SUCCESS STORY

FRANCE

PROFESSIONAL SERVICES

ELASTIC SECURITY

S3NS and Elastic deliver trust and sovereign cloud security for France

S3NS is a joint venture between Thales and Google Cloud, created to address a critical need for sovereign cloud solutions in Europe. With a mission to deliver trustworthy infrastructures to organizations handling sensitive data—such as government bodies, health providers, and critical infrastructure operators—S3NS combines the scalability and innovation of Google Cloud with Thales's world-class cybersecurity expertise.

This pioneering offer includes a sovereign Google Cloud Platform region operated independently of Google. Called 'Trusted Cloud', it runs in three French S3NS data centers on hardware accessible, operated and controlled only by S3NS personnel. At the heart of this solution, Elastic Security plays a critical role in delivering the highest level of data protection for French organizations.

Scales to provide sovereign SIEM platform

S3NS secures thousands of servers and containers by unifying large volumes of security-related data.

Boosts threat detection

S3NS security teams detect and investigate threats in near real-time.

Provides platform for AI innovation

Reduces false positives and improves alert prioritization with access to machine learning and AI capabilities.

Sovereignty and functionality: The best of both worlds

French organizations have long faced a trade-off between sovereignty and functionality. On one side are global cloud providers offering cost efficiency, scalability, and cutting-edge AI tools. On the other are local providers who prioritize sovereignty but often lack the scale, range of services, and economic efficiency that ambitious customers require.

With Trusted Cloud, organizations get the best of both worlds: operational independence and leading-edge technology. This includes cutting-edge cybersecurity orchestrated by an advanced security information and event management platform capable of managing massive volumes of logs and telemetry data.

There was no room for compromise when it came to security. “We needed a security partner with a solution that we could deploy on-premise to protect our self-managed Kubernetes-as-a-service platform,” says Victor Vuillard, CTO and CISO of S3NS. “We also sought advanced tools to support threat detection, investigation, and response.”

Elastic Security: The backbone of a sovereign cloud

When it came to selecting a partner, Elastic Security stood out for many reasons, including exceptional scalability. S3NS runs thousands of servers, often hosting thousands of containers. The volume of security-related data is enormous—and growing. Elastic's architecture enables S3NS to scale horizontally and cost-effectively while maintaining high performance. "Other SIEM platforms struggle to scale without data specialization. Crucially, Elastic has evolved beyond a data lake. It now possesses the processing and execution capabilities of a SIEM," says Vuillard.

Transparency was another winning feature. S3NS currently uses the commercial version of Elastic Security, but the availability of an open-source version enabled Vuillard and his team to inspect core logic and implementation, aligning with the organization's strict requirements for code and infrastructure review. In fact, Elastic's open APIs and clear documentation enabled full programmatic control over the deployment.

But it was Elastic's versatility across multiple security use cases that won the day. "Elastic excels at data handling," says Vuillard. "We use it to centralize logs from across our infrastructure, including compute, networking, and third-party security tools." S3NS also integrated external threat intelligence from Thales and other providers with Elastic to identify indicators of compromise, such as suspicious IP addresses or malware signatures.

In addition, S3NS's security teams use Elastic Security's built-in dashboards, scheduled queries, and alerting tools to detect and probe threats in near real-time. These investigations are traceable and thorough, thanks to Elastic's timeline tools and deep correlation capabilities.

> Elastic Security plays a vital role in helping S3NS build trust with customers, especially proactive security monitoring and rapid incident response.
>
> **Victor Vuillard**
> CTO and CISO,
> S3NS

Advanced AI out-of-the-box

Because of its tenant-isolation model, S3NS cannot access customers' workloads or data. However, it does monitor broader infrastructure signals, such as outbound traffic, and correlates these signals with threat intelligence. If, for example, a tenant's environment connects to a known command-and-control server, Elastic flags this behavior, allowing S3NS to notify the customer and support their investigation.

The deployment of Elastic Security also positions S3NS for future innovation. The team is exploring Elastic's machine learning anomaly detection and AI capabilities to help reduce false positives, detect anomalies, and prioritize alerts. These AI-powered tools are viewed not as replacements for human analysis, but as force multipliers, increasing the precision and efficiency of threat detection and the necessary response.

Vuillard stresses that S3NS's strategy extends beyond simply offering Google's managed services within the Google Cloud ecosystem. It also plans to integrate technologies and services from independent software vendors. "We anticipate providing an enhanced Elastic offering on our future cloud infrastructure, catering to French and European customers who prioritize sovereignty," he says.

In addition to using Elastic for security, S3NS is exploring the potential of Elastic observability and generative AI features. These include retrieval augmented generation and endpoint detection and response, where S3NS plans to deploy agents for endpoint security. This will enable the team to detect, investigate, and respond to threats in real time across their endpoint infrastructure.

> Elastic continues to support S3NS's broader cloud operations beyond cybersecurity. We particularly appreciate the frequent updates that align with the evolving landscape of our business.
>
> **Victor Vuillard**
> CTO and CISO,
> S3NS