firm Garter estimates that approximately 48% of the workforce will continue remote work arrangements post-pandemic, up from 30% prior.



But with the shift towards WFH arrangement comes its own set of cybersecurity challenges as employees are now connected to diverse servers, granting cyber criminals more vulnerabilities to exploit.

This is where Host Data Loss Prevention (HDPL) solutions come in. Designed to eliminate risk of sensitive information leaving the organisation, HDPL involves monitoring host devices for data and system access to ensure that it is completely within organisational and regulatory policies; filtering data stream to prevent unauthorised or suspicious activity; reporting tools for incident response and auditing and analysis; and identifying potential threats and vulnerabilities to alert security.

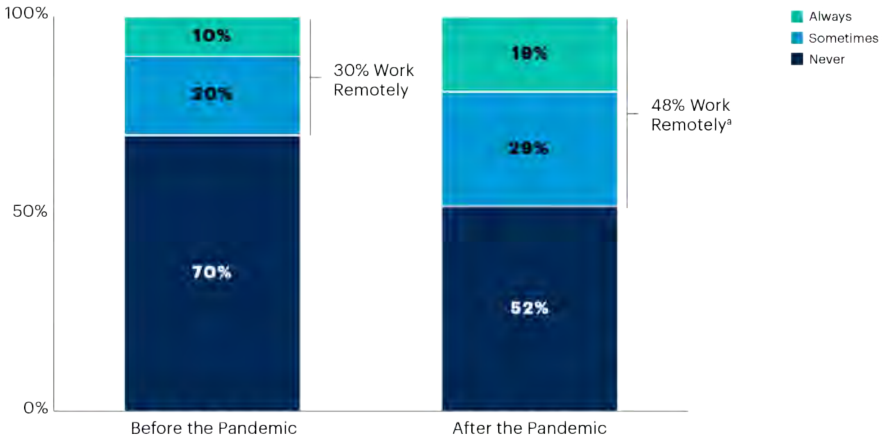
To better understand the role of HDPL in cybersecurity in an age of remote working, Security Solutions Today sits down with Hitesh Bhardwaj, Vice President, Head of Sales and Presales of Cloud4C, APAC – an organisation specialising in enterprise security and HDPL solutions.

Why are HDLPs important in ensuring the cybersecurity of an organisation?

The COVID-19 pandemic has made remote work the new normal for almost all organisations around the world. While WFH is not new to the software sector, having the entire organisation do so is unprecedented.

WFH security is still not as robust as it should be. Imagine the security requirements for organisations that prioritise data security and

Projected Percentage of Employees Working Remotely, Before and After the Pandemic



n = 421 HR leaders; 4,535 employees; 317 finance leaders

Source: Remote Work After Covid/Gartner compliance for their clients and have hundreds of controls in place even while employees are working within the office network that is equipped with their own firewalls and other security measures.

The crisis unfolding in front of us requires social distancing and isolation which has necessitated employees work remotely from their homes, but this means weaker security for data that would normally be secure within the organisational environment.

Most organisations have sensitive data that should never leave the organisation, but their data protection strategies are mainly focused on organisational network level, further enforced by preventing employees from accessing data outside their strictly regulated environment.

The truth is that most organisations are not prepared for all their employees to be working remotely, and this has become a major concern for companies in the aftermath of the pandemic.

Employees across all levels are logging into company sites, participating in online meetings, and interacting with sensitive computer data through their home networks and mobile phones. Away from the scrutiny of the office network, employees may use new software to make it easy to work that may not be authorised. Moreover, malintent is always a threat in organisations of any size.

This is where the role of HDLPs become critical. They offer the most efficient way to handle cybersecurity for data-sensitive organisations to ensure zero compromise on security.

What are the possible cyber threats against companies during a time of remote working?

The ongoing work-from-home phenomenon has made companies rush to digitalise and bring their systems and data online for employees to access work remotely. However, having more assets in the digital space also creates new vulnerabilities for attackers to exploit if companies do not implement proper cybersecurity precautions.

According to a report by PurpleSec, cybercrime rose by 600% during the Covid-19 pandemic and ransomware attacks are estimated to cost US$6 trillion annually by the end of 2021. Cyber attacks like phishing and ransomware are both common and ever-evolving, meaning that internet-savvy companies and their employees can fall prey to new tactics.

Going digital means companies can use digital tools to streamline business operations and improve collaboration – both essential for WFH situations. However, choosing the right apps is very important both from a cybersecurity and non-cybersecurity perspective. Service-as-a-Solution (SaaS) applications such as video conferencing tools are becoming more popular as they can help enhance collaboration and productivity. However, we've seen cases where hackers have exploited their security vulnerabilities to disrupt or eavesdrop on sensitive solutions.

According to a report by PurpleSec, cybercrime rose by 600% during the Covid-19 pandemic and ransomware attacks are estimated to cost US$6 trillion annually by the end of 2021. Cyber attacks like phishing and ransomware are both common and ever-evolving, meaning that internet-savvy companies and their employees can fall prey to new tactics.

Visibility and security go together, which is why enterprise solutions such as Desktop-as-a-Service and Endpoint Detection and Response (EDR)-as-a-Service are so valuable. They can help provide a detailed overview of a company's cybersecurity profile and boost its ability to counter any cyber threats.

How are cyber threats different during remote work as compared to typical work arrangements when workers are on-site?

Key work-from-home scenarios which can heighten cyber threats include but are not limited to:

- Employees sharing data via their personal email

Image: www.freepik.com

- Employees sharing data via their personal drives like Google Drive and Dropbox
- Employees performing data transfers through Secure Shell (SSH), FileTransfer Protocol (FTP) and Remote Desktop Protocol (RDP) outside the organisation's purview
- Employees storing the confidential data such as customer details on USB drives
- Employees sharing the information like access credentials with third parties with malicious intents
- Employees deleting the data by accident
- Employees storing the details via Screenshots
- Employees sharing the details with third parties like freelancers and agencies without understanding security implications
- Employees giving their mail access to third party platform (like OAuth Logins)
- Employees using social media to share information with other parties

Types of data categories that can be leaked by employees include Intellectual Property data, financial details, employee details, personally identifiable information, protected health information and customer transaction data.

How does Cloud4C's HDLP solutions address some of the cyber threats you have mentioned?

At Cloud4C, we define HDLP 'as the process of monitoring and blocking intentional and unintentional exfiltrating company's data by employees or third parties through host systems.' WFH home security can be compromised through the sharing of confidential data including corporate, transaction, customer, and personally identifiable data.

By enabling organisations to monitor data accessed and shared by end users, HDLP solutions ensure data security and regulatory compliance. HDLP software classifies and protects confidential and critical information so there is no unauthorised sharing of data. For example, if an employee tries to forward a business mail outside the corporate domain, permission would be denied. If they tried to upload a corporate file to consumer cloud storage such as Google Drive or Dropbox, they would also be denied.

Cloud4C has a robust framework that guides organisations to put in place an approach to secure their confidential data even when all their employees are working out of their home in their own networks. We leverage on our decades of understanding of providing enterprise security to provide cutting edge HDLP solutions using the best products in the market.

Some of the features that we deliver to ensure that organisational data is secure include limiting employee ability to transfer sensitive data, control user's capability to send information to other domains via various communication tools including email, arrest data transfer to employee's personal cloud drives and arrest data transfer through SSH, FTP and RDP. Our HDLP solutions are capable of extending their reach into the encrypted protocols in a completely non-disruptive transparent manner.

What is unique about Cloud4C's HDLP solutions that trumps other means of data management in remote work arrangements?

Cloud4C's DHLP is designed to ensure the safety of organisations' organisational data and employees. It is important for organisations to follow a Zero Trust policy when it comes to cybersecurity, especially in today's remote working environment. Our approach to tackling this is what sets us apart as we believe in empowering businesses with information from our assessments on possible vulnerabilities and identify solutions that are custom to their business needs.

Despite our DHLP solutions, we also highly encourage organisations to adopt the following approach to secure their data even when most of their workforce is working out of home.

- Create a clear policy framework for managing data and using IT assets. Set high security standards and enforce them religiously.
- Identify vulnerable hosts and clearly define the security protocols for using the host systems.
- Understand the risk associated with each host and categorize them accordingly. This will help plan a risk mitigation strategy.
- DLP cannot function in isolation. It has to be part of the overall IT security policy of the company. ■

The Future of Cybersecurity and Data Management Lies in Artificial Intelligence and Machine Learning

Image: www.freepik.com

In mankind's long history, the Internet is a relatively recent development. The world wide web as we know it was only introduced, but its growth has been exponential since. From an unknown concept over 30 years ago, the Digital 2021 April Global Statshot Report by Hootsuite and We Are Social finds that there are now over 4.72 billion internet users, more than 60% of the world's population (as of April 2021).

With the proliferation of the Internet comes copious amounts of data being processed in the web every second of every day. Increasingly, firms are learning to monitor and make use of this data to influence human behaviour, a phenomenon termed as the Internet of Behaviour by global research and advisory firm Gartner. Gartner predicts that by 2025, over 50% of the world's population will be exposed to at least one IoB-influenced government or commercial program. Additionally, by 2023, 40% of the global population will be digitally tracked.

With cyber traffic spiking during the pandemic, these numbers become all the more concerning, and the need for data to be properly managed and secured become more crucial than ever before. This is where artificial intelligence (AI) and machine learning (ML) technologies come in – to help manage data in a more effective and secure manner.

To this end, Security Solutions Today speaks with Managing Director of cybersecurity provider AdNovum Singapore, to learn more about how the pandemic has shaped the cyber landscape, and how AI and ML technologies are interwoven into the fabric of cybersecurity and data analytics today.

Can you tell me about yourself and AdNovum?

I've over 20 plus years of experience from information technology, and I've done a fair bit of consulting as well. Through my involvement in various organisations, I realised that many of them undermine the importance of cybersecurity.

This is especially crucial now, when we are living through the pandemic,

Image: www.freepik.com

and cyber traffic has drastically increased. Thus, a lot of organisations will need a lot of work when it comes to cyber defence and what we term the Internet of Behaviour – services their organisations will require to protect their cyber hygiene and customer data.

This is why I joined AdNovum, with the aim of expanding its footprint in the area of cybersecurity. AdNovum is an organisation with more than 20 years of experience in three areas: Digitalisation, through the use of high-end engineering; cyber defence and cyber hygiene; and data protection and analytics.

What are some of the cyber threats prevalent today during the pandemic?

While cyber threats have been present both before and during the pandemic, there has been an increase of dark web activities observed due to the rise in cyber traffic during the pandemic. Additionally, we have also observed a change in the behaviour of consumers, myself included. The number of hours that we spend on the internet, on social media, and even our buying patterns – everything has increased during Covid times. As such, the frequency of cyber attacks is going to be relatively increased.

Research by Gartner has revealed that by 2023, approximately 40% of the world's population will be digitally-tracked. From a numerical perspective, we're talking about three billion people being digitally tracked in terms of how they act on the internet or on social media. With this number in mind, you are able to see the magnitude of the increase in terms of cyber threats throughout the world.

What are the implications should data not be properly managed and a cyber attack occurs?

Data leakage and data breaches are definitely one of the biggest threats. Financially, with each of these cyber incidents, businesses lose an average of approximately $3.86 to $4 million. That's the magnitude of the impact per incident, and this is why it is so important for organisations to shore up their cyber defences.

How has data management and cybersecurity transformed over the years?

There has been greater awareness for the need of cybersecurity and data management. Three areas in particular have been the focus: authentication, authorisation, and data management.

Take for example an individual making a purchase using a credit card. Authentication involves determining if the identity of the credit card owner is correct. Meanwhile, authorisation means verifying that you indeed have been approved to spend a certain amount on the card. Finally, data management comprises using consumer patterns and behaviours to make predictions, in order to take subsequent action. In the context of a consumer, this can involve using your spending patterns to influence your psychology or behaviour in order to increase sales or increase your volume of purchase.

In the past five years, I have observed that awareness of these three areas have been greatly increased, and the systems have been improved as well.

Image: www.freepik.com

As an organisation, we have a 3D approach – digitalisation, defence, and data management. AI and ML are applicable to all three. At AdNovum, all our technology and consultancy revolve around the 3D approach.

Recently, many organisations have been utilising different technologies to address these areas. The leading edge at the moment is the use of artificial intelligence (AI) and machine learning (ML) to bolster defences in these three areas.

How does AI and ML technology play into the three areas of authentication, authorisation, and data analytics?

AI and ML are in place to handle massive amounts of data. Let me give you some examples.

Firstly, AI can play a vital role in authentication. For instance, when you are using your mobile device and you are attempting to unlock your phone, facial recognition can be used – that is an example of AI.

At the same time, you can use of the AI and as well as ML to drill into a lot of audit logs during frontline operations. This involves detecting abnormalities within audit files through learning patterns and data modelling, such that the AI/ML software is able to pick up on abnormalities when it is authenticating audit logs. Subsequently, it will be able to trigger downstream interventions such that the first line of defence is at the authentication layer.

AI and ML can also play a role in authorisation. Using credit cards as an example, if your spending pattern tends to be under $5,000, and there happens to be an anomaly where S$20,000 is being charged to the card, this can be detected by the AI engine. Following that, another cycle of authorisation can be triggered. For instance, it can detect whether you are currently in Singapore, where you are supposed to be, or overseas.

Finally, AI and ML play a role in data analytics as well. Simple things like sending customers automated alerts when they have not checked out items that are in their shopping cart utilise AI. Through AI and ML, predictions can also be made from customers' past spending habits and patterns, and actions can then be triggered to upsell customers, creating more revenue opportunities.

Do you foresee AI and ML as indispensable parts of cybersecurity and data management moving forward?

From what I can see, it is already embedded as a vital part of the cybersecurity world. With the increase in data over the years, there is no way that human beings will be able to detect abnormalities on the spot. Thus, AI and ML are undoubtedly the way to go, and is already part of most service offerings in the market right now. In fact, the usage of AI and ML expands to a range of industries including banking, logistics, healthcare, and more.

How does AdNovum provide solutions incorporating AI and ML to address some of these cyber threats that organisations may be facing?

As an organisation, we have a 3D approach – digitalisation, defence, and data management. AI and ML are applicable to all three. At AdNovum, all our technology and consultancy revolve around the 3D approach.

For instance, in freight management, AI and ML can be used in digitalisation by helping to optimise space and routes. Meanwhile, the same technology can also be used for defence, by incorporating them into authorisation and authentication processes, like I earlier explained. Finally, AI and ML technology is also used by AdNovum in data management through areas like customer satisfaction across different industries.

What do you foresee will be the future of cyber security?

I believe that cybersecurity will come into greater focus in the future, but more awareness is still required. More importantly, I believe that enterprises need to continue shoring up their data management procedures in order to ensure proper protection of their data.

What we are currently observing is that data breaches are getting more intensive with the new normal we are living in due to the pandemic. While many organisations are increasingly aware of the threat, there are still some who are unaware of how to execute their cybersecurity processes. This is especially true for many small and medium enterprises.

Digitalisation is no longer an option; it is a necessity. You need it to retain customers. As a CEO or CTO of an organisation, this is definitely a priority item that should be kept in mind. ■

The Growing Role of Artificial Intelligence in IT Security Teams

Image: www.freepik.com

The IT Security Team: 2021 and beyond survey conducted by British security software and hardware company Sophos has revealed some interesting insights. Speaking with 5,400 IT managers across 30 countries, the report details experiences of IT teams over the course of June 2020 to 2021, during the height of the pandemic.

Within, it reveals changes faced by IT teams during this time, paying a particular focus to cybersecurity. Further, the report postulates the possible future of IT security teams, examining the expectations for IT over the next five years. Specifically, it finds that within the Asia Pacific Japan (APJ) region, 63% of IT teams anticipate an increase in their in-house IT security staff by 2023, with an additional 55% expecting the number of outsourced IT security staff to grow in the same timeframe.

Alongside the projected growth in IT teams come an expectation that artificial intelligence (AI) will be playing a larger role in cybersecurity. A vast majority of 86% of APJ IT teams stated that they foresee AI playing a role in helping deal with the growing number and/or complexity of threats.

While no reasons were derived from this report, a separate survey conducted by Sophos titled State of Ransomware 2021 found that 65% of APJ IT teams believe that cyberattacks are now too advanced for in-house teams to tackle on their own.

Shedding light on these issues, Chester Wisniewski, Principal Research Scientist at Sophos, discusses some of the abovementioned trends, and speculates on the growing role of AI in cybersecurity and IT teams in the near future.

The IT Security Team 2021 and Beyond survey results that were recently published has some interesting findings. Namely, that there is expected to be an increase in in-house IT security staff by 2023. Can you shed some insight on the existing trend thus far, and possible reasons for why this anticipated increase?

We can only speculate as to the specific reasons. Possibly, as organisations embrace digital transformation, their need for both internal and external expertise will continue to increase. With all of the high-profile attacks in the news and more government regulation of security and privacy of data, this [the increasing trend of the number of in-house IT security staff] will likely continue for some time.

Why is it important for organisations to have in-house IT security staff? What role do they play?

Hybrid security teams are the best model for most organisations. Security must be adapted and applied to the specific way that an organisation operates and this will always require internal expertise. What data is collected, how it is safely stored and when it needs to be expunged is an example of something that needs to be done in-house. My opinion is that security policies and their application are internal tasks and threat hunting, monitoring and malware/attacker expertise are often better found from outside companies who specialize in these tasks.

The survey also found that there is an expectation for AI to play an increasingly important role in cybersecurity, citing the reason that cyberattacks are now too advanced for the in-house team to tackle on their own. Can you share more about the challenges in-house teams may face when tackling cyberattacks of today?

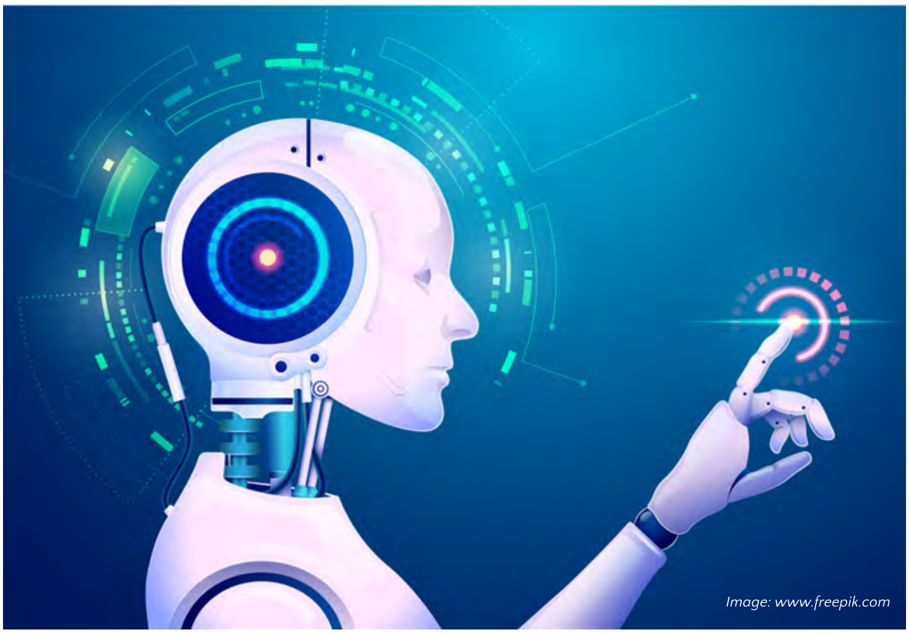


Image: www.freepik.com

Human-led attacks are the ones most organisations need to worry about the most. Automated worms and older malware can be blocked by patching, having modern security tools, etc. Humans are a much more complex adversary and knowing what the latest tactics are that are being used to gain entry, move laterally and compromise systems is an evolving art that is very difficult to do without having visibility at scale.

What are some examples of cyberattacks that may be too challenging for in-house IT security teams to handle? What is the role of AI in bolstering cybersecurity? How can AI and IT security teams work in tandem in cybersecurity?

The primary type we see day in and day out is ransomware. In many cases there may be millions of dollars at stake and the attackers are very sophisticated. They often only use legitimate tools in a malicious way which requires defenders to be looking for malicious behaviours rather than malicious files. This type of defence is often employed by having "threat hunters", a group of people monitoring systems for anomalies and then investigating those incidents to head criminals off at the pass.

Are you able to share any trends or information about how AI has been used in cybersecurity over the years?

Today, AI is primarily used to augment endpoint security products, sandboxes and UTMs by increasing their ability to detect previously unseen malicious code. We are also starting to use AI to help detect malicious emails that don't contain malicious links or code such as social engineering phishes that are very targeted and sent to high-value victims. AI is often used behind the scenes to help malware analysts find interesting new samples to analyse out of the hundreds of thousands of malicious files they receive every day. In the future there could certainly be a place where AI can help SOC analysts to sort through alerts or assist analysing attack chains and expediting incident investigations. ■

> **Today, AI is primarily used to augment endpoint security products, sandboxes and UTMs by increasing their ability to detect previously unseen malicious code.**

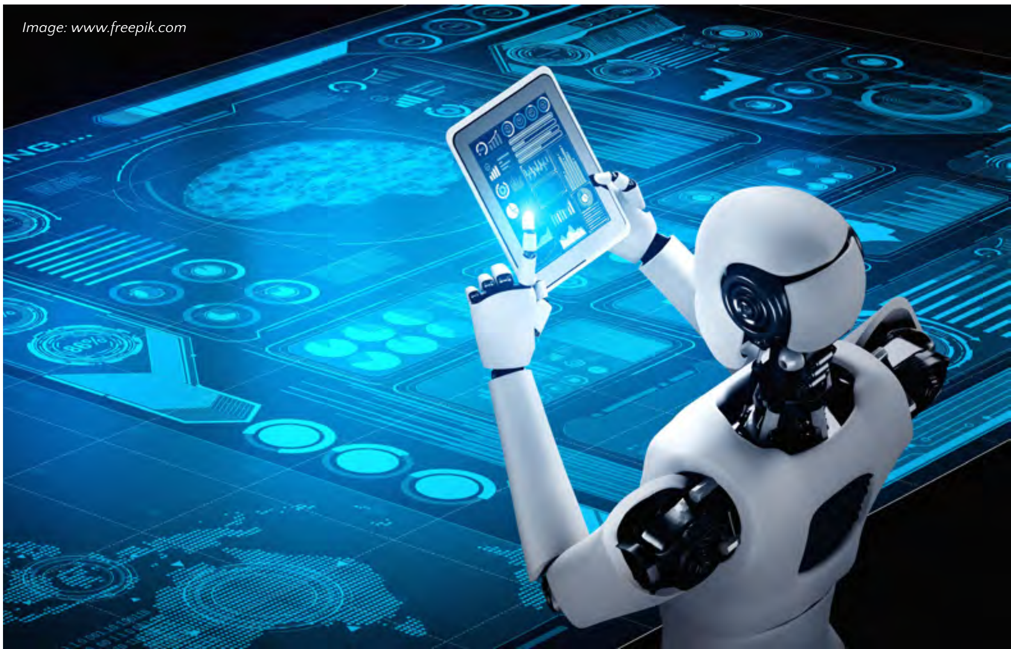


Image: www.freepik.com

LYNRED UNVEILS ATI320, AN ADVANCED THERMAL IMAGER WITH EMBEDDED IMAGE SIGNAL PROCESSING

Lynred, a leading global provider of high-quality infrared detectors for the aerospace, defense and commercial markets, has unveiled the ATI320, its first advanced thermal imager with embedded image signal processing. The product's embedded features includes an optional lens, and aims to save camera makers time and effort in integrating thermal imaging during the development and manufacturing process.

Designed as a ready-to-use product, ATI320 simplifies the calibration process during camera assembly, relieving manufacturers from performing complex steps. By eliminating tricky integration steps, infrared technology is made easily accessible for newer thermal image market entrants.

The ATI320 is particularly suitable for camera makers in industrial, consumer equipment and safety across a broad range of activities. For instance, its compact, lightweight, and low power consumption makes it an ideal fit for Unmanned Aerial Vehicles (UAVs) for aerial thermal inspection.

Image: Lynred

When required, the ATI320 also provides calibration, associated image processing algorithms and a lens.

ATI320 (16x16mm) is the most compact QVGA (320x240 pixels) resolution thermal imager available and comes with ruggedized housing. It is available in two models: ATI320L (with lens) and ATI320S (without lens). It operates as a shutterless product - providing continuous image viewing - an important function for the leisure, firefighting and security-surveillance market applications. ■

ALTRONIX'S LAUNCHES SPACE-SAVING RACK MOUNT NAC POWER EXTENDERS

Altronix, a leader in power and data transmission solutions for the professional security industry, has introduced the latest additions to its extensive line of NAC Power Extenders with a unique rack solution. These new units are ideal for installations where wall space is limited or not an option, providing system designers flexibility when specifying fire alarm systems.

Image: Altronix

The rack mount solution streamlines system design and provides installers with a versatile option to deploy fire signaling power vertically, saving valuable space. The units' extendable drawer simplifies installation and service, thus increasing total cost of ownership.

Special features include a horn/strobe sync mode that allows audible notification appliances and visual notification appliances to be silenced at the same time, signal circuit trouble memory to help identify intermittent loop problems, and common trouble input and output for external trouble signals.

The Altronix R1002ULADA and R1042ULADA NAC Power Extenders are NDAA and TAA compliant and carry a lifetime warranty. ■

BOSCH ANNOUNCES FLEXIDOME PANORAMIC 5200I CAMERAS FEATURING BUILT-IN AI CAPABILITIES

The cameras also feature Intelligent Video Analytics (IVA), a form of AI, and Camera Trainer based on machine learning to support predictive solutions in a variety of commercial environments.

In both retail and campus applications, the cameras' compact size and low profile can deliver insights through a complete overview of different locations, allowing for the tracking of persons of interest across different areas or the identification of unusual situations.

Three digital microphones are built into the cameras, allowing them to capture audio from any direction, give meaning to the sounds they hear, and trigger relevant alerts. With their AI-based software, which will be made available with a future firmware release, they are trained to detect concerning audio signatures of gunshots and glass breaking while ignoring false positives, like slamming car doors or banging carts.

With audio AI, security personnel are able to respond quickly and appropriately while privacy remains protected since no audio information is recorded or leaves the camera. When an audio alarm occurs, a trigger to a nearby moving camera simultaneously prompts it to focus near the sound and track any moving objects in the scene.

Image: Bosch

Images: Bosch

Image: Bosch

Further, by offering a detailed overview image of an area, the panoramic cameras allow users to simultaneously zoom in on an object of interest without losing the bigger picture. Close-up images are then transmitted in a separate channel so that both overview and detail can be viewed at the same time in high resolution. With 12-megapixel sensor resolution at a frame rate of 30 frames per second, these cameras provide a 360-degree overview enabling the easy capture of objects to significantly improve the quality of a surveillance operation. ■

IBM INTRODUCES ON-CHIP ACCELERATED ARTIFICIAL INTELLIGENCE PROCESSOR

IBM has launched their new Telum Processor, designed to bring deep learning inference to enterprise workloads to help address fraud in real-time. Telum is IBM's first processor that contains on-chip acceleration for AI inferencing while a transaction is taking place. Three years in development, the on-chip hardware acceleration is designed to help customers achieve business insights at scale across banking, finance, trading, insurance applications and customer interactions. A Telum-based system is planned for the first half of 2022.

Today, businesses typically apply detection techniques to catch fraud after it occurs, which can be time consuming and compute-intensive due to limitations in today's technology. This is especially so when fraud analysis and detection is conducted far away from mission critical transactions and data. Due to latency requirements, complex fraud detection often cannot be completed in real-time – meaning fraud could already have occurred before the retailer is aware of it.

According to the Federal Trade Commission's 2020 Consumer Sentinel Network Databook, consumers reported losing more than USD 3.3 billion to fraud in 2020, up from USD 1.8 billion in 2019. With the Telum Processor, IBM hopes to help clients move from a fraud detection posture to a fraud prevention one, evolving from catching cases of fraud, to a potentially new era of prevention of fraud at scale, without impacting service level agreements (SLAs), before the transaction is completed.

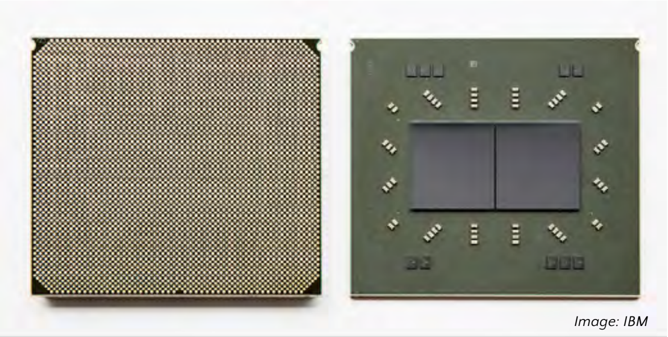


Image: IBM

Image: IBM

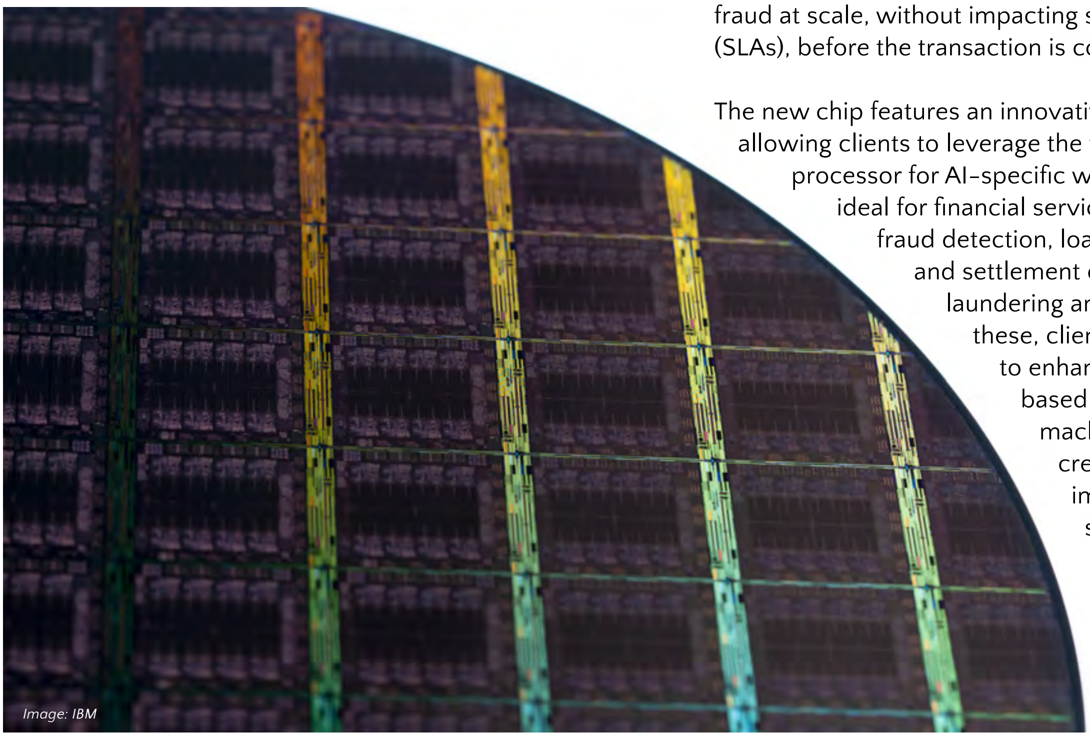


Image: IBM

The new chip features an innovative centralized design, allowing clients to leverage the full power of the AI processor for AI-specific workloads, making it ideal for financial services workloads like fraud detection, loan processing, clearing and settlement of trades, anti-money laundering and risk analysis. With these, clients will be positioned to enhance existing rules-based fraud detection or use machine learning, accelerate credit approval processes, improve customer service and profitability, identify which trades or transactions may fail, and propose solutions to create a more efficient settlement process. ■

COMING SOON

NOV
1 – 30
2021

IFSEC Southeast Asia 2021

📍 Kuala Lumpur, Malaysia
☎ +60 3-9771 2688 🌐 www.ifsec.events/kl
✉ ifsecsea@ubm.com

NOV
24 – 26
2021

Secutech Thailand 2021

📍 Bangkok, Thailand
☎ +66 2 664 6488 🌐 www.secutechthailand.tw.messefrankfurt.com
✉ stth@taiwan.messefrankfurt.com

JAN
16 – 18
2022

Intersec 2022

📍 Dubai, UAE
☎ +971 4 389 4500 🌐 www. intersec.ae.messefrankfurt.com
✉ intersec@uae.messefrankfurt.com

SEP
20 – 23
2022

Security Essen 2022

📍 Essen, Germany
☎ +49 201 72440 🌐 www.security-essen.de
✉ info@messe-essen.de

JUL - SEP 2021
SECURITY SOLUTIONS TODAY
SECURING INFRASTRUCTURE FROM RANSOMWARE
How do we defend important infrastructure against dangerous cyber threats?
MAR / APR 2020
SECURE
JAN / FEB 2020
NOV / DEC 2019

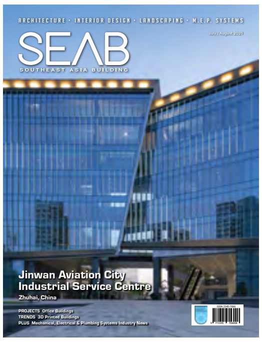
issuu.com/securitysolutionstoday

SUBSCRIPTION FORM

Email us at ***info@tradelinkmedia.com.sg***

Please (√) tick in the boxes.

PRINT



□ Southeast Asia Building
Since 1974

□ Southeast Asia Construction
Since 1994

1 year *(6 issues) per magazine*

Singapore	SGD$60.00
Malaysia / Brunei	SGD$105.00
Asia	SGD$155.00
America, Europe	SGD$185.00
Japan, Australia, New Zealand	SGD$185.00
Middle East	SGD$185.00

□ Bathroom + Kitchen Today
Since 2001

1 year *(4 issues) per magazine*

Singapore	SGD$32.00
Malaysia / Brunei	SGD$70.00
Asia	SGD$85.00
America, Europe	SGD$135.00
Japan, Australia, New Zealand	SGD$135.00
Middle East	SGD$135.00

DIGITAL

Lighting Today
is available on digital platform.
To download free PDF copy,
please visit:

http://lt.tradelinkmedia.biz

□ Lighting Today
Since 2002

SECURITY SOLUTIONS TODAY
SECURING INFRASTRUCTURE FROM RANSOMWARE
How do we defend important infrastructure against dangerous cyber threats?

Security Solutions Today
is available on digital platform.
To download free PDF copy,
please visit:

http://sst.tradelinkmedia.biz

□ Security Solutions Today
Since 1992

Personal Particulars

Name: ____________________

Position: ____________________

Company: ____________________

Address: ____________________

____

Tel: ____________________ **Fax:** ____________________

E-Mail: ____________________

IMPORTANT

Please commence my subscription in
____________________(month/year)

Professionals (choose one):

□ Architect
□ Property Manager
□ Landscape Architect
□ Manufacturer/Supplier
□ Interior Designer
□ Engineer
□ Developer/Owner
□ Others

□ I am sending a cheque/bank draft payable to:
Trade Link Media Pte Ltd, 101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399
Co. Reg. No: 199204277K * GST inclusive (GST Reg. No: M2-0108708-2)

□ Please charge my credit card (circle one): Amex / Diner's Club

Card Number: ____________________ Expiry Date: ____________________

Name of Card Holder: ____________________ Signature: ____________________

SECURITY SOLUTIONS TODAY
OUR LATEST ISSUE
LATEST
NEWS
SPONSORS
UPCOMING EVENTS

SECURITY SOLUTIONS TODAY
JUL - SEP 2021
JULY / AUGUST 2020
MAY / JUNE 2020
MAR / APR 2020
RANSOMWARE
INTELLIGENT
SECURE