CASE STUDY

Revenera Improves End-Customer Service with Wallarm API Security

Revenera eliminates 100% of bad traffic hitting their applications

Overview

- Modernization effort included a) moving from data center to AWS, b) eliminating multiple points of entry to applications with Kong API Gateway, and c) introducing API security to protect customers and operations.
- Main motivations were improving productivity and security, especially reducing threats hitting applications directly which required a lot of effort being replicated across all access points.
- Results include: incidents reduced to zero; improved visibility into and management of traffic sources; and minimal added latency.
- End-customer benefits include: reduced CPU utilization; improved rate limits; and a demonstrable API security story which they can see and understand.

> “We've made an investment in Wallarm API Security because we believe it’s the best there is on the market and it fits our needs really well.”
>
> Revenera

About Revenera

Revenera, born as InstallShield and now a Flexera company, helps software and technology companies use open source solutions more effectively, and provides software development, consulting, training and revenue recovery services.

>35,000 customers

worldwide

>37M entitlements & $40B in revenue

managed and protected per year

100 component instances

serving millions of devices and end users

Challenge

Revenera faced several challenges on their modernization journey, intended to improve both productivity and security and to provide their end users with even better service and more innovative solutions.

First, they were starting from scratch and had to manage a multi-pronged modernization effort:

Moving to **a cloud-based approach** powered by AWS to provide their customers with improved availability and scalability.

Shifting **to a single point of entry** for all applications to reduce security and management overhead.

Introducing **API security** to protect customers and operations.

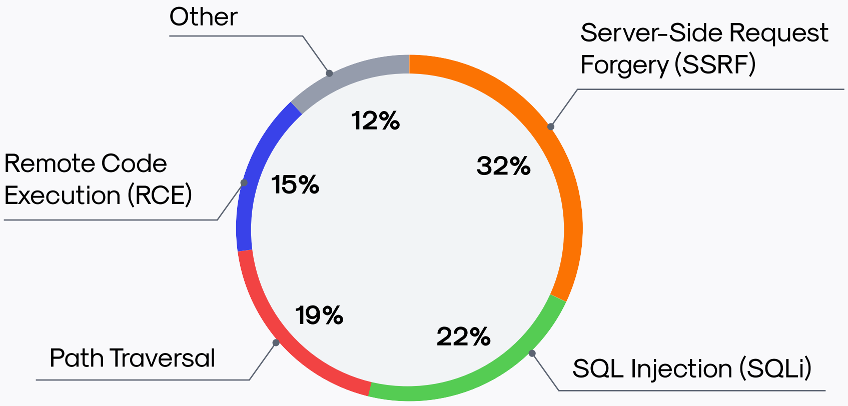
In addition, even after this modernization effort they would still have legacy applications along with APIs which utilize a variety of protocols (SOAP, REST, GraphQL) – all of which needed to be equally protected with a single solution.

Finally, they needed an off-the-shelf API security solution which was immediately effective – meaning filtering out as much of the bad traffic as possible – and easily deployed and integrated into the new tech stack.

Overall, this modernization effort allowed Revenera to start fresh, to implement current best practices, and get a leg up on their competition.

Top Attack Types

Top attack types blocked by Wallarm over 3-month sample period.



Solution

Revenera tried out several different vendors, and looked at how much bad traffic was coming through each of those vendors. Wallarm was the best at filtering out the bad traffic, outpacing some bigger, better-known competitors.

Some other factors came into play:

Ease of Deployment. Wallarm works very nicely as a plug-in solution into their new Kong API Gateway. And the way it's deployed means that it's very low touch for Revenera, as it's automatically updated.

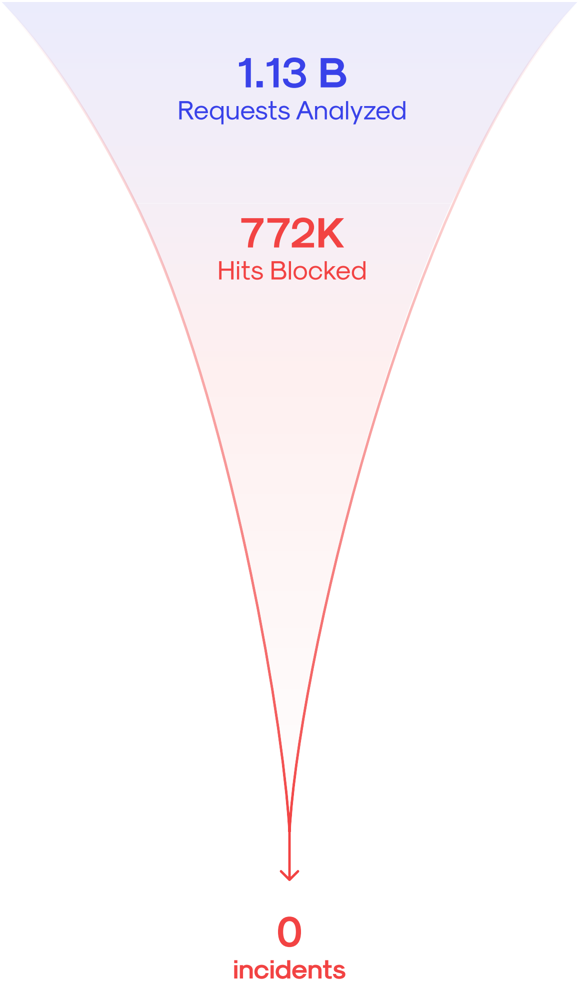
Full Protocol Support. Wallarm provides coverage for all current applications and protocols, allowing Revenera to manage their entire fleet with just one platform.

Customer Care. Wallarm experts helped immensely during the evaluation phase to understand where Revenera was going with the new infrastructure using Kubernetes on AWS and the Kong API Gateway to ensure the deployment went as smoothly as possible.

And it didn't end with the evaluation phase. As Rob Davies, VP of Engineering and Lead Architect at Revenera said:

Filtering Bad Traffic, Reducing the Strain

In Summer 2023 (Jun-Aug), Wallarm analyzed a total of 1.13B requests and blocked 772,000 attacks (or 1 every 10 seconds) – as a result, Revenera had zero (0) incidents all summer long!



> "I would give Wallarm a 9.8 out of 10, if not a 10 itself. One of the things we got from the services team at Wallarm when we were doing initial implementation was advice on the best way to do things. And they gave us a lot of good advice. But it wasn't just advice: they gave us a good technical overview; they gave us diagrams. So, they translated what we had told them into a pictorial representation, which they gave back to us, which was great. We don't see that from too many partners or vendors going to that level of detail. And I think in all our interactions since – if it's support or any other aspect of Wallarm – have been very professional, very friendly, and very responsive, which you don't get that from many vendors or partners either."

Outcomes

Before undergoing this transformation, Revenera had little insight into the bad traffic hitting their applications. With Wallarm, they are analyzing an average of over 12M requests per day with near-zero latency, and blocking almost 8,400 hits – resulting in zero (0) incidents. For Revenera, this highlights how much bad traffic they were letting go directly through to their applications before they had Wallarm in place – and forcing their applications in FlexNet Operations to deal with that.

> "I would absolutely recommend Wallarm, in a heartbeat. They do what they say on the tin – meaning what they say they can do, they really do."
>
> – Rob Davies, VP of Engineering and Lead Architect at Revenera

Other benefits that Revenera are enjoying include:

Better Control. Wallarm improves visibility into and management of traffic sources, with ability to automatically gray list certain IP ranges and deny list designated geographical locations – which not only improves security but does so with no additional effort.

Low Maintenance. With Wallarm installed and running in their gateway, Revenera can just let it run without really having to touch it again.

Improved Service Delivery. With Wallarm filtering out all the bad traffic, Revenera sees reduced CPU loads and can improve rate limits for end customers without requiring additional back-end resources.

In addition, having Wallarm in place also provides Revenera a very good security story to give their end customers. It's one that they can demonstrate to their end customers, point to both tangible and proactive benefits, and allows end customers to feel good that their use of FlexNet Operations is secure from that point of view as well.

About Wallarm

Wallarm, the integrated App and API Security company, provides robust protection for APIs, web applications, microservices, and serverless workloads running in cloud-native environments. Wallarm is the preferred choice of hundreds of Security and DevOps teams for comprehensive discovery of web apps and API endpoints, protection against emerging threats throughout their API portfolio, and automated incident response to enhance risk management. Our platform supports modern tech stacks, offering dozens of deployment options in cloud and Kubernetes-based environments, and also provides a full cloud solution. Wallarm is headquartered in San Francisco, California, and is backed by Toba Capital, Y Combinator, Partech, and other investors.

Learn more at www.wallarm.com or connect with one of our security experts here to learn how we can help you protect your web app and API portfolio.