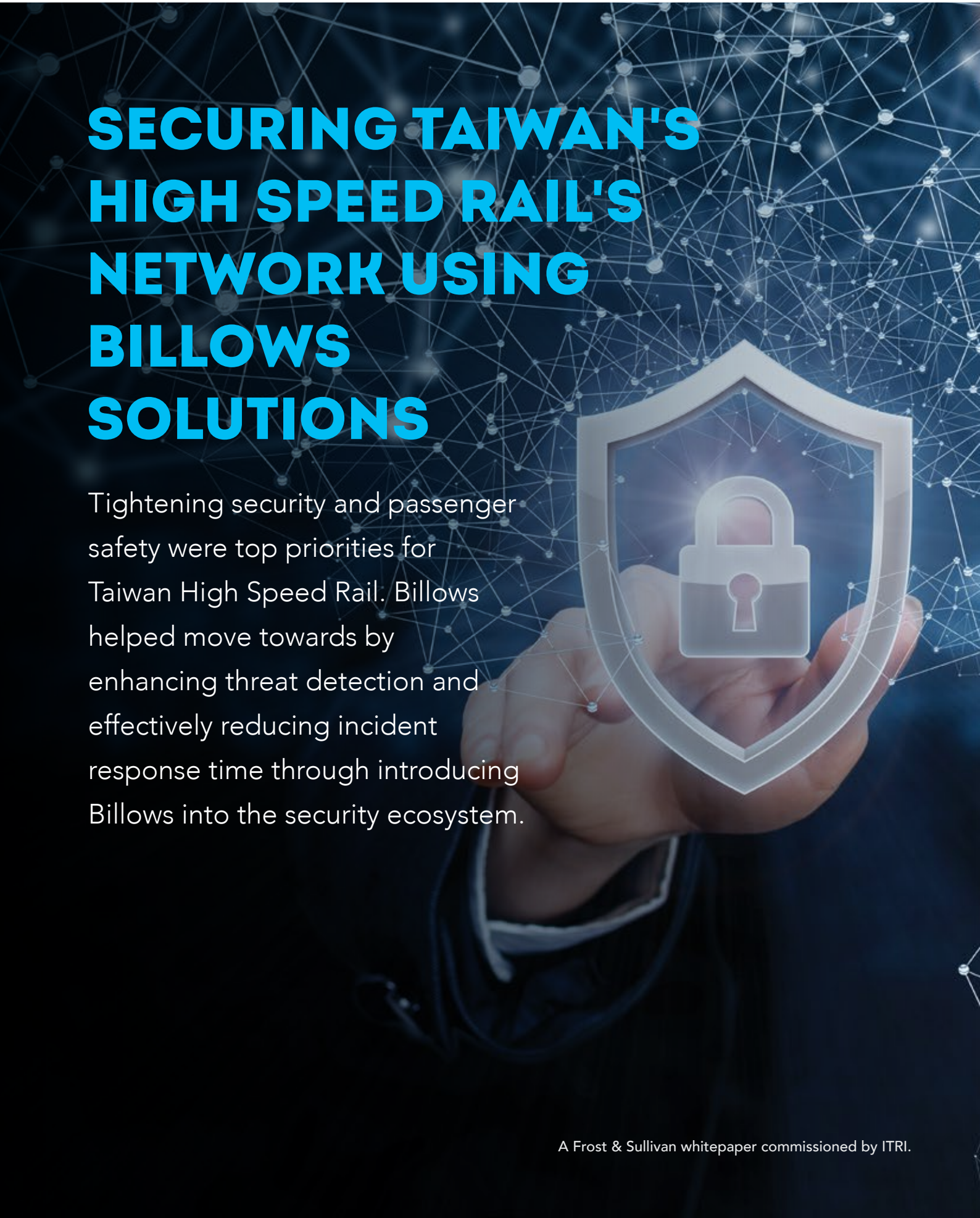
FROST & SULLIVAN

Billows 竣盟科技

SECURING TAIWAN'S HIGH SPEED RAIL'S NETWORK USING BILLOWS SOLUTIONS

Tightening security and passenger safety were top priorities for Taiwan High Speed Rail. Billows helped move towards by enhancing threat detection and effectively reducing incident response time through introducing Billows into the security ecosystem.



A Frost & Sullivan whitepaper commissioned by ITRI.

SUMMARY

Billows provides security solutions and services span over two primary areas: audit management, and Security Information and Event Management (SIEM). Their market offering aims to provide customized security audit monitoring products that are both user-friendly and automated.

Their main product is the LogMaster, which offers the following capabilities:

Data Collection

Data status and system performance monitoring, integrations with other SIEM platforms

Data Storage

Normalized/ denormalized data, non-repudiation, unlimited raw log storage

Data Value

Threat Intelligence, keyword alert, compliance reporting, real-time dashboards, AI behavioral analysis

Data Compilation

Log, Packet analysis, Information usability (SNMP, Netflow)

Billows' core software is OneMan SOC, a security management platform based in Taiwan that was created in response to international information security and auditing requirements. *OneMan SOC's strength is in managing security protocols over a span of assets: logs, traffic, vulnerability, and host intrusion and detection. The analytics aspects of this platform cover SIEM, threat intelligence and artificial intelligence, while the forensics components cover APP alerts, automated defense, forensics and incident reporting.*

CASE STUDY

The Client: Taiwan's High Speed Rail network, which provides transportation service for passengers averaging 500 million per month and earner over USD 1.5 billion in revenue as of 2018

Challenge:

Since its conception, Taiwan's high-speed railway has become an indispensable provider of transportation across Taiwan. Due to the high profile, reach and indispensability of their offerings, information and systems related to the railway network are likely targets for hackers. The risk associated with security incidents such as data theft or system intrusion is extremely high, both in terms of damaging public perceptions and leading to disastrous failures in operating capacity and train safety. Therefore, information security has been a top priority for Taiwan's high-speed railway.

Solution:

Taiwan's High Speed Rail network wanted to adopt a thorough security information and event management (SIEM) platform to be able to answer to regulatory cyber security requirements from the government. To that effect, Billows partnered up with this client assist in the overall integration and automation of their SIEM platform, both from a product as well as a service and advisory capacity.

Results:

Within the Taiwan high-speed rail system, Billows is first and foremost responsible for managing their security and risk processes from a platform perspective, so as to avoid threats and attacks. Their ongoing project with this client includes the follow capabilities:

- **Log storage:** collecting and normalizing logs while performing long-term log storage and non-repudiation verification
- **Threat analysis:** Integrating analysis within inbuilt threat modules so as to detect abnormal events
- **Packet storage:** automatically saving packets when a specific security incident occurs, preserving the integrity of digital forensics
- **Quick response:** provisioning of an automated response mechanism that effectively shortens response time and automatically generates the required event messages, simplifying and shortening incident response steps

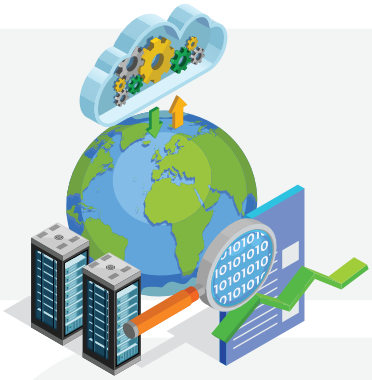
BACKGROUND

Billows' business focuses on cyber security operations, maintenance and cyber security support services.

Compliance and regulations have become a key component of cyber security, and the criteria surrounding both can be varied and complex based on geography. Enterprises need to cooperate to adjust their systems or policies to fully comply with cyber security requirements. Billows provides a complete enterprise security data analysis platform, along with consulting services that assist enterprises in implementing auditing, security compliance and automatic monitoring processes.

Currently, consultants provide guidelines to their customers, but that still requires customers to manage regulatory compliance themselves which can be difficult, time-consuming and labor intensive. In contrast, Billows directly assists in the process of integrating compliance, regulations and automated management right into their clients' IT operations. The company's in-house solution and service suite includes LogMaster, the Billows log management platform, and OneMan SOC, the Billows automatic cyber security management platform.

The highlights of Billow's reach include:

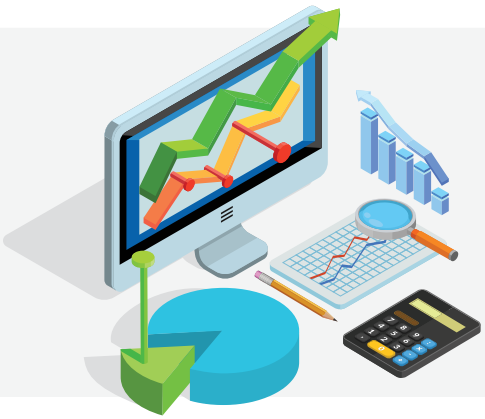


SCALE

Within the ASEAN region, Billows specifically targets two key client verticals: cyber security compliance consulting firms such as KPMG or Deloitte, and network or enterprise software outsourcing vendors.

TYPE

Key users of Billows products include securities and insurance companies. Other industries that are primary use cases of the company's technology include local government, vendors within network and enterprise software product development, and high speed rail technology (an industry that requires automatic management and has limited manpower to manage underlying infrastructure).



UNIQUE DOMAIN EXPERTISE

Billows is AT&T's value added professional services partner for security services. Their expertise as a security services partner allows them to effectively assist global software vendors to provide value added services.

PRODUCT SUITE

01 BILLOWS AUTOMATIC CYBER SECURITY MANAGEMENT PLATFORM

The requirements surrounding cyber security incidents typically revolve around providing effective and immediate responses. Billows' automatic cyber security management platform alert platform allows for collecting data on security incidents via their cybersecurity incident analysis platform, and then conducting the required notification of incidents to the correct user groups. The platform assists in the entire process management workflow: from generating notification forms to completing the entirety of each case.

02 BILLOWS LOG MANAGEMENT

This platform allows collecting, compressing and saving large volumes of raw logs. It also allows for integration with other reporting software to maximize visibility and allow effective visualization of internal information. Additionally, users can also automatically forward security logs to their threat analysis platform based on their custom cyber security analysis needs.

AWARDS AND RECOGNITION

2019 Cyber Security Vendor of Critical Infrastructure POC Site

Industrial Development Bureau, Ministry of Economic Affairs, Taiwan

2016 Receiving Subsidy from Small Business Innovation Research (SBIR) program

Small and Medium Enterprise Administration, Ministry of Economic Affairs