splunk>

CASE STUDY

Splunk® at Telenor

Delivering Insight for Incident Investigation, Troubleshooting and Improved Security

"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."

Security Architect
Telenor

OVERVIEW

INDUSTRY
- Telecommunications

SPLUNK USE CASES
- IT Operations Management – Server Monitoring, Network Monitoring
- Security – Incident Investigation

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

The Business

Founded in 1855, Telenor, Norway's largest telecom services provider, has over 150 years of telecoms experience. The company believes "growth comes from truly understanding the needs of people to drive relevant change." Considering that Telenor's mobile subscribers globally grew from 15 to 160 million in less than a decade, its belief that deeper insight leads to success is holding true. Telenor's service portfolio in Norway includes fixed and mobile telephony, broadband and data communication. Customers rely on Telenor to provide always-on voice, data and content services.

Challenges

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. Communication between far-flung departments was challenging and there were frequent miscommunications. While some log event data was being collected, the logs were difficult to analyze. In addition, 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.

Enter Splunk

Splunk has provided Telenor Norway the visibility and operational insight to keep its IT systems and networks running at peak performance. Telenor is using Splunk Enterprise for troubleshooting, monitoring and security investigations. The network operations team runs dashboards visualizing network health and monitors for error events and unfamiliar patterns. The security team uses Splunk for correlation and analysis of security alarms. With Splunk they 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 issues and performing rapid manual analysis of failing components to limit business impact.

Telenor indexes 400GBs of data per day with Splunk, including data from thousands of servers, routers and data sources ranging from the datacenter, the IP infrastructure and the mobile network, to applications and services like web, email and IPTV. This constitutes about half of Telenor's entire IT estate, and there is now a 'Splunk first' policy in place, so any new data has to be put into Splunk.

Telenor forwards data to a pool of Splunk indexers. Role-based access control ensures users get the access to the data they need without compromising security or violating customer privacy regulations.

"The operational intelligence we have with Splunk makes it much quicker and easier to investigate and resolve any incidents that occur in our infrastructure."

Security Architect
Telenor

Breakthroughs

Incident investigation and troubleshooting

When something goes wrong, it is now quick and easy for Telenor to get to the root cause of the 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 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.

Stronger security

Using Splunk, the 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.

Increased availability

Not only can the CERT, security and operations teams troubleshoot problems faster than ever, the insights gained through Splunk software lets Telenor identify a problem long before it turns into a crisis. These valuable searches are now saved and run on a schedule, providing proactive alerts in front of recurring issues. Telenor can now spot an error as soon as it occurs and start working on correcting it immediately, which can prevent or reduce downtime.

Business-critical insights

Over time, the knowledge built into 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 they can understand what constitutes normal. They have created Splunk alerts to monitor for error spikes and unfamiliar patterns. This advanced visibility lets them troubleshoot problems before users notice them or services fail.

In summary, since deploying Splunk, Telenor Norway has dramatically improved visibility into its complex IT infrastructure and networks. Not only can the internal teams now 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.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise 6 license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

250 Brannan St., San Francisco, CA 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.apps.splunk.com

Item # CS-Splunk-Telenor-104