



CUSTOMER SUCCESS STORY

# **Shutterfly Protects Customer Data and Increases Security With Imperva**

## Shutterfly at a glance

Shutterfly, Inc. is a leading digital retailer and manufacturer of high-quality personalized products and services. Founded in 1999, Shutterfly brings photos to life in photo books, gifts, cards, and stationery through its flagship Shutterfly products. Shutterfly sells premium offerings, wedding invitations, and stationaries through its Tiny Prints boutique, rents photographic and video equipment through BorrowLenses, and operates Shutterfly Business Solutions, an enterprise market company that delivers high-quality digital printing services. Shutterfly recently announced a definitive agreement to acquire Lifetouch, the leader in school photography.

## Security challenge

All companies rely on applications to drive business; but at Shutterfly, applications are the business. Its custom-built, self-service web applications enable customers to store photography, videos, and art in a single location, and create personalized products with them. With so much business value concentrated in web applications, application security is of the utmost importance to Shutterfly.

## Solution evaluation

Shutterfly approached Prevoty, the application security solution provider that is now part of Imperva, in search of a runtime application self-protection (RASP) solution that could mitigate risk to its portfolio of applications. The company evaluated Prevoty RASP against several other application security products and RASP vendors. Shutterfly required a solution that would deliver effective application security protection, and:

- Efficiently and accurately detect and prevent attacks.
- Have low overhead and not require dedicated resources.
- Integrate seamlessly into agile DevOps cycles and scale with ever-growing needs.
- Increase the company's overall security posture.

RASP was able to deliver the real-time attack protection Shutterfly needed, and meet all its performance criteria.

Aaron Peck, who heads Shutterfly's information security team, explains how the company came to select RASP: "We initially investigated RASP as an option for protecting our most critical web properties and as a tool that could buy our engineers more time to clean up our backlog of vulnerabilities. We previously used a web application firewall (WAF) but found that it created a bottleneck in our environment – which experiences massive bandwidth peaks and needs to have tight engineer engagement in order to effectively manage rulesets. We needed something that a small team could deploy quickly and run without much day-to-day support from engineering. On our smaller web properties, RASP was deployed with ease and immediately provided protection without operational impact. This led us to the decision to push forward with RASP as our primary preventative application security control."

## Deployment

RASP plugins enable applications to protect themselves leveraging a lightning-fast, attack detection method called Language Theoretic Security (LANGSEC) that understands how payloads will execute within the context of a given application and neutralizes both known and zero-day attacks.

### ABOUT RUNTIME APPLICATION SELF-PROTECTION

RASP is a Runtime Application Self-Protection solution that protects legacy and modern applications in production by monitoring attack data at run-time with real-time context and situational awareness. For more information, visit <https://www.prevoty.com/products>.

The RASP plugin is completely self-contained, portable, and works in any type of deployment architecture including on-premise or in the cloud.

Shutterfly deployed RASP plugins into a sample set of its applications to review impacts before pushing them enterprise-wide. After finding that it did not impede development cycles or application performance, Shutterfly integrated RASP into its deployment processes for critical applications. The RASP plugin is now an artifact of each application as it is deployed.

## Immediate benefits

Shutterfly's application development teams managed a backlog of known vulnerabilities that was long and prioritized into critical, moderate, and low-severity sub-lists. By using RASP, Shutterfly was able to slash its backlog of vulnerabilities and reduce the criticality of all its vulnerabilities by at least one level.

RASP boosted the security team's confidence in their application security posture when apps are deployed with known vulnerabilities. RASP provides a layer of defense that prevents vulnerabilities from being exploited by nefarious actors, buying the company time to prioritize mitigation in correlation with other business objectives.

"RASP's blocking technology has been incredibly effective at covering gaps and providing risk reduction that allows us to focus on engaging engineering teams early in the development lifecycle. We can focus on static analysis, building secure libraries and training versus reporting and pressing on vulnerability closure. We have also built correlation around blocking patterns, threat feed data, and other activity in our monitoring platform to increase the effectiveness of our SOC and its ability to respond to threats quickly." said Peck.

In addition to delivering effective application security, RASP also delivers on Shutterfly's performance success criteria, including:

### 1. Efficiently and accurately detecting and preventing attacks

RASP is based on a unique and efficient analysis engine that accurately identifies and neutralizes application-level attacks in real time using a grammar-based security analysis technique called LangSec. LangSec processes and evaluates all incoming application data, with no dependence on definitions, patterns, regular expressions, taint analysis or behavioral learning. By understanding how data will execute in an environment, it effectively prevents any obfuscation or fuzzing of data input. Identified threats are sanitized with context, nullified in real time, and logged, thus safeguarding confidential data and protecting organizations.

### 2. Be low on overhead and not require dedicated resources

RASP deploys quickly and quietly. Shutterfly's deployment of RASP is unobtrusive, allowing business to go on as usual without disrupting user experience, and delivering real, tangible value very quickly.

### 3. Integrate seamlessly into agile DevOps cycles and scale with future needs

RASP pinpoints and logs the attacks it blocks and neutralizes - down to the exact line of code that an attack tried to exploit. This real-time attack telemetry has enabled Shutterfly to augment how security is integrated into its DevOps cycles. Shutterfly developers now spend less time chasing long backlogs of vulnerabilities that essentially amount to theoretical threats, because they know exactly where they are being attacked, and can rest assured that those attacks will be blocked by RASP until a patch is implemented in the application code.

**“On our smaller web properties, RASP was deployed with ease and immediately provided protection without operational impact. This led us to the decision to push forward with RASP as our primary preventative application security control.”**

Aaron Peck, Head of Shutterfly's Information Security

This leaves Shutterfly developers with more time to do what developers do best - deliver new features and capabilities to their end users.

#### **4. Increase the company's overall security posture**

RASP arms Shutterfly with visibility into application security events in production. RASP lives and travels with applications, monitoring and logging all runtime security events. Attack telemetry and transactional data is pushed to the SIEM Shutterfly already has in place via certified first-party apps that include actionable dashboards and reports.

### **Security by default**

RASP enables Shutterfly's applications to become secure by default so that its developers can focus on building applications that solve problems, connecting people and driving business—knowing that RASP will keep them secure.

### **Results**

Shutterfly's challenges aren't unique. Security teams are commonly mandated to establish robust, mature security programs with tight budgets and small teams. As development speed, deployment frequency, and attack sophistication intensify, implementing automated, attack-based security solutions becomes imperative. With RASP, Shutterfly's applications are pushed to production faster, at scale, and with security on-board.