Customer Success Story

ArcSight

Unitel

Unitel stops IT attacks and protects its reputation prevents outages with Micro Focus® ArcSight.

Overview

When customers started calling telecommunications provider Unitel to complain that their Internet service had dropped out, the company had a problem. Because Unitel didn't immediately know the root cause of the outage, customers had to wait up to two hours before services could be restored.

The incident was a wake-up call for the Mongolian company, showing how delays in resolving IT security incidents could trigger negative rumors about Unitel's reliability and damage the company's business reputation. With three other carriers competing in a country with a population of about three million people, the risk was very real that unhappy customers could switch to a rival provider.
Today, Unitel has dramatically reduced the number of these outages. The company has done so using a combination of Micro Focus products, including ArcSight—a security information and event monitoring (SIEM) tool that allows Unitel to detect attacks in a fraction of the time the company took previously. Unitel's story shows how a proactive security management stance doesn't only reduce risk, but can also have a positive impact on the bottom line.

> **"Now we can provide management with reports using real system logs, rather than assumptions about the current situation of security at Unitel. Investments will not be wasted."**
>
> **ENKHSAIKHAN PAGVA**
> Manager of the Information Security Unit
> Unitel

Challenge

Like many growing telecommunications providers, Unitel deals with a variety of IT security challenges. The company is the second-largest mobile network provider in Mongolia, with about one million customers. Unitel also has 120,000 IPTV, voice over IP (VoIP), and Internet customers. However, with a limited number of security analysts in a company of 1,200 employees, the business was struggling to quickly resolve security incidents, resulting in extended outages and financial losses.

For example, Unitel discovered a large number of unauthorized international calls using the company's VoIP service. The carrier was not able to correlate and detect malicious attempts to access the VoIP service, meaning it took up to a month before Unitel noticed these unauthorized calls.

At a Glance

- **Industry**
  Telecommunications
- **Location**
  United States
- **Challenge**
  The organization needed to reduce financial loss and prevent negative customer sentiment by decreasing service outages.
- **Products and Services**
  ArcSight
- **Results**
  + Reduces time to identify attacks from 2 hours to 10 minutes, avoiding damage to reputation
  + Blocks fraud attempts within five minutes of detection, reducing financial losses
  + Provides reports showing value of security spending

In another case, malicious traffic sent to Unitel's web server put a strain on databases that allowed customers to pay bills through the Unitel website. The company had to find the solution, which took up to one hour, during which time none of Unitel's branches were able to process customers' bills.

Although Unitel had common security measures like firewalls in place, it wasn't always easy to diagnose the source of outages. When the unknown performance issue was detected at the firewall, Unitel's engineers could not easily work out why, unless they spent hours collecting and examining data logs from servers behind the firewall. To do this, they had to spend

Solution

Decreases Response Time

Unitel established a security operations center and chose a combination of Micro Focus products that would allow it to quickly collect logs, correlate that data with network events to rapidly pinpoint problems, and block malicious traffic. The end result is that Unitel can resolve security incidents much faster, reducing the likelihood and duration of outages. This translates to more reliable services and less risk of customers switching to another provider due to an outage.

Unitel can now detect malicious traffic targeting its Internet servers in about five minutes, instead of one hour. This is possible because the company uses ArcSight to correlate logs. For example, in the case of the Internet outage, botnet infected PCs were sending large amounts of traffic to Unitel's servers, reducing their capacity to provide Internet services to customers. Using ArcSight, Unitel found links between a slow firewall and malicious traffic targeting the company's web server. Unitel could then create a rule for all firewalls to block that IP address, restoring the firewalls' performance and preventing other firewalls and servers from experiencing the same problem.

As a result, Unitel can now resolve these web attacks in about 10 minutes instead of 2 hours. This decreases the chance that customers will lose Internet access, and reduces the risk of unhappy customers.

Unitel also uses ArcSight to prevent fraud involving unauthorized calls on the carrier's VoIP service by detecting brute force password login attempts and calls to suspicious destinations in real time. As a result, Unitel can detect a VoIP fraud attempt within 10 seconds, instead of waiting for the customer to receive an expensive bill in the mail. This has reduced revenue losses and the risk of overcharging customers.

Micro Focus Reputation Security Monitor further improves Unitel's ability to spot threats by identifying traffic from hosts or locations with a history of malicious activity. This allows Unitel to act before damage is done by stopping devices connected to malicious IPs and URLs, and assisting the company to prevent losing sensitive data after a breach.

ArcSight ThreatDetector uses analytics to identify patterns indicating coordinated attacks. These tools both contribute to more accurate alerts and allow Unitel to detect security incidents and act fast.

Saves Time

By choosing Micro Focus, Unitel also has the ability to add complementary tools and services that reduce the security burden on Unitel staff.

Security Professional Services team worked with Unitel for one month, talking to each business unit to determine use cases for ArcSight and translating that information into rules. This transfer of knowledge has allowed Unitel employees to develop additional security management rules for ArcSight at a later date, improving the accuracy of alerts and reducing their response time to incidents.

Like many companies, Unitel has a challenge making sense of the numerous logs the company's systems generate. Using the ArcSight Data Platform, Unitel now has a single interface to manage all of them. This further increases the speed at which the company can pinpoint and resolve problems, resulting in time savings for employees, and better service for customers.

Unitel's security analysts are also more productive now that ArcSight handles tasks like collecting and analyzing logs, says the company's Manager of the Information Security Unit, Enkhsaikhan Pagva. "It was very hard for them previously. Now they are not wasting time on manual tasks. They have more time to research and analyze data, and more time for forensics and advanced work," Pagva says. He estimates that Micro Focus tools have reduced Unitel's manual security analysis by about 70 percent.

Unitel also uses ArcSight to reduce the time its analysts spend manually collecting information and generating alerts about vulnerabilities. Previously, this process took many hours. Now, Unitel uses ArcSight to integrate this data in real time from vulnerability scanners and correlate it with other security events. As well as saving time, this process enables more accurate alerts, reducing the risk of breaches affecting Unitel's operations and reputation.

Choosing Micro Focus also makes it easier to audit log data. Unitel uses the ArcSight Compliance Insight Package for IT Governance,

Contact us at:
www.microfocus.com

which stores logs in archives for forensic searches and helps show the company is compliant with best practices.

Proves Value of Security Spending

By reporting the number of incidents, the Micro Focus security management tools demonstrate to Unitel managers the value of ArcSight and the company's security operations center. Pagva says the ability to detect and prevent further security incidents has led the company to hire more security analysts.

"Now we can provide management with reports using real system logs, rather than assumptions about the current situation of security at Unitel," says Pagva. "Investments will not be wasted."

Unitel's achievements demonstrate the importance of a comprehensive security strategy in not only protecting business operations, but keeping customers happy in a competitive market.

Learn More At

software.microfocus.com/software/arcsight