Xolv
Case Study

Xolv offers a fully integrated suite of healthcare solutions ranging from clinical treatment operations to revenue cycle management that helps customers manage security risks and maintain compliance with ever-changing regulatory and clinical care standards. Xolv is part of a family of non-profit organizations – including Catalight, Easterseals Northern California, Easterseals Hawaii, and the BHPN (Behavioral Health Provider Network) – that work together to deliver home and community-based care.

Xolv delivers its suite of solutions using two types of apps. The first is customer-facing. Clients interact directly with the company through their phones or other mobile devices. The second is an internal family of apps – both mobile and web-based – used by behavioral interventionists who work with clients. Data is stored and correlated in SalesForce (SFDC) and sent back to the apps, all via APIs.

The company dedicates significant resources toward security. When one of its apps started getting a lot of errors, the security engineering team discovered that the web application firewall (WAF) was blocking legitimate activity incorrectly identified as an SQL injection (SQLi) attack. The company needed to find a security solution that could accurately and consistently differentiate API calls from SQLi attacks.

With eight robust apps in use plus another four or five under development, Xolv needed a solution that could automatically and continuously discover all its APIs, eliminate blind spots, assess risk, help vet the security posture of the APIs, and protect APIs from attack without throwing false security alerts.

Xolv ran demos of three separate solutions and quickly settled on Salt Security. “One of the solutions we considered needed our documentation of our APIs and endpoints,” says Jason Weitzman, senior security engineer, “but that’s part of the problem. We’re sure we don’t know about all our APIs.

Xolv’s fully integrated suite of healthcare solutions ranges from clinical treatment operations to revenue cycle management, helping organizations deliver quality care outside of the traditional hospital setting.

Headquarters Dublin, California

Founded 2017

Infrastructure AWS, CloudFlare, GCP

www.xolv.org

> *"The hard part was getting upper management to understand the difference between this [Salt] and our WAF. We explained that Salt is the brains for our WAF, that our WAF doesn't understand APIs but Salt does."*
>
> **Jason Weitzman,**
> **senior security engineer, Xolv**

"The hard part was getting upper management to understand the difference between this [Salt] and our WAF. We explained that Salt is the brains for our WAF, that our WAF doesn't understand APIs but Salt does," says Weitzman.

"Now that we have Salt, we've got a solid idea of what's out there, and we're protected in runtime," he continues. "We used Salt to find errors while transitioning between monitoring tools, and we were able to pinpoint APIs calls that were causing issues. I'm using my Salt dashboard to see all the APIs we manage in SFDC and GCP [Google Cloud Platform] and communications between GCP and AWS [Amazon Web Services]."

Salt Security empowers Xolv to discover internal, external, and third-party APIs, including granular details that define attack surfaces and assess risks.

Top use cases for Xolv:

- **find shadow APIs:** Xolv uses Salt to discover its full inventory of APIs and document them, including shadow or unknown APIs, along with the sensitive data they expose. Xolv can also leverage Salt to identify zombie APIs, or APIs that should have been deprecated.
- **prevent data exfiltration:** By leveraging the Salt API Context Engine (ACE) to identify abnormal behavior, the Xolv security team can stop attackers during the early stages of an attempted attack, automate that blocking as desired, and share insights to improve the company's API security posture.
- **prevent account misuse/fraud:** Xolv can configure the platform to automatically block this type of activity or send alerts with a full attack timeline to incident response teams to analyze the activity and block account misuse.
- **remediation to write better APIs:** Salt provides Xolv with remediation insights derived across build and runtime to help the company's development teams strengthen API security during the development phase.