A10 Thunder TPS

Review From A Customer

IT Central Station
Unbiased reviews from the tech community

A10 Thunder TPS

Read 6 reviews of A10 Thunder TPS

From IT Central Station, the leading review site for enterprise technology solutions.

Review by a Real User

Verified by IT Central Station

Co-Founder at Acorus Networks

Raphael Maunier

WHAT IS OUR PRIMARY USE CASE?

We work like an MSSP. We provide massive capacity and other network capacity to customers. We have customers connect anywhere on back burn. It can be in Europe. It can be in the US or in Asia. We plug the attack anywhere on the back burn, trying plug the attack closest to the source of the attack. So, we don't work like all the other guys who do scrubbing centers. We try to build a scrubbing network. That is why we need to buy more TPS in order to be distributive. When we start to work with the customer, we don't know what they have. The goal for them is to be able to block any type of massive volume metric attack. The reason is why we have about a two terabytes capacity and are building to afford three to four terabytes of capacity. Therefore, anytime the customer needs to block something, we can configure for them any type of custom role. We are using them for a mitigation offer that we have globally. We have a bunch of A10s and will deploy more in a few weeks. We use both the hardware and software.

HOW HAS IT HELPED MY ORGANIZATION?

We started with them and built our network based on this solution. We started with them directly from scratch. The automation makes our team more efficient and productive. We are distributed and don't use the A10 Portal. It's easy for us to deploy. E.g., they have an aGalaxy product. Instead of connecting to all the boxes, so we will have the A10 box. We don't want to send a code to all the A10 boxes. We will just send the information to one box: the A10 aGalaxy. This one box will proxy it and send the information all the other boxes. This is exactly what we are doing today. It has improved the way that we are working.

WHAT IS MOST VALUABLE?

We use all the features, but our customers have started asking for key features around SIP. We are also using some proxy features. The solution’s response time to an attack is fast. When it is configured in line, it is automatically done. When we have to stop the attack, it takes 10 to 15 seconds. We selected the solution because of its programmable automated defense using RESTful API. We didn't want to connect to the box. We wanted to be able to do some automation. We wanted to have our own portal because we wanted to connect our customers to our own UI using the A10 API. It has been good and exactly what we need. The TPS has reduced the amount of manual intervention required during an attack. When we have an attack, and we need to block some stuff everywhere, we just click on a button and push the rules. Then, it's deployed in Asia, Europe, and US. We don't have to do anything more. The aGalaxy is a control plane for the product. It controls the entire TPS so you don't have to connect to the box. You just have to connect to this control plane.

A10 Thunder TPS

Read 6 reviews of A10 Thunder TPS

WHAT NEEDS IMPROVEMENT?

The solution’s machine-learning-powered Zero-day Automated Protection (ZAP) works for enterprise customers, but for MSSPs, we have too much traffic and analytics. Therefore, it is unusable and A10 is working on a new feature that we requested. It should be ready in two weeks. We have to be able to do some automatic rules proposals based on what is detected. We use this product internally and this feature hasn't been ready for the last eighteen months. So, this was done on the side. We would prefer them to develop this feature and pay for it rather than having us do it. We need more 100 gig ports. Right now, there are a lot of 10 gig ports and we don't need them all. We really need are more ports between 10 gig and 100 gig, which isn't possible. The upgrade process for the boxes is not efficient. We have to go through the A10 aGalaxy where we have issues, like timeouts. They told me it was fixed in the latest version, but I tried to do it on the Portal and it is not working all the time. A10 needs to be more distributed across all their customers. This would allow them to have the ability to act quickly during an attack across their entire customer base. At the moment, there isn't a way to provide information (anonymously). This is something A10 will hopefully release Q1 next year. The documentation with the A10 really needs some improvement. They need to work on this, as it's hard to find all the information that you want. The Customer Portal is sometimes really buggy.

FOR HOW LONG HAVE I USED THE SOLUTION?

I have been using it for eighteen months.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

We don't have issues with the stability. However, we did have an issue when we had the new box. We needed to have some optic support, which was not working. This was fixed in two weeks when they created a specific code for us. Compared to the industry, this is very fast. The TPS gives us increased availability because we are using it to protect our customers. It is not complicated to maintain. It takes one person to maintain it.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

We have deployed it globally in Europe and the US. We will be deploying in Singapore and Japan in a few weeks. We are increasing our deployment for customers. Today, we are serving 30 customers. While we have the biggest unit, we haven't had the chance to use the box's full capacity. As we are distributed, every time we have an attack, we are not able to reach the capacity of the box. One TPS can block 200 gigs, as well 100 and 150 gigs. So, we never been in the position that we are using the full capacity of the box, at least not today. We are not getting enough 100 gig from this box, which we have already spoken to the design team about. With the smaller boxes, they are okay, but we are not able to evaluate the box's fullest capacity because we bought two of them. The goal is not to use it at maximum capacity because we want to have good quality for our customers. We want to add more boxes in order to have a lot of distribution for DDoS attacks across all the TPS boxes. Today, we have four boxes in position. We are going to order four more boxes (minimum) in order to distribute the traffic as much as we can. The goal is to be able to not use more than 60 percent capacity of the box. We are doing stuff today to have the traffic not go through the box every time. It triggers going through the box for IOPS maybe two or three percent of the time.

A10 Thunder TPS

Read 6 reviews of A10 Thunder TPS

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Tech support is good. We have access directly to engineering where we can speak to someone to debug. All our tickets go to engineering.

WHICH SOLUTION DID I USE PREVIOUSLY AND WHY DID I SWITCH?

We had some internal stuff previously. For solutions that we purchased, this was the first. We have had the solution since the beginning. We have used it as our own mitigation and detection.

HOW WAS THE INITIAL SETUP?

The box was deployed really easily. When we had to do the distributed mitigation, it took some time because we had to work with the aGalaxy and aGalaxy was pretty new for A10. We had to work directly with the engineering. Initial setup was done within a week because it was easy. If you're just starting to work in a sample environment, what we did the first time, the process can be done really quickly. But, when you want to do something, like engineering or custom configurations, this can take sometimes months.

WHAT ABOUT THE IMPLEMENTATION TEAM?

We did the setup ourselves since we have access to engineering. It only took one person to implement. It was pretty easy. All the B2B configuration have to be done manually. As a network operator, this is easy for us. However, if you take an enterprise person who needs to do this, they may have some issues. They may spend a lot of time trying to understand how to configure it, as there is a lack of templates available. This is something which needs to be improved for the enterprise market.

WHAT WAS OUR ROI?

We had a customer who was down for six hours and the loss of revenue for him was three times the price he was paying for us per year. The customer just said, "I don't care about paying you because on only one attack I saved money. It's three times better than losing money." When customers start to get attacked, they need to be protected and we protect them. It's like insurance. When you buy your car, you don't use it. You say, "I pay for nothing." But the day someone crashes your car, and you are paying for insurance, you are happy that you are insured. This solution is exactly the same for customers.

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

We are waiting for our subscription model on our next four boxes.

WHICH OTHER SOLUTIONS DID I EVALUATE?

We also looked at Radware and Fortinet. Radware had good reporting. A10 does not have good reporting. A10 had a good B2B code and the TPS box has good capacity. The key thing for us was the direct access to engineering. However, A10 is more complex then the other solutions. You have to spend time with it to become efficient at using it. You cannot just buy it and get started on it. We use Juniper a lot. Their support would take months to fix the same issue that A10's engineering tech support team can fix in a couple of weeks.

A10 Thunder TPS

Read 6 reviews of A10 Thunder TPS

WHAT OTHER ADVICE DO I HAVE?

The solution is not for newbies. You need to know some security stuff. The box is very flexible and capable with a lot of possibilities. We are using A10, not just as a mitigation box. We provide the TPS box and all its mitigation backbone to our customer as a tool. At some point, we are obliged to do some training and do some testing in our lab for them. DDoS attacks are evolving every day. Attackers are getting smarter. You have to continue to learn and experiment.

Learn more: Read 6 reviews of A10 Thunder TPS