SHIELDX

Case Study: Alaska Airlines

ShieldX ESP Allows Alaska Airlines To Automate Security Policies And Migrate Faster To Cloud

HIGHLIGHTS

The Adaptive Intention Engine is fantastic. It allows us to develop security policies using the language of our internal customers. It's machine-learning applied to security workflows. That allows us to much more easily construct the policies that will protect those workflows....It takes the exact same policies that you would apply to your on-premise environment and enables you to simply apply them to the cloud. It becomes one policy for both on-prem and for the cloud.

ShieldX also enables us to migrate to cloud environments faster. That is an important part of it for sure because it takes the exact same policies that we would apply to our on-premise environment and enables us to simply apply them to the cloud. It becomes one policy for both on-prem and for the cloud.

ABOUT ALASKA AIRLINES

Alaska Airlines is a major American airline headquartered in SeaTac, Washington, within the Seattle metropolitan area. It is the fifth largest airline in the United States when measured by fleet size, scheduled passengers carried, and the number of destinations served. Alaska, together with its regional partners Horizon Air and SkyWest Airlines, operate a large domestic route network, primarily focused on connecting from the Pacific Northwest and Alaska to over one hundred destinations in the contiguous United States, Hawaii, Canada, Costa Rica, and Mexico.

What is our primary use case?

Our primary use case is to provide microsegmentation and microsecurity controls in a multi-cloud and multi-data center environment.

How has it helped our organization?

The primary driver, as far as how it improves our business, is that rather than having to have infrastructure teams work with our application teams on a very long and complex process to help identify the security controls and the firewall rules that should be applied to their applications, we're able to take that - say, two-week effort - down to hours, using machine-learning, in order to construct those rules automatically. ShieldX makes the cloud safer than on-prem deployments. That is because that the number- one cause of security incidents today is human error, and those errors are often a result of very complex security structures.
ShieldX makes it a lot easier and a lot simpler to define your policies and define your rules, and that greatly reduces the opportunity for user error.

What is most valuable?

The primary features are being able to isolate and segment workloads, both within our data center and in the cloud, and to get visibility into what the applications are doing. The application visibility is the most important feature for us at the moment. The reason that it is so important is that we are migrating a lot of workloads from a legacy data center to a new data center, and that ability to have visibility into the application flows allows us to build the rules and policies for the newer data center. The Adaptive Intention Engine is fantastic. It allows us to develop security policies using the language of our internal customers. It's machine- learning applied to security workflows. That allows us to much more easily construct the policies that will protect those workflows. ShieldX also enables us to migrate to cloud environments faster. That is an important part of it for sure because it takes the exact same policies that we would apply to our on-premise environment and enables us to simply apply them to the cloud. It becomes one policy for both on-prem and for the cloud. It gives us a lower dollar-per-protected-megabyte than a traditional firewall, but it's also consuming fewer resources in our network environment because we're not having to send our traffic out of the virtual environment just to send it back in. It also helps with lower maintenance costs.

What needs improvement?

The product is pretty good today. The areas of improvement are primarily going to be around resource consumption. With any kind of tool like ShieldX, where you're in the cloud instead of a traditional firewall, you're using CPU resources in those environments to provide the protection. So there's a cost associated with CPU resources. I'm pressing upon them to make the product much more efficient and use less CPUs to do the same thing.

How long has Alaska used the solution?

One to three years.

What do I think about the stability of the solution?

The stability is very good. This is one of the strengths in the way that ShieldX works. They've essentially created a button to easily turn it off in case things are not running well. Honestly, it's been very stable, but we have a one-button click that will disable ShieldX from the environment in the event that it is going disastrously wrong. We've never had to do that, but it's there and we've tested it and it works. I'm really comfortable with both stability and the ability to address problems in the event that the system isn't working well.

What do I think about the scalability of the solution?

There are two parts to the scalability. The first part is that for virtual firewall-types of platforms, virtual security controls, and virtual microsegmentation controls, they scale better than anyone in the industry. The key differentiator there is that they've implemented what they refer to as microservices. In a traditional, virtual firewall - a Palo Alto, Check Point, or Fortinet-type of firewall - if you virtualize it, in the event you need more capacity, you're just adding CPUs to the firewall as a whole. ShieldX has taken every single service that is required to protect workloads and instantiated them as individual services that can individually scale. That's really important because if, for example, SSL decryption - which is one of the most CPU-intensive functions - needs additional horsepower, we can provide CPUs just to SSL decryption, without having to provide CPUs to an entire monolithic firewall. That's really key to ShieldX's story and there's no one else in the industry that does that. I can scale horizontally as far as I can imagine. As long as I've got the CPU resources, I can continue to scale it. The second part is the downside. Compared to a traditional firewall, which isn't really a fair comparison, you're not taking advantage of ASICs. You don't have hardware-based firewall processing. You're dependent upon standard Intel CPUs, and that's where we want ShieldX to get more efficient in how they're using those CPUs so that we're using less of them. We have about 2,000 servers currently protected. We will continue to grow. It's in the heart of our data center, so as we grow our data center, the ShieldX environment grows along with it.

How are customer service and technical support?

We have used their tech support but because of our early adoption we have not been calling an "800" number. We've been calling the CTO.

Which solution did I use previously and why did I switch?

Prior to ShieldX, we were using very traditional security controls, meaning traditional perimeter firewalls. We switched to ShieldX because traditional firewalls are more expensive, and they require you to take all of your traffic outside of your virtual environment to inspect it and then return it back to the virtual environment. ShieldX lives inside of your virtual environment so it's able to protect your workloads without having to send them north to a firewall only to come back down south to another resource.

How was the initial setup?

The setup is pretty straightforward. It's fairly easy to install. It's fairly to administer. It's intuitive. Where it is complex is that you have to think about security in a different way, so you have to spend some time up front figuring out how you're going to define the tags that secure your resources. You have to think about how you want to segment your network, how you want to segment your applications in a way that's a little bit more abstract than what firewall administrators are used to. The complexity is not in the setup of the product itself but, rather, in the planning beforehand. From install to testing to what we would consider production, it took about two weeks. There were about two months of planning ahead of that, but the actual deployment, where we were installing it, testing it, tweaking it, configuring it, was a couple of weeks. I would stress that our environment is complex and we were customer number-one. We were learning a lot through those two weeks. We could probably do it in two hours now. Our strategy was to first put it into our QA environment, in a visibility-only mode. ShieldX can operate as just providing visibility, and then you can tell it to actually start enforcing the security controls. Our strategy was first to do QA, ahead of production, and, in both of those cases, to first do it visibility mode only. That let us learn about the environment, and let ShieldX learn about the environment, so that the Intention Engine could go to work. Then, in a future phase, we would come back around and enable the controls so that it actually started blocking bad traffic.

What about the implementation team?

We partnered directly with ShieldX. Our experience with them was very positive. They have a fantastic engineering team. Again, we were customer number-one, so we were directly interfacing with the people who are writing the code and developing the product. That might not be normal.

What was our ROI?

With security, it's hard to articulate a return on the investment. It's a cost burden. We could probably say that it's a lower cost burden, but I think that we're a year out from being able to really determine that. I believe that it is a lower cost to operate. For sure it's going to be a lower cost to create the security controls. Probably in a year's time we'll know more. We'll see that our AppDev teams are able to build their own security policies, for example, but that's more of a vision statement than it is reality, right now.

What's my experience with pricing, setup cost, and licensing?

Pricing is on par with some of the better firewalls. ShieldX's licensing model is based on bandwidth consumption, and that part is a little bit different. They're priced more the way cloud services are priced, which is a right fit for this type of product. You pay by the amount of workloads that need to be protected. If you look at what it would take on traditional firewalls to do the same, ShieldX will be less expensive. The difference, though, and what enterprises are getting their heads wrapped around, is that it's licensing like the cloud, which traditional firewalls aren't quite like. With the latter, you buy a big box and you size it accordingly. So you do have to think about how much bandwidth is going through the ShieldX environment. There is an issue that our company, particularly struggles with. I'm sure that we're not alone, but because licensing is, again, different, you're not buying a physical box. A physical box is capital asset. Because you're not buying a capital asset, and instead you're buying what is essentially a subscription license, you're taking costs that normally would've been capital cost and you're shifting them over to operating expense. Not all enterprises are set up to deal with operating expenses like this. Cloud has taken us there and it's forcing the conversation, but it is a change in paradigms. We're not capitalizing big pieces of hardware anymore. We're buying subscription services. There's a budgetary difference there.

Which other solutions did I evaluate?

We evaluated vArmour and Illumio. They didn't meet our requirements. ShieldX is a superior solution and I can give you the quick differences: Illumio is really an orchestrator so it's not providing security controls. It is managing the security controls provided by the operating system. It manages Windows Firewall, for example. vArmour, which is a closer comparison to ShieldX because it does provide security controls inside of the virtual environment, is one of those monolithic firewalls, so it does not scale as well.

What other advice do I have?

The advice here really is two-fold. The first is a comment I made earlier. The bulk of the security incidents that are going to be made in the environment that security professionals will be working in, in 2019, are going to be caused by human error. More than 80 percent of all of the security incidents that were reported last year in the cloud were a result of human error. So my advice is to get a solution that is dead-easy to administer and one that is not being done in the types of controls that we're used to in traditional firewalls: IP addresses, ports, protocols. We've got to stop thinking about it that way and start thinking about the language of our customers, such as the applications that they need to protect, as opposed to the ports and protocols they need to protect. Number two is that with a traditional approach to firewalls, you do not have visibility in east/west traffic inside of your virtual environment, inside of your data center, and it's no longer enough to simply segment. You've got to segment and secure the segments. Separating traffic isn't enough. You've got to put controls around the segments, meaning microsecurity in addition to microsegmentation. If we go beyond security professionals, my advice to senior management, people like me, is going to be around making sure that you're prepared, from the top down, to be supportive of a change in model in security so that you are driving security through your AppDev teams and through your DevOps teams. What you really want to do is make it dead-simple, super easy for those folks to develop secure applications. You're going to do that by taking security and reframing it into the words and language that they use instead of the words and language that a network engineer uses. We were an early adopter, and our company worked with ShieldX as they were launching the product, so we've been engaged with ShieldX for about two years, prior to the product launch, mostly helping to shape the vision of the product. As far as who is administrating ShieldX, we have about a dozen people, and that would include traditional firewall administrators, but also our DevOps teams. The teams that are developing the automated pipelines to build servers, they're also using it to automate the application of the security controls. Staffing for deployment and maintenance is similar to how you would think about traditional firewalls. If I had a team of four people that were administering my firewall and security controls in a traditional environment, I'd probably still have the same, and that's about the number we have. They are security engineers. I would rate ShieldX at eight out of ten. This product is hitting all of the marks for us. I would put it at a nine if the CPU utilization was lower. They're getting there and that's on their roadmap. It's a part of developing a new product. You first build the features and then you tune it and make it more efficient, so they're focused on efficiency right now.

ShieldX Networks, Inc.
2025 Gateway Place, Suite 400
San Jose, CA 95110 USA

+1 408.758.9400
info@shieldx.com
www.shieldx.com

December 2019