▮▮ LOGPOINT

CUSTOMER CASE

Secure energy delivery

How Logpoint Secures Başkentgaz's 18,000 km Natural Gas Distribution network

Başkentgaz

Industry | **Natural Gas, Critical National Infrastracture**
Location | **Ankara, Turkey**

Başkent (Capital City) Natural Gas Distribution was established in 2007 and became part of Torunlar Energy after privatization in 2013. As Turkey's first and largest private natural gas distribution company, Başkentgaz provides natural gas services to 11% of the country's population under a distribution license valid until 2037.

Serving approximately 2 million subscribers in Ankara with high-quality, safe, and uninterrupted natural gas, Başkentgaz operates with a customer satisfaction-focused approach. After privatization, the company expanded its natural gas distribution network from 9,500 km to 13,000 km by the end of 2020 and reached 18,000 km by 2024.

THE CHALLENGE
Long term log storage

Başkentgaz wanted to uplevel their log management and security processes. As a publicly traded company undergoing independent audits every three months, ensuring seamless log collection and retention was critical. Başkentgaz also required a solution that could provide long-term log storage while maintaining compliance with security policies. Managing VPN login and logout logs for remote employees was a particular concern, as it was essential to ensure effective access control and prevent unauthorized access.

The company sought a scalable SIEM solution that could integrate seamlessly with various critical systems, including ERP, EDR, Proxy, Firewall, and IPS. The lack of a centralized monitoring system made it challenging to quickly respond to security incidents, create custom reports, and efficiently classify and normalize data.

One SIEM solution for everything

SAP Integration

Logpoint has successfully achieved full integration with Başkentgaz's SAP systems. Through this integration, user activities, security events, and access logs from all SAP applications are collected and analyzed.
Potential anomalies within SAP systems are quickly detected, allowing necessary actions to be taken while preventing log loss and accumulation.

To enhance log management efficiency, a dedicated server has been configured to store SAP logs for one week. This approach partially backs up the SIEM solution while enabling the identification of missing logs, which are then securely forwarded to Logpoint.

Log management and security with Logpoint

Logpoint enables Başkentgaz to securely store log records for many years. In particular, VPN login and logout logs of remote employees are thoroughly analyzed and reported in a tabular format.
This ensures that access controls are effectively implemented in compliance with security policies

Automation and case management integration

Logpoint enables the integration of automation and case management across all Başkentgaz systems, allowing for faster and more effective responses to security incidents.
With this integration, threats are automatically detected, and appropriate actions are taken immediately.

RESULTS

Operational efficiency

Logpoint is actively used by users with different authorization levels within Başkentgaz. Dedicated accounts are created for users, allowing access only to personalized dashboards, reports, and user-specific alarms.

With the security and operational advantages provided by Logpoint, Başkentgaz continues to efficiently manage its log management processes. Logpoint is integrated with all systems in Başkentgaz, including critical components such as ERP, EDR, Proxy, Firewall, and IPS.

BENEFITS

- Monitor all systems from a single point and respond quickly to security incidents.
- Flexibly create custom alarms, reports, and dashboards in addition to built-in ones, enhancing operational efficiency.
- Classify and normalize data according to user needs.
- Generate daily, weekly, and monthly reports.
- Integrate with most global products, providing flexibility in product selection.
- Instantly access needed information through fast and easy queries.

> We analyze global cyber threats and create dashboards in Logpoint as additional security measures. This gives us extensive capabilities in threat observability.
>
> Logpoint functions like a search engine, making it easy to find the logs we need. The support team is highly competent, not only resolving issues but also explaining solutions, which aids in learning and self-improvement.

Abdurrahman Polat
Cybersecurity Expert, Baskentgaz