LOGPOINT

HEALTHCARE

REGION JÄMTLAND HÄRJEDALEN

HOW REGION JÄMTLAND HÄRJEDALEN USES LOGPOINT TO MONITOR IT INFRASTRUCTURE, PROTECT PRIVACY AND DEVELOP BEST PRACTICE

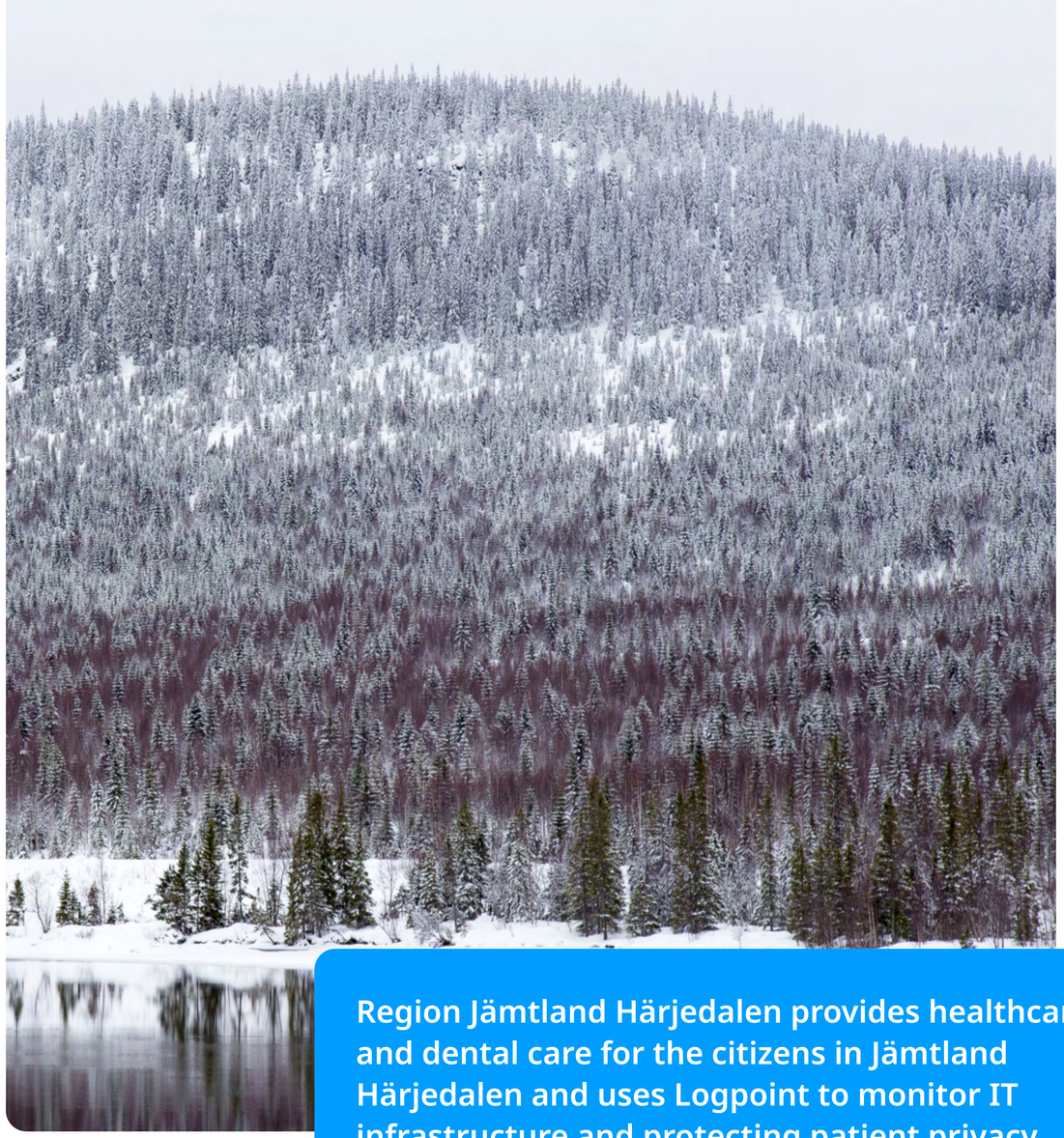
HEALTHCARE

REGION JÄMTLAND HÄRJEDALEN

FACTS	
Customer	Region Jämtland Härjedalen
Industry	Healthcare
Location	Jämtland Härjedalen, Sweden
Objectives	Monitoring IT infrastructure and protecting patient privacy

LOGPOINT

- Effectively monitors IT infrastructure and helps ensure compliance with the Swedish Patient Data Act
- Increases transparency by providing citizens quick and easy access to information about the access and use of their medical records
- Pinpoints unwanted and unintentional use of medical records, and helps improve user behavior via audit dashboards and log reports



Region Jämtland Härjedalen provides healthcare and dental care for the citizens in Jämtland Härjedalen and uses Logpoint to monitor IT infrastructure and protecting patient privacy.

BACKGROUND

Region Jämtland Härjedalen is located in the middle of Sweden, bordering Norway to the west. With a population of around 127,000, it's one of the smallest among the 21 Swedish regions. But in terms of territory, it's the third-largest. This makes for a region sparsely populated, characterized by large woods, mountains, and beautiful lakes, with almost half of the population living in the only major city Östersund.

The Region is responsible for the healthcare and dental care of the citizens in Jämtland Härjedalen and the primary medical facility is Östersund Hospital, the only hospital in the region. Approx. 3,000 employees work in the regional healthcare sector, and the Cambio COSMIC medical record system is one of the primary digital tools keeping health-related information of all citizens.

THE CHALLENGE

As the healthcare sector is going through a rapid digital transformation and electronic medical records form the information backbone in hospitals, the volume of sensitive data is increasing. Simultaneously, the number of users accessing sensitive data is rising, and hospitals are increasingly relying on networked devices, systems, and applications to provide efficient care.

As complexity increases, so is the risk of cyberattacks disrupting vital services, or breaches leading to privacy infringements. At Region Jämtland Härjedalen, keeping medical records containing sensitive and personally identifiable information of 127,000 citizens requires high standards. The Swedish Patient Data Act protects the integrity of citizens by only allowing healthcare professionals who have an active care relation with the patient to access their medical records.

To lock down all records and provide access on a need-to-know basis is unsustainable as it is impossible to predict what records medical professionals need to access in case of an emergency. Consequently, information needs to be accessible for those who might need it, but control with access audits must be rigorous.

Realizing that in many cases, unwanted access to medical records is unintentional, by accident, or due to wrong use of systems, developing preventive methods to improve compliance with the Patient Data Act is key. Collecting audit data about the use of medical record systems and identifying trends in potential access violations is needed to prevent future violations, impact user behavior and promote best practices for using patient data most efficiently.

THE SOLUTION

Lars Christerson is Information Security Officer at Region Jämtland Härjedalen. He leads a data security and data protection team of five colleagues, including legal resources. The team uses the Logpoint SIEM solution to collect, aggregate, and analyse security data across the infrastructure, including domain controllers, web servers, and other critical parts of the regional network.

The Logpoint SIEM collects, categorizes, and analyses log data to identify potential cybersecurity incidents and events. Based on predefined rules, it delivers real-time alerts and presents security information to the data security team in on-screen dashboards or reports provided with regular intervals.

“The Logpoint SIEM allows us to monitor the state of our infrastructure continuously and provides alerts if something out of the ordinary is occurring. In addition, it provides us with the necessary tools to drill down into an incident and to establish whether there is a technical problem, user error, or an actual breach of security,” says Lars Christerson.

The Logpoint SIEM solution is also collecting log data from the COSMIC medical record system in audit trails for further processing and reporting to responsible healthcare roles. For that Jämtland Härjedalen is using the Logpoint Applied Analytics module, to make audit data about access to patient records available for a broader, non-technical group of local administrators. They can monitor access to patient records, perform targeted searches, evaluate incidents, and use the data to help improve user behaviour and develop best practices for the use of medical records. Best practices for predefined rules and dashboards for patient record access have been developed in collaboration with Region Värmland, who is also a Logpoint user.

“Working with a mix of cluster sampling, predefined non-compliance rules, and dashboards showing aggregated outcomes, we get distinct views of the access patterns. The option to drill down in specific cases increases our ability to evaluate violations and anomalies and helps us understand user behaviour. This allows us to improve our ways of working and help develop best practices for medical record platforms. In that way, Applied Analytics has helped us evolve from ’policing’ users in a direction towards a quality improvement mission”, says Lars Christerson.

“Using automated rules for log filtering, we can reduce the number of false positives for potential breaches. Adding a severity level with rules can filter the incidents to identify and prioritize cases where a real violation has been found. That saves precious time.”

CONTACT LOGPOINT

If you have any questions or want to learn more about Logpoint and our modern SIEM solution visit www.logpoint.com

THE RESULTS

With the Logpoint SIEM solution and the Applied Analytics module, Region Jämtland Härjedalen can monitor their IT infrastructure, ensure compliance with the Swedish Patient Data Act and provide citizens quick and easy access to information about who accessed their medical records. Logpoint enables accelerated detection and response to cybersecurity incidents and helps safeguard citizens' rights to privacy.

"As security information was previously dispersed across multiple systems, and we had to manually sift through logs, analyzing data was previously a time-consuming and tedious job. Also, it was most often done in response to a problem and not proactively. This has changed as the Logpoint SIEM is automatically filtering and analyzing logs in real-time and alerting us of issues that requires attention," says Lars Christerson.

"Using Logpoint Applied Analytics to automate reports for specific target groups, we can deliver on specific needs. A great example is a patient requesting an access summary for his and her records. This data is now available for citizens through the public digital self-service portal 1177.se, allowing citizens to access their information online using their standard BankID login", says Lars Christerson.

Using Logpoint has increased transparency and reduced time spent on log reporting in Region Jämtland Härjedalen. And plans are made to add more log sources to get an even more granular view of security in the network.

"We are looking into the potential of the Logpoint UEBA module and advanced machine learning to increase security by adding behavioral analytics to our security toolbox.
We believe there is a huge potential in the data collection and analytics capabilities in the Logpoint solution That could potentially be used to improve patient safety or quality testing, which is an exciting perspective", says Lars Christerson.

"The Logpoint SIEM allows us to monitor the state of our infrastructure continuously and provides alerts if something out of the ordinary is occurring. In addition, it provides us with the necessary tools to drill down into an incident and to establish whether there is a technical problem, user error, or an actual breach of security."

Lars Christerson
Information Security Officer