

SOUTH KOREA'S BUSAN BANK STANDS UP TO THREATS WITH RSA



South Korea is likely the most digitally connected country on earth. According to Akamai Technologies Inc., 97 percent of South Korea's population had internet access in 2017. Average internet speeds in South Korea are the fastest in the world, topping 28.9 megabytes per second (Mbps). It's the only country with average internet speeds above 25 Mbps, and it leads the world in mobile broadband penetration, too, reaching 120 percent of its population of 51 million.ⁱ

South Korea's widespread connectivity has transformed its economy, but it has also made the technologically sophisticated country a prime target for cyber attacks, according to the U.S. Department of Commerce.ⁱⁱ In March and June 2013, the country was hit by a series of cyber attacks that deleted data from nearly 48,000 computers and temporarily shut down operations across several large banks and media companies.ⁱⁱⁱ The June attack coincided with the 50th anniversary of the start of the Korean War, giving it greater emotional resonance.^{iv}

Attacks on South Korea's central banks and other entities have continued since 2013; it is against this backdrop that Busan Bank Co. Ltd., a regional bank with global aspirations, has invested in RSA NetWitness® Platform and RSA Archer® IT & Security Risk Management to improve its ability to mitigate cyber attack risk.

"We face internal and external threats, such as phishing, ransomware, and command and control communications that can lead to data loss and breaches," says Sunghun Woo, Busan Bank's security strategy manager. "RSA NetWitness Platform has helped us identify and stop these activities in their earliest stages. Integration with RSA Archer IT & Security Risk Management lets us see which affected systems are most critical, so we can prioritize incidents and respond more quickly to the ones that matter most."

VISIBILITY ACROSS LOGS AND NETWORK TRAFFIC

Busan Bank first deployed RSA NetWitness® Logs to centrally manage and monitor logs from on-premises and cloud-based systems. The solution is capable of collecting logs in real time from more than 350 event sources and uses patented parsing and indexing technology to perform three critical functions: interpreting relevant security information from a range of protocols, enriching log data at capture time, and dramatically accelerating alerting and analysis. In addition, RSA NetWitness Logs provides short- and longer-term retention capabilities and applies advanced analytics to speed event correlation and attack detection.

BNK Busan Bank

ABOUT BUSAN BANK

- Founded in 1967
- Headquartered in Busan, South Korea
- 3,398 employees
- 260 branches in South Korea

Following the successful implementation of RSA NetWitness Logs, Busan Bank added RSA NetWitness® Network to gain real-time visibility into all of its network traffic, including encrypted traffic. Like RSA NetWitness Logs, RSA NetWitness Network parses network data at capture time into sessionized metadata and enriches this data with threat intelligence from live feeds. RSA NetWitness Network combines deep inspection of hundreds of protocols with powerful forensic investigation capabilities and native decryption support. Together, RSA NetWitness Logs and RSA NetWitness Network make up two of the main pillars of RSA NetWitness Platform, which drives analytics, alerting, prioritization, detection, investigation and response activities for the bank.

“RSA NetWitness Platform has superior capabilities for storing and analyzing all traffic,” says Minjun Kim, security operations manager for Busan Bank. “It provides a single repository for all security data from across the bank and equips our analysts with the tools and information they need to investigate incidents.”

COMBINING THREAT DETECTION AND RESPONSE WITH INTEGRATED RISK MANAGEMENT

Busan Bank’s success with RSA NetWitness Platform prompted leaders to explore solutions from RSA Archer® Suite for security compliance and risk management. Woo, the bank’s security strategy manager, says decision-makers chose RSA Archer for its vision and reputation: “RSA Archer leads in the market by building solutions that anticipate industry challenges. It’s in widespread use in a number of industries, including banking, and is known for its modular, use case-based approach.”

The RSA Archer IT & Security Risk Management solution that Busan Bank has implemented includes use cases for managing security policies and vulnerabilities, accelerating incident and breach response processes, quantifying the financial impact of cyber risks, monitoring and testing IT controls, managing regulatory compliance obligations, and more. Busan Bank is using RSA Archer IT & Security Risk Management to centrally catalog the bank’s IT assets, identify those that are most critical to the business, and implement processes for escalating, investigating and resolving security incidents.

RSA Archer IT & Security Risk Management integrates seamlessly with RSA NetWitness Platform, so when a security analyst sees an alert in RSA NetWitness Platform, data from RSA Archer indicates what asset is affected and how important the asset is. In other words, an analyst can see, for example, if the asset in question is a PC or a mission-critical server, and if it’s a PC, who it belongs to—all in a single user interface, without having to pivot from screen to screen or application to application. Meanwhile, security incident data from RSA NetWitness Platform feeds back into RSA Archer IT & Security Risk Management to help risk managers get a clearer picture of their organization’s overall security risk profile.

“Together, RSA NetWitness Platform and RSA Archer IT & Security Risk Management deliver much greater visibility into security risks across the bank,” says Woo. “We’re now able to identify threats that previously eluded us, and we can prevent cyber attacks from spreading by detecting lateral movement and command and control communications.”

ABOUT RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.

“RSA NetWitness Platform has helped us identify and stop these activities in their earliest stages. Integration with RSA Archer IT & Security Risk Management lets us see which affected systems are most critical, so we can prioritize incidents and respond more quickly to the ones that matter most.”

– Sunghun Woo, Security Strategy Manager

- i <https://www.export.gov/article?id=Korea-Cyber-Security>
- ii <https://www.export.gov/article?id=Korea-Cyber-Security>
- iii “A Sign of Cyber Attacks to Come,” Deloitte, June 26, 2013 <https://deloitte.wsj.com/cio/2013/06/26/a-sign-of-cyber-threats-to-come/>
- iv “Cyber attack hits South Korea Websites,” BBC News, June 25, 2013 <https://www.bbc.com/news/world-asia-23042334>

