Forcepoint

Customer Story

Turkish Petroleum Giant Tupras Keeps its Information Security Processes Safe with the Help of Forcepoint

Turkey's largest petroleum refiner relies on Forcepoint Web Security Hybrid and DLP to help protect its users and data from bad actors and malicious organizations.

Tupras is responsible for processing and delivering the majority of petroleum products to Turkey's domestic market, and the four refineries the company operates represent the backbone of Turkey's critical infrastructure. Keeping those facilities safe and secure is crucial in an age when malicious organizations, including nation states, target such facilities. And Tupras relies on Forcepoint to help provide that protection.

CUSTOMER PROFILE:
Leading Turkish petroleum refiner, controlling the majority of Turkey's oil refining capacity and almost 60 percent of the country's petroleum products storage capacity.

INDUSTRY:
Oil & Gas

HQ COUNTRY:
Turkey

PRODUCTS:
- Forcepoint Web Security Hybrid
- Forcepoint Data Loss Prevention

It's a dynamic, competitive time for Fortune 500 manufacturers—large-scale, heavy industry around the globe is rapidly embracing new technologies like machine learning that enable the automation of manufacturing processes, and the worldwide industrial automation market is projected to nearly double in size between 2018 and 2026 to $296.7 billion. Nowhere is that happening more broadly than in the petrochemical sector. Tupras, Turkey's largest petroleum refiner, is at the forefront of the global Industry 4.0 movement, embracing technologies like AI-based smart robots, IoT, and big data analytics.

Industry 4.0 technologies have made manufacturing more efficient and productive, but they have also made the safeguarding of industrial data, systems, and networks more important than ever. Cyberattacks on critical infrastructure like the four oil refineries Tupras operates can target any weak link in a manufacturer's chain of connected users, applications, and networked systems and devices.

"Nearly three-quarters of global oil and gas companies have experienced at least one cyber incident," said Alper Sulan, Chief Information Security Officier at Tupras. "And attacks are growing in frequency, sophistication, and impact as the industry employs ever more connected technology throughout organizations. These attacks can result in severe consequences to human and environmental safety in the form of ruptures, explosions, fires, releases, and spills. We need to be extra vigilant to prevent any disruption of service and deliverability that could be devastating for people and infrastructure."

Choosing the right cybersecurity partner was crucial to maintaining Tupras' position as an industry leader and essential part of Turkey's infrastructure.

Protecting the back office to help safeguard the refinery floor

Not happy with its existing web security and concerned about potential leaks of valuable and sensitive data, Tupras decided it needed to improve its cybersecurity.

"When we look at the attack vectors and bad actors, they usually try to infiltrate the company network by using malicious links via email or the web," said Cansu Altinisik, IT Risk and Compliance Supervisor at Tupras. "We also had problems with false positives and visibility, were not sure that security was fully ensured, and our coverage was limited to in-office use only. Finally, we did not know who used our data, how it was used and for what purpose."

Tupras was looking for a cybersecurity solution that could safeguard sensitive personal data, while also preventing its back-office operations from becoming a vector for an attack on its refineries and other industrial facilities. Specifically, it looked for a security solution to meet several needs:

- → Block risky ransomware links in emails and guard against external attacks like phishing and botnets, run by hacker groups like Dragonfly 2.0 which target critical infrastructure.
- → Expand web security outside the office to protect users wherever they work and connect from.
- → Enable compliance with regulations like the EU's GDPR and Turkey's KVKK data protection law.
- → Monitor and better control how data travels inside and outside the organization.

Challenges

Safeguard back-office IT operations from external and internal threats.

Assist compliance with data protection regulations like GDPR.

Approach

Deploy Forcepoint Web Security Hybrid with DLP in an agent-based solution installed on all company computers and devices.

Critical infrastructure requires a top-scoring security solution

In selecting a new web security and DLP solution, the refining giant assembled several vendors for a Proof of Concept (PoC). Tupras was looking for a solution that could combine web security and DLP capabilities and which could be installed as an agent on all computers and devices connected to the corporate network.

Forcepoint Web Security GW Hybrid and Forcepoint DLP turned in the best score in the PoC by far, more than doubling the next closest score in countering web attacks while minimizing false positives. Tupras was also impressed with Forcepoint's customizable policy libraries which greatly simplify complying with regulations like GDPR and KVKK, as well as Forcepoint's risk-adaptive protection and human-centric approach to cybersecurity, which was seen as being in alignment with Tupras' own technology-based roadmap.

"With Forcepoint Web Security Hybrid, we are able to provide full protection inside or outside the office, and our employees are safe from any threats that may come over the web or email," Altinisik said. "With Forcepoint DLP, we now have full control over how we use our data, where it is sent, which data is critical and which is not critical, and we have full visibility to our user and data interaction. Forcepoint offers us an eagle-eye reporting opportunity."

Tupras was especially pleased with the easy DLP rollout. "We implemented our data security policies very quickly, especially using thousands of predefined DLP rules offered by Forcepoint. We also added some special policies to distinguish between good faith or malicious behavior," Altinisik said. "We can identify personal data as defined by our legal or audit team through filters and apply policies that restrict or block its transfer outside or inside the organization. As a consequence, users will no longer be able to upload, copy/paste or print personal data."

Having Forcepoint as a partner became even more important when the global situation changed radically. "Due to the COVID-19 outbreak, all our employees had to work from home, safe from cyber risk," Altinisik said. "We didn't have any concern about what we would do because we have Forcepoint Web Security Hybrid for 24-7 protection. Forcepoint quickly supported our transition to cloud security and better performance for web browsing."

Protected against external and internal threats

With Forcepoint solutions in place, Tupras is now meeting its goal of system-wide protection against both external and internal threats. The company is protected against botnet attacks from the web and attacks in emails with links that lead to phishing scams or ransomware, with Web Security blocking URLs that may cause a cyber-threat. The Forcepoint agent directly stops incoming email attack campaigns with the help of Web Security ACE Engine, while also protecting sensitive data from being exfiltrated via email, web and through popular endpoint channels like portable disk, printer and 3rd party apps.

Tupras is now meeting its own standards and regulatory guidelines for safeguarding critical data such as company IP, critical systems data, employee data, and financial data with robust, risk-adaptive Forcepoint Web Security and DLP.

"Forcepoint is a trusted advisor and information security solution partner for us," said Alper Sulan, CISO, Tupras. "They're our important assistant in terms of compliance with KVKK and similar regulations. They offer fully ensured Web Security and DLP, and at the same time, we know we can grow with Forcepoint in our digital transformation today and tomorrow as we consider solutions like CASB and Dynamic Edge Protection to protect us as we expand into the cloud."

Results

- **Better protection** against botnets, phishing attacks, ransomware, insider threats.
- **Simplified compliance** with data protection laws and standards.