

# Splunk at Telenor

## Delivering Insight for Continuous Service Improvement



“Today’s monitoring tools just tell you when something isn’t working. With Splunk, we now proactively manage operations and respond before an outage occurs or service erodes.”

**Henrik Strom**  
Security Architect,  
Telenor

### OVERVIEW

#### INDUSTRY

- Telecommunications

#### SPLUNK USE CASES

- IT Operations Management – Server Monitoring, Network Monitoring
- Security – Incident Investigations

#### BUSINESS IMPACT

- Established distributed search and proactive monitoring for security issues and performance monitoring to identify issues before they become problems.
- Supplied role-specific, dashboard views to give appropriate data access to all users across IT without compromising security.
- Delivered the IT team infrastructure-wide visibility via dashboards, ad hoc searches, reporting and trend analysis.

#### DATA SOURCES

- Infrastructure logs: Network switch, firewall and router logs
- Server logs: Linux, Windows and Unix
- Application logs: Web, email, IPTV
- IP backbone logs
- Storage: RAID controller logs

## The Business

Telenor, Norway’s largest telecom services provider, believes “growth comes from truly understanding the needs of people to drive relevant change.” Considering that Telenor’s mobile subscribers grew from 15 to 160 million in less than a decade, its belief that deeper insight leads to success is holding true. Customers rely on Telenor to provide always-on voice, data and content services. And Splunk provides Telenor the visibility and operational insight to keep IT running at peak performance.

## Challenges

With 160 million customers, thousands of servers and routers, and datacenters located throughout Norway, Europe and Asia, it was impossible for anyone to truly understand the essential operating details of the infrastructure. Communication between far-flung departments was extremely difficult or sometimes didn’t happen. Some logs were being aggregated, but they were still difficult to search. Access to single components meant access to everything—a definite security risk.

The few people with authorized access faced the impossible task of manually browsing through north of 100 GB of records a day. No wonder kernel errors and other issues sporadically slipped by unnoticed.

## Enter Splunk

The Telenor team uses Splunk Enterprise for troubleshooting, performance monitoring and security investigations.

### Operations

The operations team uses baseline measurements so they can understand what constitutes normal. They 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.

For example, the team learned that on average twenty errors occur across all distribution routers on the IP backbone every fifteen minutes. The day after discovering this, Splunk detected and alerted on 4,000 errors and was used to quickly determine the root cause.

### Security

Once the security team determined the baseline for brute force logins and other security issues, they used easy-to-compose dashboards to monitor servers and systems for anomalous activity. By correlating timing and IPs, they now determine if attacks are coordinated. They also identify vulnerable web services.

## Breakthroughs

### Affordable Scalability

With the Splunk's ability to integrate with Telenor's existing tools, users continually think up new ways to deploy it. Unlike other appliance-based solutions Splunk operates on commodity hardware and runs on nearly any operating system, including Windows, Mac, Linux, Unix, AIX or Solaris.

### Productivity

Telenor has deployed Splunk in each of its regional datacenters to index data and support the local staff's searches. They also take advantage of the Splunk distributed searching capabilities that enable searches across datacenters and across all of the Splunk data when needed.

The Splunk toolkit for creating ad hoc reports and dashboards gives Telenor the means to drive new efficiencies and success.

### Responsiveness

Not only can the security and operations teams troubleshoot problems faster than ever, the understanding gained through Splunk baselines 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.

### Secure Access

Telenor funnels data to one of three secure Splunk instances. Role-based access controls ensures users get the access they need without compromising security or violating customer privacy regulations.

### Insights

Over time, the knowledge built into Splunk has enabled the Telenor team to learn more about their IT infrastructure and its potential for the business. Their team is now responding to incidents more proactively and as a result providing better service.

"We have a lot of data, a lot of tools, many groups of people, and too little communication. This makes it difficult to investigate incidents as no one person holds the keys to the data needed to conduct a proper analysis."

**Henrik Strom**  
Security Architect,  
Telenor

## Free Download

[Download Splunk](#) for free. You'll get a Splunk Enterprise 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](mailto:sales@splunk.com).