splunk>

CASE STUDY

# One of Mexico's Largest Supermarket Chains Improves Response Times by 99%

### Key Challenges

A lack of visibility into Soriana's infrastructure led to higher risk of fraud and security issues, while delayed reporting processes and disparate platforms meant slower response and repair times.

### Key Results

Soriana gained real-time visibility into its hybrid infrastructure and all 15,000 points of sale, reducing MTTR, providing deeper insights to the security team and reducing fraud and security risks.

Soriana

**Industry:** Retail

**Solutions:** IT, Security, DevOps

## Where do you shop for essentials when you need them — fast?

Your baby runs out of diapers at 10 pm. You're restocking your pantry (how long does garlic powder last?). You have to pay off your credit card. Your teenager broke his cell phone. Again. For families in more than 280 municipalities and 32 states across Mexico, retail giant Soriana has been their one-stop shop for, well, pretty much everything, for decades.

To make shopping easier, Soriana offers both in-store experiences and app-based options to manage those diapers, banking services, groceries or cell phones. Behind the scenes, CISO Sergio Gonzalez and his security team are monitoring and securing the company's 40,000 devices (like servers and laptops) and 15,000 points of sale (POS) — all while keeping Soriana's digital systems running. In 2020, Soriana began its move to the cloud. With lots of servers processing a lot of data, monitoring a hybrid infrastructure was tough. They couldn't integrate their systems easily with the platforms they were using, so the security team had to take a swivel-chair-monitoring approach when responding to events, wasting valuable time.

Outdated reporting tools were also causing delays. Without real-time data or easy-to-read dashboards, information was coming into Gonzalez's team in Excel spreadsheets, slowing down remediation times. Another problem with the lack of visibility? Higher risk of fraud and, in certain cases, a higher mean time to repair (MTTR).

### Outcomes

**40,000+**
devices monitored and secured, including 15,000 POS

**96%**
faster mean time to repair for POS monitoring process to two hours, down from two days

**99%**
faster total incident detection, investigation and response time (30 minutes, down from 48 hours)

Seeking a complete view into its IT systems — and a better way to secure them — Soriana turned to Splunk Cloud Platform and Splunk Enterprise Security so it could unify and simplify its SOC to adapt better when digital disruptions came its way.

### Add to cart: 96% Faster MTTR and better business decisions

Soriana customers should be able to get their groceries or pay off their credit cards seamlessly, whether they do it in-store, online or on their phone. With so many POS devices to monitor and secure, having Splunk's unified security and observability platform was key for Gonzalez and his team. Now, they're able to monitor more effectively and rebound faster when issues arise.

Before, when stores had transactional IT issues, Gonzalez's team members would have to wade through information they received on Excel spreadsheets that might not arrive for two days to a whole week after the incident took place. Splunk's real-time dashboards provide alerts that allow them to automatically assign a support ticket to the service desk, taking a remediation process that once could take days down to thirty minutes. They can solve customers' transactional issues faster to improve the shopping experience, which is critical whether shoppers are purchasing in-store or online.

> Since deploying Splunk, we haven't had any critical security incidents. We're more resilient than ever."
>
> **Sergio Gonzalez**, CISO, Soriana

The benefits of real-time dashboards go beyond hugely improved MTTR and a more positive purchasing experience. "We can also now offer our finance teams more information, including better insight into customer behaviors," Gonzalez says. It's also a lot easier to show internal decision-makers the value and impact his security team has on the business — allowing Gonzalez to secure funding for other important projects that will continue to mature Soriana's security posture.

## They've got the receipts: Two years and zero critical security incidents

As a CISO, Gonzalez is responsible for finding ways to better prevent major incidents from impacting Soriana and its customers. The dashboard indicators his team relies on helps them monitor issues that start small and proactively address them before they get too big.

In the couple of years before transitioning to Splunk, Gonzalez recalled that Soriana had complex processes for detecting and handling security events. Since deploying Splunk Enterprise Security, the SOC's simplified processes empower the team to easily spot unusual behavior and suspicious traffic. "Now we can identify vulnerabilities in our systems we weren't able to before with other platforms," Gonzalez says. "With Splunk, we have what we need to improve our security strategy and better protect Soriana's assets and information."

Swivel-chair monitoring is also a thing of the past. "Since we could so easily integrate Splunk with our anti-phishing systems, for example, we can detect phishing attacks in real-time," Gonzalez says, as opposed to spending valuable time checking platform by platform. Now it might take only two hours for the whole process to detect and investigate threats, whereas before, they needed more than two days to just investigate — a 96% improvement.

## Moving easily to the cloud for comprehensive visibility and better compliance

Moving to the cloud and establishing a hybrid infrastructure can seem messy and complicated. But with Splunk and the help of Splunk partner ADV Consultores, Soriana deployed its Splunk instances, set up a SOC and integrated more than 1,000 components seamlessly across Azure and on-premises. It got all its records into Splunk in just a month.

The full-stack visibility they gained was crucial to fight fraud. "We used to have zero visibility surrounding fraud," Gonzalez says. Now they can do more prevention to protect customers when they're making purchases. The visibility helps them meet national compliance standards more easily, saving the company from potential legal and financial stress.

As Gonzalez looks to the future, he sees Splunk playing an even larger role in improving Soriana's business processes. A project is already underway to rely on Splunk for Soriana's SAP visibility and monitoring, and Gonzalez wants to dive into more automation with Splunk SOAR. "I'm very happy with Splunk. It's a powerful and reliable tool with powerful support — the product, the teams and the partners that come with it."



23-117456-Splunk-Soriana-CS-SS-101