

# Telepass: Keeping 6 million drivers safe from security threats

More than 6 million people use the onboard device created by Telepass to pay for highway tolls, parking, and more. A household name in its native Italy, Telepass is [the most widely used](#) electronic tolling system across Europe. It's used in 11 countries and offers a single, unified platform for paying tolls, parking fees, taxes, and even insurance.

"Security is a top priority for us," says Manuela Italia, Chief Information Security Officer at Telepass. "Every day, we use data to make mobility a better experience for our customers, and that makes protecting client information one of our main objectives at every organizational level." The company is under pressure to deliver for those drivers, too. Once the only tolling service provider in the country, Telepass now competes with alternative providers on convenience, availability, and integrity.

To do that, the Telepass team looked for a scalable solution to detect security events at speed, comply with complex regulations, and minimize disruption.

"We need to protect our 6 million customers from security threats using multiple services across international borders," says Italia. "[Chronicle](#) is the perfect partner in our threat hunting and detection process. It integrates easily across all of our security log sources, then unifies that data to find threats fast."

## Result

- Tracks security incidents 10 times faster than the previous solution by unifying data sources
- Helps meet compliance requirements for GDPR, PSD2, and Italian data protection laws
- Completes analysis of security events within hours, instead of days

## Containing threats before they spread

Companies operating in the EU must comply with strict regulations regarding data security and financial information. Compliance with GDPR means Telepass must report data breaches within 72 hours of the event, while the PSD2 financial data rules mandate rigorous oversight of multiple security domains, from CIAM to the company's Wi-Fi network. In addition, Italian privacy laws require that Telepass keeps secure and detailed records of all administrative access to systems for a minimum of six months.

Previously, Telepass was storing some data on [Google Cloud](#) and some within on-premises security logs and it was using [Google Cloud Monitoring](#) to track operations. Running multiple searches across different tools, added a lot of unnecessary layers to security protocols. Security investigations were time-consuming and, because the various security tools use different threat detection languages or syntax, locating the cause or the threat of any data breach often proved tricky.

The combined tasks of running multiple searches, writing in specialist syntax, and merging results delayed the company's response to events, reporting complex events within the 72-hour GDPR limit was sometimes challenging.

For comprehensive, scalable, fast-acting oversight across its entire architecture, Telepass chose [Chronicle Security](#). "You would typically expect a comprehensive security analytics solution to take at least three months to install," says Matteo Rosi, IT Cyber Security Expert at Telepass. "We might install syslog servers, configure hardware, create authentications, parse log sources. But with Chronicle it took one person less than two weeks to integrate all of the Google Cloud data, without the aid of a specialist system integrator. In less than a month all of our cloud services were integrated, providing complete coverage of all of our security log sources."

With Chronicle, Telepass runs comprehensive searches of its entire system, mapping out the extent and potential ramifications of a security event. From there, Telepass defines new automated actions with the Chronicle rule engine to evolve the system in anticipation of threats. And, by using the tool to evaluate the impact of security changes before they are applied, Chronicle supports decision-making on future developments.

"I recently searched for every connection from a malicious IP address to our infrastructure, communications, and buildings," says Rosi. "With one RegEx search, I could see each relevant log entry in just a few seconds, so that containment and analysis could begin. We completed a thorough investigation of the incident in just a few hours."

## Scaling to integrate new services and customers

According to Rosi, Telepass can now track and mitigate security incidents ten times faster than before, improving the company's protection of its 6 million customers and their information. The platform is compliant with the overlapping demands of GDPR, PSD2, and Italian law, too. And, as a SaaS tool with unlimited storage capacity, Chronicle is a perfect fit for the company strategy of data-driven growth. Unlike many Security Operations Centers (SOCs), Chronicle does not restrict Telepass to limits on space or events per second, so the team can send all logs to the solution without making complex predictions about future activity or provisioning new capacity.



**For us, Chronicle is more than a cutting-edge security tool. We use it to monitor operational activity, too. It informs our understanding of how colleagues use our infrastructure and gives us visibility over our entire environment. With that overview and these tools, the only limit is our imagination.**

– Manuela Italia, Chief Information Security Officer, Telepass

