securonix

GOLOMT BANK

CASE STUDY

Securonix Helps Golomt Bank to Detect Cyber and Insider Threats

CASE STUDY

Securonix Helps Golomt Bank to Detect Cyber and Insider Threats

About Golomt Bank

Golomt Bank was established on March 6, 1995 as a subsidiary company of Bodi International LLC, a major player in the social and economic sector of Mongolia. The bank operates with a well-balanced presence in all of three market segments: Retail, Corporate, and SME. Golomt Bank is one of the systemically important banks in Mongolia, which is a leader in the country's development and operates under the motto, "Investing for a brighter future". The bank successfully accomplished their position as a well-recognized brand in Mongolia through our accomplishments and culture over the past few decades.

The Challenge: Moving from On-Premises to an Advanced Analytics Cloud SIEM

Golomt Bank, a large bank in Mongolia, lacked centralized visibility with their previously deployed SIEM solution. The bank's previous solution used a traditional rules-based approach that lacked behavioral analytics needed to detect insider threat or advanced cyber threats.

Golomt Bank needed a robust and scalable cloud based SIEM solution that could ingest huge volumes of data and use advanced analytics to detect and identify complex threats. With many security solutions deployed for intrusion prevention, distributed denial of service (DDoS) protection, email security, and data loss prevention (DLP), their environment was complex. They wanted to ensure that their new SIEM could consolidate all of this data together including their AWS cloud environment. Additionally, Golomt Bank needed their new next-generation SIEM to be able to cover their top use cases, detecting both cyber and insider threats. The SOC team evaluated several cloud SIEMs including Securonix.

Key Challenges

- Need centralized visibility across multiple security solutions and their AWS environment
- Require behavioral analytics to detect insider and advanced cyber threats
- Increase both stability and scalability to handle and ingest huge volumes of data from multiple custom data sources
- Strengthen technical support from the security solution vendor for reliable and secure bank operations

About Securonix

Securonix is leading the transformation of cybersecurity with the industry's first Unified Defense SIEM powered by agentic AI and built natively on Snowflake and AWS. By leveraging Amazon Bedrock (including Anthropic's Claude 3) for advanced AI agents and a split-data architecture, Securonix delivers elastic, privacy-preserving analytics that keep telemetry where customers want it while cutting storage costs and accelerating detection. Our platform collects and correlates logs across AWS services — including ECS, CloudTrail, CloudWatch, and S3 — applies behavioral analytics and AI-driven threat models, and automates response with built-in SOAR to provide end-to-end visibility for containerized workloads and hybrid environments. Recognized as a Leader in the Gartner® Magic Quadrant™ for SIEM and a Customers' Choice by Gartner Peer Insights™, Securonix empowers organizations to move from reactive security to proactive, autonomous operations. Learn more at www.securonix.com.

Securonix is built on and powered exclusively by Amazon Web Services (AWS), ensuring scalability, resilience, and enterprise-grade security. Securonix utilizes AWS Services including Bedrock, S3, EC2, RDS, and many others.

aws partner network
Advanced Technology Partner
Security Competency

aws marketplace

Visit Securonix in AWS Marketplace

The Solution: Complete Visibility and Sophisticated Threat Detection

Golomt Bank purchased the Securonix Next-Gen SIEM solution because of its cloud-native design and robust advanced analytics for user and entity behavior analytics (UEBA). Securonix's capacity to ingest more data sources than Golomt Bank's prior ArcSight SIEM was a deciding factor, in addition to the solution's AWS monitoring capabilities. With Securonix, the security team gained insight into the differences in behavior between malicious insiders and regular employees in order to effectively monitor for insider threats.

Securonix ingests all logs from their various data sources including custom data sources and provides single-pane-of-glass visibility into Golomt Bank's environment. Securonix Next-Gen SIEM's ability to enrich data with better context gives the security team better insights compared to other competing solutions.

Securonix Next-Gen SIEM with strong analytics and UEBA capabilities helped the bank to stay on top of detecting cyber and insider threats. The security team now has a better grasp of how entities act on their network and can identify deviations from what is typical by using sophisticated analytics, including peer analysis. The security team's understanding of entities and users, such as the actions of employees, has improved and they are now able to detect malicious employee activities.

Business Impact: Golomt Combats Threats with Securonix Security Analytics at Cloud Scale

Golomt Bank now enjoys full visibility into their data, whether it is cloud-based, on-premises, or hybrid, in a single security dashboard with Securonix. The bank uses Securonix Next-Gen SIEM to detect threats at scale and simplify security investigations. With a flexible, open architecture that ingests huge volumes of data, including from custom data sources, the security team can monitor their cloud data for misuse or compromise within their AWS infrastructure.

Securonix Next-Gen SIEM provides full security monitoring capabilities with no additional cost for UEBA capabilities. The fact that Securonix pricing for Next-Gen SIEM included UEBA made a huge difference in the total cost as compared to other competing solutions. Golomt enjoyed cost savings with better detection and response technology with Securonix.

Finally, Securonix's top-notch professional technical support provided seamless onboarding and timely resolution of issues to help Golomt Bank stay on top of detecting and responding to threats in their environment 24x7.