Asia Pacific Digital Forensics - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Asia Pacific Digital Forensics Market size is estimated at USD 0.87 billion in 2024, and is expected to reach USD 1.65 billion by 2029, growing at a CAGR of 13.91% during the forecast period (2024-2029).

Key Highlights
-Banks across the Asia-Pacific region plan to increase their cloud spending, and 93% of banks in the region anticipate reaching an inflection point and utilizing hybrid and multi-cloud infrastructures by 2023. Adopting cloud solutions by these BFSIs will create a demand for cyber security measures, which will increase investments in digital forensics.
-Many cyber risks are rapidly targeting Thai businesses. According to a report shared by Hi-Tech Crime Trends, with 27 victim organizations whose data was exposed on ransomware-specialized leak sites, Thailand ranked fifth in the Asia Pacific region. Group-IB's Digital Crime Resistance Centre in Thailand was established to counter this increasing number of cyber attacks. Group-IB's highly skilled digital forensics and incident response experts helped decrypt a medical organization's network in Thailand.
-Since the Covid-19 outbreak, there has been a significant increase in cyber crime attacks. Federal Bureau of Investigation (FBI) recorded a 400% increase in cyber crimes during the pandemic. With increasing digital activities, cybercrimes in the cloud environment are growing, and to detect these frauds, digital forensics was adopted.

Asia Pacific Digital Forensics Market Trends

Growing Cybercrimes and Security Concerns Across Industries to Drive the Market

- The instances of cyber crimes have increased drastically over time. According to cyber security firm CloudSEK, Asia Pacific was one of the top targets of cyber crimes, and the number of attacks increased by 26.4% in 2022. Ransome attacks increased during 2022 with the emergence of new ransomware operators.
- A report released by IBM depicted 48% of the cases of attacks were from the manufacturing sector, while the finance and insurance sector share was 18%. Attackers used spear phishing by attaching to the target; nearly 40% of such cases were observed. Due to its low tolerance for downtime, the manufacturing sector was an easy target for attackers.
- IT companies are enhancing their tool and infrastructure to manage these cyber security issues. In May 2022, Cisco launched a cybersecurity assessment tool for small and medium-sized businesses (SMBs) in the Asia Pacific to identify and analyze their overall security posture. User and Identity, Device, Networks, Workload (applications), Data, and Security Operations will be accessed using this new tool. This will help SMBs looking to transform their business from traditional infrastructure to digital platforms.
- Public security entities in China use US technology like DNA analysis, thermal imaging, digital forensics, and cyber security to monitor groups and censor material in the country. This technology could help build population databases and carry out mass surveillance.
- Financial crime has always been a concern in Malaysia, which has resulted in high demand for legal forensics. CyberSecurity Malaysia received over 7,000 reports involving cyber security incidents in Malaysia. To control cyber attacks government intends to set up the Malaysian Cyber Security Commission to strengthen cyber security in the country.

Mobile Forensic Segment to Witness High Market Growth

- Accelerating mobile subscriptions creates a demand for e-commerce, banking, retail, and other services in every sector. As vast data is generated through mobile phone transactions, it threatens cyber security. In January 2023, hackers stole over 3,000 login credentials from Fortune 500 organizations and significant IT firms after infiltrating two sizable data centers in Asia. Shanghai-based GDS Holdings and Singapore-based ST Telemedia Global Data Centers (STT GDC) operated the breached data centers. Thus customers were forced to change their login credentials.
- In another phishing attack, a group of Shangri-La hotels was hit by a data breach. Including Singapore and Hong Kong, six other branches in the Asia region were affected by this attack. The hackers stole the guests' names, e-mail addresses, and phone numbers. A Cyber forensic team was hired, which investigated and revealed that the e-mail was used to attack the hotel's IT security monitoring systems.
- Australia was yet another country that became the prey of these cyber attacks. In Oct 2022, Medibank, the health service provider, suffered a data breach where records of 9.7 million citizens were affected. After this incident, the health company instructed its members not to download sensitive personal data from the dark web unnecessarily and to refrain from contacting customers directly.
- Nearly every smartphone app collects data from a customer's device. If those servers are hacked, or a technical error leaves them vulnerable, all that data can be stolen and used by criminals for fraud. Therefore users need to set security controls to limit the data collected by each app or before downloading any new app that requests a lot of permissions.

Asia Pacific Digital Forensics Industry Overview

There is moderate competition in the Asia Pacific Digital Forensics Market. Still, the demand will grow as law firms adopt AI-based solutions to control crime during the study period. The vendors involved in this business continuously introduce new product features, seeking collaborations to withstand competition and maintain their brand reputation.

- March 2023 - Singapore based cybersecurity company Group-IB signed a deal with Thailand's cybersecurity provider nForce. nForce will form the first Incident Response (IR) team, where Group IB will provide training and dedicated support to them. The team at Group-IB employs cutting-edge technology driven by threat intelligence, and they have a track record of successfully researching and resolving complicated cybercrime cases. This partnership will thus help nForce to improve coverage of the Thai market and assist local companies in dealing with ever-evolving cyber threats.
- August 2022 - Thermo Fisher Scientific collaborated with National Forensic Sciences University (NFSU) in India to equip the facility with systems for DNA extraction, real-time PCR instruments, genetic analyzer, and other software-based DNA technologies. These digital forensic technologies will help law organizations with investigative leads to make evidence-based decisions.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

SCOTTS INTERNATIONAL

Asia Pacific Digital Forensics - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 120 pages | Mordor Intelligence

To place an Order with Scotts International:
- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.
** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2026-03-05
		Signature	

Scotts International. EU Vat number: PL 6772247784
tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com

Scotts International. EU Vat number: PL 6772247784
tel. 0048 603 394 346 e-mail: support@scotts-international.com
www.scotts-international.com