



# oscar

Oscar's radical approach to healthcare requires unparalleled application security

## **CASE STUDY: ENTERPRISE APPLICATION SECURITY**

---

April 2015

## GOALS

- 1** Raise the bar for innovation, efficiency, integrated security and transparency in healthcare provider technology
  - 2** Earn users' trust by securing their identities against theft, fraud, and applicationlayer breaches
  - 3** Provide technology-enabled tools that promote better health outcomes and maintain engineering agility as company scales
- 

## THE SOLUTION

Oscar leveraged Prevoty's Runtime Application Self-Protection (RASP) suite of products to prevent application layer threats such as cross-site scripting (XSS), cross-site request forgery (CSRF) and SQL injections (SQLi). Partnering with Prevoty allows Oscar to continue delivering security at a level far beyond basic compliance requirements blocking data exfiltration, user identity theft and fraud, and brand defacement. The team is also able to refocus valuable engineering time and resources on developing feature-rich software.

---

## OSCAR TECHNOLOGY - FIRST AND FOREMOST: THE MEMBER IS EVERYTHING

Born in 2013 out of a vision to eliminate the confusion and inefficiency surrounding what it means to be a patient in today's U.S. health insurance system, Oscar Healthcare aims to increase access to care, boost transparency, and improve long-term health outcomes. Currently making its services available to the nearly 20 million citizens residing in the New York metropolitan area, the company emphasizes using simply designed, forward-thinking web and mobile applications to drive user enablement and satisfaction.

It's not easy being the newcomer to an industry long plagued by bureaucracy, regulatory constraints, legacy systems, and high-profile data breaches. Many watchful eyes are upon Oscar as the company enters a difficult market ripe for innovation.

*“Earning the trust of our members is a shared interest for everyone at Oscar. Building an insurance company is a significant undertaking for our engineering team, so we are very invested in security. One stumble can be devastating.”*

*- Mackenzie Kosut, Head of Technical Operations, Oscar Healthcare*

---

## OSCAR BREAKS THROUGH IN A WELL-ESTABLISHED MARKET

Not only is Oscar emerging as the first new privately owned insurance company in New York in 15 years, but they are also building the technology and infrastructure from scratch. Oscar's web and mobile applications also manage a tremendous throughput of sensitive personal data. Despite these challenges, Oscar's star-studded team, comprised of top talent from the fields of technology and healthcare administration, leapt at the opportunity to start with a clean slate and put due forethought and creativity into member interactions.

Today, Oscar’s simple, intuitive end-user facing applications power the majority of member interactions -- including on-demand tele-doctor appointments. It’s not hard to see that the company prioritizes superior technology and dead-simple usability. It’s something customers also appreciate:

 **Nate Poekert**  
@natepoekert ⚙️ Follow

The best customer service experience I've had in a while is from a health insurance company. Thank you @OscarHealth... #YouWonMeOver

 **Brian Singerman**  
@briansin ⚙️ Follow

First hand exp why @oscarhealth is so important: People NEED a catch all contact point for medical needs. Push a button, chat with doc.

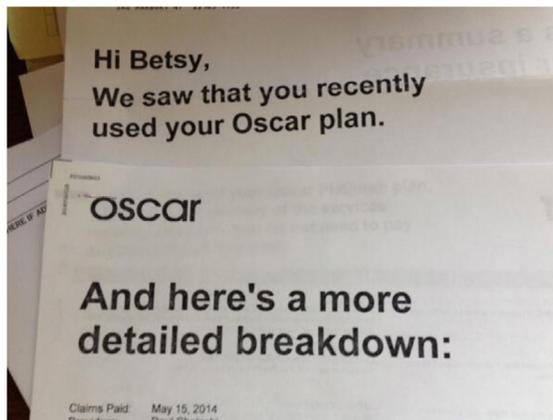
 **Sarah Doody**  
@sarahdoody ⚙️ Follow

Just used @OscarHealth's "have a doctor call you" feature. So helpful and friendly. Great customer experience. #cx

 **Betsy Kent**  
@bevisible ⚙️ Follow

@oscarhealth is amazing! they use normal language! check it out:

↩ Reply ↻ Retweet ★ Favorite ⋮ More



---

## CAN AGILE DEVELOPMENT AND SECURITY PLAY NICE?

Since Oscar uses applications as a primary mode of member engagement, it's mission-critical for the company to deliver complex healthcare management functionalities with an easy-to-use software experience. Moreover, due to constantly changing industry policies, even a two-week release cycle can sometimes be too slow for the fast-moving team. Oscar's engineering process is designed for rapid iteration and deployment -- moving from staging to production quickly using their own transparent, building-block version of the agile methodology.

*“A lot of popular enterprise software solutions get pushed on us, but we find that we only need a small part of each product's functionality. We keep a lean shop and try to build as much in-house as possible.”*

- Mackenzie Kosut, Head of Technical Operations, Oscar Healthcare

---

## INTEGRATED SECURITY

Everything at Oscar is built with an emphasis on security:

*“Security is not an afterthought at Oscar. We build everything with security in mind. We crunch a lot of valuable data, from a member's medical and patient history, prescriptions, premium payments, claims, family information, and other back-end data - it all bubbles its way up to the web, where people are securely accessing it”* - Mackenzie Kosut, Head of Technical

Operations, Oscar Healthcare

Oscar began investigating various pieces of open source software to complement their existing security measures, but soon found that they did not provide adequate coverage against sophisticated unknown (a.k.a. zero-day) application layer attacks.

Another priority for the Oscar team was to avoid the impact of “false positives” from their vulnerability scanners (i.e. potential vulnerabilities that after investigation turn out to be benign). With the development team permanently committed to critical business projects, time wasted hunting down these non-issues was becoming problematic. Oscar was hunting for more than just a one-size-fits-all solution with no contextual awareness.

---

## OSCAR AND PREVOTY: AN ALLIANCE FOR SUPERIOR APPLICATION DELIVERY

Oscar ultimately chose to team up with Prevoty to reinforce its Secure Software Development Life Cycle (SSDLC) with runtime self-protection capability. Prevoty's engineers worked alongside Oscar's security resources to develop an application security strategy and custom configuration that would automatically prevent threats with far less maintenance.

“Whatever out-of-the-box or open source solution you considered, Prevoty was doing it better, period. Take their token auth system, for example. Every popular web framework has CSRF protection, but only a service that is generating single use tokens will make it virtually impossible to orchestrate a replay attack. We at Oscar really want to go the extra mile, so it was a no-brainer to choose Prevoty.”

- Andrew Jones, Platform Engineer at Oscar Healthcare

With applications that could self-protect against targeted attacks automatically upon deployment, Oscar's in-house team kept up optimum productivity -- realizing a few benefits along the way:

### MORE THAN JUST COMPLIANCE

Oscar describes itself as “a new kind of health insurance company that is using technology to make insurance simple, intuitive, and human.” The company makes it a point to go beyond established industry baselines -- especially when it comes to garnering member trust and handling sensitive personal information. Oscar is able to partner with Prevoty and still exceed compliance requirements.

### THREAT PREVENTION

Prevoty's contextual security engine analyzes and sanitizes content, queries and state changing activities. Any attempts at cross-site scripting (XSS), SQL injection (SQLi), cross-site request forgery (CSRF) are prevented in real-time, without relying on past definitions or signatures. By including Prevoty, secure coding best practices are followed and vulnerabilities aren't just identified -- they are mitigated instantaneously.

Such runtime security allows Oscar's development team to dedicate more time to cranking out new features for deadlines without stalling due to the burden of security.

## PERFORMANCE

Application performance is a prized factor for Oscar's member experience. Luckily, Prevoty's solution is architected so that all the analysis and prevention is done in a matter of milliseconds. Deployment is easy too: it took Oscar less than one hour of one engineer's time to deploy the full Prevoty enterprise suite.

“Everything is humming along as it was before, and that is a beautiful demonstration of Prevoty. If security is done well, you don't even see it. Now there is an additional layer of protection for all our members and there was zero impact on our users or systems. It's something we really admire about the product.”

- Mackenzie Kosut, Head of Technical Operations, Oscar Healthcare

---

## THE BOTTOM LINE

A security breach for any organization is significant regardless, but in the healthcare space, the effects can be colossal: the negative impact on brand equity and loss of consumer confidence is compounded by large fines levied by regulators. By working with Prevoty, Oscar is off to a head start in avoiding these costs.

“In a way, we are insuring the health of our members, and in turn, Prevoty is insuring our sense of security and data. It's really hard to put a price on that.” - Mackenzie Kosut, Head of Technical Operations, Oscar Healthcare

More importantly, a partnership with Prevoty enables Oscar's development team to be more productive, focus its energy on developing a great product and spend less time worrying about application security. This means more opportunity to innovate and modernize healthcare in New York and beyond.

---

## ABOUT PREVOTY

Prevoty was founded in 2013 with a vision to revolutionize application security: why not enable applications to protect themselves?

Prevoty delivers breakthrough RASP (Runtime Application Self Protection), making it easy for security professionals and application developers to block top application layer attacks automatically, eliminate vulnerabilities, and secure both legacy and new software. In-app calls to Prevoty's contextual security engine validate inputs, queries and user tokens before they hit your application and database.