splunk>

CASE STUDY

Telenor Gains Greater Insight for Incident Investigation, Troubleshooting and Improved Security

telenor

Executive summary

Founded in 1855, Telenor, Norway's largest telecom services provider, has over 150 years of telecoms experience, including fixed and mobile telephony, broadband and data communication. Telenor's customers rely on it to provide always-on voice, data and content services. The company needed to gain operational visibility into its distributed infrastructure and streamline processes for incident investigation and network monitoring. Since deploying Splunk Enterprise, Telenor has seen benefits including:

- Quick and easy troubleshooting of business-critical issues
- Faster and stronger security
- Increased availability

Why Splunk

With millions of customers, thousands of servers and routers, and datacenters located throughout Norway, Telenor needed to understand the essential operating details of its infrastructure. Communications between different departments were challenging and log event data was difficult to analyze. Granting access to certain logs on a server often meant giving access to all the logs collected on that server, which posed definite security and privacy risks. The few people with authorized access faced the impossible task of manually browsing through hundreds of millions of log records a day. Unsurprisingly, kernel errors and other issues sporadically slipped by unnoticed.

Splunk has provided Telenor Norway the visibility and operational insight to keep its IT systems and networks running at peak performance. Telenor's network operations team runs dashboards visualizing network health and monitors for error events and unfamiliar patterns. The security team uses Splunk Enterprise for correlation and analysis of security alarms. With Splunk software it can look for, and be proactively alerted on, abnormal remote access patterns and investigate attacks on Internet-exposed services. Finally, Splunk also underpins the Telenor Computer Emergency Response Team (CERT), which is a cross-departmental incident response team. This virtual team uses Splunk for incident investigation, pinpointing the origin of large

Industry

- Telecommunications

Splunk Use Cases

- IT operations management
- Security

Challenges

- Needed to gain operational visibility into distributed infrastructure
- Wanted to improve inter-departmental collaboration
- Needed to address potential security and privacy breaches
- Laborious manual processes did not scale

Business Impact

- Established distributed search, alerting, event correlation and proactive monitoring for security
- Health monitoring using baselines to identify anomalies and issues before they become problems
- Quick and easy troubleshooting of business-critical issues
- Supplied role-specific, dashboard views to give appropriate data access to users across IT without compromising security
- Delivered the IT and network teams infrastructure-wide visibility via dashboards, ad hoc searches, reporting and trend analysis

Data Sources

- Infrastructure logs: Network switch and firewall logs
- Server logs: Linux, Windows and Unix
- Application logs: Web, email, IPTV, etc.
- IP backbone: router logs
- Storage: SAN and NAS logs
- Mobile network logs

Splunk Products

- Splunk Enterprise

issues and performing rapid manual analysis of failing components to limit business impact.

Improved security posture helps prevent revenue loss

With Splunk Enterprise, Telenor can easily get to the root cause of any issue and resolve it. For example, the team noticed that Telenor WebMail accounts were being abused to send hundreds of thousands of SMS messages abroad. They used Splunk Enterprise to analyze the incident and were immediately able to identify which accounts were being abused and how many SMS were being sent, as well as when and where the logins were coming from. Armed with this insight, it was a simple job to shut down the offending accounts and stop the abuse, preventing further revenue loss.

Using the Splunk platform, Telenor's security teams can now determine the baseline for "normal" and track any deviations from that standard. This gives Telenor the ability to quickly and efficiently detect brute force login attacks and other security issues. With this established, they can now use easy-to-compose dashboards to monitor systems and services for anomalous activity. Other examples include correlating timing and IP addresses to determine if attacks from multiple countries are coordinated, and the ability to identify vulnerable Internet exposed services.

Proactive troubleshooting leads to increased service availability

Splunk has enabled Telenor to learn more about the organization's IT and network infrastructure and its potential for the business. Telenor is now responding to incidents more proactively and providing better service as a result. The network operations team uses baseline measurements so it can understand what constitutes normal. It has created Splunk alerts to monitor for error spikes and unfamiliar patterns.

> **"Traditional monitoring tools just tell you when something isn't working. With Splunk, we can now proactively manage operations and respond before an outage occurs or service erodes. The Operational Intelligence we have with Splunk software makes it much quicker and easier to investigate and resolve any incidents that occur in our infrastructure."**
>
> Security Architect
> Telenor

These valuable searches are now saved and run on a schedule, providing proactive alerts in front of recurring issues. This advanced visibility lets Telenor's CERT, security and operations teams spot an error as soon as it occurs and start working on correcting it immediately, which can prevent or reduce downtime. Problems are typically mitigated before users notice them or services fail.

Operational visibility improves the customer experience

Since deploying Splunk Enterprise, Telenor Norway has dramatically improved visibility into its complex IT infrastructure and networks. There is now a 'Splunk first' policy in place, so any new data has to be put into Splunk Enterprise. Role-based access control ensures users get the access to the data they need without compromising security or violating customer privacy regulations.

Not only can Telenor's internal teams investigate and resolve issues much more quickly, they are also able to use Operational Intelligence to create baseline views to catch errors or anomalies early on, often addressing these issues before they impact the customer experience.