splunk>

CASE STUDY

Unitel Accelerates Incident Response by 2x to Keep Customers Connected 24/7

Key Challenges

Due to low visibility into its systems, Unitel struggled to quickly resolve incidents and protect its sensitive data.

Key Results

After automating complicated manual processes and gaining comprehensive visibility, Unitel now responds to incidents in real time, which has lowered the risk of security breaches.

UNITEL

Industry: Communications

Solutions: Security, Platform

Keeping an overwhelming majority of Mongolia's population connected is no easy feat.

Unitel, Mongolia's leading information communications technology group, provides hundreds of thousands of subscribers with mobile telephone services. Keeping its network resilient requires securing all digital assets and network resources, as well as maintaining the confidentiality, integrity and availability of information. But Unitel's previous SIEM lacked the data analysis, monitoring and threat intelligence capabilities for effective incident investigation and response, which made cyber threats a serious risk for the business.

Outcomes

Up to **50%**
higher SIEM efficiency

2-3x
quicker incident response

50%
faster log management

Unitel needed a new SIEM solution that could provide full-stack, real-time visibility into its cybersecurity posture and enable quick recovery when the inevitable incident did arise. After evaluating 10 solution providers and conducting multiple technical assessments, Unitel chose Splunk. "Splunk offers the flexibility, customizability, scalability, ease of use and integration capability we need for executing our security operations," says Mendsaikhan Amarjargal, CISO of Unitel group. "We were also impressed with Splunk as a thought leader in the security space."

Achieving holistic visibility

Security requirements are multifaceted at Unitel. "We have to maintain good security controls to prevent cyber threats and vulnerabilities while monitoring and responding to security incidents. We also have to enforce and improve policies and procedures to systematically manage our sensitive data," Amarjargal explains.

Beyond these requirements, Unitel needed an all-in-one data analytics platform. Log management became much simpler on the centralized Splunk platform, cutting the time needed for log search and ingestion by half across all its data sources — from network traffic and intrusion detection logs to endpoint protection and threat intelligence information.

"Splunk gives us the big picture and full visibility into the cybersecurity posture of our organization. This means we can identify and respond to security threats in real time, reducing the risk of security breaches and the impact of security incidents," says Amarjargal. "We also appreciate how Splunk's partner Unity helped us deploy the solution with ease while providing initial training for our engineers and coordinating with Splunk to ensure we receive optimal support."

A big leap forward in efficiency

Thanks to Splunk, Unitel resolves issues much faster, keeping systems up and running around the clock. "In the past, it used to take an hour for us to manually find and fix a single problem, which is already too long in today's fast-paced world," says Amarjargal. "The Splunk platform automatically correlates and analyzes data, which has made incident response two to three times faster than before."

Faster incident response has ripple effects throughout the business. Customers are happier because they're minimally affected by issues, and faster fixes also extend battery life for user devices. Within Unitel, automating security event correlation has saved hours of manual work and halved the time spent on system integration and data parsing.

"In the past, it used to take an hour for us to manually find and fix a single problem, which is already too long in today's fast-paced world. The Splunk platform automatically correlates and analyzes data, which has made incident response two to three times faster than before."

Mendsaikhan Amarjargal, CISO, Unitel Group

"Splunk is a robust and reliable cybersecurity solution that helps us safeguard our network, infrastructure, applications and data. Our systems are better prepared against threats and are better positioned to recover from whatever issues that arise," says Amarjargal. "As the largest information communications technology (ICT) company in Mongolia, Unitel operates not only in telecommunications, but also other services such as triple play and over-the-top media services. Because Splunk is customizable and flexible, we can easily process data from multiple sources to keep our business digitally resilient."

Unlocking new possibilities with Splunk

In addition to product functionality, Splunk's large user base in Mongolia is also a bonus for Unitel. "We are able to learn from many other local use cases and derive maximum benefits from Splunk," Amarjargal explains. Apart from out-of-the-box security use cases, additional applications from the Splunkbase App have been helpful in fulfilling Unitel's specific needs.

"Right now we're looking to extend the use of Splunk to other areas such as customer experience management to improve customer service, reduce churn and identify new revenue opportunities," Amarjargal adds. "We're also considering using Splunk as an IoT analytics platform to monitor device performance, detect anomalies and improve operational efficiency. Furthermore, we may also put Splunk on network performance monitoring, anomaly detection and troubleshooting."

Our Partner
Unity Data Technology LLC

UNITY

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2023 Splunk Inc. All rights reserved.

23-207662-Splunk-APAC Unitel Case Study-CS-SS-104