Prevoty

CASE STUDY

The retail and e-commerce company needed a solution that could secure its applications without slowing down aggressive, continuous development cycles.

AARON'S, INC. SAFEGUARDS ITS APPLICATIONS WITH PREVOTY AUTONOMOUS APPLICATION PROTECTION

August 2017

Protecting Aaron's, Inc. Applications With Prevoty

Headquartered in Atlanta, Aaron's, Inc. is a 3.2 billion dollar omni-channel provider of lease-purchase solutions that was founded in 1955 and has been publicly traded since 1982. Aaron's, Inc. owns the brands Aaron's, Progressive Leasing and HELPcard. The company sells and leases furniture, consumer electronics, home appliances and accessories through more than 1,860 company-operated and franchised stores in 47 states and Canada and its e-commerce platform Aarons.com. Progressive Leasing, a virtual lease-to-own company, provides lease-purchase solutions through approximately 19,000 retail locations in 46 states. The company's second-look credit arm, HELPcard, provides a variety of credit products that are originated through a federally insured bank.

Aaron's sought out Prevoty in search of a runtime application self-protection (RASP) solution that could mitigate risk to its portfolio of highly customized apps with unique business, legal and regulatory requirements. A solution that could fit into the company's agile culture and enable rapid development cycles was a must, as well as a tool that would empower developers to integrate security into a DevSecOps cycle without "cramming security down their throats."

"Prevoty has been a real force multiplier for our application security program. It has enabled us to move fast and scale while providing enhanced visibility and security as we embed core DevSecOps principles in our organization."

- Almir Hadzialjevic
VP of Enterprise Risk & Security, Aaron's, Inc.

DevOps Approach

Prevoty can be the impetus that puts the sec in DevSecOps. Aaron's began its deployment with a kick-off that brought developers and security practitioners together to align

configuration with business needs. Developers identified what the most critical applications needed to do, and security teams configured Prevoty to meet those business requirements. Developers were empowered to enable or disable Prevoty, test, tune, troubleshoot and access security logs through integration with Splunk. Prevoty instilled Aaron's developers with the confidence to be more aggressive with app deployments. Unlike web application firewalls (WAFs) that often made them nervous because of their potentially obstructive impact on production, Prevoty provides peace of mind because it deploys quietly and allows business to go on as usual without disrupting user experience.

> "Prevoty allows us to take a lot more risk and be more aggressive with our deployments in our highly customized environment."

Risk Mitigation

Risk mitigation was Aaron's highest priority. Prevoty adds a different kind of layer of security to their stack, akin to a special ops unit inside their perimeter. The increased monitoring and visibility Prevoty delivers, plus its real-time defense capabilities, provide Aaron's with an immediate reduction in risk to both known and zero-day attacks.

> "Even if we don't know about a risk today, we know Prevoty provides a different layer of security on our most critical apps. It has really helped us avoid those risks going forward."

Aaron's also discovered that Prevoty's mitigation capabilities drive some interesting insights. Prevoty enables visibility into which applications are most targeted by injection and scripting attacks, which helps them know where they need to invest their resources on fixing vulnerabilities. "It's what we internally refer to as attack-fix-insight, which is something that starts with mitigation," said David Nolan, Director of Information Security at Aaron's. "When we see that someone is determined to get into a particular app and we've got the data to prove it, we can then go to the team and say, 'Let's actually fix this thing.' "

Protection

Many development teams have a back-log of security vulnerabilities that they know they should fix. They believe security is important and want to resolve them, but a developer's first priority is pushing applications into production. Aaron's uses Prevoty's security-by-default capability as an automatic mitigation of the known vulnerabilities that the team doesn't have the time or resources to address right away. Turning Prevoty on defends the applications until the time and resources are available to implement a proper fix.

"When the team has vulnerabilities they want to fix, but don't have the time or money, we say, 'Great, while you find the time and money, we're going to go ahead and turn Prevoty on.'"

In a breach scenario, when security leaders need to show progress quickly, Prevoty is a great option. "If you've got it deployed out there – even just in monitor mode – and all of the sudden you start seeing some action, within the span of seconds, you can turn Prevoty on and have defenses up. So that's pretty cool," said Nolan.

Intelligence

Protection is great but so is intelligence. Before deploying Prevoty, Aaron's did not have visibility into application security events in production and particularly struggled with limited visibility into access and exfiltration attempts. Prevoty lives and travels within the application, logging all runtime security events to dashboards that monitor and visualize the who, what, when and where of security events. These insights can be fed into any SIEM or analytical platform for any number of use cases including incident response, fraud detection, even line-of-business use cases.

"Unprecedented visibility translates into valuable intelligence."

Cost of Ownership

Prevoty is significantly less expensive than a WAF. While WAFs require dedicated personnel to deploy and maintain, Prevoty is designed to fit into the organization that's already in place. Its architecture is light, quick to deploy and easy to maintain in production, resulting in substantial savings. "It's a money saver. It's to the level that I probably have less than a quarter of a full-time equivalent dedicated to Prevoty," said Nolan.

"A WAF can require two full-time staff members dedicated to deployment and support. Prevoty requires two hours a week from one staff member. And it protects better. "

- David Nolan
Director of Information Security, Aaron's, Inc.

About Prevoty

Prevoty protected applications are secure by default. Prevoty delivers powerful Autonomous Application Protection via its runtime application self-protection (RASP) technology. It enables fast, efficient and secure software development life cycles, monitors and protects applications at runtime, and neutralizes known and zero-day attacks.